Linux Professional Institute

Security Essentials

Verzió 1.0
Magyar

020

Table of Contents

Linux Professional Institute

Témakör 021: Biztonsági koncepciók

Linux Professional Institute

021.1 Célok, szerepek és szereplők

Hivatkozás az LPI célkitűzésre

Security Essentials version 1.0, Exam 020, Objective 021.1

Súlyozás

1

Kulcsfontosságú ismeretek

- Az IT-biztonság fontosságának megértése
- A közös biztonsági célkitűzések megértése
- A közös biztonsági szerepek megértése
- Az informatikai rendszerek és eszközök elleni támadások közös céljainak megértése
- Az attribúció fogalmának és a kapcsolódó kérdéseknek a megértése

A használt fájlok, kifejezések és segédprogramok listája

- Titoktartás, integritás, rendelkezésre állás, nem-tagadhatóság
- Hackerek, crackerek, script kiddiek
- Fekete és fehér kalapos hackerek
- Adatokhoz való hozzáférés, azok manipulálása vagy törlése
- Szolgáltaátsok megszakítása és váltságdíj követelése
- Ipari kémkedés

Linux Professional Institute

Lecke 1

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	021 Biztonsági koncepciók
Fejezet:	021.1 Célok, szerepek és szereplők
Lecke:	1/1

Bevezetés

Az elmúlt néhány évtizedben az internetes technológiák jelentősen megváltoztatták a társadalmi interakciók, valamint az alapvető szükségletek és vágyak kielégítésének módját. Míg az alapvető emberi szükségletek — legyenek azok fizikai, pszichológiai, érzelmi vagy intellektuális szükségletek — ugyanazok maradtak, az internet térhódítása örökre megváltoztatta azokat a módszereket, amelyekkel ezeket a szükségleteket kielégítjük. Az internet szimulálja a fizikai világot, olyan virtuális teret hozva létre, amelyben a valós világ számos tevékenysége digitális eszközökkel valósulhat meg.

Például a vásárlás, amihez hagyományosan szükséges volt egy üzlet fizikai meglátogatása, ma már online is elvégezhető a vásárlás élményét replikáló weboldalakon és alkalmazásokon keresztül. A fogyasztók böngészhetnek a termékek között, digitális kuponokat használhatnak és vásárolhatnak — mindezt otthonuk kényelméből. Ez a váltás soha nem látott kényelmet és hatékonyságot hozott, ugyanakkor új kockázatokat is rejt magában. Ellentétben a húsz évvel ezelőtti időszakkal, amikor a vásárlást elsősorban személyesen végezték, a mai fogyasztóknak tisztában kell lenniük a digitális tranzakciókkal kapcsolatos lehetséges kockázatokkal.

A digitális platformokra való fokozott támaszkodással kritikus igény mutatkozik a robusztus

digitális biztonságra is. Ahogy az online tranzakciók és az adattárolás mindennapossá válik, úgy válik a személyes információk és a pénzügyi adatok védelme a kiberfenyegetésekkel szemben létfontosságúvá. Az információbiztonság garantálása ma már a modern élet alapvető része, amelyet a digitális technológia nyújtotta kényelem tesz szükségessé.

Az IT-biztonság fontossága

Az információs technológiai (Information Technology — IT) biztonság alapvető fontosságú, hogy az adatok védve legyenek a a jogosulatlan hozzáféréstől, felhasználástól és terjesztéstől. Biztosítja, hogy az érzékeny információk — legyenek azok személyes, pénzügyi vagy védett adatok — bizalmasak és biztonságosak maradjanak a tárolás, a felhasználás és a jogos felhasználók közötti megosztás során. Az IT security elsődleges célja az információk által képviselt személyek és szervezetek védelme, megelőzve a jogosulatlan nyilvánosságra hozatalból vagy visszaélésből eredő károkat.

Az IT security az adatok széles skáláját védi, a nyilvános információktól, mint például a térképek és kézikönyvek, a rendkívül érzékeny adatokig, mint például az egészségügyi adatok és a bizalmas pénzügyi dokumentumok. Bár a nyilvános adatokhoz való jogosulatlan hozzáférés nem jelenthet közvetlen veszélyt, az érzékeny információk veszélyeztetése súlyos következményekkel járhat, beleértve a személyazonosság-lopást, a pénzügyi veszteségeket és a jó hírnév sérülését. Ezért az ilyen kritikus adatok védelme érdekében az IT-biztonsági intézkedések prioritást élveznek.

Ráadásul az internetes technológiák elterjedésével párhuzamosan a kibertámadások lehetőségei is bővültek, ami egyre fontosabbá teszi az informatikai biztonságot. Az internet világszerte több millió eszközt köt össze, ami növeli a biztonsági résekből eredő potenciális károk mértékét. Ennek eredményeképpen az ilyen fenyegetésekkel szembeni védelemhez robusztus IT-biztonsági gyakorlatokra van szükség, amelyek széles körben biztosítják az adatok biztonságát és sértetlenségét. Ezáltal az IT-biztonság nemcsak a technológiát és a rendszereket, hanem az embereket és a hozzájuk kapcsolódó adatokat is védi a lehetséges károktól és kizsákmányolástól.

A közös? biztonsági célkitűzések megértése

Az információbiztonsági célok köre éppoly változatos és sokszínű, mint a védett adatokért felelős személyek és szervezetek. A következő szakaszokban részletesen tárgyalunk számos konkrét célt és módszertant. A szilárd alapok megfelelő megteremtéséhez célszerű a sok információbiztonsági szakember által elfogadott alapokkal kezdeni. Ennek a megértésének az érdekében az IT-biztonság három alapvető céljával fogunk foglalkozni.

A CIA Triad

Az információbiztonság három alapvető célja a *titoktartás* (confidentiality), az *integritás* (integrity) és a *rendelkezésre állás* (availability), amelyeket az információbiztonsági szakemberek általában a *CIA-triádként* emlegetnek, ahol a CIA elnevezés az alapvető célok első három betűjéből származik: (Titoktartás, integritás és rendelkezésre állás az IT-biztonság alapvető céljai).

Figure 1. Titoktartás, integritás és rendelkezésre állás az IT-biztonság alapvető céljai

A *titoktartás* az információkhoz való jogosulatlan hozzáféréstől és nyilvánosságra hozatalától való védelmére összpontosít, biztosítva, hogy az adatok bizalmasak maradjanak, és csak a megfelelő jogosultsággal rendelkezők számára legyenek hozzáférhetők. A technológiai hálózatokban a titkosság fenntartása alapvető fontosságú, mivel megőrzi a felhasználók és az általuk használt rendszerek közötti bizalmat, és megakadályozza, hogy az érzékeny információkat felfedjék vagy visszaéljenek velük.

Ez az elv azon a feltételezésen alapul, hogy a hálózaton áthaladó vagy azon belül tárolt minden információ meghatározott személyeknek és célokra szolgál. Ezen információk jogosulatlan felfedése jelentős károkat okozhat mind a szervezeteknek, mind az egyéneknek. Például az üzleti titkok jogosulatlan kiadása pénzügyi veszteségekhez vezethet, és veszélyeztetheti a vállalat versenyelőnyét, míg a személyes adatok nyilvánosságra kerülése személyazonosság-lopáshoz és a magánszféra súlyos megsértéséhez vezethet.

A szervezetek a titoktartást többféle stratégiával védik, beleértve a titkosítást, a hozzáférés-szabályozást és a hálózati biztonsági intézkedéseket.

Az *integritás* fogalma a második alapvető biztonsági cél az információbiztonsági alapelvek hármasában. Az integritás biztosítja, hogy a hálózaton belüli vagy azon áthaladó minden információ változatlan maradjon, kivéve, ha a módosításokat a megfelelő személyek engedélyezik. Ez az elv azon a feltételezésen alapul, hogy az adatok pontossága és konzisztenciája az életciklusuk során megmarad, ami lehetővé teszi az információ hitelességébe vetett bizalmat. Ha illetéktelen személyek engedély nélkül hozzáférnek az adatokhoz és módosítják azokat, az veszélyezteti az adatok integritását, és megszünteti a hitelességbe vetett bizalmat, ami jelentős károkat okozhat.

Az integritást úgy is felfoghatjuk, mint “bizalmat”. Egy olyan világban, ahol semmi írott vagy közölt dologban nem lehetne megbízni vagy ellenőrizni, káosz alakulna ki, és egész rendszerek bukhatnának el. A digitális térben biztonsági eszközöket és módszereket alkalmaznak az információk érvényességének és az adatcserében részt vevők identitásának ellenőrzésére. Az információk integritásának biztosítása megteremti a *nem-tagadhatóság* (non-repudiation) alapját, ami azt jelenti, hogy a feladó nem tagadhatja le a tranzakcióban való részvételét. A digitális hálózatokban a nem-tagadhatóság alapvető fontosságú az igazság és az elszámoltathatóság fenntartásához annak megerősítése révén, hogy a végrehajtott műveleteket nem lehet letagadni.

A nem-tagadhatóság eléréséhez olyan speciális módszerek szükségesek, amelyek garantálják a műveletek hitelességét és integritását. A digitális aláírás olyan általános eszköz, amely egyedileg azonosítja a feladót, és megerősíti, hogy a tartalmat nem manipulálták, biztosítva, hogy a feladó ne tudja letagadni az információ elküldését.

Az integritás célja túlmutat a letagadásmentességen; magában foglalja az adatok pontosságának, konzisztenciájának és megbízhatóságának fenntartását. Ez létfontosságú annak biztosításához, hogy az adatok eredeti állapotukhoz képest változatlanok maradjanak, lehetővé téve a megbízható információkon alapuló pontos döntéshozatalt.

A *rendelkezésre állás* fogalma a harmadik alapvető biztonsági cél az információbiztonsági alapelvek hármasában. A rendelkezésre állás biztosítja, hogy a hálózaton belüli vagy azon keresztülhaladó összes információ bármikor hozzáférhető legyen az arra jogosult felhasználók számára. Ez az elv azon a feltételezésen alapul, hogy a felhasználóknak és a rendszereknek képesnek kell lenniük arra, hogy az információt időben lekérdezzék, különösen, ha az kritikus vagy időérzékeny. Ha egy hálózat sérül, és a kért információ nem érhető el, sem a szervezet, sem a felhasználók nem tudnak hatékonyan funkcionálni, ami működési zavarokhoz és termelékenységcsökkenéshez vezethet.

A rendelkezésre állás garantálja, hogy az arra jogosult felhasználók szükség szerint megbízhatóan hozzáférjenek az információkhoz és erőforrásokhoz, ami elengedhetetlen az üzletmenet folytonosságának fenntartásához, valamint a kritikus szolgáltatások és műveletek zavartalanságának biztosításához. Ennek elérése érdekében számos kulcsfontosságú stratégiát

alkalmaznak, például redundanciát és failover-mechanizmusokat.

A közös biztonsági szerepek megértése

A közhiedelemmel ellentétben nem minden, az információbiztonsággal kapcsolatos szerep és felelősség tisztán technológiai jellegű. Ez a szakasz röviden megvizsgálja az információbiztonsággal kapcsolatos négy legnépszerűbb szerepkört: *Chief Information Officer*, *Chief Information Security Officer*, *Enterprise Architect* és a *Network* vagy *System Administrator*.

A *Chief Information Officer* (CIO) a szervezet “C-Suite”-jában (executive offices) található, és a szervezeten belüli technológia minden aspektusáért felelős. Kisebb vállalatoknál ez a szerepkör az adminisztratív és fizikai biztonsági feladatokat is magában foglalhatja. Ez a személy felelős az irányítása alá tartozó, technológiai funkciót betöltő eszközök költségvetéséért, igényléséért és megvalósításáért.

A *Chief Information Security Officer* (CISO) a szervezet átfogó informatikai biztonsági stratégiájáért felelős vezető beosztású személy. Ez a szerepkör magában foglalja az irányelvek és eljárások kidolgozását, a szabályozásoknak való megfelelés biztosítását, valamint a szervezet kiberfenyegetések elleni védekezésének vezetését. A CISO kritikus szerepet játszik a biztonsági kezdeményezések és az üzleti célkitűzések összehangolásában, valamint a biztonság fontosságának kommunikálásában a vezetőség és az érdekelt felek felé. A CISO pozíciót olyan személyek töltik be, akik mind a vállalat üzleti, mind a technológiai szektorában szilárd alapokon nyugvó ismeretekkel rendelkeznek. Az üzleti és a technológiai nyelvek ismeretében elvárás, hogy “híd” legyen a vállalati vezetés felső szintje és a technológiai kezdeményezések vezetői között. Ez a pozíció viszonylag új, és korlátozott sikereket ért el. Csak az idő fogja megmutatni, hogy ez a pozíció megmarad-e a szervezeti ábrán belül.

Az *Enterprise Architect* általában közvetlenül a CIO-nak jelent, és a szervezet fizikai és logikai informatikai rendszeréért felelős. Ez a személy általában nagyfokú technikai szakértelemmel rendelkezik (különösen a hálózati adminisztráció terén), és úgy tervezi meg a szervezet hálózatát, hogy az megfeleljen a szükséges biztonsági követelményeknek.

A *Network System Administrator*-ok tervezik, végrehajtják és karbantartják a szervezet informatikai infrastruktúráját védő műszaki biztonsági ellenőrzéseket. Ők felelősek a tűzfalak, behatolásjelző rendszerek (intrusion detection system — IDS) és titkosítási protokollok telepítéséért. Automatizálási scripteket is fejlesztenek a biztonsági folyamatok racionalizálása és a rendszerek támadásokkal szembeni ellenállóképességének biztosítása érdekében.

A legitim technológiai szakemberek soraiban létező számos szereppel párhuzamosan számos olyan szerep és cím is létezik, amelyet az illegitimek vesznek fel. Őket együttesen *hackerek* néven ismeri a világ. Ez az összefoglaló kifejezés azonban a hackerek számos alcsoportját tartalmazza,

akik a legkülönbözőbb készségekkel és szándékokkal tevékenykednek.

A hackerek olyan személyek, akik fejlett ismeretekkel rendelkeznek a számítógépes rendszerek és hálózatok terén. Bár a hackerekről alkotott közmegítélés gyakran negatív, nem minden hackernek vannak rosszindulatú szándékai. A hackereknek különböző típusai vannak, elsősorban *black hat* (fekete kalapos) és *white hat* (fehér kalapos) hackerekre oszthatók.

A black hat hackerek technikai képességeiket arra használják, hogy rosszindulatú célokra, például adatlopásra, a szolgáltatások megzavarására vagy a rendszerek károsítására használják ki a sebezhetőségeket. Törvényes kereteken kívül, anyagi haszonszerzés, politikai célok vagy személyes elégedettség által motiválva tevékenykednek. A black hat hackerek által használt technikák közé tartozik a rosszindulatú szoftverek telepítése, az adathalászat és a social engineering, amellyel manipulálják az embereket, hogy azok bizalmas információkat fedjenek fel.

Ezzel szemben a white hat hackerek, más néven etikus hackerek arra használják képességeiket, hogy segítsenek a szervezeteknek azonosítani és kijavítani a biztonsági réseket. White hat hackereket gyakran alkalmaznak vállalatok, vagy független tanácsadóként dolgoznak behatolástesztek (penetration testing) és sebezhetőségi felmérések elvégzésére. A fekete kalaposokkal ellentétben a fehér kalapos hackerek szigorú etikai kódexhez tartják magukat, és jogi keretek között dolgoznak a szervezet biztonsági helyzetének megerősítése és a potenciális fenyegetések elleni védekezés érdekében.

A *crackerek* olyan személyek, akik illegális tevékenységet folytatnak, például betörnek a rendszerekbe, megkerülnek jelszavakat, és kijátsszák a szoftverlicenceket, azzal a szándékkal, hogy kárt okozzanak, információt lopjanak vagy megzavarják a szolgáltatásokat. A crackereket rosszindulatúbbnak tekintik, mint az etikus hackereket, mivel tetteiket pusztán a rendszerek kihasználásának és a károkozásnak a szándéka vezérli, a törvényességre vagy az etikára való tekintet nélkül.

A *script kiddie*-k más kategóriát képviselnek a hacker közösségen belül, amelyet a szakértelem hiánya jellemez, és az, hogy előre megírt scriptekre és eszközökre támaszkodnak a kibertámadások végrehajtásához. A képzett hackerekkel ellentétben a script kiddiek nem értik teljesen az általuk használt eszközöket, és általában nem rendelkeznek a saját fejlesztéseikhez szükséges technikai képességekkel sem. Ehelyett könnyen elérhető, gyakran elavult, online található scripteket használnak a kevésbé biztonságos rendszerek elleni támadásokhoz. Motivációjukat gyakran nem az anyagi haszonszerzés vagy politikai célok, hanem a zavarok okozása vagy a hírnév megszerzése iránti vágy vezérli. A script kiddiek a képzettségük hiánya ellenére is jelentős fenyegetést jelenthetnek az információbiztonságra, mivel az automatizált eszközök használata jelentős károkat okozhat, különösen, ha rosszul védett rendszereket vesznek célba.

Az informatikai rendszerek és eszközök elleni támadások közös céljainak megértése

Ahogy a számítástechnikai eszközök egyre inkább a társadalom szerves részévé válnak, a kibertámadók taktikája és indítékai a technológiával együtt fejlődnek. Minden új eszköz vagy technológia, amely széles körben elterjedt, potenciális célponttá válik, mivel a rosszindulatú szereplők megpróbálnak visszaélni ezekkel az eszközökkel a törvényes felhasználók ellen. E támadások kifinomultsága nagymértékben változhat, a rendkívül fejlett, speciális készségeket igénylő technikai műveletektől az egyszerűbb, alapvető számítógépes ismeretekre és más rosszindulatú szereplőkkel való együttműködésre épülő rendszerekig.

A kibertámadók közös célja az *adatokhoz való hozzáférés, azok manipulálása vagy törlése*. A jogosulatlan hozzáférés lehetővé teszi a támadók számára, hogy érzékeny információkat, például szellemi tulajdont, pénzügyi nyilvántartásokat vagy személyes adatokat lopjanak el. Ezeket az adatokat aztán pénzügyi haszonszerzésre, zsarolásra vagy versenytársaknak való eladásra használhatják fel. Az adatmanipuláció magában foglalja az információk megváltoztatását a műveletek megzavarása, a bizalom aláásása vagy az eredmények manipulálása érdekében olyan kritikus ágazatokban, mint a pénzügyi piacok vagy a választások. A fontos adatok törlése jelentősen károsíthatja egy szervezet működését, pénzügyi veszteséget és működési leállást okozva. Erre kiváló példa a Sony Pictures elleni 2014-es kibertámadás, ahol a támadók bizalmas adatokhoz fértek hozzá és hoztak nyilvánosságra, manipulálták az alkalmazottak adatait, és értékes információkat töröltek, hogy káoszt teremtsenek és váltságdíjat követeljenek.

A kibertámadók másik elsődleges célja a *szolgáltatások megszakítása és váltságdíj követelése*. Ezt olyan módszerekkel érhetik el, mint a *Distributed Denial of Service* (DDoS) támadások, amelyek a célpont hálózatát túlzott forgalommal árasztják el, így a szolgáltatások elérhetetlenné válnak a törvényes felhasználók számára. Ezeket a támadásokat gyakran váltságdíj követelésére vagy az áldozat jó hírnevének megrongálására használják. A zsarolóprogram-támadások során a kritikus adatokat vagy rendszereket titkosítják, és a hozzáférés helyreállításáért pénzt követelnek, közvetlenül zsarolva ezzel azokat az áldozatokat, akik nem engedhetik meg maguknak a hosszabb leállást. A 2017-es WannaCry zsarolóvírus-támadás figyelemre méltó példa erre, amely világszerte számos szervezet szolgáltatásait zavarta meg az adatok titkosításával és váltságdíj követelésével.

Az *ipari kémkedés* (industrial espionage) a kibertámadók másik jelentős célja, különösen azoké, akik értékes üzleti titkokat vagy védett információkat akarnak ellopni a vállalkozásoktól. Ezeket a támadásokat gyakran versenytársak vagy nemzetállamok követik el gazdasági előnyökre törekedve. Az ipari kémkedés céljai közé tartozik az üzleti titkok ellopása a versenytársak sikerének megismétlése érdekében, egy vállalat piaci pozíciójának aláásása érzékeny információkhoz való hozzáféréssel, valamint a műveletek, ellátási láncok vagy gyártási folyamatok szabotálása pénzügyi veszteségek okozása és a hírnév megrongálása érdekében. Az

ipari kémkedés egyik kiemelkedő példája a 2010-es Aurora-művelet, amelynek során a támadók olyan nagyvállalatokat vettek célba, mint a Google és az Adobe, hogy szellemi tulajdont és érzékeny információkat lopjanak el.

Az attribúció fogalmának megértése

Az *attribúció* (attribution) fogalma alapvető fontosságú a digitális környezetben, és az információbiztonsági szakemberek egyik legfontosabb feladata. Egyszerűbben fogalmazva, az attribúció magában foglalja az egyének azonosítását és felelősségének kijelölését a virtuális térben végzett cselekedeteikért. Ez a lecke röviden bemutatja a fogalmat, mivel a tanfolyam során különböző összefüggésekben fogjuk vizsgálni. Az attribúció alkalmazása és fontossága az adott területtől, például adatvédelem, titkosítás, hálózati hardver vagy adatbázis-kezelés függően eltérő lehet, és ezeket a variációkat a későbbiekben részletesen tárgyaljuk.

A megbízható biztonsági helyzet fenntartásához elengedhetetlen annak megértése, hogy ki a felelős a hálózaton belül végrehajtott műveletekért — legyen szó dokumentumok módosításáról vagy tárolt adatok törléséről. Az attribúció nemcsak a biztonsági intézkedéseket erősíti, hanem az elszámoltathatóságot is. Egy felhasználó számára kihívást jelent, hogy letagadja a technológiai környezetben végzett tevékenységeit, ha több olyan naplózó rendszer, speciális szoftver és internetes protokoll van érvényben, amelyek egyértelműen nyomon követik és rögzítik ezeket a tevékenységeket.

Az attribúció létrehozza az elszámoltathatóság keretét, de nem kizárólag a visszaélések azonosítására összpontosít. A digitális téren belüli pozitív cselekedetek elismerésére és ellenőrzésére is használható.

A fizikai világban az attribúció elvét mindenki rendszeresen tapasztalja, a technikai és nem technikai felhasználók egyaránt. Amikor például egy szerzőt egy könyv vagy cikk megírásáért elismerésben részesítenek, akkor megkapja az attribúciót. Hasonlóképpen, amikor egy személyt díjazottként neveznek meg, akkor is elismerésben részesül teljesítményéért. Még akkor is, amikor egy szerző idéz egy idézetet, attribúcióról van szó. Gondoljunk rá úgy, mint a “felelősség ujjlenyomatára”, amely az információbiztonság alapvető szempontja, és amely a biztonsági karrierünk során mindig visszatérő lesz.

A digitális térben azonban a pontos attribúció elérése összetett feladat, amely számos kihívást jelent a biztonsági szakemberek számára. A technológia lehetővé teszi a rosszindulatú szereplők számára, hogy álcázzák személyazonosságukat, elrejtsék fizikai tartózkodási helyüket és elfedjék valódi szándékaikat. E kihívások ellenére léteznek olyan szoftveres és hardveres megoldások, amelyek célja, hogy segítsenek a biztonsági csapatoknak a digitális környezetekben az attribúció meghatározásában, hasonlóan azokhoz az eszközökhöz, amelyeket a bűnüldöző szervek a hamis pénz azonosítására és kivizsgálására használnak. A bűncselekmények elkövetőinek

attribúciójához rendelkezésre álló tudás, szakértelem és eszközök ellenére a gyakorlott bűnözők gyakran találnak módot a sikerre. A fizikai világbeli hozzárendeléssel kapcsolatos összetettség és kihívások a digitális környezetben is érvényesek.

Gyakorló feladatok

1. Miért kulcsfontosságú az informatikai biztonság a digitális tranzakciók és az adattárolás szempontjából?

2. Mi az információbiztonság három alapvető célja, és miért fontosak?

3. Mi a Chief Information Security Officer (CISO) szerepe, és miért fontos egy szervezetben?

Gondolkodtató feladatok

1. Miért sikeres sok támadás a digitális információforrások ellen?

2. Van-e legitim oka annak, hogy olyan hackereszközt tegyünk fel az internetre, amelyet a script kiddiek használhatnak zavaró és rosszindulatú támadások végrehajtására?

Összefoglalás

Az információs technológia, amely oly sok ember elérését és erejét növelte pozitív módon, a rosszindulatú szereplők elérését és erejét is növeli. Az emberek biztonságának és jogainak védelme érdekében manapság mindannyiunknak tisztában kell lennünk a rosszindulatú tevékenységekkel, és lépéseket kell tennünk azok megelőzésére vagy a belőlük való helyreállásra.

Az információbiztonság céljai a titoktartás, az integritás és a rendelkezésre állás általános kategóriáiba sorolhatók. Ezek mind fontosak a modern szervezetek működéséhez. Az integritás egyik legfontosabb szempontja a cselekvések megfelelő személyekhez való tulajdonítása. Mindhárom cél adminisztratív, technikai és fizikai szintű támogatást igényel.

A munkaerőpiacon sokféle biztonsági pozíció létezik, ahogy sokféle támadó is. A legtöbb black hat hackert pénzügyi célok vezérlik, de vannak, akiket kormányzati kezdeményezések, ideológiai állásfoglalások vagy egyszerűen csak a zavarok okozásának öröme motivál.

Válaszok a gyakorló feladatokra

1. Miért kulcsfontosságú az informatikai biztonság a digitális tranzakciók és az adattárolás szempontjából?

   Az informatikai biztonság kulcsfontosságú a digitális tranzakciók és az adattárolás összefüggésében, mivel megvédi az érzékeny információkat a jogosulatlan hozzáféréstől, a visszaéléstől és a terjesztéstől. Az internetes technológiák térhódításával számos olyan tevékenységet, amelyet hagyományosan személyesen végeztek, például a vásárlást, ma már online végzik. Ez az eltolódás megnövelte az interneten tárolt és továbbított személyes és pénzügyi adatok mennyiségét, ami elengedhetetlenné teszi ezen adatok védelmét a kiberfenyegetésekkel szemben. A hatékony informatikai biztonsági intézkedések biztosítják, hogy az adatok bizalmasak maradjanak, megőrizzék integritásukat, és az arra jogosult felhasználók számára hozzáférhetőek legyenek, ezáltal megelőzve a személyazonosság-lopást, a pénzügyi veszteségeket és a jó hírnév sérülését.

2. Mi az információbiztonság három alapvető célja, és miért fontosak?

   Az információbiztonság három alapvető célja CIA-triád néven ismert, a titoktartás, az integritás és a rendelkezésre állás. A titoktartás biztosítja, hogy az érzékeny információkhoz csak azok férjenek hozzá, akik jogosultak megtekinteni, megvédve azokat a jogosulatlan hozzáféréstől és nyilvánosságra hozataltól. Az integritás biztosítja, hogy az adatok pontosak és változatlanok maradjanak, kivéve, ha az arra jogosult felhasználók módosítják őket — ez elengedhetetlen az információkba vetett bizalom fenntartásához. A rendelkezésre állás biztosítja, hogy a felhatalmazott felhasználók szükség esetén időben hozzáférjenek az információkhoz és erőforrásokhoz, ami elengedhetetlen az üzletmenet folytonosságának és a működési hatékonyság fenntartásához. Ezek a célok együttesen segítenek megvédeni az adatokat a jogsértésektől, fenntartani a digitális interakciókba vetett bizalmat, és biztosítani az informatikai rendszerek megbízhatóságát.

3. Mi a Chief Information Security Officer (CISO) szerepe, és miért fontos egy szervezetben?

   A Chief Information Security Officer (CISO) feladata a szervezet átfogó információbiztonsági stratégiájának felügyelete és irányítása. A CISO felelős a biztonsági irányelvek és eljárások kidolgozásáért és végrehajtásáért, a vonatkozó szabályozásoknak való megfelelés biztosításáért, valamint a szervezet kiberfenyegetésekkel szembeni védelmére irányuló erőfeszítések vezetéséért. Ez a szerep azért fontos, mert összehangolja a biztonsági kezdeményezéseket az üzleti célkitűzésekkel, kommunikálja a kiberbiztonság fontosságát az érdekeltek felé, és biztosítja, hogy a szervezet felkészült legyen a lehetséges biztonsági incidensekre való reagálásra és az azokból való felépülésre. A szervezet biztonsági helyzetének irányításával a CISO segít megvédeni a szervezet digitális eszközeit, fenntartani a hírnevét és

támogatni az általános működési sikerét.

Válaszok a gondolkodtató feladatokra

1. Miért sikeres sok támadás a digitális információforrások ellen?

   A támadások sikerének számos oka van. Először is, mivel az interneten keresztül történő támadások a fizikai támadásokhoz képest alacsony költségűek és gyakran nagyon jövedelmezőek, egyre több rosszindulatú szereplő jelenik meg a terepen, mindig új utakat keresve a védelem megkerülésére.

   Sajnos a támadás által okozott költség és hírnévkárosodás gyakran kisebb, mint a megelőzés költségei (bár a zsarolóvírusok hatalmas károkat és költségeket okozva megváltoztatják az egyenletet). Az erőforrások védelmére való ösztönzés hiánya, valamint a szakértő biztonsági személyzet szűkössége sok szervezetet arra késztet, hogy ne fektessen kellő mértékben a védelembe.

   Az adathalászat (phishing, hamis e-mailek) lehetővé teszik, hogy egy viszonylag alulképzett és figyelmetlen alkalmazotton keresztül is be lehessen jutni egy hálózatba.

Van-e legitim oka annak, hogy olyan hackereszközt tegyünk fel az internetre, amelyet a script kiddiek használhatnak zavaró és rosszindulatú támadások végrehajtására?

+ Igen. A hackereszközök nagyon fontosak a hálózatok biztonságának vizsgálatához és ellenőrzéséhez. A white hat hackerek folyamatosan használják ezeket az eszközöket az eszközök megvédése érdekében. Ha a jó minőségű behatolási eszközök nem állnának a törvényes felhasználók rendelkezésére, a terület sebezhetőbb lenne a rosszindulatú szereplők által létrehozott nagy teljesítményű eszközök támadásaival szemben.

021.2 Kockázatértékelés és -kezelés

Hivatkozás az LPI célkitűzésre

Security Essentials version 1.0, Exam 020, Objective 021.2

Súlyozás

2

Kulcsfontosságú ismeretek

- Biztonsági információk általános forrásainak ismerete
- A biztonsági incidensek osztályozási sémájának és a biztonsági sebezhetőségek fontos típusainak megértése
- A biztonsági értékelések és az IT Forensics megértése
- Az Information Security Management System (ISMS), valamint az információbiztonsági incidensekre reagáló tervek és csapatok ismerete

A használt fájlok, kifejezések és segédprogramok részleges listája

- Common Vulnerabilities and Exposures (CVE)
- CVE ID
- Computer Emergency Response Team (CERT)
- Penetration testing
- Nem célzott támadások és fejlett tartós fenyegetések (APT)
- Nulladik-napos sebezhetőségek
- Távoli végrehajtás és a biztonsági rések
- Jogosultságok kiterjesztése biztonsági sebezhetőségek miatt

Lecke 1

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	021 Biztonsági koncepciók
Fejezet:	021.2 Kockázatértékelés és -kezelés
Lecke:	1/1

Bevezetés

A biztonságos és ellenálló környezet fenntartása szempontjából alapvető fontosságú annak megértése, hogy hogyan lehet felmérni a biztonsági réssel kapcsolatos kockázatot, és meghatározni a válaszadás szükségességét és sürgősségét. Ez a lecke a rendelkezésre álló biztonsági adatok széles skáláján való hatékony eligazodáshoz szükséges készségekkel és folyamatokkal foglalkozik, kiemelve a kritikus fenyegetések és a kisebb aggodalmak megkülönböztetésének fontosságát, valamint olyan megalapozott döntések meghozatalát, amelyek megvédik a rendszereket és az adatokat a lehetséges károktól.

A biztonsági információk forrásai

Napjaink gyorsan fejlődő digitális környezetében a releváns biztonsági információk megtalálásának és értelmezésének képessége alapvető fontosságú minden kiberbiztonsági szakember számára. Ez a szakasz a biztonsági információk legfontosabb forrásait tárja fel, és elmagyarázza, hogyan járulnak hozzá a robosztus kiberbiztonsági helyzethez.

Először is fontos ismerni a biztonsági információk általános forrásait. Ezek a források jellemzően olyan jó hírű helyek vagy szervezetek, amelyek naprakész és pontos adatokat szolgáltatnak a

biztonsági sebezhetőségekről, az új fenyegetésekről és a legjobb gyakorlatokról (best practices). E források ismerete lehetővé teszi a kiberbiztonsági szakemberek számára, hogy a potenciális fenyegetések előtt járjanak, azonnal reagáljanak a felmerülő kockázatokra, és a legújabb biztonsági intézkedéseket alkalmazzák rendszereik védelmére.

A biztonsági információk egyik legszélesebb körben elismert forrása a *Common Vulnerabilities and Exposures* (CVE) rendszer. A CVE egy szabványosított lista, amely azonosítja és kategorizálja a szoftver- és hardverrendszerek sebezhetőségeit. Referenciapontként szolgál a kiberbiztonsági szakemberek számára világszerte, közös nyelvet biztosítva a sebezhetőségek megvitatásához és kezeléséhez. A sebezhetőségek azonosításának szabványosításával a CVE megkönnyíti a különböző platformok és szervezetek közötti információcserét, lehetővé téve a biztonsági fenyegetésekre adott összehangolt válaszlépéseket.

A CVE-adatbázisban szereplő minden egyes sebezhetőséghez egyedi azonosítót rendelnek, amelyet *CVE ID* néven ismerünk. Ezek az azonosítók kritikus fontosságúak az egyes sebezhetőségek nyomon követéséhez és annak biztosításához, hogy minden érdekelt fél ugyanazt a problémát tárgyalja. A CVE-azonosító általában a sebezhetőség aspektusainak, az érintett rendszereknek és a lehetséges hatásoknak a részleteit tartalmazza.

Egy CVE-bejegyzés általában egy adott szoftver vagy hardver azonosított, dokumentált és nyilvánosságra hozott biztonsági résést írja le. Íme egy példa egy CVE-bejegyzésre (CVE-2024-29824):

```
Name: Ivanti Endpoint Manager (EPM) SQL Injection Vulnerability
Description: An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022
SU5 and prior allows an unauthenticated attacker within the same network to execute
arbitrary code.
Score: 9.6
Severity: Critical
Version: 3.0
Vendor: Ivanti
Product: EPM
Action: Apply mitigations per vendor instructions or discontinue use of the product if
mitigations are unavailable.
Date Added: 2024-10-02
Due Date: 2024-10-23
Published: 2024-05-31
Updated: 2024-05-31
```

A biztonsági információk egy másik fontos forrása a_Computer Emergency Response Team_ (CERT). A CERT-ek a kiberbiztonsági szakértők speciális csoportjai, amelyek feladata a

kiberbiztonsági incidensekre való reagálás és a potenciális sebezhetőségekkel és fenyegetésekkel kapcsolatos információk terjesztése. Ezek a csoportok gyakran kormányzati szervekhez, oktatási intézményekhez vagy nagyvállalatokhoz kapcsolódnak, és a kiberincidensek kezelésének és enyhítésének első védelmi vonalaként szolgálnak. A CERT-ek kritikus szerepet játszanak a széles körben elterjedt kiberfenyegetésekre adott válaszlépések koordinálásában, az időben történő riasztások biztosításában és a kockázatok mérséklésére vonatkozó útmutatás nyújtásában. A CERT-ek értékes információmegosztó központokként is működnek, amelyek betekintést nyújthatnak a kialakulóban lévő fenyegetési mintákba, és ajánlásokat tehetnek a jövőbeli támadások megelőzésére szolgáló legjobb gyakorlatokra.

A biztonsági incidensek osztályozása és a sebezhetőségek típusainak megértése

A kiberbiztonság területén a biztonsági incidensek osztályozásának megértése és a kihasználható sebezhetőségek különböző típusainak felismerése kulcsfontosságú a hatékony védekezés kialakításához.

A biztonsági incidensek osztályozási sémái olyan keretrendszerek, amelyek a biztonsági incidenseket meghatározott kritériumok, például típus, súlyosság és hatás alapján kategorizálják. Ezek a sémák segítenek a szervezeteknek gyorsan felmérni az incidens jellegét és mértékét, meghatározni a megfelelő választ, és hatékonyan kommunikálni a helyzetet az összes érintett fél felé.

Ugyanilyen fontos a támadók által kihasználható sebezhetőségek típusainak megértése. A sebezhetőségek olyan gyenge pontok egy rendszerben, amelyeket ki lehet használni jogosulatlan hozzáférés megszerzésére, károkozásra vagy információlopásra. A sebezhetőségek különböző formái léteznek, és ezek eredhetnek a szoftver, a hardver vagy akár emberi hibákból is. A sebezhetőségek legaggasztóbb típusai közé tartoznak a *nulladik-napos sebezhetőségek* (zero-day vulerabilites). Ezek olyan, korábban ismeretlen hibák a szoftverben vagy hardverben, amelyeket a gyártó vagy a fejlesztő még nem fedezett fel, így a rendszerek védtelenek és rendkívül sebezhetőek a támadásokkal szemben. A nulladik-napos sebezhetőségek azért különösen veszélyesek, mert még nincs patch vagy fix, így a támadók szabadon kihasználhatják őket, amíg fel nem fedezik és ki nem javítják őket.

A sebezhetőség egy másik jelentős típusa a *távoli végrehajtáshoz* (remote execution) kapcsolódik. A távoli végrehajtás sebezhetőségek lehetővé teszik a támadók számára, hogy távoli helyről tetszőleges kódot hajtsanak végre a célrendszeren. Ez a képesség a rendszer teljes kompromittálódásához vezethet, lehetővé téve a támadók számára rosszindulatú programok telepítését, érzékeny információk ellopását vagy akár az egész hálózat irányításának átvételét. A távoli végrehajtási sebezhetőségeket gyakran hálózati alapú támadásokon keresztül használják ki,

ahol a támadók a sebezhetőség kiváltásához és az illetéktelen hozzáférés megszerzéséhez speciálisan kialakított csomagokat vagy kártékony terhelést használnak.

A *jogosultságok kiterjesztése* (privilege escalation) elnevezésű sebezhetőségek egy másik kritikus fenyegetést jelentenek. Ezek a sebezhetőségek akkor fordulnak elő, amikor a támadó a normálisan megengedettnél magasabb szintű hozzáférést vagy jogosultságokat szerez, és ezáltal jogosulatlan műveletek végrehajtására vagy korlátozott adatokhoz való hozzáférésre válik képessé. A jogosultságok kiterjesztése lehet vertikális, amikor a támadók a jelenlegi szintjüknél magasabb szintű jogosultságokat szereznek, vagy horizontális, amikor a támadók más, hasonló hozzáférési szintű felhasználókhoz rendelt jogosultságokhoz férnek hozzá. Ez a fajta sebezhetőség különösen veszélyes olyan környezetekben, ahol a jogosultsági hozzáférést szigorúan ellenőrzik, mivel lehetővé teheti a támadók számára a biztonsági intézkedések megkerülését és a kritikus rendszerek vagy adatok veszélyeztetését.

A *nem célzott támadások* (untargeted attacks) széleskörű, nem specifikus kísérletek bármely elérhető rendszer sebezhetőségének kihasználására, amelyeket gyakran automatizált scriptek vagy ismert gyenge pontokat kereső eszközök segítségével hajtanak végre. Ezek a támadások opportunista jellegűek, és nem tesznek különbséget a célpontok között, ehelyett a lehető legtöbb zavart akarják okozni, vagy jogosulatlan hozzáférést kívánnak szerezni bármely sebezhető rendszerhez.

Ezzel szemben a *fejlett tartós fenyegetések* (Advanced Persistent Threat — APT) rendkívül kifinomult és célzott támadások, amelyeket arra terveztek, hogy hosszú időn keresztül beszivárogjanak bizonyos szervezetekbe vagy entitásokba. Az APT-ket gyakran jól finanszírozott és képzett támadók, például állami támogatású csoportok vagy szervezett kiberbűnözők hajtják végre, akiknek világos céljuk van, és hajlandóak jelentős időt és erőforrásokat befektetni annak elérésére. Az APT-ket a lopakodás és a kitartás jellemzi, gyakran több támadási vektort és fejlett technikákat alkalmaznak, hogy elkerüljék a felderítést és a lehető legtovább fenntartsák a hozzáférést a célzott hálózathoz.

A biztonsági értékelések és az IT Forensics megértése

A kiberbiztonság területén két alapvető fontosságú gyakorlat elengedhetetlen a rendszerek védelméhez és az incidensekre való reagáláshoz: a *biztonsági értékelések* (security assessments) és az *IT törvényszéki vizsgálat* (IT forensics).

A biztonsági értékelések a szervezet információs rendszereinek és hálózatainak szisztematikus értékelései a sebezhetőségek azonosítása, a kockázatok felmérése és a meglévő biztonsági intézkedések hatékonyságának meghatározása céljából. Ezek az értékelések segítik a szervezeteket abban, hogy megértsék biztonsági helyzetüket, és azonosítsák a fejlesztésre szoruló területeket. A biztonsági értékelések különböző formákat ölthetnek, beleértve a sebezhetőségi

értékeléseket, a biztonsági auditokat és a behatolásvizsgálatokat. Az értékelések minden típusa más-más betekintést nyújt a szervezet biztonsági keretrendszerébe, lehetővé téve a potenciális kockázatok átfogó megértését.

A *penetration testing* (behatolástesztelés), amelyet gyakran etikus hackingként is emlegetnek, egy proaktív biztonsági értékelési technika, amely egy rendszer elleni támadásokat szimulál, hogy azonosítani lehessen a sebezhetőségeket, mielőtt a rosszindulatú szereplők kihasználhatnák azokat. A penetration test során képzett tesztelők, akiket gyakran *pentester*-nek neveznek, a valós támadók taktikáit, technikáit és eljárásait utánozzák, hogy feltárják a szervezet védelmének gyenge pontjait. A penetration testing célja olyan biztonsági rések azonosítása, amelyek nem feltétlenül válnak nyilvánvalóvá az automatikus sebezhetőségi vizsgálatok vagy a tesztelés más formái révén. E gyenge pontok azonosításával a szervezetek korrekciós intézkedéseket tehetnek biztonsági intézkedéseik megerősítése és a sikeres támadás valószínűségének csökkentése érdekében.

A biztonsági értékelések mellett az *IT forensics* vagy digitális törvényszéki szakértői tevékenység a kiberincidensek kivizsgálására és elemzésére összpontosít, hogy meghatározzák azok okát, kiterjedését és hatását. Az informatikai törvényszéki vizsgálat magában foglalja a számítógépes rendszerekből, hálózatokból és egyéb digitális eszközökből származó digitális bizonyítékok összegyűjtését, megőrzését és vizsgálatát. Az informatikai törvényszéki vizsgálat elsődleges célja a biztonsági incidens részleteinek feltárása, beleértve azt, hogy hogyan történt, ki volt a felelős, és milyen adatokat vagy rendszereket érintett.

Az informatikai törvényszéki eljárás a releváns digitális bizonyítékok azonosításával és összegyűjtésével kezdődik, amelyeket gondosan meg kell őrizni, hogy fenntartsák integritásukat és elfogadhatóságukat a bírósági eljárásokban. A törvényszéki elemzők speciális eszközöket és technikákat használnak az összegyűjtött bizonyítékok elemzésére, az események rekonstruálására és az incidens forrásának azonosítására. Ez az elemzés gyakran magában foglalja a naplófájlok, a hálózati forgalom és más digitális leletek vizsgálatát, hogy nyomon kövessék a támadó tevékenységét, és meghatározzák, hogyan jutott hozzá a rendszerhez.

Az informatikai törvényszéki vizsgálat egyik legfontosabb szempontja az incidensek elhárításában betöltött szerepe. Ha a biztonság megsértése megtörténik, a gyors és hatékony reagálás kulcsfontosságú a károk minimalizálása és a további veszélyeztetés megelőzése érdekében. Az informatikai törvényszéki vizsgálat biztosítja a támadás jellegének megértéséhez és a célzott válaszadási terv kidolgozásához szükséges információkat. A támadók által használt módszerek és a kár mértékének azonosításával a szervezetek megfelelő lépéseket tehetnek az incidens megfékezésére, a hatásainak mérséklésére és a jövőbeli események megelőzésére.

Information Security Management System (ISMS) és incidenskezelés

A mai digitális korban az érzékeny információk védelme kritikus prioritás a szervezetek számára, méretüktől függetlenül. Ennek érdekében a vállalkozásoknak átfogó megközelítést kell alkalmazniuk az információbiztonság terén, amely proaktív és reaktív intézkedéseket egyaránt magában foglal.

Az *információbiztonsági irányítási rendszer* (Information Security Management System — ISMS) a szervezet érzékeny adatainak kezelésére és biztonságának biztosítására szolgáló szisztematikus keretrendszer. Az ISMS elsődleges célja az információk bizalmasságának, sértetlenségének és rendelkezésre állásának védelme kockázatkezelési folyamat alkalmazásával. Ez magában foglalja az információs eszközöket fenyegető potenciális veszélyek azonosítását, az ezekhez a veszélyekhez kapcsolódó kockázatok értékelését és a veszélyek mérséklésére szolgáló megfelelő ellenőrzések végrehajtását. Egy hatékony ISMS nem csak a technológiáról szól, hanem magában foglalja az embereket és a folyamatokat is, holisztikus megközelítést alkotva az információbiztonsági kockázatok kezeléséhez.

Az ISMS megvalósítása általában olyan nemzetközi szabványokat követ, mint az ISO/IEC 27001, amely iránymutatást ad az információbiztonsági irányítási rendszer létrehozására, megvalósítására, fenntartására és folyamatos fejlesztésére. E szabványok betartása segíti a szervezeteket a biztonsági kockázatok szisztematikus azonosításában és a kockázati szintnek megfelelő ellenőrzések végrehajtásában. Az ISMS keretrendszert úgy tervezték, hogy dinamikus legyen, lehetővé téve a szervezetek számára, hogy alkalmazkodjanak a fejlődő fenyegetésekhez és a változó üzleti környezethez. Az ISMS rendszeres felülvizsgálatával és frissítésével a szervezetek biztosíthatják, hogy biztonsági intézkedéseik hatékonyak maradnak, és összhangban vannak üzleti célkitűzéseikkel.

Az ISMS a legfelsőbb szintű felelősséget vállal a szervezet biztonságáért. Biztosítja, hogy a hálózati és rendszergazdák minden eszközzel tisztában legyenek. Megdöbbentő, hogy milyen gyakran maradnak védtelenül számítógépek, adatok vagy mobileszközök, mert a felhasználók elfelejtették jelenteni a létezésüket a biztonságért felelős személyeknek.

Az ISMS meghatározza, hogy kinek kell hozzáférnie az egyes adattípusokhoz, és kijelöli azokat az embereket, akik gondoskodnak arról, hogy a technológia tükrözze ezeket az irányelveket. Más irányelvek irányadóak lehetnek a létesítményben engedélyezett berendezések típusai tekintetében, milyen vizsgálatokat és biztonsági teszteket kell végezni, és hogyan kell kezelni a támadásokat, ha felfedezik őket.

A megbízható ISMS mellett a szervezeteknek fel kell készülniük arra is, hogy gyorsan és hatékonyan reagáljanak a biztonsági incidensekre, ha azok bekövetkeznek. Ehhez egy jól

meghatározott *eseményreagálási terv* (Incident Response Plan — IRP) és egy képzett *információbiztonsági incidensekre reagáló csapat* (Information Security Incident Response Team — ISIRT) szükséges. Az IRP felvázolja azokat az eljárásokat és intézkedéseket, amelyeket a szervezetnek biztonsági jogsértés vagy egyéb incidensek esetén meg kell tennie. Egyértelmű ütemtervet biztosít az incidensek észlelésére, elemzésére, megfékezésére, felszámolására és helyreállítására, biztosítva, hogy a szervezet a lehető leghamarabb minimalizálni tudja a károkat és helyre tudja állítani a normál működést.

A hatékony IRP kulcsfontosságú eleme az ISIRT létrehozása. Ez a csapat meghatározott szerepkörökkel és felelősségi körökkel rendelkező személyekből áll, köztük műszaki szakértőkből, jogi tanácsadókból és kommunikációs szakemberekből, akik együtt dolgoznak a biztonsági incidensek kezelésén és hatásainak enyhítésén. Az ISIRT felelős az incidensre adott válaszfolyamat koordinálásáért, annak biztosításáért, hogy minden lépést a tervnek megfelelően hajtsanak végre, valamint a szervezeten belüli és kívüli érdekelt felekkel való kommunikációért.

Az ISMS és az incidensekre való reagálás ismerete a szervezeten belül minden alkalmazott számára alapvető fontosságú, nem csak az informatikai vagy biztonsági szerepkörben dolgozók számára. Mindenkinek szerepe van az információs eszközök védelmében, a biztonsági irányelvek és eljárások betartásától a gyanús tevékenységek bejelentéséig. A biztonságtudatosság kultúrájának előmozdításával a szervezetek képessé tehetik alkalmazottaikat arra, hogy a potenciális fenyegetésekkel szembeni első védelmi vonalként lépjenek fel. A rendszeres képzések és tudatosságnövelő programok elengedhetetlenek ahhoz, hogy a munkatársak tájékozottak legyenek a legújabb fenyegetésekkel kapcsolatban, a biztonsági protokollok betartásának fontosságával és az incidensek esetén teendő lépésekkel.

Ezen túlmenően az ISMS és az incidensekre való reagálás integrációja alapvető fontosságú a rugalmas biztonsági helyzet megteremtéséhez. Míg az ISMS az információbiztonság proaktív kezelésének alapját képezi, az incidensre reagálási terv biztosítja, hogy a szervezet felkészült legyen a gyors és hatékony reagálásra az esetleges jogsértésekre. Ez a kettős megközelítés lehetővé teszi a szervezetek számára, hogy minimalizálják a biztonsági incidensek valószínűségét, és ha bekövetkeznek, enyhítsék azok hatását, ezáltal megvédve a szervezet hírnevét, jogi helyzetét és működési folyamatosságát.

Gyakorló feladatok

1. Miért fontos ellenőrizni annak a szoftvernek a verziószámát, amelyről a sebezhetőséget jelentették?

2. Mi a különbség a sebezhetőségi vizsgálat (vulnerability scanning) és a behatolásvizsgálat (penetration testing) között?

3. Miért van szükség jogászokra egy információbiztonsági incidensekre reagáló csoportban (ISIRT)?

Gondolkodtató feladatok

1. Soroljuk fel azoknak a személyeknek a szervezeti szerepét, akiknek az információbiztonsági irányítási rendszert (ISMS) tervező csapatban kell lenniük!

2. Képzeljük el, hogy egy támadó átvette egy központi adatbázis irányítását! Mi az, amit egy információbiztonsági incidensekre reagáló csapat (ISIRT) tehet?

Összefoglalás

A Common Vulnerabilities and Exposures (CVE) adatbázis a szoftverek és eszközök biztonsági hibáit követi nyomon. A biztonsági szakértők számára számos eszköz, mind zárt és nyílt forráskódú, segít a hibák felkutatásában. Minden szervezetnek rendszeresen kellene sebezhetőségi vizsgálatokat és behatolásteszteket végeznie.

Mivel a szoftverek összetettek és a számítógépes rendszerek összekapcsolódnak, a támadók a szervezet rendszereinek apró hibáit kihasználva komoly problémákat okozhatnak. Az információbiztonsági irányítási rendszer (ISMS) csapatának és az információbiztonsági incidensekre reagáló csapatnak (ISIRT) szükséges lenne rendszeresen összeülnie a kockázatok felmérése és egy olyan terv létrehozása érdekében, amely megelőzi a támadásokat és reagál rájuk.

Válaszok a gyakorló feladatokra

1. Miért fontos ellenőrizni annak a szoftvernek a verziószámát, amelyről a sebezhetőséget jelentették?

   Lehet, hogy olyan verziót használunk, amelyet nem érint a hiba, és ebben az esetben biztonságban vagyunk. Másrészt viszont el kell kerülnünk az automatikus “frissítést” (upgrade) a szoftver egy olyan verziójára, amely veszélyes sebezhetőséget tartalmaz..

2. Mi a különbség a sebezhetőségi vizsgálat (vulnerability scanning) és a behatolásvizsgálat (penetration testing) között?

   A sebezhetőségi vizsgálat csak arról ad jelentést, hogy a rendszerben vannak-e ismert hibák. A behatolásvizsgálat sokkal erősebb, mivel aktívan megpróbál betörni a rendszerbe.

3. Miért van szükség jogászokra egy információbiztonsági incidensekre reagáló csoportban (ISIRT)?

   A jogszabályok meghatározzák a válaszadás egyes aspektusait, és gyakran megkövetelik, hogy a szervezet jogi dokumentumokat nyújtson be a támadásról.

Válaszok a gondolkodtató feladatokra

1. Soroljuk fel azoknak a személyeknek a szervezeti szerepét, akiknek az információbiztonsági irányítási rendszert (ISMS) tervező csapatban kell lenniük!

   Egy rendszergazda (system administrator) minden fő részlegből, hogy megértse az adott részleg eszközeit. Egy üzleti vezető (business leader) is hasznos lenne, mind az eszközök azonosításához, mind annak meghatározásához, hogy kinek kell hozzáférnie azokhoz.

   A biztonsági vezetőknek (security manager) a szakértelem miatt a csapatban kellene lenniük.

   A biztonság teszteléséért felelős rendszergazdáknak is a csapatban kell lenniük, hogy tisztában legyenek minden ellenőrizendő rendszerrel, és a csapattal együtt ki tudják dolgozni a lefuttatandó tesztek fajtáit és gyakoriságát.

   Szükség van jogászokra a megfelelőség biztosításához, a humánerőforrás-osztályra pedig azért, hogy mindenki, aki a biztonságért felelős, ismerje a szerepét és képzést kapjon.

   Egy C-szintű vezetőnek jelen kell lennie, hogy a vezetőség biztosítsa a szükséges erőforrásokat. A vezetőség azt is rangsorolhatja, hogy egy támadás után mely rendszerek álljanak újra működésbe, és a helyreállítási terv által esetleg okozott szükséges fennakadások idején is támogatni kell a dolgozókat.

   Valószínűleg vannak más személyek is, akiket érdemes felvenni a csapatba, például a létesítmény fizikai biztonságáért felelős személyek.

2. Képzeljük el, hogy egy támadó átvette egy központi adatbázis irányítását! Mi az, amit egy információbiztonsági incidensekre reagáló csapat (ISIRT) tehet?

   Az adatbázist futtató rendszereket, a hozzájuk kapcsolódó rendszereket és az őket kiszolgáló routereket valószínűleg el kell távolítani a hálózatról. A biztonsági személyzetnek át kell vizsgálnia a rendszereket törvényszéki vizsgálat céljából.

   Értesíteni kell az adatbázissal dolgozó kulcsfontosságú munkatársakat és a vezetőséget. A pánik elkerülése és az információknak a támadók kezén kívül tartása érdekében valószínűleg kerülni kell az általános bejelentést mindaddig, amíg nem áll rendelkezésre a helyreállítás ütemterve.

   Attól függően, hogy mit lehet tudni a támadás mértékéről, az ISIRT-nek le kell állítania az e-mail és a vállalati eszközök kommunikációra való használatát.

   Az adatbázist ért károk azonosítása után keresni kell egy olyan biztonsági másolatot, amelyről ismert, hogy helyes és mentes a rosszindulatú programoktól, és egy új rendszert kell indítani

ennek az adatbázisnak a futtatására, hogy a szervezet megkezdhesse a működés helyreállítását.

A megfelelőség érdekében ki kell tölteni az incidensről szóló űrlapokat, és értesíteni kell a bűnüldöző szervek kapcsolattartóit.

A helyreállításhoz vezető úton bizonyára vannak még egyéb feladatok is.

021.3 Etikus magatartás

Hivatkozás az LPI célkitűzésre

Security Essentials version 1.0, Exam 020, Objective 021.3

Súlyozás

2

Kulcsfontosságú ismeretek

- A biztonsággal kapcsolatos intézkedések következményeinek megértése
- A biztonsági résekkel kapcsolatos információk felelős kezelése
- Bizalmas információk felelős kezelése
- Az informatikai szolgáltatások hibáinak és kieséseinek személyes, pénzügyi, ökológiai és társadalmi következményeinek ismerete
- A biztonsági vizsgálatok, értékelések és támadások jogi

A használt fájlok, kifejezések és segédprogramok részleges listája

- Felelős közzététel és teljes közzététel
- Bug Bounty programok
- Közjog és magánjog
- Büntetőjog, adatvédelmi jog és szerzői jog
- Felelősség és kártérítési igények

Linux Professional Institute

Lecke 1

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	021 Biztonsági koncepciók
Fejezet:	021.3 Etikus magatartás
Lecke:	1/1

Bevezetés

A biztonsági tevékenységekkel kapcsolatos munka gyakran hozzáférést biztosít érzékeny személyes információkhoz, vállalati titkokhoz és más értékes adatokhoz. Az emberek és az adatok védelmét szolgáló irányelvek meghatározása és végrehajtása során a szakembereknek minden lépésnél fel kell mérniük munkájuk következményeit.

A biztonsági szakemberek olyan eszközöket is használnak, amelyekkel kárt okozhatnak, például behatolástesztelő szoftvereket. A szakemberek tehát egy szürke zónában tevékenykednek, és tisztában kell lenniük munkájuk valamennyi gazdasági, etikai és jogi következményével.

A biztonsággal kapcsolatos intézkedések következményei

A biztonsággal kapcsolatos intézkedések másokra gyakorolt hatásának megértése alapvető készség a kiberbiztonság területén. A biztonsági szakemberek cselekedetei tevékenységük végzése során nemcsak a közvetlenül a gondjaikra bízott rendszerekre és adatokra vannak hatással, hanem messzemenő jogi, etikai és társadalmi következményei is lehetnek. Ezért kulcsfontosságú, hogy ezek a szakemberek tisztában legyenek azzal, hogy döntéseik és cselekedeteik milyen hatással lehetnek másokra, köztük egyénekre, szervezetekre és a társadalom egészére.

A *közjogi és magánjogi* (public and private law) fogalom ebben az összefüggésben alapvető fontosságú. A kiberbiztonság terén hozott intézkedéseknek különböző jogi következményei lehetnek a joghatóságtól és a tevékenység jellegétől függően. A *közjog*, amely az egyének és az állam közötti kapcsolatot szabályozza, gyakran tartalmaz olyan szabályozásokat, amelyek hatással vannak a kiberbiztonsági gyakorlatokra. Az adatvédelemre és a magánélet védelmére vonatkozó állami rendeletek például kötelezettségeket írhatnak elő a személyes adatok kezelésével kapcsolatban, ami hatással van arra, hogy a kiberbiztonsági szakemberek hogyan hajtják végre a biztonsági intézkedéseket. A *magánjog* másfelől, amely az egyének és szervezetek közötti kapcsolatokkal foglalkozik, a szerződések, a felelősség és a biztonsági résekből eredő károkkal kapcsolatos helyzetekben kerülhet szóba. A kiberbiztonsági szakembereknek ismerniük kell ezeket a jogi kereteket, hogy elkerüljék az olyan lépéseket, amelyek akaratlanul törvénysértést vagy jogvitát eredményezhetnek.

A közjog és a magánjog mellett különösen fontosak az olyan speciális területek, mint a *büntetőjog* (penal law), az *adatvédelmi jog* (privacy law) és a *szerzői jog* (copyright law). A *büntetőjog* a bűncselekményekkel és azok szankcióival foglalkozik. A kiberbiztonság területén bizonyos cselekmények, mint például a rendszerekhez való jogosulatlan hozzáférés vagy az adatsértés, bűncselekménynek minősülhetnek, ami súlyos következményekkel jár az érintettekre nézve. Például egy rendszerbe való engedély nélküli behatolás vagy rosszindulatú szoftverek terjesztése büntetőjogi vádakat vonhat maga után. E jogi határok megértése létfontosságú a nem szándékos jogsértések elkerülése, valamint a digitális infrastruktúra és a személyes adatok védelmét szolgáló törvényeknek való megfelelés biztosítása érdekében.

Az *adatvédelmi jog* szabályozza a személyes adatok gyűjtését, felhasználását és megosztását. A digitális korban, amikor az adatok értékes értéket képviselnek, a magánélet védelme jelentős aggodalomra ad okot. A kiberbiztonsági szakembereknek jól kell ismerniük az adatvédelmi szabályokat, mint például az Európai Unió *általános adatvédelmi rendeletét* (General Data Protection Regulation — GDPR) vagy az Egyesült Államokban a *kaliforniai fogyasztói adatvédelmi törvényt* (California Consumer Privacy Act — CCPA). Ezek a törvények előírják, hogy a szervezeteknek hogyan kell kezelniük a személyes adatokat, és az előírások be nem tartása súlyos bírságokat és hírnevük romlását eredményezheti. Az adatvédelmi törvények megértése segít a kiberbiztonsági szakembereknek olyan biztonsági ellenőrzések végrehajtásában, amelyek védik a személyes adatokat és tiszteletben tartják az egyének adatvédelmi jogait.

A *szerzői jog* egy másik olyan terület, ahol a kiberbiztonsági intézkedések másokra is hatással lehetnek. A szerzői jog védi az eredeti szerzői műveket, beleértve a szoftvereket, dokumentációkat és egyéb digitális tartalmakat. A kiberbiztonsági szakembereknek tisztában kell lenniük azzal, hogy a szerzői jog hogyan vonatkozik a munkájukra, különösen, ha az szoftverek másolásával vagy módosításával, harmadik féltől származó eszközök használatával vagy információk megosztásával jár. A szerzői jogok megsértése jogi vitákhoz és pénzügyi szankciókhoz vezethet, ezért a biztonsági értékelések elvégzése vagy a biztonsági megoldások kidolgozása során

elengedhetetlen, hogy tisztában legyünk ezekkel a szabályozásokkal.

A biztonsági résekkel kapcsolatos információk kezelése

A biztonsági résekkel kapcsolatos információk felelősségteljes kezelése a kiberbiztonsági gyakorlat kritikus szempontja. A biztonsági rések felfedezése olyan potenciális gyenge pontokat jelent, amelyeket rosszindulatú szereplők kihasználhatnak jogosulatlan hozzáférés megszerzésére, adatlopásra vagy a szolgáltatások megzavarására. Az ilyen sebezhetőségekkel kapcsolatos információk kezelésének módja jelentős hatással lehet a digitális rendszerek és a tágabb értelemben vett internetes ökoszisztéma biztonságára és stabilitására. A sebezhetőséggel kapcsolatos információk felelős kezelése nem csupán technikai szükségszerűség, hanem etikai kötelezettség is a felhasználók és szervezetek károkozással szembeni védelme érdekében.

A *felelős közzététel* (responsible disclosure) olyan gyakorlat, amely magában foglalja a biztonsági rések olyan módon történő bejelentését, hogy az érintett feleknek legyen idejük a probléma kezelésére, mielőtt az információ nyilvánosságra kerülne. Ez a folyamat általában magában foglalja a közvetlen kommunikációt a sebezhetőséget tartalmazó szoftver vagy rendszer gyártójával vagy fejlesztőjével. A cél annak biztosítása, hogy a sebezhetőség javítható vagy csökkenthető legyen, mielőtt a részleteket szélesebb körben megosztanák, így minimalizálva a rosszindulatú szereplők általi kihasználás kockázatát. A felelős nyilvánosságra hozatalt a kiberbiztonsági közösség legjobb gyakorlatnak tekinti, mivel egyensúlyt teremt az átláthatóság és a tudatosság igénye, valamint a rendszerek és adatok károsodástól való védelme között.

Ezzel szemben a *teljes közzététel* (full disclosure) a sebezhetőség részleteinek azonnali nyilvánosságra hozatalára utal, anélkül, hogy az érintett feleknek előbb esélyt adnának a hiba kijavítására. A teljes közzététel hívei azzal érvelnek, hogy ez gyorsabb javításra ösztönöz azáltal, hogy nyomást gyakorol a gyártókra a sebezhetőségek azonnali orvoslása érdekében. Ugyanakkor nagyobb kockázatnak is kiteheti a rendszereket, mivel a rosszindulatú szereplők kihasználhatják a sebezhetőséget, mielőtt a javítás elérhetővé válna. A felelős közzététel és a teljes közzététel közötti döntés gyakran különböző tényezőktől függ, többek között a sebezhetőség súlyosságától, a kihasználás valószínűségétől és az érintett felek reagálóképességétől.

A *Bug Bounty programok* olyan kezdeményezések, amelyek arra ösztönzik az egyéneket, hogy pénzjutalomért vagy elismerésért cserébe találjanak és jelentsenek sebezhetőségeket. Ezeket a programokat általában szervezetek indítják, hogy ösztönözzék az etikus hackelést és a felelős közzétételt. A bug bounty programok azáltal, hogy egyértelmű iránymutatásokat adnak a sebezhetőségek bejelentésére és az elfogadható viselkedésre vonatkozóan, segítenek biztosítani, hogy a biztonsági hiányosságokra vonatkozó információkat megfelelően kezeljék. Emellett elősegítik a szervezetek és a szélesebb körű kiberbiztonsági közösség közötti együttműködést, proaktívabb és elkötelezettebb megközelítést teremtve a sebezhetőségek kezelésében.

A biztonsági sebezhetőségekkel kapcsolatos információk etikus kezelése az összes érdekelt félre gyakorolt lehetséges hatások gondos mérlegelését igényli. A sebezhetőség felfedezésekor a kiberbiztonsági szakembereknek mérlegelniük kell a nyilvánosságra hozatal kockázatait az előnyökkel szemben. Figyelembe kell venniük a sebezhetőség kihasználásából eredő potenciális károkat, annak valószínűségét, hogy a rosszindulatú szereplők már ismerik a sebezhetőséget, valamint az érintett felek hatékony reagálási képességét. Sok esetben az érintett szervezettel való szoros együttműködés, a részletes tájékoztatás és a javítás kidolgozásához nyújtott támogatás a legfelelősségteljesebb lépés.

A biztonsági rések felelősségteljes kezelésének végső soron az a célja, hogy megvédje a felhasználókat és a rendszereket a károktól, miközben elősegíti az átláthatóság és az elszámoltathatóság kultúráját. A kiberbiztonsági szakemberek az olyan bevett gyakorlatok betartásával, mint a felelős közzététel és a bug bounty programokban való részvétel, hozzájárulhatnak a védettebb és biztonságosabb digitális környezethez. A sebezhetőségekkel kapcsolatos információk gondos kezelése nemcsak a kihasználás megelőzésében segít, hanem a kutatók, fejlesztők és felhasználók közötti bizalmat és együttműködést is erősíti, elősegítve ezzel egy mindenki számára rugalmasabb és biztonságosabb internet kialakulását.

Bizalmas információk kezelése

A bizalmas információk felelősségteljes kezelése a hatékony kiberbiztonsági gyakorlat egyik sarokköve. A bizalmas információkat — legyenek azok személyes adatok, védett üzleti információk vagy érzékeny kommunikáció — védeni kell a bizalom fenntartása, a jogi követelményeknek való megfelelés és a károk megelőzése érdekében. A digitális korban, amikor az adatsértések és a jogosulatlan hozzáférés súlyos következményekkel járhat, a bizalmas információk védelmének megértése minden kiberbiztonsági szakember számára kiemelkedő fontosságú.

A bizalmas információk kezelésének kritikus szempontja az adatvédelmi törvényeknek való megfelelés. Az adatvédelmi jogszabályok, például a GDPR és a CCPA részletes iránymutatásokat határoznak meg a személyes adatok gyűjtésének, feldolgozásának, tárolásának és megosztásának módjára vonatkozóan. E szabályozások célja, hogy megvédjék az egyének magánélethez és a személyes adataik feletti ellenőrzéshez való jogát. A kiberbiztonsági szakembereknek biztosítaniuk kell, hogy gyakorlatuk összhangban legyen ezekkel a jogi követelményekkel, és olyan erős biztonsági intézkedéseket kell bevezetniük, mint a titkosítás, a hozzáférés ellenőrzése és a rendszeres auditok, hogy megakadályozzák a jogosulatlan hozzáférést és az adatbiztonság megsértését. Az adatvédelmi törvények be nem tartása jelentős bírságokat, jogi lépéseket és a szervezet hírnevének romlását eredményezheti, ezért elengedhetetlen, hogy minden bizalmas információt a lehető legnagyobb gondossággal kezeljenek.

Az adatvédelmi törvényeken túl a büntetőjog is döntő szerepet játszik a bizalmas információk

kezelésében. A büntetőjog a jogosulatlan hozzáféréssel, az adatokkal való visszaéléssel és az információk bizalmas jellegét veszélyeztető egyéb cselekményekkel kapcsolatos bűncselekmények széles körére terjed ki. Például egy rendszerbe való betörés üzleti titkok ellopása céljából, vagy valakinek a magánjellegű kommunikációjához való hozzájárulás nélküli hozzáférés büntetőjogi vádakat vonhat maga után. A kiberbiztonsági szakembereknek ébernek kell lenniük az e törvények által meghatározott határok megértésében, hogy elkerüljenek minden olyan cselekményt, amely illegálisnak minősülhet. Ez magában foglalja a robusztus hitelesítési módszerek bevezetését, a rendszerek jogosulatlan hozzáférési kísérletek figyelemmel kísérését, valamint annak biztosítását, hogy minden tevékenységet dokumentáljanak és legitim biztonsági megbízás alapján igazolják.

A bizalmas információk kezelésének felelőssége túlmutat a jogosulatlan hozzáférés megakadályozásán; magában foglalja a biztonságtudatosság és a megfelelőség kultúrájának kialakítását is a szervezeten belül. Az alkalmazottakat minden szinten ki kell képezni a bizalmas adatok védelmének fontosságáról, valamint a biztonságukat biztosító konkrét irányelvekről és eljárásokról. Ez magában foglalja a legkisebb kiváltság (least privilege) elveinek megértését, ahol a bizalmas információkhoz való hozzáférés csak azokra korlátozódik, akiknek szükségük van rá a munkaköri feladataik ellátásához, valamint az adatbiztonságot veszélyeztető potenciális social engineering támadások ismeretét.

A technikai biztosítékok és a szervezeti irányelvek mellett a kiberbiztonsági szakembereknek a bizalmas információk kezelésének etikai vonatkozásait is figyelembe kell venniük. Nem elég csupán a jogi követelményeknek megfelelni, hanem erkölcsi kötelességük is tiszteletben tartani az egyének magánéletét és megvédeni adataikat a visszaélésektől. Ez az etikai szemlélet a biztonság proaktív megközelítését követeli meg, a potenciális fenyegetések és sebezhetőségek előrejelzését, valamint lépéseket azok mérséklésére, mielőtt azok kihasználhatók lennének.

A bizalmas információk felelősségteljes kezelése olyan biztonságos környezet megteremtését jelenti, amelyben az adatok védve vannak mind a külső fenyegetésekkel, mind a belső visszaélésekkel szemben. A kiberbiztonsági szakemberek az adatvédelmi és büntetőjogi törvények megértésével és betartásával, a robusztus biztonsági intézkedések végrehajtásával, valamint a tudatosság és az etikai felelősségvállalás kultúrájának előmozdításával segíthetnek abban, hogy a bizalmas információk biztonságban maradjanak. Ez nemcsak a szervezetet és az érdekelt feleket védi, hanem fenntartja a magánélethez való alapvető jogot az egyre digitálisabb világban.

Az informatikai szolgáltatások hibáinak és kieséseinek következményei

Az informatikai szolgáltatások hibáinak és kieséseinek személyes, pénzügyi, ökológiai és társadalmi következményeinek tudatosítása a kiberbiztonság alapvető eleme. Egyre inkább

digitális világunkban a technológiától való függés a személyes kommunikációtól a kritikus infrastruktúrákig minden téren azt jelenti, hogy bármilyen zavar messzemenő következményekkel járhat. A kiberbiztonsági szakembereknek tisztában kell lenniük ezekkel a következményekkel, hogy hatékonyan csökkentsék a kockázatokat, és ne csak a rendszereket és az adatokat, hanem a tőlük függő embereket és környezetet is megvédjék.

A hibák és a kiesések *személyes szempontból* jelentős hatással lehetnek az egyének életére. Például egy olyan adatvédelmi incidens, amely személyes adatokat, például társadalombiztosítási számokat, banki információkat vagy orvosi feljegyzéseket hoz nyilvánosságra, személyazonosság-lopáshoz, pénzügyi veszteséghez és a privátszféra mélyreható elvesztéséhez vezethet. A kiberbiztonsági szakembereknek fel kell ismerniük az ilyen személyes károk lehetőségét, és robusztus intézkedéseket kell bevezetniük az érzékeny adatok védelme érdekében. E személyes következmények tudatosítása biztosítja, hogy a biztonsági intézkedések ne csak technikailag legyenek megalapozottak, hanem empatikusak is legyenek a felhasználókkal szemben, akiket védeni kívánnak.

A kiberbiztonsági incidensek *pénzügyi következményei* gyakran a legközvetlenebbül láthatóak. A hibák és kiesések közvetlen pénzügyi veszteségeket okozhatnak a vállalkozások számára a leállások, a termelékenység csökkenése és a helyreállítási erőfeszítések költségei miatt. Súlyosabb esetekben jelentős *felelősségi* problémák merülhetnek fel, amikor az érintett felek pénzügyi kártérítési igényt támasztanak a felmerült károkért. Például egy e-kereskedelmi platformot megzavaró kibertámadás az értékesítés és a vásárlók bizalmának elvesztését eredményezheti, míg egy pénzintézet elleni támadás nagyszabású pénzügyi csaláshoz vezethet. E pénzügyi következmények megértése segít a kiberbiztonsági szakembereknek abban, hogy prioritásként kezeljék az olyan eszközök és infrastruktúrák védelmét, amelyek veszélyeztetése jelentős gazdasági károkat okozhat.

A személyes és pénzügyi következményeken túlmenően a kiberbiztonsági incidensek *ökológiai következményeit* is figyelembe kell venni. Az olyan ágazatokban, mint az energia-, víz- és hulladékgazdálkodás, az informatikai rendszerek döntő szerepet játszanak a műveletek irányításában és ellenőrzésében. Ezekben az ágazatokban egy kibertámadás vagy rendszerleállás veszélyes anyagok kibocsátásához, vízszennyezéshez vagy akár széles körű környezeti károkhoz vezethet. Például egy szennyvíztisztító telep elleni kibertámadás következtében kezeletlen szennyvíz kerülhet a természetes vízfolyásokba, ami károsíthatja az ökoszisztémákat és a közegészségügyet. A kiberbiztonsági szakembereknek tisztában kell lenniük ezekkel a lehetséges ökológiai hatásokkal, és biztosítaniuk kell, hogy a rendszerek védettek legyenek mind az olyan szándékos támadások, mind az olyan véletlen hibák ellen, amelyek környezeti károkat okozhatnak.

A kiberbiztonsági incidensek *társadalmi következményei* ugyanilyen jelentősek. A mai összekapcsolódott világban a technológia a társadalmi infrastruktúra számos aspektusát

támogatja, beleértve az egészségügyet, az oktatást, a közlekedést és a kormányzati szolgáltatásokat. E rendszerek kiesése vagy hibája megzavarhatja a mindennapi életet, késleltetheti a kritikus szolgáltatásokat, és akár a közbiztonságot is veszélyeztetheti. Például egy kórház informatikai rendszereit érő kibertámadás késleltetheti a sürgős orvosi ellátást, míg a tömegközlekedési hálózatok elleni támadás széles körű káoszt és kellemetlenségeket okozhat. A kiberbiztonsági szakembereknek tisztában kell lenniük munkájuk társadalmi hatásaival, biztosítva, hogy a közjólét és a közbiztonság szempontjából alapvető fontosságú szolgáltatások védelmét helyezzék előtérbe.

Az informatikai szolgáltatások hibáinak és kieséseinek széleskörű következményeinek megértéséhez multidiszciplináris szemléletre van szükség. A kiberbiztonsági szakembereknek nemcsak a technikai megoldásokra kell összpontosítaniuk, hanem figyelembe kell venniük azokat a jogi, etikai és társadalmi összefüggéseket is, amelyekben ezek a technológiák működnek. A felelősség és a kártérítési igények lehetőségének, valamint a kiberbiztonsági incidensek személyes, pénzügyi, ökológiai és társadalmi következményeinek felismerésével holisztikusabb megközelítést alkalmazhatnak a digitális infrastruktúra védelmében, amelytől a modern társadalom függ. Ez a tudatosság biztosítja, hogy a kiberbiztonsági erőfeszítések ne csak a jogsértések megelőzéséről szóljanak, hanem összekapcsolódott világunk alapvető szerkezetének védelméről is.

Gyakorló feladatok

1. Melyek a kiberbiztonsági szakemberek számára a kulcsfontosságú szempontok az érzékeny információk kezelése és a biztonsági tevékenységek végzése során?

2. Miért fontos a biztonsági rések felelős kezelése, és milyen gyakorlatok támogatják ezt?

3. Hogyan befolyásolják a jogi vonatkozások a kiberbiztonsági szakemberek által végzett biztonsági vizsgálatok, értékelések és tesztek lebonyolítását?

Gondolkodtató feladatok

1. Hogyan viszonyulna egy szervezet egy security officerhez aki a bátyja elhidegült barátnőjéről keresett információkat az adatbázisában, hogy a testvére felkutathassa a lányt?

2. Mi alapján gyaníthatja egy szakértő, hogy a támadók tudnak egy olyan nulladik napi sebezhetőségről, amelyet ő nemrég fedezett fel?

Összefoglalás

Az etikai, jogi, biztosítási követelmények és egyéb tényezők egymásba fonódva határozzák meg a jogsértések kezelésére vonatkozó szabályokat. Minden biztonsági szakembernek számos egységgel szemben van felelőssége: a szervezet, amelynek dolgozik, a szervezet alkalmazottai, az ügyfelek, a kormányok és a társadalom egésze felé.

A biztonsági szakértők hozzáférnek a hálózatokat vizsgáló hatékony eszközökhöz, valamint hozzáférnek az érzékeny adatokhoz. Az etika megköveteli a szakembertől, hogy ezeket az eszközöket és adatokat csak a biztonsági célok eléréséhez használja. Az auditálással elkaphatók azok, akik visszaélnek az adatokhoz való hozzáféréssel.

A jogsértéseknek jogi, pénzügyi és hírnevet érintő következményei vannak. A szakembereknek meg kell ismerniük az iparágukra vonatkozó állami és magánjogi előírásokat, és a lehető legnagyobb mértékben meg kell felelniük ezeknek.

Végül pedig felelősségteljesen kell eljárniuk a biztonsági hibákat bejelentő személyeknek is, az érintett termékekért felelős személyeknek pedig ésszerű időn belül ki kell javítaniuk a hibákat.

Válaszok a gyakorló feladatokra

1. Melyek a kiberbiztonsági szakemberek számára a kulcsfontosságú szempontok az érzékeny információk kezelése és a biztonsági tevékenységek végzése során?

   A kiberbiztonsági szakembereknek tisztában kell lenniük mind a technikai, mind az etikai következményekkel. Ez magában foglalja a kiberbiztonsági tevékenységeket szabályozó jogi keretek — például a köz- és magánjog — megértését, amelyek előírják, hogyan kell kezelni a személyes és vállalati adatokat, és hogy milyen körülmények között megengedhetőek bizonyos tevékenységek.

2. Miért fontos a biztonsági rések felelős kezelése, és milyen gyakorlatok támogatják ezt?

   A biztonsági sebezhetőségek felelős kezelése létfontosságú, mivel ezek a sebezhetőségek potenciális gyenge pontokat jelentenek, amelyeket rosszindulatú szereplők kihasználhatnak. A felelős kezelést támogató két kulcsfontosságú gyakorlat a felelős közzététel és a teljes közzététel.

3. Hogyan befolyásolják a jogi vonatkozások a kiberbiztonsági szakemberek által végzett biztonsági vizsgálatok, értékelések és tesztek lebonyolítását?

   A jogi vonatkozások jelentősen befolyásolják, hogy a kiberbiztonsági szakemberek hogyan végzik a biztonsági vizsgálatokat, értékeléseket és támadásokat. Az olyan tevékenységek, mint a behatolásvizsgálat vagy a sebezhetőségi felmérések jogi szürke zónába eshetnek, amelyeket a köz- és magánjog, valamint a büntetőjog szabályoz. Kifejezett engedély nélkül ezek a tevékenységek jogosulatlannak minősülhetnek, ami bírságokat, jogi lépéseket vagy büntetőjogi vádakat vonhat maga után. A kiberbiztonsági szakembereknek be kell szerezniük a kifejezett hozzájárulást a nem szándékos jogsértések elkerülése érdekében.

Válaszok a gondolkodtató feladatokra

1. Hogyan viszonyulna egy szervezet egy security officerhez aki a bátyja elhidegült barátnőjéről keresett információkat az adatbázisában, hogy a testvére felkutathassa a lányt?

   Ez egy nagyon súlyos belső jogsértés, amely erőszakhoz vezethet. A szervezetnek valószínűleg azonnal meg kell szüntetnie a security officer munkaviszonyát, és a helyi rendőrséghez kell fordulnia az üggyel. Mivel a barátnő személyes adatai sérültek, a szervezetnek őt is értesítenie kell.

2. Mi alapján gyaníthatja egy szakértő, hogy a támadók tudnak egy olyan nulladik napi sebezhetőségről, amelyet ő nemrég fedezett fel?

   A szakértő talán hallotta, hogy a szervezeteket egy bizonyos típusú SQL-lekérdezéssel vagy API-hívással támadták meg, amely a sebezhetőséggel hozható összefüggésbe. A szervezetek számára értékes, hogy kapcsolatban maradjanak és megosszák egymással a jogsértésekkel kapcsolatos információkat, hogy ilyen részletek is előkerüljenek.

Linux Professional Institute

Témakör 022: Titkosítás

022.1 Kriptográfia és nyilvános kulcsú infrastruktúra

Hivatkozás az LPI célkitűzésre

Security Essentials version 1.0, Exam 020, Objective 022.1

Súlyozás

3

Kulcsfontosságú ismeretek

- A szimmetrikus, asszimetrikus és a hibrid kriptográfia fogalmainak megértése
- A Perfect Forward Secrecy fogalmának megértése
- Hash-funkciók, rejtjelek (cipher) és kulcscsere-algoritmusok fogalmainak megértése
- Az end-to-end titkosítás és a szállítási titkosítás közötti különbségek megértése
- A Public Key Infrastructure (PKI), a Certificate Authorities, és a Trusted Root-CA fogalmainak megértése
- Az X.509 tanúsítványok fogalmának megértése
- Az X.509 tanúsítványok igénylésének és kiadásának megértése
- A tanúsítványok visszavonásának ismerete
- A Let’s Encrypt ismerete
- A fontos kriptográfiai algoritmusok ismerete

A használt fájlok, kifejezések és segédprogramok részleges listája

- Public Key Infrastructures (PKI)
- Certificate Authorities
- Trusted Root-CAs
- Tanúsítványaláírási kérelmek (CSR) és tanúsítványok

- X.509 tanúsítvány mezői: Tárgy, Kiállító, Érvényesség
- RSA, AES, MD5, SHA-256, Diffie-Hellman kulcscsere, Elliptikus görbe kriptográfia

Linux Professional Institute

Lecke 1

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	022 Titkosítás
Fejezet:	022.1 Kriptográfia és nyilvános kulcsú infrastruktúra
Lecke:	1/2

Bevezetés

A kriptográfia a modern kiberbiztonság egyik alapvető eleme, amely az érzékeny adatok és a kommunikáció jogosulatlan hozzáféréstől való védelmét szolgálja. A kriptográfia lényege a *titkosítás* (encrpytion), amely az olvasható információt speciális algoritmusok segítségével olvashatatlan formátumba alakítja át. Ez a folyamat biztosítja, hogy csak a megfelelő *kulccsal* (key) rendelkező személyek tudják visszafejteni a szöveget az eredeti formájába. A titkosítás kulcsfontosságú az adatok továbbítás vagy tárolás közbeni védelméhez, legyen szó személyes üzenetekről, pénzügyi információkról vagy üzleti titkokról.

A titkosítás mellett a kriptográfia magában foglalja a *hashing* eljárást is, amely a bemeneti adatokból egy egyedi, rögzített méretű kimenetet, az úgynevezett *hash*-t generál. A zárolás az adatok integritásának ellenőrzésére szolgál, biztosítva, hogy az információt nem változtatták meg.

A kriptográfia ezen alapfogalmainak megértése alapvető fontosságú mindazok számára, akik meg akarják érteni a digitális információk biztonságának és az adatok integritásának védelme mögött meghúzódó elveket. Ezeket a kriptográfiai technikákat a mindennapi alkalmazásokban használják, kezdve a weboldalak és online tranzakciók védelmétől, egészen a személyes adatok és

digitális üzenetek biztonságának biztosításáig.

Hash-funkciók, rejtjelek (cipher) és kulcscsere-algoritmusok

A kriptográfia mélyebb megértéséhez elengedhetetlen a hash-függvények, a rejtjelek és a kulcscsere-algoritmusok (Key Exchange Algorithms) mögötti fogalmak megismerése, amelyek együttesen alkotják a biztonságos kommunikáció és adatvédelem építőköveit.

A *hash-függvény* egy olyan kriptográfiai algoritmus, amely a tetszőleges hosszúságú bemeneti adatokat egy fix méretű karakterlánccá alakítja, amelyet *hash* vagy *digest* néven ismerünk. A hash-függvények legfontosabb tulajdonsága, hogy a bemeneti adatokban bekövetkező legkisebb változás is drámaian eltérő hasht eredményez, ami rendkívül érzékennyé teszi őket a változásokra. Ez a tulajdonság biztosítja az adatok integritását, mivel bármilyen módosítás könnyen felismerhető. A hash-funkciókat egyirányúnak is tervezték, ami azt jelenti, hogy a hashból számítással nem lehetséges az eredeti adatok visszafejtése.

Például a Linux forráskódjának és a különböző GNU eszközöknek az üzemeltetői biztosítják a *Secure Hash Algorithm* (SHA-256) aláírást a szoftver repositoryjaikban található fájlokra. Ez lehetővé teszi a felhasználók számára annak ellenőrzését, hogy a letöltött fájlokat nem módosították-e az átvitel során.

A *digitális aláírások* kontextusában a hash-funkciókat arra használják, hogy létrehozzák egy üzenet vagy dokumentum tömörített változatát, ez az úgynevezett *message digest*. Ezt a kivonatot ezután a feladó *privát kulcsával* (private key) titkosítják, hogy létrehozzák a digitális aláírást. A címzett úgy tudja ellenőrizni az aláírást, hogy visszafejti azt a feladó *nyilvános kulcsával* (public key), és összehasonlítja a kapott dokumentum hashével. Ha a két hash egyezik, az megerősíti, hogy a dokumentumot nem módosították, és hitelesíti a feladó identitását is. Ezt a módszert például széles körben használják az olyan biztonságos e-mail kommunikációban, mint például a *Pretty Good Privacy* (PGP) és a szoftverek terjesztésében, hogy biztosítsák a továbbított információ hitelességét és integritását.

A hash-függvények kritikus fontosságúak a jelszavak biztonságos tárolása szempontjából is. A tényleges jelszó tárolása helyett a rendszerek egy hash-funkciót használnak a jelszó egyedi hash-értékké alakítására, amelyet aztán az adatbázisban tárolnak. Amikor a felhasználó megpróbál bejelentkezni, a rendszer a beírt jelszót hasheli, majd összehasonlítja a tárolt hashhel. Ha a kettő megegyezik, a hozzáférés engedélyezésre kerül. Ez a megközelítés biztosítja, hogy még ha egy támadó hozzá is fér a jelszóadatbázishoz, ne tudja könnyen visszaszerezni az eredeti jelszavakat. A biztonság további fokozása érdekében sok rendszer a *salting* (sózás) nevű technikát alkalmazza, amikor a jelszóhoz egy véletlen értéket (a *salt*) adnak hozzá a hashelés előtt. Ez biztosítja, hogy még az azonos jelszavak is különböző hasheket eredményeznek, így a támadók számára sokkal nehezebbé válik az előre kiszámított táblázatok (*szivárványtáblák* (rainbow table)) használata a

hashek feltöréséhez.

Hogy bemutassuk a hashelést működés közben, nézzük meg az SHA-256-ot (az SHA-2 család tagja)! Ez a szabvány 256 bites hash-t eredményez, amelyet széles körben használnak olyan technológiákban, mint a blokklánc (blockchain) és a biztonságos kommunikáció. Íme egy példa:

Eredeti szöveg

`HelloWorld`

SHA-256 hash

`a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b53d83a38ac8f0287`

Ezzel szemben a régebbi hash-függvények, mint például az *MD5*, többnyire kivonásra kerültek a forgalomból, mivel jelentős biztonsági hibák miatt *ütközéses támadásokat* (collision attack) tesznek lehetővé. Az ütközéses támadás akkor következik be, amikor két különböző bemenet ugyanazt a hash-értéket generálja, ami veszélyezteti a hash egyediségét. Ez a sebezhetőség lehetővé teszi a támadók számára, hogy egy rosszindulatú fájlt vagy üzenetet észrevétlenül kicseréljenek egy legitimre, mivel mindkettő azonos hash értéket eredményez. Az ilyen gyengeségek veszélyeztetik a hash-eljárás integritását és biztonságát, így az MD5 nem alkalmas a hasheket használó feladatokra, például a fájlok integritásának ellenőrzésére, a digitális aláírásra vagy a jelszavak biztonságos tárolására a modern kriptográfiai alkalmazásokban.

Szimmetrikus és aszimmetrikus titkosítás

A kriptográfia másik központi eleme a *cipher*-ek (rejtjel), a titkosítás és a visszafejtés elvégzésére használt algoritmusok. Az egyszerű szöveget egy titkosítási kulcs (encryption key) segítségével alakítják át rejtjelezett szöveggé, és a folyamat egy visszafejtési kulcs (decryption key) segítségével visszafordítható. A kódok két fő kategóriába sorolhatók: *szimmetrikus* és *aszimmetrikus*.

Szimmetrikus cipherek

A *szimmetrikus cipherek*, mint például a széles körben használt AES (*Advanced Encryption Standard*), ugyanazt a kulcsot használják mind a titkosításhoz, mind a visszafejtéshez. Ez a megközelítés rendkívül hatékony, különösen nagy mennyiségű adat titkosítása esetén, mivel a titkosítási és visszafejtési műveletek viszonylag gyorsak és számítási szempontból olcsóak.

Az AES algoritmust különösen kedvelik erős biztonsági jellemzői és gyors teljesítménye miatt, így sok alkalmazás választja alapértelmezetten az érzékeny információk védelmére. Általánosan használják a vezeték nélküli hálózatokban az adatok védelmére olyan protokollokon keresztül, mint a WPA2 (*Wi-Fi Protected Access 2*), valamint kormányok és szervezetek is a minősített információk védelmére.

A szimmetrikus kulcscsere jellemzően egy titkos kulcs biztonságos megosztását jelenti a felek között, mielőtt kommunikálni tudnának. Mivel mind a feladó, mind a címzett ugyanazt a kulcsot használja a titkosításhoz és a visszafejtéshez, ezt a kulcsot úgy kell továbbítani, hogy az illetéktelen felek ne tudják lehallgatni.

A biztonságos kulcscsere egyik gyakori módszere a megbízható fizikai adathordozó vagy *előre megosztott kulcs* (pre-shared key — PSK) használata, ahol a kulcsot előre, manuálisan cserélik ki a felek között. A digitális kommunikációban azonban biztonságosabb és hatékonyabb módszer az aszimmetrikus titkosítás vagy a szimmetrikus kulcs létrehozásához olyan kulcscsere-protokollok használata, mint a *Diffie-Hellman*.

A Diffie-Hellman lehetővé teszi két fél számára, hogy közös titkos kulcsot hozzanak létre egy nem biztonságos csatornán, például az interneten keresztül anélkül, hogy magát a kulcsot közvetlenül továbbítanák. Ezt egy nagy prímszámokat tartalmazó matematikai eljárás segítségével érik el, amely számítási szempontból lehetetlenné teszi egy támadó számára a megosztott titkos kulcs meghatározását. Ha a megosztott titok megvan, az szimmetrikus titkosításra használható a felek közötti későbbi kommunikáció biztosítására. Ez a módszer számos modern kriptográfiai protokoll alapját képezi, és létfontosságú a biztonságos kommunikáció létrehozásához olyan környezetben, ahol a hagyományos kulcscsere-módszerek nem kivitelezhetőek.

Íme egy egyszerű példa arra, hogyan működik az AES szimmetrikus algoritmus a gyakorlatban:

Titkosítás

Input (plaintext, egyszerű szöveg): `SensitiveData`

Szimmetrikus kulcs: `mysecretkey12345`

Az AES algoritmus titkosítja az egyszerű szöveget a kulccsal, és létrehozza a kimenetet (ciphertext): `4f6a79e0f2e041b4c6d61e64a98f0d5a`

Visszafejtés

Input (ciphertext): `4f6a79e0f2e041b4c6d61e64a98f0d5a`

Szimmetrikus kulcs: `mysecretkey12345` (ugyanaz a kulcs, mint a titkosításnál)

Az AES algoritmus a kulcs segítségével visszafejti a titkosított szöveget, visszaállítva az eredeti üzenetet kimenetként (plaintext): `SensitiveData`

A szimmetrikus titkosítás esetében azonban problémát jelent a kulcsok elosztása. Mindkét félnek ugyanazt a kulcsot kell biztonságosan megszereznie. Ennek a kulcsnak a biztonságos továbbítása azonban, különösen a nem védett hálózatokon keresztül, összetett feladat. Ennek a problémának a megoldására jött létre az aszimmetrikus kriptográfia.

Aszimmetrikus cipherek

A szimmetrikus titkosítással ellentétben, amelyhez mindkét félnek ugyanazzal a kulccsal kell rendelkeznie, az aszimmetrikus titkosítás két különböző kulcsot használ: egyet a titkosításhoz (*public key*) és egyet a visszafejtéshez (*private key*).

Ez a *kulcspár* (key pair) alapvető fontosságú a biztonságos kommunikáció szempontjából, mivel lehetővé teszi, hogy bárki titkosíthasson egy üzenetet a nyilvános kulcs segítségével, de csak a privát kulcs tulajdonosa tudja visszafejteni azt. Ez a megközelítés hatékonyan megoldja a nem védett csatornán történő biztonságos kulcscsere kihívását, így a biztonságos kulcscsere és a digitális aláírás alapvető eszköze.

Az RSA (*Rivest-Shamir-Adleman*) az aszimmetrikus titkosítás egyik kiemelkedő példája, amelyet gyakran használnak digitális tanúsítványokban és biztonságos e-mail kommunikációban, hogy biztosítsák az adatok védett cseréjét a kulcs előzetes megosztása nélkül.

Az RSA a nagy számok számítási nehézségeire támaszkodik, ami rendkívül biztonságossá, és alkalmassá teszi különböző alkalmazásokhoz, beleértve a PGP (Pretty Good Privacy) biztonságos e-mail kommunikációt és a felhasználói hitelesítést az SSH-ban (*Secure Shell*).

Az aszimmetrikus kriptográfia egyik kihívása annak ellenőrzése, hogy a nyilvános kulcs valóban a címzetté. Ezen ellenőrzés nélkül egy támadó elfoghatná és kicserélhetné a nyilvános kulcsot a sajátjával, ami *man-in-the-middle támadáshoz* vezetne.

Ennek megakadályozására létezik egy *Public Key Infrastructure* (PKI) rendszer, amely keretet biztosít a nyilvános kulcsok hitelesítésére a megbízható *Certificate Authorities* (hitelesítésszolgáltatók, CA-k) által kibocsátott digitális tanúsítványok segítségével. Ez biztosítja, hogy a nyilvános kulcsok legitimek és nem manipuláltak, lehetővé téve a biztonságos és megbízható kommunikációt a hálózatokon keresztül.

Az RSA mellett más aszimmetrikus algoritmusok, például az *Elliptic Curve Diffie-Hellman* (ECDH) is hasonló biztonságot nyújtanak, de kisebb kulcsmérettel, ami hatékonyabbá teszi őket a korlátozott feldolgozási teljesítményű eszközök, például okostelefonok számára. Az ECDH az elliptikus görbék matematikáját használja a biztonságos kulcscserék megkönnyítésére, és a hagyományos RSA-hoz képest kisebb számítási ráfordítással nyújt robusztus biztonságot.

Hibrid kriptográfia

A *hibrid kriptográfia* hatékonyan ötvözi a szimmetrikus és az aszimmetrikus titkosítás erősségeit a biztonságos és hatékony kommunikáció elérése érdekében. Így a hibrid kriptográfia kihasználja mindkettő előnyeit. A hibrid titkosítás tipikus alkalmazása megtalálható az olyan széles körben elterjedt protokollokban, mint a *Secure Sockets Layer/Transport Layer Security* (SSL/TLS), amelyek

az interneten keresztül biztosítják az adatátvitelt.

A hibrid kriptográfia kiváló választás, mert a szimmetrikus és az aszimmetrikus titkosítási módszerek erősségeit egyesítve robusztus és hatékony adatvédelmi rendszert hoz létre. A szimmetrikus titkosítás, például az AES, rendkívül hatékony és gyors, így ideális nagy mennyiségű adat titkosítására. Kevesebb számítási teljesítményt igényel, mint az aszimmetrikus titkosítás. Ez a hatékonyság alapvető fontosságú a nagy sebességű adatátvitelt igénylő alkalmazások, például a videostreaming vagy a nagyméretű fájlmegosztás esetében. Másrészt az aszimmetrikus titkosítás, mint például az RSA, számításigényesebb, de biztonságos módszert kínál a nem megbízható hálózatokon történő kulcscseréhez.

A hibrid kriptográfiában az aszimmetrikus titkosítást a szimmetrikus kulcs biztonságos továbbítására használják, amelyet aztán a tényleges adattitkosításhoz használnak. Ez a stratégia kihasználja mindkét módszer legjobb tulajdonságait: az aszimmetrikus titkosítás robusztus biztonságát a kulcscseréhez, valamint a szimmetrikus titkosítás nagy teljesítményét az adatátvitelhez.

Így működik: A kommunikáció kezdeti fázisában a feladó létrehoz egy *ideiglenes szimmetrikus kulcsot*, az úgynevezett *munkamenet kulcsot* (session key) a tényleges adatok titkosításához. Ezt a kulcsot a címzett nyilvános kulcsával titkosítja, és a titkosított adatokkal együtt elküldi. Az üzenet kézhezvételekor a címzett a saját privát kulcsával visszafejti a munkamenet kulcsot, majd a visszafejtett szimmetrikus kulcsot használja az adatok visszafejtéséhez. Ez az eljárás biztosítja, hogy az adatok tényleges titkosítása és visszafejtése hatékony legyen, miközben a kulcscsere biztonságos marad.

Például egy biztonságos weboldal HTTPS-en keresztüli meglátogatásakor a felhasználó böngészője és a szerver Diffie-Hellman kulcscserét hajt végre egy közös szimmetrikus kulcs létrehozásához, amelyet aztán a munkamenet során kicserélt összes adat titkosítására használnak. Ez biztosítja, hogy még ha egy támadó le is hallgatja a kommunikációt, a szimmetrikus kulcs nélkül nem tudja elolvasni a titkosított tartalmat, amelyet nem tud kinyerni a lehallgatott adatokból.

A hibrid kriptográfia a modern biztonságos kommunikáció egyik sarokköve. Védett adatátvitelt tesz lehetővé az online banki és elektronikus kereskedelemtől kezdve a biztonságos e-mail és VPN-kapcsolatokig. A két titkosítási típus legjobb aspektusainak kombinálásával a hibrid kriptográfia robusztus keretet biztosít az adatok szállítás közbeni védelméhez, biztosítva a teljesítményt és a biztonságot a különböző digitális környezetekben.

Perfect Forward Secrecy (PFS)

A cipherek döntő szerepet játszanak a digitális kommunikáció védelmében, mivel az adatok titkosításával megakadályozzák a jogosulatlan hozzáférést. Azonban még a legbiztonságosabb

kódok is sebezhetőek lehetnek, ha egy támadó hozzáfér a titkosításhoz használt hosszú távú kulcsokhoz. Itt lép képbe a *Perfect Forward Secrecy* (PFS).

A kriptográfia egyik alapelve annak biztosítása, hogy a múltbeli kommunikáció még akkor is biztonságos maradjon, ha a hosszú távú titkosítási kulcs veszélybe kerül. A PFS garantálja, hogy minden egyes kommunikációs munkamenethez *egyedi titkosítási kulcsot* generálnak, és a munkamenet befejezése után eldobják.

Ez azt jelenti, hogy még ha egy támadónak sikerül is megszereznie a kommunikációhoz használt privát kulcsot, a korábbi munkameneteket nem tudja visszafejteni, mivel a munkamenet-specifikus kulcsok már nem állnak rendelkezésre. Ez a megközelítés megakadályozza az adatok visszamenőleges visszafejtését, és védi a korábbi kommunikáció integritását.

A PFS különösen fontos olyan környezetekben, ahol gyakran cserélnek érzékeny információkat, például webes alkalmazásokban, e-mail szolgáltatásokban és VPN-ek esetén. A PFS bevezetésével a szervezetek biztosíthatják, hogy a múltbeli adatok még egy jövőbeli biztonsági rés esetén is biztonságban maradjanak. Ez növeli az általános biztonságot azáltal, hogy nemcsak a jelenlegi, hanem a múltbeli kommunikációt is védi, így szilárd védelmet nyújt a potenciális fenyegetésekkel szemben.

Az olyan kriptográfiai protokollok, mint a Diffie-Hellman (DH) és az Elliptic Curve Diffie-Hellman (ECDH) alapvető fontosságúak a PFS eléréséhez, mivel ezek efemer munkamenetkulcsokat generálnak, amelyeket csak egyszer használnak, majd eldobják őket. Ezek az algoritmusok biztosítják, hogy minden egyes kommunikációs munkamenet egyedi kulccsal rendelkezik, így a korábbi munkamenetek visszafejtése még akkor is lehetetlenné válik, ha a hosszú távú privát kulcs veszélybe kerül.

Ez az elv szerves részét képezi a modern biztonságos kommunikációs protokolloknak, például a TLS-nek, amelyek a PFS-re támaszkodnak az adatok áramlása közbeni védelmében és az internetes kommunikáció titkosságának fenntartásában.

End-to-End titkosítás vs. szállítási titkosítás

Ahogy tovább vizsgáljuk a kriptográfiai megoldásokat, fontos különbséget tenni az adatok védelmére széles körben használt két megközelítés között, amelyek alkalmazási körükben és megvalósításukban különböznek egymástól.

Az *End-to-end titkosítás* (végponttól végpontig, E2EE) biztosítja, hogy az adatok titkosítása már a forrásuknál megtörténjen, és az egész útjuk során titkosítva maradjanak, amíg el nem érik a címzettet. Csak a feladó és a címzett rendelkezik az adatok titkosításához és visszafejtéséhez szükséges kulcsokkal, így az E2EE ideális a privát kommunikációhoz. A közvetítők, például a

szolgáltatók vagy szerverek nem férnek hozzá a titkosítatlan adatokhoz. Az olyan üzenetküldő alkalmazások, mint a WhatsApp, az E2EE-t használják a felhasználók adatainak védelmére.

Az E2EE fő erőssége, hogy teljes titoktartást biztosít, mivel harmadik fél nem tudja visszafejteni az adatokat. A megvalósítása azonban összetettebb, mivel a titkosítási kulcsok gondos kezelését igényli annak biztosítása érdekében, hogy csak a címzett férhessen hozzá az adatokhoz.

A *szállítási titkosítás* (transport encryption) ezzel szemben csak akkor titkosítja az adatokat, amikor azokat két pont között továbbítják, például a felhasználó eszköze és egy szerver között. Amint az adatok elérik a szervert, visszafejtésre kerülnek, és eredeti formájukban tárolhatók vagy feldolgozhatók. A HTTPS-ben használt TLS protokoll a szállítási titkosítás egyik példája.

A szállítási titkosítás egyszerűbben megvalósítható, mint az E2EE, és elegendő védelmet nyújt az adatok szállítás közbeni védelméhez. Azonban amint az adatokat a szerveren tárolják vagy feldolgozzák, azok kiszolgáltatottá, és potenciálisan sebezhetővé válnak a belső vagy külső fenyegetésekkel szemben.

Gyakorló feladatok

1. Mi a különbség a szimmetrikus és az aszimmetrikus kriptográfia között?

2. Hogyan növeli a Perfect Forward Secrecy (PFS) a kommunikációs protokollok, például az SSL/TLS biztonságát?

3. Milyen szerepet játszanak a hash-függvények az adatok integritásának ellenőrzésében? Adjunk példát egy olyan forgatókönyvre, ahol ez kulcsfontosságú!

Gondolkodtató feladatok

1. Vizsgáljuk meg és magyarázzuk el, hogyan valósul meg a hibrid kriptográfia a biztonságos webböngészésben a HTTPS protokollon keresztül!

2. Vizsgáljuk meg a kvantumszámítástechnika koncepcióját, valamint azt, hogy az hogyan jelent veszélyt a jelenlegi kriptográfiai rendszerekre, különösen az olyan aszimmetrikus titkosításokra, mint az RSA!

Összefoglalás

A kriptográfia döntő szerepet játszik a digitális információk védelmében; az adatok és a kommunikáció biztonsága érdekében olyan titkosítási technikákat alkalmaz, mint a szimmetrikus és aszimmetrikus chiperek. A szimmetrikus titkosítás, mint például az AES, nagy adatmennyiségek esetén rendkívül hatékony, de a kulcsok elosztásához biztonságos módszerre van szükség. Az aszimmetrikus titkosítás, mint például az RSA, ezt a kihívást úgy oldja meg, hogy a biztonságos kulcscseréhez nyilvános és privát kulcspárokat használ, igaz számításigényesebb módon. A hash-függvények emellett azzal fokozzák a biztonságot, hogy az adatok integritását egyedi, rögzített méretű kimenetek létrehozásával ellenőrzik, így biztosítva, hogy az adatok bármilyen módosítása könnyen felderíthető legyen.

Ez a lecke a hibrid kriptográfiával is foglalkozik, amely a szimmetrikus és az aszimmetrikus titkosítás erősségeit ötvözi. A hibrid megközelítések, például az SSL/TLS protokollokban használtak, kihasználják a szimmetrikus titkosítás sebességét az adatátvitelhez, valamint az aszimmetrikus titkosítás biztonságos kulcscsere képességeit. A Perfect Forward Secrecy (PFS) továbbá a biztonság egy további szintjét növeli azáltal, hogy minden egyes kommunikációs munkamenethez egyedi, efemer kulcsokat generál, biztosítva, hogy a múltbeli kommunikáció még akkor is védett maradjon, ha a hosszú távú titkosítási kulcsok veszélybe kerülnek. Ezek a kriptográfiai technikák együttesen szilárd védelmet nyújtanak az érzékeny adatok számára, és alapvető fontosságúak a biztonságos digitális kommunikációhoz olyan alkalmazásokban, mint az online bankolás, a VPN-ek és a biztonságos webböngészés.

Válaszok a gyakorló feladatokra

1. Mi a különbség a szimmetrikus és az aszimmetrikus kriptográfia között?

   A szimmetrikus kriptográfia ugyanazt a kulcsot használja mind a titkosításhoz, mind a visszafejtéshez, hatékonnyá téve azt, de a kulcs biztonságos elosztása kihívást jelent. Az aszimmetrikus kriptográfia kulcspárokat használ — egy nyilvános és egy privát kulcsot --, ahol a nyilvános kulcs titkosítja az adatokat, és csak a megfelelő privát kulcs képes visszafejteni azokat. Ez kiküszöböli a titkos kulcs megosztásának szükségességét, de számításigényesebb.

2. Hogyan növeli a Perfect Forward Secrecy (PFS) a kommunikációs protokollok, például az SSL/TLS biztonságát?

   A Perfect Forward Secrecy biztosítja, hogy minden egyes kommunikációs munkamenetnek egyedi, efemer titkosítási kulcsa van, amely a munkamenet befejezése után elvetésre kerül. Ez azt jelenti, hogy még ha a hosszú távú privát kulcs kompromittálódik is, a múltbeli kommunikációt nem lehet visszafejteni. Az olyan protokollokban, mint az SSL/TLS, a PFS olyan algoritmusokat használ, mint például a Diffie-Hellman, hogy létrehozza ezeket az ideiglenes kulcsokat, megvédve az adatok titkosságát és fokozott biztonságot nyújtva az internetes kommunikáció számára.

3. Milyen szerepet játszanak a hash-függvények az adatok integritásának ellenőrzésében? Adjunk példát egy olyan forgatókönyvre, ahol ez kulcsfontosságú!

   A hash-függvények egyedi, rögzített méretű hasht generálnak egy bemenetből, amely drasztikusan megváltozik még a bemenet apró módosításakor is. Ez a tulajdonságuk ideális az adatok sértetlenségének ellenőrzésére, mivel az adatok bármilyen módosítása más hash-értéket eredményez. A hashek használatára az egyik legfontosabb példa a szoftverletöltések ellenőrzése. A Linux és GNU eszközök üzemeltetői gyakran megadnak egy hasht (például SHA-256) a fájljaikhoz, így a felhasználók ellenőrizhetik, hogy a fájlokat nem módosították-e az átvitel során. Ha a letöltött fájl hash-e megegyezik a megadott hash-sel, akkor a fájl sértetlen és változatlan.

Válaszok a gondolkodtató feladatokra

1. Vizsgáljuk meg és magyarázzuk el, hogyan valósul meg a hibrid kriptográfia a biztonságos webböngészésben a HTTPS protokollon keresztül!

   A HTTPS-ben a hibrid kriptográfia aszimmetrikus titkosítás, jellemzően RSA használatával valósul meg, hogy biztonságosan kicserélje a szimmetrikus munkamenetkulcsot a kliens és a szerver között. Ezt a munkamenetkulcsot ezután az összes későbbi adatátvitel titkosítására használják szimmetrikus titkosítással, például AES használatával. Az aszimmetrikus titkosítás használata még egy nem megbízható hálózaton is biztosítja, hogy a munkamenetkulcs cseréje biztonságosan történik, míg a szimmetrikus titkosítás gyors és hatékony adattitkosítást biztosít a tényleges kommunikációhoz. Ez a kombináció egyszerre nyújt biztonságot és teljesítményt, így ideális a biztonságos webböngészéshez.

2. Vizsgáljuk meg a kvantumszámítástechnika koncepcióját, valamint azt, hogy az hogyan jelent veszélyt a jelenlegi kriptográfiai rendszerekre, különösen az olyan aszimmetrikus titkosításokra, mint az RSA!

   A kvantumszámítás, amely a klasszikus számítógépeknél exponenciálisan gyorsabb komplex számítások elvégzésére képes, jelentős fenyegetést jelent a jelenlegi kriptográfiai rendszerekre, különösen az olyan aszimmetrikus titkosítási módszerekre, mint az RSA és az ECC. Az RSA különösen a nagy prímszámok faktorálásának nehézségén alapul, amit a kvantumszámítógépek a Shor algoritmus segítségével hatékonyan meg tudnának oldani. Ez lehetővé tenné, hogy a kvantumszámítógépek feltörjék az RSA titkosítást, és ezzel védtelenné tennék azt.

   E kihívások kezelésére a kutatók kvantumrezisztens algoritmusokat fejlesztenek ki, amelyeket úgy terveztek, hogy ellenálljanak a kvantumszámítógépek támadásainak. A kvantumrezisztens algoritmusok elengedhetetlenek ahhoz, hogy a jövőbeni titkosítási módszerek a kvantumszámítógépek fejlődésével együtt is biztonságosak maradjanak. Ezek az algoritmusok segítenek majd megvédeni az érzékeny kommunikációt, a pénzügyi tranzakciókat és a kormányzati adatokat a kvantumos dekódolási képességek potenciális fenyegetésével szemben.

Lecke 2

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	022 Titkosítás
Fejezet:	022.1 Kriptográfia és nyilvános kulcsú infrastruktúra
Lecke:	2/2

Bevezetés

A kriptográfiai alapelvekre épülő *Public Key Infrastructure (PKI)* a biztonságos kommunikáció és az identitás ellenőrzése szempontjából alapvető fontosságú a digitális világban. A PKI keretet hoz létre a *nyilvános* és *privát* kulcsok titkosításban való használatához, biztosítva, hogy a kommunikációban részt vevő entitások megbízhassanak egymásban.

A PKI középpontjában a *digitális tanúsítványok* állnak, amelyek egy nyilvános kulcsot egy entitáshoz, például egy személyhez vagy szervezethez kapcsolnak, és amelyeket a *Certificate Authority*-k (hitelesítésszolgáltatók, CA-k) kezelnek. Ezek a tanúsítványok döntő szerepet játszanak az adatok titkosításában és az identitások érvényesítésében, ami nélkülözhetetlenné teszi a PKI-t a biztonságos webböngészéshez, az e-mail kommunikációhoz és más online tevékenységekhez. A megbízható *Root Certificate Authority*-k (Root CA-k) alkotják a bizalmi modell legfelső szintjét, létrehozva a végfelhasználói tanúsítványokig terjedő bizalmi láncot.

Ez a strukturált kapcsolat biztosítja, hogy a felhasználók és a rendszerek megbízhatnak a digitális tanúsítványok hitelességében. A PKI és a CA-k működésének megértése alapvető fontosságú a biztonságos információcsere és a digitális tanúsítványok szerepének átlátásához az online

kommunikáció integritásának és biztonságának fenntartásában.

Public Key Infrastructure (PKI)

A *Public Key Infrastructure* (PKI) kulcsfontosságú a bizalom megteremtésében és a digitális kommunikáció biztosításában. Alapvetően a PKI strukturált keretet biztosít a digitális tanúsítványok és a publikus-privát kulcspárok kezeléséhez, amelyek elengedhetetlenek az identitások ellenőrzéséhez és az internetes adatcsere biztosításához. Amikor két entitásnak, például egy felhasználónak és egy weboldalnak biztonságosan kell kommunikálnia egymással, a PKI biztosítja, hogy mindkét fél biztos lehet a másik fél identitásában és a megosztott adatok sértetlenségében.

A PKI a nyilvános és a privát kulcspárok kezelésével lehetővé teszi a biztonságos kommunikációt. Az olyan entitások, mint például webhelyek, szerverek vagy magánszemélyek *digitális tanúsítványt* kapnak, amely identitásukat egy nyilvános kulcshoz köti.

A digitális tanúsítványok elektronikus "útlevélként" szolgálnak egy entitás számára — legyen az személy, eszköz vagy szolgáltatás. Ezt a tanúsítványt egy megbízható harmadik fél, az úgynevezett *Certificate Authority* (CA) állítja ki.

A tanúsítvány kiállítása előtt a CA alapos ellenőrzési folyamatot végez az entitás identitásának jogszerűségének megerősítése érdekében. Ez a folyamat megakadályozza, hogy a kártékony szereplők hamisan másnak adják ki magukat. A tanúsítvány kiadása után a tanúsítványt az entitás nyilvános kulcsával lehet használni az adatok titkosítására. Az adatokat csak a megfelelő, az entitás által biztonságosan tárolt privát kulcs tudja visszafejteni, így biztosítva, hogy az érzékeny információk bizalmasak és csak a címzett számára hozzáférhetőek maradnak.

CA-k és Trusted Root CA-k

A PKI középpontjában a Certificate Authority-k és a *Trusted Root Certificate Authority*-k állnak, amelyek a webböngészésben, a biztonságos e-mailben és más alkalmazásokban használt digitális tanúsítványok biztonságát alátámasztó *bizalmi lánc* (chain of trust) gerincét alkotják.

A CA-k kritikus szerepet játszanak a PKI-ban a digitális tanúsítványok kiadásával, érvényesítésével és kezelésével. A kiállítást követően a CA tekintélyére támaszkodó más felhasználók vagy rendszerek megbízhatnak a tanúsítványban.

A root CA-k alkotják a PKI bizalmi hierarchiájának csúcsát. A root CA-k tanúsítványokat állítanak ki a *közvetítő CA-k* (intermediate CA) részére, létrehozva egy bizalmi láncot, amely a végfelhasználói tanúsítványokig terjed. A root tanúsítványok előre telepítve vannak az operációs rendszerekben és a webböngészőkben, és a hierarchiában kiadott összes tanúsítvány alapját

képezik.

Ez a bizalmi lánc alapvető fontosságú, hiszen hierarchikus kapcsolatot hoz létre a root CA-k, a köztes CA-k és az általuk kiállított tanúsítványok között. A láncban minden egyes tanúsítványt a felette lévő CA hitelesít, ami végül egy trusted (megbízható) Root CA-hoz vezet vissza. Ez a hierarchikus modell biztosítja, hogy a felhasználók és a rendszerek megbízhatnak a digitális interakciók során felmerülő tanúsítványokban.

Példa a bizalmi láncra

Íme egy példa egy bizalmi láncra, amely egy Root CA-t, egy köztes CA-t és végfelhasználói tanúsítványokat (end-entity certificate) foglal magában.

Root CA tanúsítvány

A Root CA a legfelsőbb hatóság a láncban, és minden rendszer megbízik benne. Önaláíró, ami azt jelenti, hogy saját maga hitelesíti a saját identitását.

```
- Root CA Name: "GlobalTrust Root CA"
  - Subject: "CN=GlobalTrust Root CA, O=GlobalTrust Inc., C=US"
  - Issuer: "CN=GlobalTrust Root CA, O=GlobalTrust Inc., C=US" (Self-signed)
  - Public Key: Contains the public key of GlobalTrust Root CA
  - Validity Period: 20 years (e.g., 2020-2040)
  - Signature: Self-signed using the Root CA's private key
```

A Root CA tanúsítvány a legtöbb operációs rendszerben és böngészőben előre telepítve van, így megbízható hatóságként van azonosítva.

Köztes CA tanúsítvány

A közbenső CA számára a Root CA állít ki tanúsítványt. Ez a CA hídként működik a Root CA és a végfelhasználók között, lehetővé téve a jobb biztonsági menedzsmentet és a bizalom megosztását.

```
- Intermediate CA Name: "GlobalTrust Intermediate CA 1"
  - Subject: "CN=GlobalTrust Intermediate CA 1, O=GlobalTrust Inc., C=US"
  - Issuer: "CN=GlobalTrust Root CA, O=GlobalTrust Inc., C=US" (Signed by Root CA)
  - Public Key: Contains the public key of GlobalTrust Intermediate CA 1
  - Validity Period: 10 years (e.g., 2022-2032)
  - Signature: Signed using the Root CA's private key
```

A köztes CA tanúsítványokat állít ki a végfelhasználók, például weboldalak vagy alkalmazások számára, miután hitelesítette azok identitását.

Végfelhasználói tanúsítvány (weboldal vagy alkalmazás)

A végfelhasználói tanúsítványt a köztes CA állítja ki egy weboldal vagy alkalmazás számára. Ezt látja a végfelhasználó, amikor csatlakozik egy biztonságos weboldalhoz.

```
- End-Entity Name: "example.com"
  - Subject: "CN=example.com, O=Example Inc., C=US"
  - Issuer: "CN=GlobalTrust Intermediate CA 1, O=GlobalTrust Inc., C=US" (Signed by
Intermediate CA)
  - Public Key: Contains the public key of example.com
  - Validity Period: 1 year (e.g., 2023-2024)
  - Signature: Signed using the Intermediate CA's private key
```

Ebben a példában a láncban minden egyes tanúsítványt a felette lévő tanúsítvány ellenőriz, visszavezetve végül egy trusted Root CA-hoz, amely biztosítja a digitális kommunikáció integritását és biztonságát: (A bizalmi lánc vizuális reprezentációja).

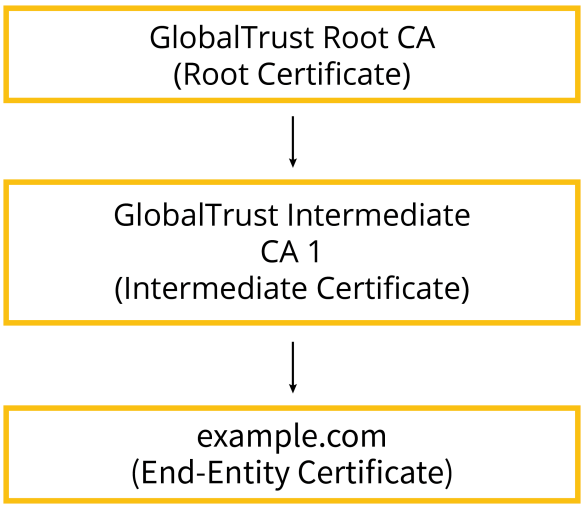

Figure 2. A bizalmi lánc vizuális reprezentációja

Amikor egy felhasználó meglátogatja a *example.com* weboldalt, a böngészője megkapja ezt a tanúsítványt. A böngésző ezután a bizalmi láncot követve ellenőrzi a tanúsítvány érvényességét:

1. Végfelhasználói tanúsítvány ellenőrzése

   A böngésző megerősíti, hogy az *example.com* tanúsítványát a `GlobalTrust Intermediate CA`

`1` írta alá.

2. Köztes CA tanúsítvány ellenőrzése

   A böngésző ellenőrzi, hogy a `GlobalTrust Intermediate CA 1` tanúsítványt a `GlobalTrust Root CA` írta alá.

3. Root CA ellenőrzése

   A böngésző megerősíti, hogy a Root CA egy előre telepített megbízható hatóság a saját trust store-ban.

Ha a láncban lévő összes tanúsítvány érvényes és megfelelően aláírt, a böngésző biztonságos kapcsolatot hoz létre a *example.com* címmel, és a felhasználó biztonságosan kapcsolatba léphet a weboldallal.

X.509 tanúsítványok

Az *X.509 tanúsítványok* a nyilvános kulcsú infrastruktúrában (PKI) használt szabványos digitális tanúsítványformátumok, amelyek elengedhetetlenek a biztonságos kommunikációban részt vevő entitás identitásának ellenőrzéséhez. Gyakran “digitális útlevélként” is emlegetik ezeket a tanúsítványokat, amelyek megbízható kapcsolatot hoznak létre egy entitás identitása és nyilvános kulcsa között egy megbízható Certificate Authority (CA) általi tanúsítás révén.

Minden X.509 tanúsítvány tartalmaz olyan mezőket, amelyek részletezik az entitás nyilvános kulcsát, a kiállító CA nevét és olyan egyedi azonosító információkat, mint például az entitás domainneve vagy a szervezet neve. Ez a szabványosított formátum biztosítja, hogy az X.509 tanúsítványok a digitális alkalmazások széles körében egységes és megbízható módszert biztosítanak a szervezetek hitelesítésére.

Az X.509 tanúsítványok szerepének megértése alapvető fontosságú, mivel ezeket a tanúsítványokat számos alkalmazásban használják a védett kapcsolatok megkönnyítésére, beleértve a biztonságos webböngészéshez használt HTTPS-t, az adattitkosításhoz használt SSL/TLS-t, valamint az elektronikus dokumentumok hitelességének és integritásának ellenőrzéséhez használt digitális aláírásokat.

A tanúsítvány tartalmaz egy *digitális aláírást*, amelyet a CA a saját privát kulcsának felhasználásával állít elő, és amely a nyilvános kulcsot az entitás identitásához köti. Ezt a digitális aláírást bárki ellenőrizheti a CA nyilvános kulcsát használva, így biztosítva, hogy a tanúsítványt nem hamisították meg, és hogy az valóban a megbízható CA-tól származik.

Az X.509 tanúsítványok struktúrája

Az X.509 tanúsítvány számos mezőt tartalmaz, amelyek részletes információkat szolgáltatnak az entitásról és magáról a tanúsítványról. Ezek közé tartozik a *subject*, amely a tanúsítványt kiállító entitást azonosítja, valamint az *issuer*, amely a tanúsítványt kiállító CA-t azonosítja. A tanúsítvány tartalmazza továbbá az entitáshoz tartozó *publikus kulcsot* (public key), valamint a CA *digitális aláírását* (digital signature), amely a tanúsítvány hitelességét igazolja.

A tanúsítvány tartalmaz egy *érvényességi időszakot* (validity period) is, amely azt az időtartamot jelzi, mialatt a tanúsítvány érvényesnek tekinthető. Ezen időszak után a tanúsítványt meg kell újítani vagy le kell cserélni a biztonságos kommunikáció fenntartásához. Ezeken a mezőkön kívül az X.509 tanúsítványok tartalmazhatnak *bővítményeket* (extension), amelyek meghatározzák a tanúsítvány rendeltetését, például a szerver hitelesítésére vagy az e-mail titkosítására.

X.509 tanúsítványok kérése és kiadása

Az X.509 tanúsítvány megszerzésének folyamata a *Certificate Signing Request* (tanúsítványaláírási kérelem — CSR) létrehozásával kezdődik. A CSR egy olyan fájl, amely tartalmazza az entitás nyilvános kulcsát, valamint azonosító információkat, például az entitás domainnevét, organizációját és székhelyét. Ezek az információk segítenek a tanúsítványt igénylő szervezet egyedi azonosításában. A CSR-t ezután benyújtják a CA-hoz érvényesítésre.

A CA kritikus szerepet játszik a CSR-ben megadott információk jogszerűségének ellenőrzésében. Ez az érvényesítési folyamat a kért tanúsítvány típusától függően különböző szigorúságú lehet. A *Domain Validated* (DV) tanúsítvány például megköveteli, hogy a CA ellenőrizze, hogy az entitás kontrollálja-e a megadott domaint, jellemzően egy egyszerű e-mail vagy DNS-ellenőrzési folyamat révén. A szigorúbb tanúsítványok, például az *Organization Validated* (OV) vagy *Extended Validation* (EV) tanúsítványok esetében a CA további ellenőrzéseket végez, például ellenőrzi a szervezet jogi létezését és fizikai elhelyezkedését.

Miután a CA sikeresen ellenőrizte a szervezet adatait, a CA privát kulcsával digitálisan aláírva kiállítja az X.509 tanúsítványt. Ez a digitális aláírás biztosítja a tanúsítvány hitelességét és sértetlenségét, így a tanúsítványt minden olyan szervezet megbízhatónak ismeri el, amely a CA-t megbízható hatóságként ismeri el. A kiállított tanúsítványt ezután visszaküldik a kérelmező szervezetnek, ahol az telepíthető egy szerverre vagy eszközre.

A telepítés után az X.509 tanúsítványt az SSL/TLS titkosítás engedélyezésével biztonságos kommunikáció létrehozására használják. Amikor egy kliens (pl. egy webböngésző) csatlakozik a szerverhez, a szerver prezentálja a tanúsítványt. A kliens ezután ellenőrzi a tanúsítvány hitelességét a CA aláírásának a trusted root tanúsítványok listáján történő ellenőrzésével. Ha az ellenőrzés sikeres, titkosított kommunikációs csatorna jön létre, amely biztosítja, hogy a kliens és

a szerver között kicserélt adatok bizalmasak és védettek maradnak a lehallgatástól.

X.509 tanúsítványok SSL/TLS-ben

Az X.509 tanúsítványok központi szerepet játszanak az SSL/TLS protokollban, amelyet a kliensek és szerverek közötti kommunikáció biztosítására használnak az interneten keresztül. Az alábbiakban lépésről lépésre bemutatunk egy példát a tanúsítványaláírási kérelem (CSR) létrehozására egy domain számára az OpenSSL, egy széles körben használt kriptográfiai könyvtár segítségével.

Amikor egy felhasználó csatlakozik egy biztonságos weboldalhoz, a szerver az SSL/TLS kézfogás részeként bemutatja X.509 tanúsítványát a felhasználó böngészőjének. A böngésző ezután ellenőrzi a tanúsítvány hitelességét a trusted root CA-ig visszavezetett bizalmi lánc ellenőrzésével. Ha a tanúsítvány érvényes és megbízható, a böngésző folytatja az SSL/TLS kézfogást, és titkosított kapcsolatot hoz létre a felhasználó és a szerver között.

Az X.509 tanúsítványokat más alkalmazásokban is használják, például e-mail titkosításra és digitális aláírásra, a feladó identitásának ellenőrzésére és az üzenet integritásának biztosítására.

Let’s Encrypt

A világon több tucat CA létezik, amelyek többsége fizetős tanúsítványkiállítási szolgáltatásokat kínál. A jól ismert CA-k közé tartozik a *Let’s Encrypt*, amely ingyenes, automatizált SSL/TLS tanúsítványokat biztosít, és elősegíti a HTTPS széles körű elterjedését.

A Let’s Encrypt ingyenes, automatizált SSL/TLS tanúsítványok biztosításával átalakította az X.509 tanúsítványok beszerzésének és kezelésének folyamatát. Ez a kezdeményezés elősegíti a HTTPS széles körű elterjedését, és a titkosítás akadályainak csökkentésével biztonságosabbá teszi az internetet.

A Let’s Encrypt előtt az SSL/TLS tanúsítványok beszerzése gyakran költséges és technikailag összetett folyamat volt. A Let’s Encrypt a tanúsítványok kiállításának és megújításának automatizálásával egyszerűsíti ezt a folyamatot, lehetővé téve a webhelyek számára, hogy egyszerűen és ingyenesen tegyék biztonságossá kommunikációjukat.

A Let’s Encrypt jelentős szerepet játszott a HTTPS elterjedésében, javítva a biztonságot és az adatvédelmet a világhálón. Fontos azonban megjegyezni, hogy a Let’s Encrypt Domain Validated (DV) tanúsítványokat állít ki, amelyek igazolják a domain tulajdonjogát, de nem nyújtanak olyan szintű biztosítékot, mint az Organization Validated (OV) vagy Extended Validation (EV) tanúsítványok.

A Let’s Encrypt tanúsítványok csak 90 napig érvényesek. Ez a rövid érvényességi idő biztosítja a

tanúsítványok rendszeres frissítését, ami kompromittálódás esetén csökkenti a visszaélések kockázatát. A Let's Encrypt tanúsítványok rövid élettartama miatt az automatikus megújítás elengedhetetlen a biztonság fenntartásához.

Gyakorló feladatok

1. Hogyan biztosítja a bizalmat a digitális kommunikációban a Public Key Infrastructure (PKI)?

2. Mi a szerepe az X.509 tanúsítványoknak SSL/TLS protokollok esetén?

3. Magyarázzuk el a bizalmi lánc fogalmát a PKI-ban! Miért fontos a bizalmi lánc a biztonságos kommunikáció létrehozásához, és hogyan biztosítja a digitális tanúsítványok megbízhatóságát? n+

Gondolkodtató feladatok

1. Vizsgáljuk meg az Extended Validation (EV) tanúsítványok szerepét a webes biztonságban, és magyarázzuk el, miben különböznek a Domain Validated (DV) és az Organization Validated (OV) tanúsítványoktól!

2. Generáljunk CSR-t a *www.example.com* domainhez az OpenSSL használatával! Adjuk meg a használt parancsot, és magyarázzuk el a parancs egyes részeit!

Összefoglalás

Ez a lecke a nyilvános kulcsú infrastruktúrát (Public Key Infrastructre — PKI) vizsgálja meg, elmélyedve a hitelesítésszolgáltatók (Certificate Authorithies — CA-k), az X.509 tanúsítványok és a biztonságos digitális kommunikáció alapjául szolgáló bizalmi lánc szerepében. Ezen kívül tárgyalja a Let's Encrypt megjelenését és annak hatását a HTTPS széles körű elterjedésére.

Válaszok a gyakorló feladatokra

1. Hogyan biztosítja a bizalmat a digitális kommunikációban a Public Key Infrastructure (PKI)?

   A PKI a bizalmat egy bizalmi láncon keresztül hozza létre, amelyben hitelesítésszolgáltatók (CA-k) vesznek részt. A CA-k digitális tanúsítványokat állítanak ki, amelyek összekapcsolják egy entitás publikus kulcsát annak ellenőrzött identitásával. A böngészők és operációs rendszerek által megbízhatónak tartott root CA-k rögzítik a bizalmi láncot, és érvényesítik a köztes CA-k által kiadott tanúsítványokat. Ez a hierarchikus struktúra a digitális tanúsítványok hitelességének ellenőrzésével biztosítja a biztonságos kommunikációt.

2. Mi a szerepe az X.509 tanúsítványoknak SSL/TLS protokollok esetén?

   Az X.509 tanúsítványokat az SSL/TLS protokollok használják a szerverek identitásának hitelesítésére és a biztonságos kommunikáció létrehozására. Az SSL/TLS kézfogás során a szerver bemutatja X.509-es tanúsítványát a kliensnek, aki a bizalmi láncon keresztül ellenőrzi a tanúsítvány hitelességét. Ha a tanúsítvány érvényes, a kézfogás folytatódik, és létrejön a titkosított kapcsolat.

3. Magyarázzuk el a bizalmi lánc fogalmát a PKI-ban! Miért fontos a bizalmi lánc a biztonságos kommunikáció létrehozásához, és hogyan biztosítja a digitális tanúsítványok megbízhatóságát?

   A bizalmi lánc a PKI-ban a a Root Certificate Authority (Root CA), az intermediate Certificate Authority-k (CA-k) és a végfelhasználói tanúsítványok közötti hierarchikus kapcsolatra utal. A hierarchia csúcsán álló Root CA-t az operációs rendszerek és a böngészők eredendően megbízhatónak tartják. Tanúsítványokat állít ki a köztes CA-knak, amelyek tanúsítványokat állítanak ki a végfelhasználóknak, például a weboldalaknak és a szervereknek. Ez a struktúra biztosítja, hogy minden egyes tanúsítványt a felette lévő tanúsítványokkal lehet hitelesíteni, és végső soron a trusted Root CA-hoz vezet vissza.

   A bizalmi lánc kulcsfontosságú a biztonságos kommunikáció szempontjából, mivel lehetővé teszi a felhasználók és a rendszerek számára a digitális tanúsítványok hitelességének ellenőrzését. Ha a lánc megszakad, vagy egy tanúsítvány sérül, a rendszer a kommunikációt nem biztonságosnak jelöli, így védve a felhasználókat a potenciális fenyegetésektől.

Válaszok a gondolkodtató feladatokra

1. Vizsgáljuk meg az Extended Validation (EV) tanúsítványok szerepét a webes biztonságban, és magyarázzuk el, miben különböznek a Domain Validated (DV) és az Organization Validated (OV) tanúsítványoktól!

   Az Extended Validation tanúsítványok (EV) a digitális tanúsítványok közül a legmagasabb szintű megbízhatóságot nyújtják. A Domain Validated (DV) és az Organization Validated (OV) tanúsítványokkal ellentétben, amelyek elsősorban domainellenőrzést végeznek és az entitás alapvető adatait ellenőrzik, az EV tanúsítványok szigorú ellenőrzési folyamatokat foglalnak magukban. A hitelesítésszolgáltatóknak (CA-k) az EV-tanúsítvány kiadása előtt ellenőrizniük kell a kérelmező entitás jogi létezését, fizikai elhelyezkedését és működési státuszát. Míg a DV-tanúsítványok könnyebben beszerezhetők és elegendőek az alapvető titkosítási igények kielégítésére, az EV-tanúsítványok a személyazonosság ellenőrzésének további rétegeit biztosítják, növelve a felhasználók bizalmát az olyan érzékeny tranzakciók során, mint az online banki ügyintézés vagy vásárlás.

2. Generáljunk CSR-t a *www.example.com* tartományhoz az OpenSSL használatával! Adjuk meg a használt parancsot, és magyarázzuk el a parancs egyes részeit!

   Ahhoz, hogy a *www.example.com* webhelyhez CSR-t hozzunk létre OpenSSL használatával, a következő parancsot kell kiadni:

   ```
   openssl req -new -key private.key -out example.csr
   ```

   A `req -new` jelenti az új CSR létrehozását.

   A `-key private.key` a CSR generálásához használandó privát kulcs fájlt határozza meg. Ezt a privát kulcsot már korábban létre kellett hoznunk!

   Az `-out example.csr` jelenti a létrehozandó CSR fájl nevét.

   A parancs futtatása után a rendszer megkér minket az olyan információk megadására, mint a domainnév, a szervezet és a hely, amelyek szerepelni fognak a CSR-ben. Ezt a fájlt ezután be lehet küldeni a tanúsító hatósághoz, hogy X.509 tanúsítványt kérjünk.

022.2 Webes titkosítás

Hivatkozás az LPI célkitűzésre

Security Essentials version 1.0, Exam 020, Objective 022.2

Súlyozás

2

Kulcsfontosságú ismeretek

- Az egyszerű szöveges protokollok és a szállítási titkosítás közötti jelentős különbségek megértése
- A HTTPS fogalmának megértése
- Az X.509 tanúsítványok fontos mezőinek megértése HTTPS használata esetén
- X.509-tanúsítványok egy adott webhelyhez való kapcsolódásának megértése
- A böngészők teljesítményének érvényességellenőrzésének megértése X.509 tanúsítványok esetén
- Annak megállapítása, hogy egy weboldal titkosított-e vagy sem, beleértve a gyakori böngészőüzeneteket is

A használt fájlok, kifejezések és segédprogramok részleges listája

- HTTPS, TLS, SSL
- X.509 tanúsítvány mezői: subject, Validity, subjectAltName

Linux Professional Institute

Lecke 1

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	022 Titkosítás
Fejezet:	022.2 Webes titkosítás
Lecke:	1/1

Bevezetés

A webes titkosítás létfontosságú szerepet játszik a weboldalak és látogatóik között kicserélt adatok védelmében, biztosítva az adatvédelmet és a jogosulatlan hozzáférés elleni védelmet. Az erre a célra használt elsődleges protokoll a *Hypertext Transfer Protocol Secure* (HTTPS). A HTTPS nemcsak titkosítja az adatokat, hanem digitális tanúsítványok segítségével ellenőrzi a webszerverek identitását is. Ez a kettős funkció lehetővé teszi a látogatók számára, hogy magabiztosan lépjenek kapcsolatba legitim webhelyekkel.

Fontos megérteni, hogyan működik a HTTPS, milyen szerepet játszanak a hitelesítésszolgáltatók (CA-k) a szerver ellenőrzésében, és hogyan jelzik a böngésző figyelmeztetései a látogatóknak a lehetséges biztonsági kockázatokat. Ezeknek a fogalmaknak az elsajátításával az egyének biztosíthatják a biztonságos és védett webes interakciókat.

Ez a lecke a HTTPS mögött meghúzódó alapelveket vizsgálja, a szerver ellenőrzésére, a titkosításra és a digitális tanúsítványok jelentőségére összpontosítva. A tananyag kitér a biztonsággal kapcsolatos böngészőben lévő gyakori hibaüzenetekre is, például a lejárt vagy nem megbízható tanúsítványokra, és betekintést nyújt abba, hogy ezek a figyelmeztetések hogyan segítik a látogatók védelmét az olyan fenyegetésekkel szemben, mint a man-in-the-middle támadások.

Jelentős különbségek az egyszerű szöveges protokollok és a szállítási titkosítás között

A webes kommunikációban alapvető fontosságú különbséget tenni az *egyszerű szöveges protokollok* (plain text protocol) és a *szállítási titkosítás* (transport encryption) között. Az egyszerű szöveges protokollok olvasható formátumban küldik az adatokat, ami azt jelenti, hogy az információk könnyen lehallgathatók és rosszindulatú szereplők számára is megtekinthetők. A HTTP (*Hypertext Transfer Protocol*) egy egyszerű szöveges protokoll, ahol az összes adat mindenféle titkosítás nélkül kerül továbbításra, így az adatok lehallgathatóak és manipulálhatóak.

A HTTP határozza meg, hogy a webes kliensek (pl. a böngészők) hogyan kommunikálnak a webszerverekkel. Alkalmazási szintű protokollként a HTTP független az alapul szolgáló szállítási vagy munkamenetszintű protokolloktól (HTTP az internet internetes stack részeként). Eredeti formájában azonban a HTTP az adatokat egyszerű szövegként, titkosítás nélkül, szállítási szegmensekbe (pl. TCP) zárva továbbítja, így lehallgathatóvá válik.

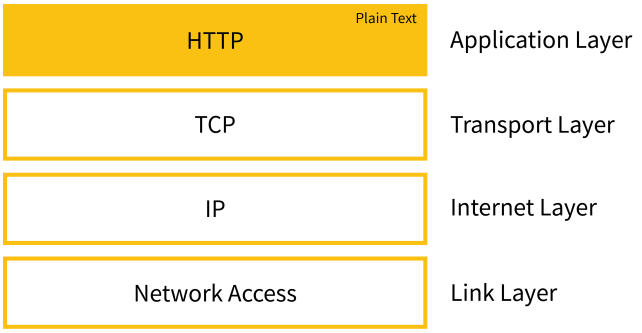

Figure 3. HTTP az internet internetes stack részeként

A *szálltási titkosítás* megoldást kínál azáltal, hogy az adatokat az átvitel során kódolja, és olvashatatlan formátumba alakítja át. Még ha az adatokat le is hallgatják, a megfelelő dekódoló kulcsok nélkül nem lehet visszafejteni. Ez a megközelítés biztosítja az adatok titkosságát és sértetlenségét, megakadályozva a jogosulatlan hozzáférést és módosítást. A *Transport Layer Security* (TLS) a legszélesebb körben használt protokoll a szállítás titkosítására, amely a HTTP biztonságos verziójának, a HTTPS-nek az alapját képezi.

TLS

Ahogy az internet fejlődött, hogy érzékeny és kereskedelmi tranzakciókat kezeljen, szükségessé vált egy olyan protokoll, amely védi ezeket az adatokat. Az 1990-es években bevezetett *Secure Sockets Layer* (SSL) ezt a célt szolgálta, de azóta leváltotta az utódja, a *Transport Layer Security* (TLS). A TLS a kliensek és a szerverek közötti, nem védett csatornákon keresztüli kommunikáció biztosításának szabványa.

A TLS több kulcsfontosságú elemből áll, beleértve a titkosítási protokollokat, a szerver identitásának ellenőrzésére szolgáló digitális tanúsítványokat és két elsődleges TLS protokollt: a *TLS handshake* protokollt és a *TLS record* protokollt. Ezek a komponensek együttesen biztosítják a biztonságos kapcsolatot a kliens és a szerver között (TLS protokollok az internetes stack részeként.).

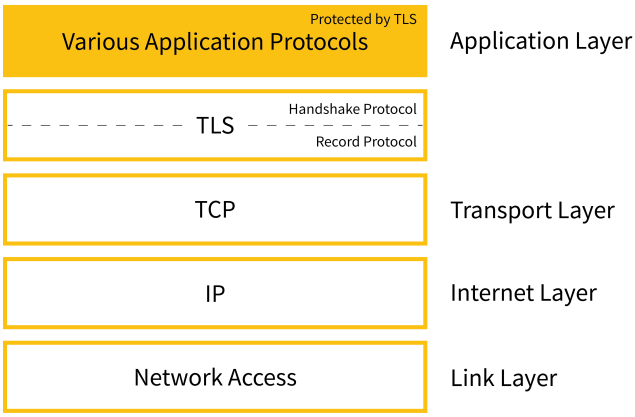

Figure 4. TLS protokollok az internetes stack részeként.

A TLS handshake protokoll felelős a kliens és a szerver közötti kezdeti hitelesítésért, amelynek során kriptográfiai kulcsokat cserélnek, és megállapodnak egy titkosítási algoritmusban. A TLS handshake biztosítja, hogy a kapcsolat biztonságos legyen, mielőtt bármilyen alkalmazási adat cseréjére sor kerülne. A sikeres hitelesítéshez a szervernek be kell mutatnia egy megbízható hitelesítési szolgáltató (CA) által aláírt digitális tanúsítványt, amely megerősíti az identitását.

A TLS magában foglalja a TLS record protokollt is, amely magasabb szintű protokollokat zár egységbe, adatvédelmet és adatintegritást biztosítva. Az adatvédelem szimmetrikus titkosítással valósul meg, míg az adatok sértetlenségét az átvitel során történő manipuláció észlelésére szolgáló *Message Authentication Code* (MAC) beépítése biztosítja. Ez a kétrétegű megközelítés garantálja, hogy a kommunikáció privát és biztonságos marad.

A HTTPS mögötti koncepció

A HTTPS, azaz a Hypertext Transfer Protocol Secure egyszerűen a TLS fölött futó HTTP (HTTPS az internetes stack részeként). A HTTPS célja, hogy a látogató böngészője és a webszerver között továbbított adatokat titkosítással és a szerver identitásának ellenőrzésével védje.

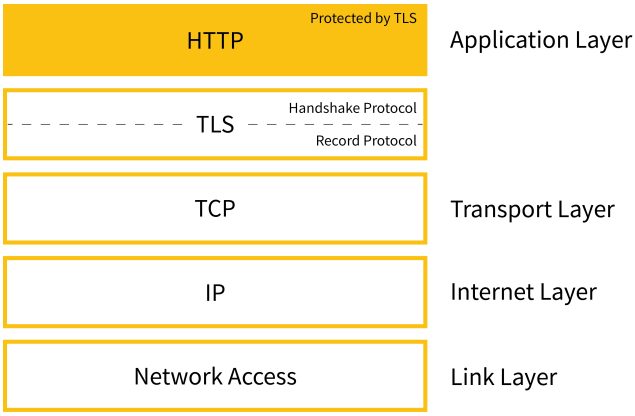

Figure 5. HTTPS az internetes stack részeként

Amikor egy látogató HTTPS használatával hozzáférést kér egy weboldalhoz, a szerver egy *X.509 digitális tanúsítványt* mutat be a böngészőnek. Ez a tanúsítvány, amelyet egy megbízható hitelesítési szolgáltató (CA) állít ki, hitelesíti a szerver identitását. A hitelesítés után a böngésző biztonságos kapcsolatot hoz létre szimmetrikus titkosítással, amelyet gyakran Diffie-Hellman vagy Elliptic Curve Diffie-Hellman (ECDH) kulcscsere-módszerek segítenek elő.

A HTTPS elsődleges előnye, hogy a webes kommunikáció számára titkosságot, integritást és hitelesítést biztosít. A HTTPS-en keresztül továbbított adatok védve vannak a lehallgatástól vagy a manipulációtól, és szerver identitását ellenőrzik, hogy megakadályozzák, hogy a látogatók tudtukon kívül rosszindulatú webhelyekkel lépjenek kapcsolatba.

A modern böngészők vizuális jelzőkkel, például a címsoron megjelenő lakat ikonjával jelzik, hogy egy weboldal HTTPS protokollt használ. Ha azonban a tanúsítvány lejárt, helytelenül van beállítva vagy nem megbízható, a böngészők figyelmeztető üzeneteket jeleníthetnek meg, hogy tájékoztassák a látogatókat a lehetséges biztonsági kockázatokról. Ezek a figyelmeztetések segítenek megelőzni az olyan támadásokat, mint például a man-in-the-middle típusú lehallgatások, mivel figyelmeztetik a látogatókat, ha a kapcsolat veszélybe kerülhet.

A HTTP-ről a HTTPS-re való áttérést a webes adatvédelem és biztonság iránti növekvő igény vezérelte. A legtöbb böngésző és keresőmotor ma már a HTTPS-képes weboldalakat részesíti előnyben, ami tükrözi a biztonságos kommunikáció fontosságát a mai digitális világban.

A HTTPS-kommunikáció alapértelmezett portja a TCP 443, míg a HTTP a TCP 80-as portot használja. A portszámok közötti különbség lehetővé teszi a szerverek számára, hogy különbséget tegyenek a biztonságos és a nem biztonságos forgalom között. Amikor egy böngésző HTTPS-en keresztül kér le egy weboldalt, a kezdeti kapcsolat a TLS kézfogást foglalja magában, amelynek során a szerver identitásának hitelesítése és a titkosítási kulcsok cseréje történik.

A TLS kézfogás befejezése után a böngésző elküldi az első HTTP-kérést, és minden további

adatcsere titkosítva van, így biztosítva, hogy az érzékeny információk, például a bejelentkezési adatok vagy a fizetési adatok a munkamenet során biztonságban maradjanak.

Sok weboldal úgy van beállítva, hogy a biztonságos kapcsolat érdekében a látogatókat automatikusan átirányítsa a HTTP-ről a HTTPS-re. Ha például egy látogató a `http://www.example.com` címet nyitja meg, a szerver átirányíthatja a `https://www.example.com` címre, így garantálva a titkosított és biztonságos kommunikációt.

Az X.509 tanúsítványok fontos mezői HTTPS használatához

A HTTPS-kiszolgáló hitelesítése digitális tanúsítványokra, különösen X.509 tanúsítványokra támaszkodik a szerver identitásának ellenőrzésekor. Amikor a látogató beír egy URL-címet, a böngésző lekérdezi a szerver digitális tanúsítványát, amely tartalmazza a nyilvános kulcsot és az identitási adatokat. Ezt a tanúsítványt egy megbízható hitelesítési szolgáltató (CA) írja alá, így biztosítva a szerver legitimitását.

Az X.509 tanúsítványok, más néven SSL vagy TLS tanúsítványok, egy nyilvános kulcsot kötnek a szerver identitásához, amelyre a tanúsítványban `Subject` néven hivatkoznak. A CA digitális aláírása megerősíti ennek a kötődésnek az érvényességét, amelyet a tanúsítvány `signatureValue` mezőjében tárol.

Az X.509 szabvány határozza meg a digitális tanúsítványok szerkezetét. A 3. verzió (X.509v3) bevezette a tanúsítványok kiterjesztésének lehetőségét, amely lehetővé teszi további információk, például a szerver alternatív nevének feltüntetését.

Hogyan kapcsolódnak az X.509-tanúsítványok egy adott webhelyhez

A *Subject Alternative Name* (SAN) kiterjesztés lehetővé teszi, hogy egy tanúsítvány több identitást, például DNS-neveket vagy IP-címeket társítson ugyanahhoz a szerverhez. Ez a rugalmasság kulcsfontosságú a több domainnév vagy IP-cím alatt működő szerverek számára, mivel lehetővé teszi, hogy egyetlen tanúsítvány az összes releváns identitást lefedje.

A tanúsítvány ellenőrzésének folyamata során a `Subject `vagy `Subject Alternative Name` a szerver identitásával összevetve kerül ellenőrzésre. Ha találunk egyezést, a tanúsítványt érvényesnek tekintjük. A joker jelek, mint például a `*.example.com`, több aldomainnel való egyezéshez is használhatók, ami nagyobb rugalmasságot biztosít a tanúsítványkezelésben.

A tanúsítványokat az Intermediate CA-k állítják ki, amelyek a trusted root CA-hoz visszavezető bizalmi lánc részét képezik. A böngésző úgy ellenőrzi a bizalmi láncot, hogy minden egyes tanúsítvány `Issuer` mezőjét összeveti a láncban következő tanúsítvány `Subject` mezőjével, és

végül eljut a trusted Root CA-hoz.

A tanúsítványok meghatározott *érvényességi időszakkal* (validity period) rendelkeznek, amely azt az időtartamot jelzi, ami alatt a tanúsítvány érvényes. Ha egy tanúsítvány a lejárata előtt veszélybe kerül, a CA visszavonhatja azt, és sorozatszámát közzéteszi a *Certificate Revocation List* -en (Tanúsítvány-visszavonási lista — CRL). A böngészők a CRL-ek segítségével ellenőrzik a tanúsítvány állapotát, és biztosítják, hogy azt nem vonták vissza.

A HTTPS-kiszolgálók gyakran úgy vannak beállítva, hogy a HTTP-forgalmat automatikusan átirányítsák HTTPS-re. Képzeljünk el egy helyzetet, amikor a webes kliens, például egy böngésző, az alábbi kérést küldi a következő URI-ra, kifejezetten megadva a HTTP-t:

```
http://www.example.com/~carol/home.html
```

A HTTPS-kiszolgáló átirányítja a klienst egy HTTPS-t megadó URI-re, például:

```
https://www.example.com/~carol/home.html
```

A böngészők teljesítményének érvényességellenőrzése X.509 tanúsítványok alatt

Amikor egy webböngésző HTTPS használatával csatlakozik egy weboldalhoz, számos alapvető érvényességi ellenőrzést, vizsgálatot végez a weboldal X.509 tanúsítványán, hogy biztosítsa a kapcsolat biztonságosságát és megbízhatóságát. Ezek a vizsgálatok ellenőrzik a tanúsítvány hitelességét, megerősítik a weboldal identitását, és megvédik a látogatókat az olyan potenciális biztonsági fenyegetésektől, mint például a man-in-the-middle támadások. A böngésző egy sor lépést hajt végre a tanúsítvány érvényességének értékeléséhez.

A publikus kulcsú tanúsítványok formátumát az X.509 szabvány határozza meg, amelyet először 1988-ban tettek közzé. Az 1996-ban kifejlesztett X.509 3. verziójú (v3) tanúsítványformátum további `Extensions` mezőkkel bővíti a formátumot (X.509 v3 tanúsítvány).

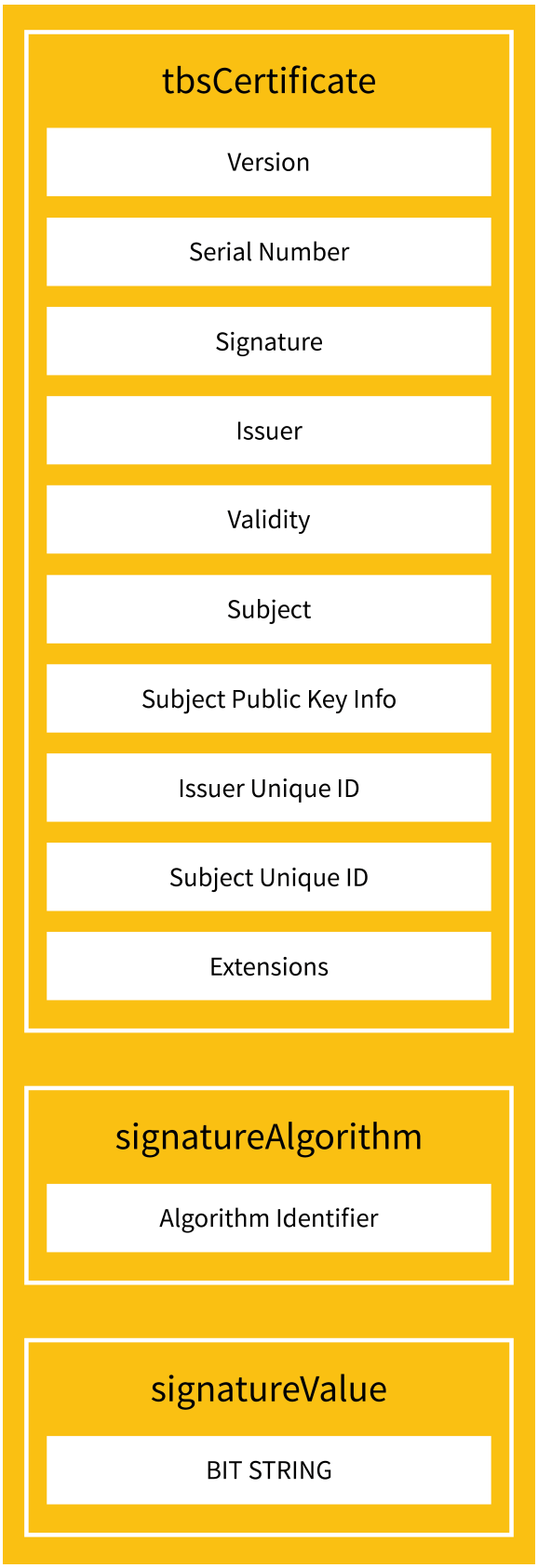

Figure 6. X.509 v3 tanúsítvány

A nyilvános kulcsú tanúsítvány `Subject` mezője azonosítja a `Subject Public Key Info` mezőben tárolt nyilvános kulcshoz tartozó HTTPS-kiszolgálót. Az `Extensions` mező olyan adatokat közölhet, mint további alanyt azonosító információk.

Az X.509 specifikáció Subject Alternative Name extensionje lehetővé teszi, hogy a tanúsítvány alanyához további identitásokat lehessen kötni. A Subject Alternative Name opciók között szerepelhet DNS hostnév, IP-cím és egyebek.

Az alany neve szerepelhet a `Subject` mezőben, a Subject Alternative Name extensionben vagy mindkettőben. Ha a SAN kiterjesztés `DNS Name` meg van adva, akkor a rendszer azt használja a szerver azonosítójaként. Ellenkező esetben a tanúsítvány `Subject` mezőjében található `Common Name` mezőt kell azonosítóként használni.

Ha a tanúsítványban egynél több azonosító szerepel egy adott típusból — pl. egynél több `DNS Name` mező --, akkor a halmaz bármelyik mezőjének egyezése elfogadhatónak tekinthető. A nevek tartalmazhatják a `*` (asterisk) joker (wildcard) karaktert, hogy bármelyik tartománynév komponens vagy komponenstöredék egyezzen. Így, ha az URI a `https://www.example.com/~carol/home.html`, és a szerver tanúsítványa a `*.basket.com`, `abcd.com` és `*.example.com` lehetőségeket tartalmazza a `DNS Name` opcióként, akkor van elfogadható egyezés: A `*.example.com` megfeleltethető a `www.example.com` névvel. Ez a wildcard név nem feleltethető meg a `basket.carol.example.com` névvel, mivel ez utóbbi tartománynév tartalmaz egy extra komponenst.

Hasonlóképpen, a `c*.com` egyezik a `carol.com` kifejezéssel, mert a csillag (asterisk) egyezhet egy komponens töredékével, de nem egyezik a `basket.com` kifejezéssel.

Ha az URI host mezője nem hostnevet, hanem IP-címet tartalmaz, például `https://8.8.8.8`, a kliens ellenőrzi a Subject Alternative Name extension `IP Address` mezőjét. Az `IP Address` mezőnek meg kell jelennie a tanúsítványban, és pontosan meg kell egyeznie az URI-ban szereplő IP-címmel.

Ezután a böngésző ellenőrzi a tanúsítvány bizalmi láncát. Megerősíti, hogy a tanúsítványt egy megbízható hitelesítési szolgáltató (CA) állította-e ki és írta-e alá. Ennek során a tanúsítványláncot a weboldal tanúsítványától a köztes tanúsítványokon keresztül egészen a trusted root CA-ig követi, amely a böngésző előre telepített *root certificate store*-ban szerepel. Ha ebben a láncban bármelyik tanúsítvány érvénytelen, vagy nem megbízható CA állította ki, a böngésző a kapcsolatot nem-biztonságosnak jelöli, és figyelmezteti a látogatót.

Egy másik kritikus ellenőrzés a tanúsítvány érvényességi idejét érinti. Minden X.509 tanúsítvány meghatároz egy időkeretet, amelyen belül érvényes, ezt pedig a `notBefore` és a `notAfter` mezők határozzák meg. A böngésző az aktuális dátumot és időt az érvényességi időszakhoz viszonyítja. Ha a tanúsítvány lejárt vagy még nem érvényes, a böngésző figyelmezteti a látogatót, jelezve, hogy

a kapcsolat nem biztonságos. Ez a folyamat biztosítja a tanúsítványok rendszeres megújítását a biztonságos kommunikáció fenntartása érdekében.

A böngészők emellett azt is ellenőrzik, hogy a CA visszavonta-e a tanúsítványt. Ez olyan módszerekkel történik, mint például a *Certificate Revocation List* (CRL) lekérdezése vagy az *Online Certificate Status Protocol* (OCSP) használata. Ha a tanúsítványt olyan okok miatt vonták vissza, mint például egy kompromittált kulcs vagy téves kiállítás, a böngésző figyelmezteti a látogatót, hogy a tanúsítvány már nem megbízható, és a kapcsolat nem biztonságos.

A böngésző a tanúsítvány digitális aláírását is érvényesíti, hogy megerősítse, hogy a tanúsítványt a kiállítása óta nem manipulálták. Ez magában foglalja a kiállító CA kriptográfiai aláírásának ellenőrzését. Ha az aláírás ellenőrzése nem sikerül, az arra utal, hogy a tanúsítványt megváltoztatták vagy meghamisították, ami a böngészőt a kapcsolat blokkolására készteti a látogató biztonsága érdekében.

Végül a böngészők áttekintik a tanúsítványban található kulcshasználati vagy kiterjesztési mezőket. Ezek a mezők meghatározzák a tanúsítvány rendeltetését, például a szerver hitelesítését vagy kódaláírását. A böngésző biztosítja, hogy a tanúsítványt e meghatározott céloknak megfelelően használják. Ha a tanúsítványt a megengedett körön kívül eső célra használják, a böngésző figyelmeztetést küld a látogatónak.

Ezek az ellenőrzések együttesen biztosítják a webes kommunikáció biztonságát az X.509 tanúsítványok hitelességének, sértetlenségének és megfelelő használatának érvényesítésével. Ha ezen ellenőrzések bármelyike sikertelen, a böngésző biztonsági figyelmeztetést vagy hibaüzenetet jelenít meg, és arra kéri a látogatót, hogy óvatosan járjon el, vagy teljesen kerülje el a webhelyet. Ez a szigorú hitelesítési folyamat kritikus szerepet játszik az online interakciók megbízhatóságának fenntartásában, és segít megakadályozni, hogy rosszindulatú entitások legitim webhelyeknek adják ki magukat.

Annak meghatározása, hogy egy weboldal titkosított-e

Annak megállapítása, hogy egy weboldal titkosított-e, döntő fontosságú lépés a látogató böngészője és a weboldal szervere közötti biztonságos kommunikáció garantálásában. A titkosított webhelyek HTTPS protokollt használnak, amely a TLS protokollon keresztül titkosítást biztosít, így a látogató és a webhely között kicserélt adatok bizalmasak és védettek maradnak a lehallgatástól vagy a manipulációtól.

Annak megállapításához, hogy egy weboldal titkosított-e, a látogatók a webböngészők által biztosított néhány vizuális jelre támaszkodhatnak. A leggyakoribb ilyen a lakat ikon, amely a böngésző címsorában jelenik meg az URL bal oldalán. Ha a weboldal HTTPS protokollt használ, a lakat zárt vagy zárolt állapotban jelenik meg, jelezve, hogy a kapcsolat biztonságos. Egyes

böngészőkben a lakat ikonra kattintva részletesebb információk jelennek meg a weboldal titkosításáról, mint például a használt titkosítás típusa és a kibocsátó CA.

A lakat mellett maga az URL-cím is jelzi, hogy egy webhely titkosított-e. A biztonságos webhelyek a `https://`-sel, míg a nem titkosított webhelyek a `http://`-vel kezdődnek. A `https://` jelenléte azt jelzi, hogy a kapcsolat TLS-titkosítással védett. Egyes böngészők ezt a címsor színének megváltoztatásával is kiemelhetik, ha biztonságos kapcsolat jön létre.

Ha egy weboldal nem használ titkosítást, a modern böngészők gyakran figyelmeztető üzenetet jelenítenek meg, hogy tájékoztassák a látogatókat a lehetséges kockázatokról. Ha például egy látogató egyszerű HTTP protokollal (titkosítás nélkül) próbál meg elérni egy webhelyet, a böngésző a címsoron egy olyan üzenetet jeleníthet meg, mint például a “Not Secure”. Bizonyos esetekben a böngészők egy feltűnőbb, “connection is not private” figyelmeztetést is megjeleníthetnek, amely arra figyelmezteti a látogatót, hogy a kapcsolat nem privát, és azt tanácsolják, hogy kerüljük az érzékeny adatok, például jelszavak vagy hitelkártyaszámok megadását. Az olyan böngészők, mint a Google Chrome, a Mozilla Firefox és a Microsoft Edge egyre szigorúbban jelzik a nem titkosított webhelyeket, különösen azokon az oldalakon, ahol a látogatókat személyes adatok megadására kérik.

Ha egy weboldal HTTPS-konfigurációja érvénytelen vagy helytelenül van beállítva, a böngészők további figyelmeztető üzeneteket jelenítenek meg. Ha például egy webhely “expired” (lejárt), “misconfigured” (rosszul konfigurált) vagy “untrusted” (nem megbízható) tanúsítvánnyal rendelkezik, a böngésző egy egész oldalas figyelmeztető üzenetet jeleníthet meg a probléma leírásával. Az olyan üzenetek, mint a “Your connection is not private” (A kapcsolat nem privát), vagy a “Potential Security Risk Ahead” (Lehetséges biztonsági kockázat), azt jelzik, hogy a tanúsítvány lejárt, visszavont vagy nem megbízható CA által aláírt. Ezek a figyelmeztetések általában azt javasolják, hogy a látogatók szakítsák meg a webhellyel való kapcsolatot a biztonságuk érdekében, bár gyakran lehetőséget adnak arra, hogy a látogató saját felelősségére kivételt tegyen.

Annak megállapításához, hogy egy weboldal titkosított-e, olyan vizuális jelzőket kell keresni, mint a lakat ikon és a `https://` az URL-ben. A böngészők egyértelmű figyelmeztetéseket is megjelenítenek, ha egy webhely nem biztonságos, így garantálva, hogy a látogatókat tájékoztassák a titkosítatlan vagy rosszul konfigurált kapcsolatokkal összefüggésben lévő lehetséges kockázatokról. Ezeknek a böngészőüzeneteknek a megértése elengedhetetlen a biztonságos böngészéshez és a biztonsági fenyegetések elkerüléséhez.

Gyakorló felaadatok

1. Milyen jellemzők tartoznak a HTTP protokollhoz és melyek a HTTPS protokollhoz?

Jellemzők	**HTTP**	**HTTPS**
A webes adatokat közvetlenül egy szállítási réteg protokoll, általában a TCP zárja egységbe.		
A támadók lehallgathatják a kommunikációt.		
Titkosított adatok továbbítása az interneten keresztül.		
A 80-as port az alapértelmezett TCP port.		
A 443-as port az alapértelmezett TCP port.		
Egyszerű szöveges adatok továbbítása az interneten keresztül.		
A webes adatokat a TLS protokoll zárja egységbe.		
A webes adatok “man in the middle” által módosíthatók.		
A webszerver identitása ellenőrzésre kerül.		
A protokoll biztosítja az adatok integritását.		

2. Az alábbi esetek közül melyekben tekinthető érvényesnek vagy érvénytelennek a webszerver identitása?

URI	A szervertanúsítvány subject és subject alternative name tartalma	A szerver identitásának érvényessége
`https://www.example1.com/penguin.html`	`*.penguin.com`, `www.example.com`	
`https://hotlinux.org`	`www.xyz.com`, `hot*.com`	
`https://www.securityessent.com`	`*.security.com`, `security*.org`	
`https://www.certsun.com/`	`ohlala.com`, `cert*.com`	
`https://www.justaparadigm.com/`	`www.carol.com`, `www.justaparadigm.com`	
`https://www.128.263.5.98/`	`www.carol.com`, `128.263.6.98`	
`https://251.32.75.42/`	`www.abc.com`, `251.32.75.42`	

Gondolkodtató feladatok

1. Hogyan ellenőrzi a HTTPS-kliens az X.509 tanúsítvány kibocsátójának azonosságát?

2. Milyen információkat tartalmaznak a webszerver X.509v3 tanúsítványának következő mezői?

`Issuer`	
`Validity`	
`Subject`	
`Extensions`	
`SignatureValue`	

3. Írjunk le egy olyan helyzetet, amely az X.509-tanúsítvány érvénytelenségét okozhatja az érvényességi idő lejárta előtt!

Összefoglalás

Ez a lecke a webes titkosítás fontosságát vizsgálja, arra összpontosítva, hogy a HTTPS hogyan biztosítja a látogatók és a webhelyek közötti kommunikációt az adatok titkosításával és a szerver identitásának digitális tanúsítványok segítségével történő ellenőrzésével. A TLS (Transport Layer Security) protokollon keresztül futó HTTPS létfontosságú szerepet játszik a webes kommunikáció titkosságának és integritásának biztosításában. A lecke elmagyarázza a különbségeket az olyan egyszerű szöveges protokollok, mint a HTTP, amelyek az adatokat lehallgatásnak teszik ki, és a szállítási titkosítás között, amely védi az adatokat az átvitel során.

A lecke még jobban elmélyül a HTTPS működésében, kiemelve az X.509 tanúsítványok szerepét a webszerverek hitelesítésében. Bemutatja az ellenőrzési folyamatot, amelynek során a webböngészők ellenőrzik a tanúsítvány megbízhatóságát, beleértve a tartománynév egyezésének, a tanúsítvány bizalmi láncának, érvényességi idejének, visszavonási státuszának és a kulcskiterjesztéseken alapuló megfelelő használatának ellenőrzését. Emellett a látogatók megtudhatják, hogy a böngészők hogyan figyelmeztetnek a lehetséges biztonsági kockázatokra, ha a tanúsítványok lejártak, nem megbízhatóak vagy rosszul vannak beállítva. Ezek a figyelmeztetések jelentős szerepet játszanak a látogatók védelmében a man-in-the-middle támadásoktól és más fenyegetésektől.

Válaszok a gyakorló feladatokra

1. Milyen jellemzők tartoznak a HTTP protokollhoz és melyek a HTTPS protokollhoz?

Jellemzők	HTTP	HTTPS
A webes adatokat közvetlenül egy szállítási réteg protokoll, általában a TCP zárja egységbe.	X	
A támadók lehallgathatják a kommunikációt.	X	
Titkosított adatok továbbítása az interneten keresztül.		X
A 80-as port az alapértelmezett TCP port.	X	
A 443-as port az alapértelmezett TCP port.		X
Egyszerű szöveges adatok továbbítása az interneten keresztül.	X	
A webes adatokat a TLS protokoll zárja egységbe.		X
A webes adatok “man in the middle” által módosíthatók.	X	
A webszerver identitása ellenőrzésre kerül.		X
A protokoll biztosítja az adatok integritását.		X

2. Az alábbi esetek közül melyekben tekinthető érvényesnek vagy érvénytelennek a webszerver identitása?

URI	A szervertanúsítvány subject és subject alternative name tartalma	A szerver identitásának érvényessége
`https://www.example1.com/penguin.html`	`*.penguin.com`, `www.example.com`	Nem érvényes
`https://hotlinux.org`	`www.xyz.com`, `hot*.com`	Nem érvényes
`https://www.securityessent.com`	`*.security.com`, `security*.org`	Nem érvényes
`https://www.certsun.com/`	`ohlala.com`, `cert*.com`	Érvényes
`https:///www.justaparadigm.com/`	`www.carol.com`, `www.justaparadigm.com`	Érvényes
`https://www.128.263.5.98/`	`www.carol.com`, `128.263.6.98`	Nem érvényes
`https://251.32.75.42/`	`www.abc.com`, `251.32.75.42`	Érvényes

Válaszok a gondolkodtató feladatokra

1. Hogyan ellenőrzi a HTTPS-kliens az X.509 tanúsítvány kibocsátójának azonosságát?

   A HTTPS-kliensek feldolgozzák a kibocsátó megkülönböztető nevét és az alany megkülönböztető nevét felsoroló mezőket, hogy a hitelesítési útvonal érvényesítéséhez névláncolást hajtsanak végre. A névláncolás úgy történik, hogy a kibocsátó megkülönböztető neve egy tanúsítványban egyezik a másik tanúsítványban szereplő subject névvel. Végül a root tanúsítványban szereplő kibocsátó megkülönböztető nevének meg kell egyeznie a kliens root store-ban lévővel.

2. Milyen információkat tartalmaznak a webszerver X.509v3 tanúsítványának következő mezői?

`Issuer`	A CA általános neve és egyéb információ a CA-ról
`Validity`	A tanúsítvány érvényességi idejét meghatározó dátumok
`Subject`	A subject általános neve és a subject-tel kapcsolatos egyéb információk
`Extensions`	A subject DNS-neve, IP-címe és egyéb kiterjesztett adatok
`SignatureValue`	A CA aláírása

3. Írjunk le egy olyan helyzetet, amely az X.509-tanúsítvány érvénytelenségét okozhatja az érvényességi idő lejárta előtt!

   A hozzá tartozó privát kulcs feltételezett vagy valós kompromittálódása.

022.3 Email titkosítás

Hivatkozás az LPI célkitűzésre

Security Essentials version 1.0, Exam 020, Objective 022.3

Súlyozás

2

Kulcsfontosságú ismeretek

- Az email titkosítás és az e-mail aláírások megértése
- Az OpenPGP megértése
- Az S/MIME megértése
- Az OpenPGP kulcsszerverek szerepének megértése
- Az S/MIME tanúsítványok szerepének megértése
- A PGP kulcsok és az S/MIME tanúsítványok email címekkel való kapcsolódásának megértése
- A Mozilla Thunderbird használata titkosított emailek küldéséhez és fogadásához OpenPGP és S/MIME segítségével

A használt fájlok, kifejezések és segédprogramok részleges listája

- GnuPGP, GPG kulcsok, kulcsszerverek
- S/MIME és S/MIME tanúsítványok

Linux Professional Institute

Lecke 1

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	022 Titkosítás
Fejezet:	022.3 Email titkosítás
Lecke:	1/1

Bevezetés

A mai digitális környezetben az e-mail továbbra is kritikus fontosságú kommunikációs eszköz marad, de a lehallgatás és a jogosulatlan hozzáférés szempontjából sebezhető is. Az e-mailben kicserélt érzékeny információk védelme érdekében az olyan titkosítási technológiák, mint az *OpenPGP* és az *S/MIME* biztosítják a titoktartást, az integritást és a hitelességet. E két titkosítási szabvány megértése alapvető fontosságú mindazok számára, akik a biztonságos kommunikációban részt vesznek.

Az *Open Pretty Good Privacy* (OpenPGP) és a *Secure/Multipurpose Internet Mail Extensions* (S/MIME) két széles körben elfogadott protokoll az e-mail üzenetek titkosítására és digitális aláírására. Az OpenPGP decentralizált bizalmi modellre támaszkodik, lehetővé téve a felhasználók számára, hogy saját titkosítási kulcsaikat generálják és kezeljék, míg az S/MIME központosított bizalmi modellel működik, amely megbízható hitelesítésszolgáltatók (CA-k) által kibocsátott digitális tanúsítványokat használ. Mindkét szabvány titkosítást tesz lehetővé az e-mailek tartalmának a nem kívánt címzettek általi elolvasásától való védelmére, valamint digitális aláírást a feladó személyazonosságának igazolására és annak biztosítására, hogy az üzenetet nem manipulálták.

Megismerjük a Mozilla Thunderbirdöt, egy cross-platform e-mail klienst, amely arról ismert, hogy támogatja és integrálja az OpenPGP-t és az S/MIME-t, lehetővé téve a végponttól végpontig tartó titkosítást. A konfigurálás jellemzően az OpenPGP és az S/MIME beállítását, publikus és privát kulcspárok létrehozását, X.509 tanúsítványok importálását, valamint a titkosított üzenetek biztonságos küldésének és fogadásának kezelését foglalja magában.

E-mail titkosítás és digitális aláírások

Az e-mailek titkosításához a rendszerek *nyilvános kulcsú* vagy *aszimmetrikus kriptográfiát* használnak. A szimmetrikus kriptográfiával ellentétben, amely ugyanazt a kulcsot használja mind a titkosításhoz, mind a visszafejtéshez, a nyilvános kulcsú kriptográfia minden felhasználó számára egy *publikus kulcsból* és egy *privát kulcsból* álló kulcspárt biztosít.

Ahogy a nevek is jelzik, a publikus kulcsot nyilvánosan megosztják, és bárki hozzáférhet, aki titkosított e-mail kommunikációban részt szerete venni. A titkos kulcs azonban bizalmas marad, a felhasználó soha nem osztja meg vagy továbbítja.

A titkosítási folyamat a következőképpen működik: A küldő a címzett publikus kulcsát használja a nyílt szövegű üzenet titkosítására, így egy olyan *ciphertext* (rejtjelezett szöveg) keletkezik, amely a megfelelő privát kulcs nélkül nem olvasható. Csak az a címzett tudja vissafejteni a rejtjelezett szöveget és tud hozzáférni az eredeti egyszerű szöveghez, aki a privát kulcs birtokában van.

A publikus kulcsú kriptográfiát számos alkalmazásban alkalmazzák, például a HTTPS (*Hypertext Transfer Protocol Secure*) segítségével történő biztonságos webböngészésnél, az S/MIME vagy PGP segítségével történő biztonságos e-mailezésnél, valamint a digitális dokumentumok hitelességét és integritását biztosító digitális aláírásoknál.

A nyilvános kulcsú kriptográfiában az RSA és a DSA két széles körben használt algoritmus. Az RSA-t az alkotókról (Ron Rivest, Adi Shamir és Leonard Adleman) nevezték el, míg a DSA a *Digital Signature Algorithm* (digitális aláírási algoritmus) rövidítése. Az elliptikus görbületű kriptográfia, egy újabb fejlesztés, amely az *Elliptic Curve Digital Signature Algorithm* (ECDSA) algoritmust foglalja magában.

OpenPGP

Amint az OpenPGP weboldaláról megtudhatjuk, ez a technológia eredetileg a Phil Zimmermann által létrehozott PGP szoftverből származik. Ma az OpenPGP a legszélesebb körben használt e-mail titkosítási szabvány. A működésének bemutatásához a *GNU Privacy Guard* (GnuPG vagy röviden GPG), egy ingyenes OpenPGP implementációt fogunk használni az adatok és a kommunikáció titkosítására és digitális aláírására. A GPG-t a GNU General Public License feltételei szerint adják ki.

A GPG szimmetrikus és aszimmetrikus kulcsú kriptográfiát egyaránt használhat. A támogatott algoritmusok közül talán az AES a legismertebb a szimmetrikus titkosításhoz, míg az RSA-t és az ECDSA-t a GPG leggyakrabban aszimmetrikus titkosításhoz használja.

Kezdjük egy terminál megnyitásával és egy egyszerű szöveges üzenetet tartalmazó fájl szimmetrikus titkosításával:

```
$ echo "Hello world" > message_file.txt
$ gpg --symmetric message_file.txt
```

A rendszer kétszer kéri a jelszót (passphrase), és létrehozza a titkosított `message_file.txt.gpg` fájlt. Ha most megpróbáljuk elolvasni a szöveget, akkor valami az alábbihoz hasonló zagyvaságot látunk:

```
$ cat message_file.txt.gpg
???_?#?[??Qw?h:0???V?)??z/LBzL>?Q$??#U.srm[?.3?O??V?p!\@!J?w?|??90?,R??
```

A titkosítás feloldásához egyszerűen használjuk a `--decrypt` kapcsolót, és adjuk meg a jelszót, amikor a rendszer kéri:

```
$ gpg --decrypt message_file.txt.gpg
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
Hello world
```

Az üzenetet egyetlen parancsban is aláírhatjuk és titkosíthatjuk (feltéve, hogy korábban már létrehoztunk egy privát kulcsot):

```
$ gpg --sign --symmetric message_file.txt
```

Egy szinttel feljebb léphetünk, és használhatjuk a GPG-t kifinomultabb módon is úgy, hogy az üzenet aszimmetrikusan titkosítjuk egy adott címzett számára. Ehhez létre kell hoznunk egy kulcspárt. Bár a lecke későbbi részében megtanuljuk, hogyan lehet könnyen kulcspárt létrehozni a Mozilla Thunderbird segítségével, érdemes megjegyezni, hogy a parancssorban az `gpg`-t is használhatjuk ehhez:

```
$ gpg --full-generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
```

```
There is NO WARRANTY, to the extent permitted by law.

gpg: directory '/home/carol/.gnupg' created
gpg: keybox '/home/carol/.gnupg/pubring.kbx' created
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
  (14) Existing key from card
Your selection?
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072)
Requested keysize is 3072 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0)
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Carol Doe
E-mail address: carol.doe@example.com
Comment: Generating keys is fun!
You selected this USER-ID:
    "Carol Doe (Generating keys is fun!) <carol.doe@example.com>"

Change (N)ame, (C)omment, (E)-mail or (O)kay/(Q)uit? O

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilise the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: /home/carol/.gnupg/trustdb.gpg: trustdb created
gpg: key 683714AD69979321 marked as ultimately trusted
gpg: directory '/home/carol/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/carol/.gnupg/openpgp-
```

```
revocs.d/FFA136F2E1B69CAA35DE55CE683714AD69979321.rev'
public and secret key created and signed.

pub   rsa3072 2023-05-03 [SC]
      FFA136F2E1B69CAA35DE55CE683714AD69979321
uid                      Carol Doe (Generating keys is fun!) <carol.doe@example.com>
sub   rsa3072 2023-05-03 [E]
```

Kész! A kulcspárunk készen áll. A kulcspár létrehozásának további, gyorsabb lehetőségei a `--quick-generate-key` és a `--generate-key`.

NOTE Talán a legfontosabb `gpg` kapcsoló a `--help`, mert minden szükséges opciót és információt biztosít.

Az aszimmetrikus titkosítás azt jelenti, hogy az üzenetet a mi privát kulcsunkkal és a címzett publikus kulcsával együtt titkosítjuk, így az üzenet csak a címzett privát kulcsával dekódolható. Ehhez szükség van a címzett publikus kulcsára. Ez meg lehet osztva velünk, vagy — ami még gyakrabban előfordul --, publikus kulcsú szervereken kereshetjük meg. Ez a téma egyenesen a következő fejezetünkhöz vezet minket.

Az OpenPGP kulcsszerverek szerepe

Az OpenPGP kulcsszerverek elsődleges funkciója a nyilvános kulcsok tárolása és elérhetővé tétele bárki számára, aki biztonságosan kíván kommunikálni a kulcs tulajdonosával. Amikor egy felhasználó titkosított e-mailt akar küldeni vagy digitális aláírást ellenőrizni, megkeresheti a címzett nyilvános kulcsát a kulcsszerveren, így biztosítva, hogy a titkosítási folyamat manuális kulcscsere nélkül folytatódhasson.

A kulcsszerverek nyilvános kriptográfiai kulcsokat tárolnak és szolgáltatnak, és publikus kulcsok cseréjére szolgálnak. A szabványos eljárás a következő (tételezzük fel, hogy két felhasználó van, Carol és John):

1. Carol létrehoz egy kulcspárt (publikus és privát) a GPG segítségével.
2. Carol megtartja a privát kulcsot.
3. Carol exportálja (feltölti) a publikus kulcsát egy nyilvános kulcsszerverre, hogy John használhassa azt.
4. John importálja (letölti) Carol publikus kulcsát a kulcstartójába.

Most John aszimmetrikusan aláírhat egy olyan üzenetet, amelyet csak Carol privát kulcsával lehet visszafejteni.

NOTE

A publikus kulcs általában egy kriptográfiai tanúsítványfájlban található, amely nemcsak a kulcsot, hanem a tulajdonosára vonatkozó információkat is tartalmaz.

S/MIME

Az S/MIME az e-mail kliensek túlnyomó többsége (például az Apple Mail, a Microsoft Outlook és a Mozilla Thunderbird) által támogatott szabványos protokoll az e-mailek védelmére és hitelesítésére nyilvános kulcsú kriptográfiával: titkosítással és digitális aláírással. Így az S/MIME biztosítja az e-mailek titkosságát, integritását és hitelességét.

A következő kifejezéseket gyakran összekeverik, ezért fontos, hogy tisztában legyünk azzal, hogy mit jelentenek:

Titoktartás (confidentiality)

Az üzenetet címzettnek kell visszafejtenie és csak neki kell elolvasnia. Ez titkosítással érhető el.

Integritás (integrity)

Az üzenetnek pontosan úgy kell célba érnie, ahogyan megírták (megváltoztatlanul). Ezt a digitális aláírással érjük el.

Hitelesség (authenticity)

A feladó és a címzett személyazonosságát ellenőrizni kell. Ez az e-mailek digitális aláírásával és ellenőrzésével érhető el a feladó privát, valamint a címzett publikus kulcsának felhasználásával.

Az S/MIME végponttól végpontig (end-to-end) tartó biztonságot nyújt az e-mail alapú kommunikációhoz. A feladó az e-mailt a címzett publikus kulcsával titkosítja, így az csak a címzett privát kulcsával dekódolható. Ez rendkívül fontos, mivel garantálja, hogy az üzenetet csak a címzett olvashatja, és azt nem módosíthatják illetéktelenek az útja során.

Az S/MIME emellett digitális aláírást is biztosít, amely lehetővé teszi a küldők számára, hogy üzeneteiket digitálisan aláírják saját privát kulcsukkal, a címzettek pedig ellenőrizhetik, hogy az üzenet az állítólagos feladótól származik. Ez a következő módon történik: A feladó digitális aláírást hoz létre az üzenet kivonatának a saját privát kulcsával történő titkosításával. A címzett ezután úgy tudja ellenőrizni az aláírást, hogy a hash-t a feladó publikus kulcsával visszafejti és összehasonlítja azt a saját maga által kiszámított hash értékkel.

NOTE

Egy hash-függvény bemeneti adatokat vagy üzenetet vesz fel, és algoritmusok sorát alkalmazza rá, hogy egyedi, rögzített hosszúságú kimenetet hozzon létre: karakterek vagy bitek sorozatát, amelyet *message digest*, *hash code* vagy egyszerűen *hash* néven ismerünk. Ezt az eredményként kapott hasht ezután

általában a bemeneti adatok integritásának érvényesítésére használják. A hashelés egyik előnye, hogy lehetővé teszi az adatok gyors és hatékony összevetését anélkül, hogy az adatok teljes tartalmát össze kellene hasonlítani.

A tanúsítványok szerepe az S/MIME esetében

Az S/MIME használatához mind a feladónak, mind a címzettnek rendelkeznie kell S/MIME-képes e-mail klienssel és egy megbízható hitelesítésszolgáltató által kiállított digitális tanúsítvánnyal. A tanúsítvány a tulajdonos publikus kulcsán kívül más fontos azonosító információkat is tartalmaz, és a tulajdonos identitásának, valamint a publikus kulcs hitelességének igazolására szolgál.

Egyes hitelesítésszolgáltatók egy évig ingyenesen biztosítják az S/MIME digitális tanúsítványokat. Az OpenSSL segítségével mi magunk is készíthetünk saját aláírású tanúsítványt.

A PGP kulcsok és az S/MIME tanúsítványok e-mail címhez való társulása

Mint már említettük, a PGP-t és az S/MIME-t egyaránt használják e-mail titkosításra és digitális aláírásra. Abban azonban különböznek egymástól, hogy kulcsokat vagy tanúsítványokat társítanak egy e-mail címhez.

A PGP megköveteli, hogy a felhasználó létrehozzon egy PGP-kulcspárt, és a publikus kulcsot az e-mail kliensben hozzárendelje az e-mail címéhez. Ez általában úgy történik, hogy a publikus kulcsot egy kulcsszerveren osztják meg. Más felhasználók ezután megkereshetik a kulcsszerven a felhasználó e-mail címéhez társított publikus kulcsot, és azt használhatják a felhasználónak szánt titkosított üzenetek küldésére.

Másrészről az S/MIME tanúsítványokat használ a publikus kulcs és az e-mail cím összekapcsolására. A digitális tanúsítványt egy megbízható hitelesítésszolgáltató állítja ki, amely ellenőrzi a felhasználó identitását és a publikus kulcs hitelességét. A felhasználónak az e-mail kliensében rendelkeznie kell a digitális tanúsítvánnyal. A tanúsítvány tartalmazza a felhasználó publikus kulcsát, valamint egyéb azonosító adatokat, többek között az e-mail címet. Más felhasználók ezután ellenőrizhetik a felhasználó digitális aláírását, az e-mail címéhez tartozó nyilvános kulcs segítségével pedig titkosíthatják a felhasználónak küldött üzeneteket.

A Mozilla Thunderbird használata titkosított e-mailek küldésére és fogadására

A Mozilla Thunderbird egy multiplatform, ingyenes és nyílt forráskódú e-mail kliens, amely end-to-end e-mail titkosítást végez, és integrálja az OpenPGP és az S/MIME protokollt, valamint

beépített kulcskezelési funkciókat. A következő alfejezetek bemutatják, hogyan lehet a Thunderbirdöt konfigurálni az e-mailek aszimmetrikusan titkosításához és dekódolásához.

Az utasítások feltételezik, hogy a Thunderbird telepítve van a rendszeren, és hogy egy e-mail fiók már be van állítva.

OpenPGP konfigurálása és kulcspár generálása

Miután létrehoztuk a fiókunkat, lépjünk az “Inbox” fülre és kattintsunk a fogaskerék ikonra (“Settings”) a bal alsó sarokban. Ezután a “Settings” fülön kattintsunk az “Account Settings”-re, majd végül a “End-To-End Encrypion”-ra. Ez a End-To-End Encryption képernyő.

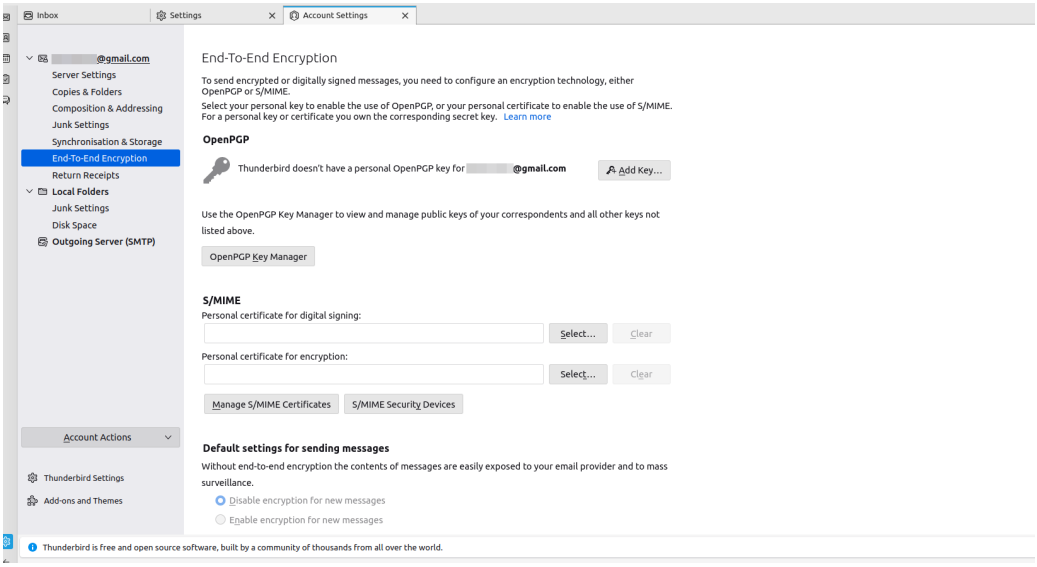

Figure 7. End-To-End Encryption képernyő

Jelenleg nem állnak rendelkezésre kulcsok a fiókunkhoz (vagy S/MIME személyes tanúsítványok), ezért kattintsonunk az “Add key...” gombra. Most választhatunk, hogy importálunk egy meglévő OpenPGP kulcsot az e-mail címünkhöz, vagy létrehozunk egy új OpenPGP kulcsot a semmiből. Mi a második lehetőséget választjuk: (Új PGP kulcspár létrehozása).

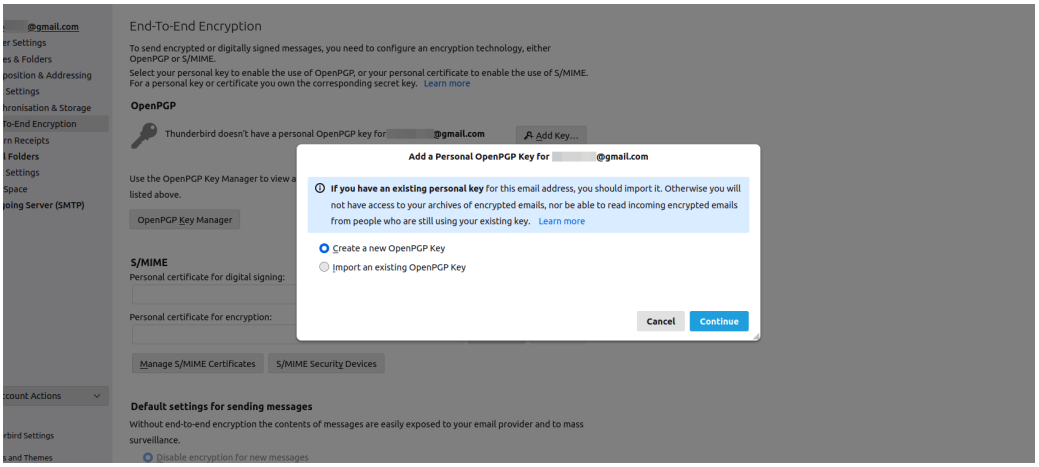

Figure 8. Új PGP kulcspár létrehozása

Ezután el kell végeznünk néhány konfigurációs műveletet, például ki kell választani a kulcs lejárati idejét, a kulcstípust és a kulcs méretét: (Kulcspár konfigurálása).

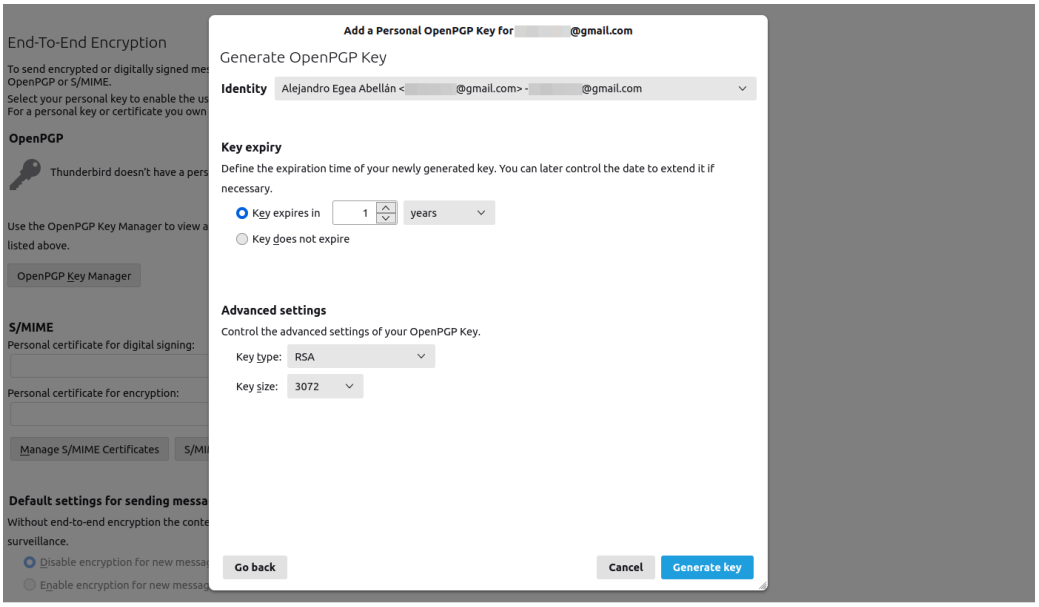

Figure 9. Kulcspár konfigurálása

Végül tájékoztatást kapunk a kulcsgeneráláshoz szükséges időről és meg kell erősítenünk a műveletet: (A kulcspár létrehozásának megerősítése).

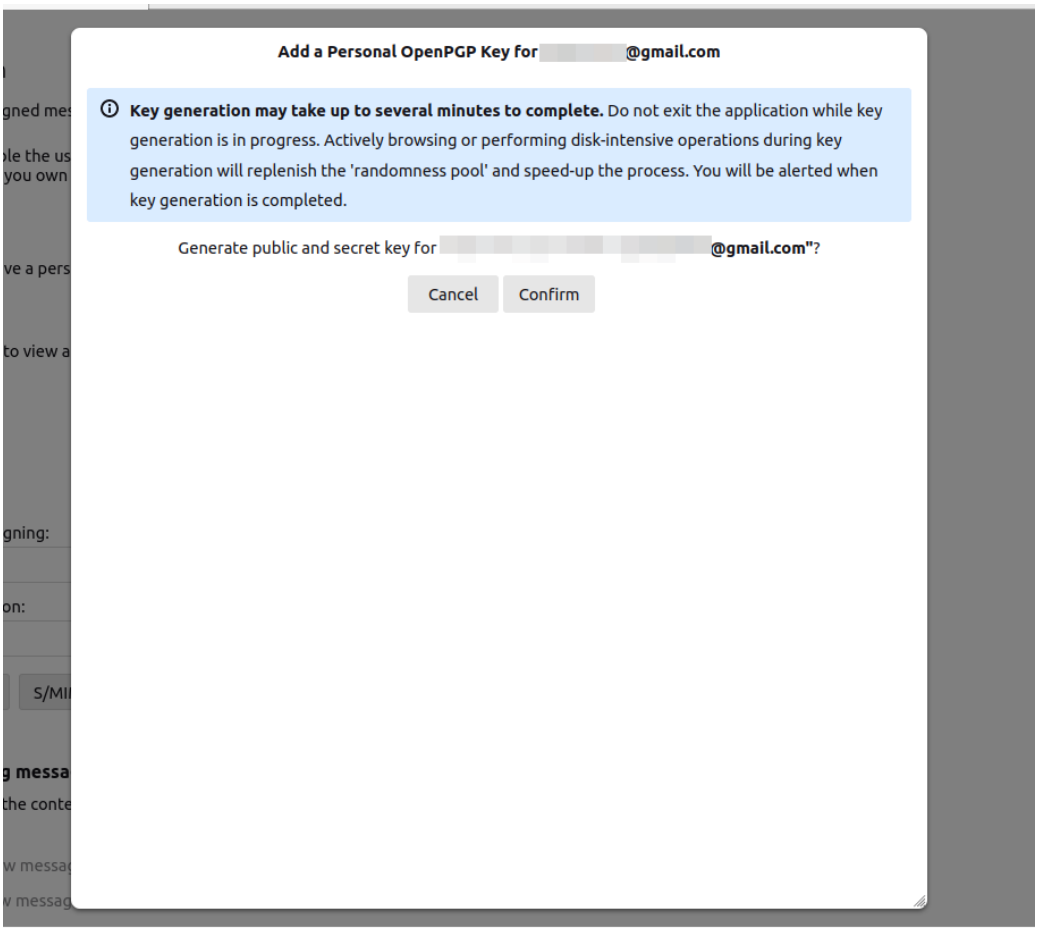

Figure 10. A kulcspár létrehozásának megerősítése

A kulcspárnak létre kellett jönnie: (A kulcspár sikeresen generálva).

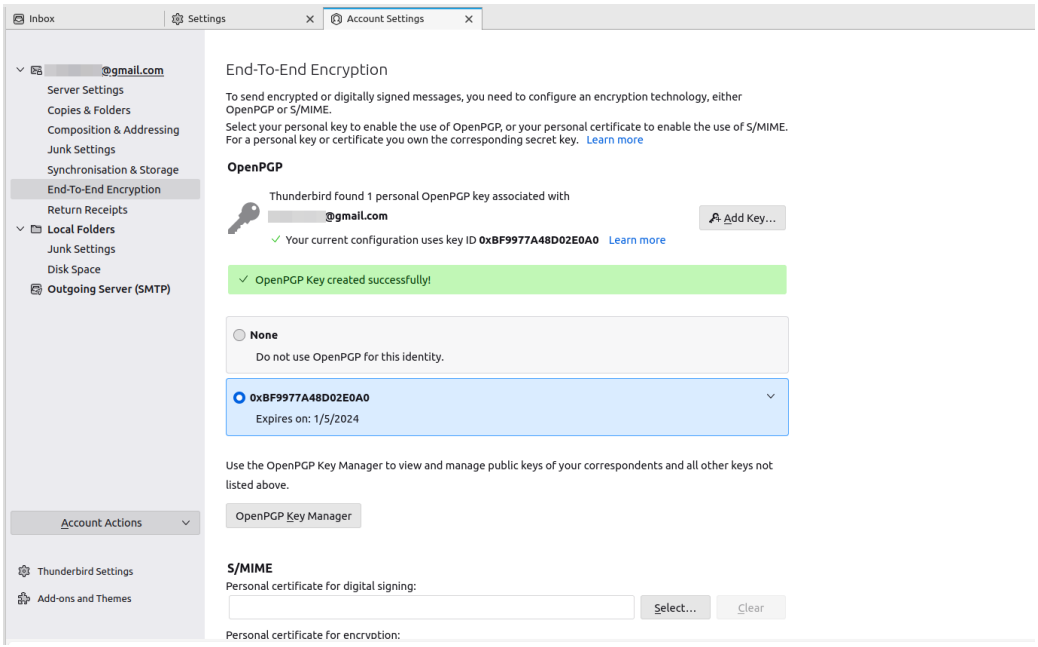

Figure 11. A kulcspár sikeresen generálva

Most a “OpenPGP Key Manager”-ra kattintva számos dolgot beállíthatunk, például egy kulcsszervert, amelyet a potenciális címzettek publikus kulcsainak keresésére használhatunk: (Kulcsmenedzser felülete).

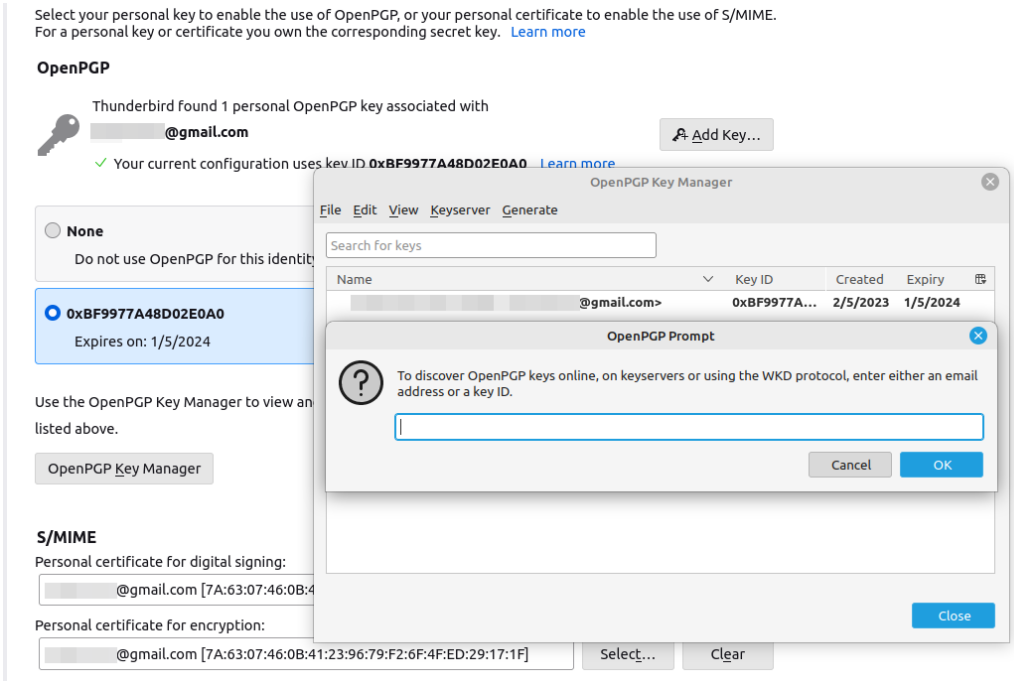

Figure 12. Kulcsmenedzser felülete

S/MIME konfigurálása és tanúsítvány importálása

Most az S/MIME-re térünk rá. Az S/MIME segítségével történő digitális aláíráshoz és titkosításhoz szükséges érvényes X.509 tanúsítvány beszerzésével és importálásával kezdjük. Az egyszerűség kedvéért beszerezhetünk ingyenes tanúsítványt egy megbízható CA-tól. (A magunk számára, saját aláírású tanúsítvány generálása nem tartozik ennek a leckének a tárgykörébe). Ha kész vagyunk, kattintsunk a “Manage S/MIME Certificates”-ra, keressük meg a tanúsítványt a helyi meghajtón, és importáljuk azt. Ha jelszót kér, adjuk meg azt az Jelszó megadása tanúsítvány importálásakor ábrán látható módon.

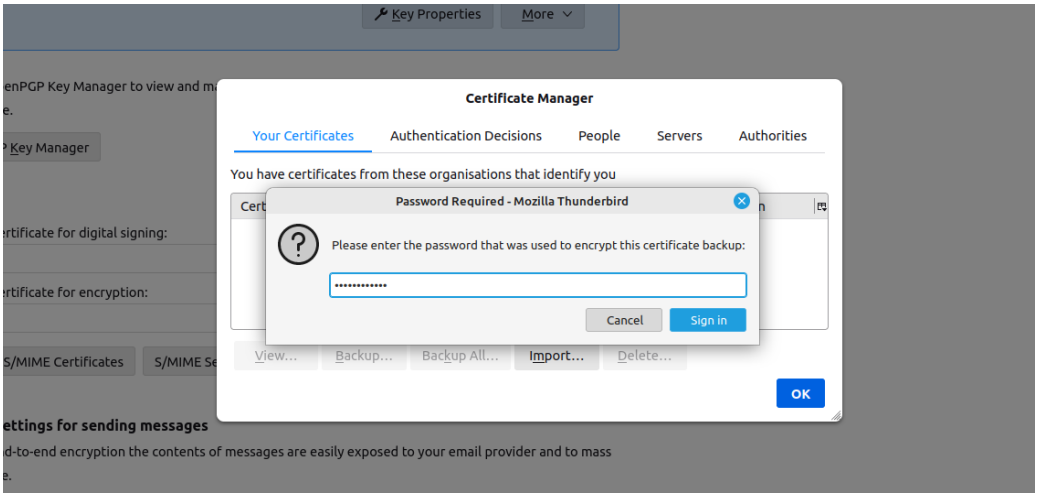

Figure 13. Jelszó megadása tanúsítvány importálásakor

Majd válasszuk ki a tanúsítványunkat: (S/MIME tanúsítvány kiválasztása).

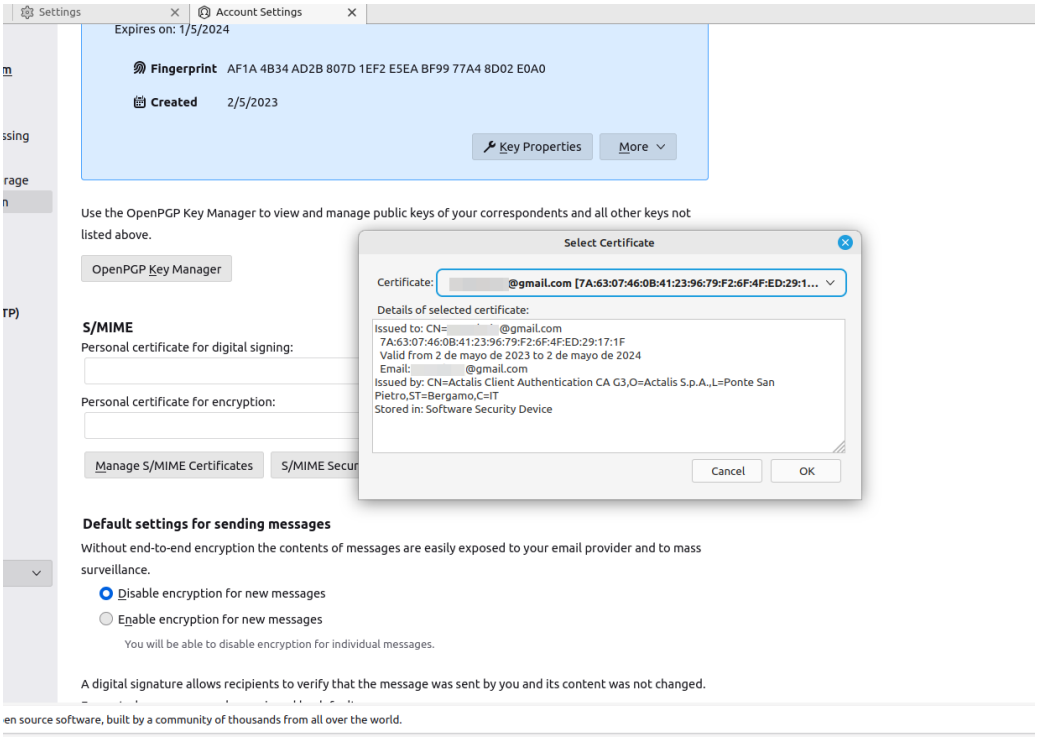

Figure 14. S/MIME tanúsítvány kiválasztása

Ezután egy második tanúsítványt kér, amelyet mások fognak használni, amikor titkosított üzeneteket küldenek nekünk. Választhatjuk ugyanazt a tanúsítványt:S (Második tanúsítvány kiválasztása).

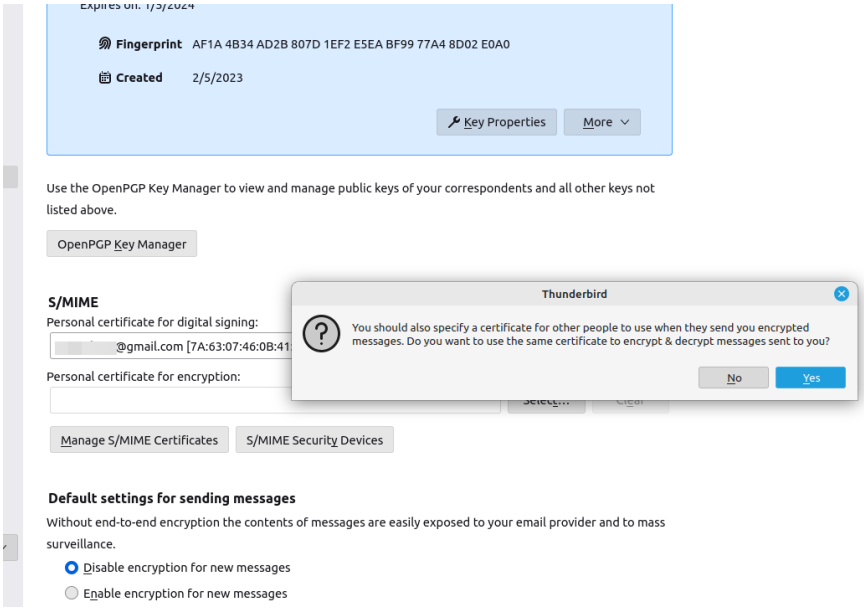

Figure 15. Második tanúsítvány kiválasztása

Végül ellenőrizhetjük, hogy a tanúsítvány mind a digitális aláírásra, mind a titkosításra ki van-e

választva: (Tanúsítványok használatra készen).

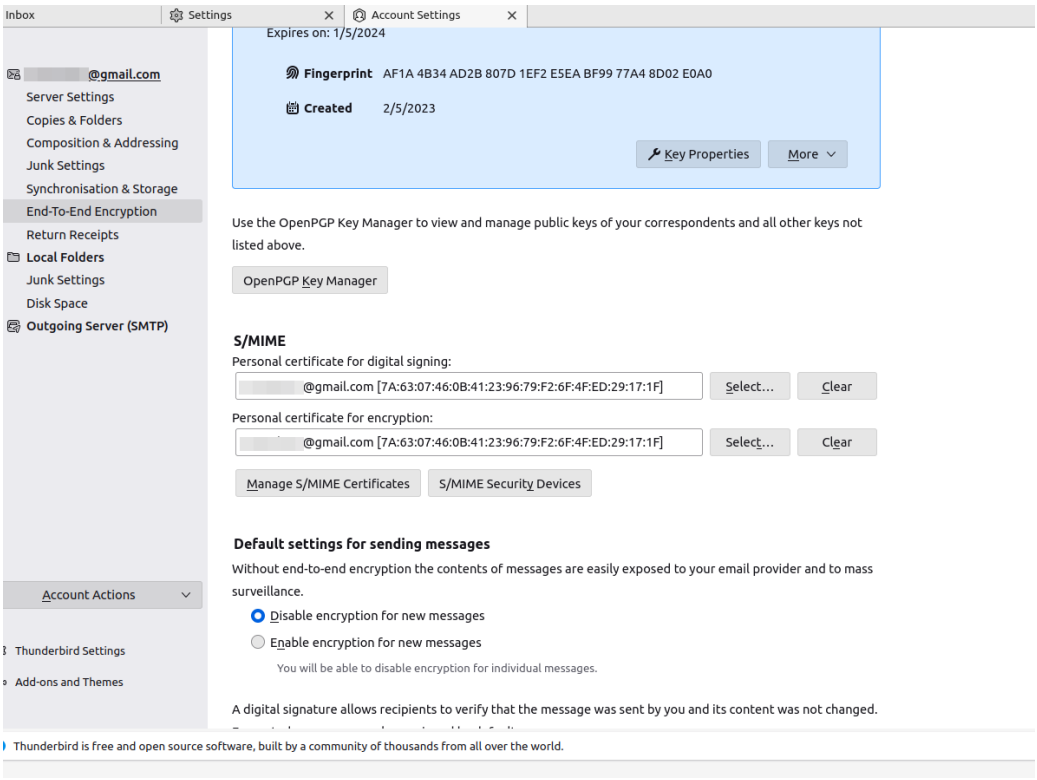

Figure 16. Tanúsítványok használatra készen

Most, hogy mind az OpenPGP, mind az S/MIME beállításait elvégeztük, az oldal aljára lépve kiválaszthatjuk a kívánt titkosítási technológiát: OpenPGP, S/MIME vagy automatikus választás a rendelkezésre álló kulcsok vagy tanúsítványok alapján: (Előnyben részesített titkosítási technológia).

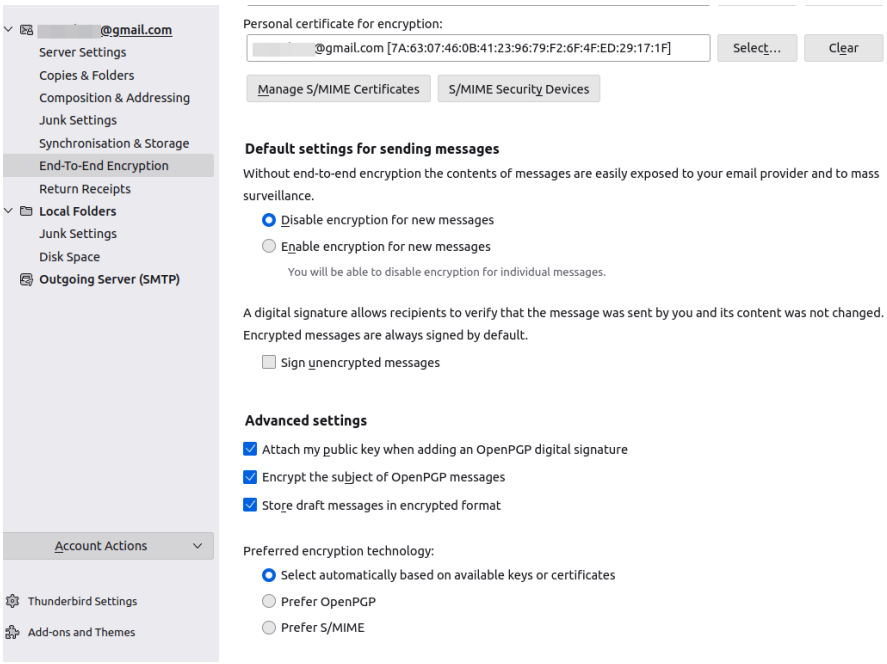

Figure 17. Előnyben részesített titkosítási technológia

Titkosított e-mailek küldése és fogadása az OpenPGP-vel

Ha megpróbálunk üzenetet küldeni valakinek, akinek ismerjük a publikus kulcsát, a Thunderbird tudatja velünk, hogy az e-mail titkosítás elérhető, és használhatjuk azt. A következő, A titkosítás akkor lehetséges, ha rendelkezünk a címzett publikus kulcsával ábra mutatja az e-mail alján megjelenő üzenetet. A felület meglehetősen felhasználóbarát.

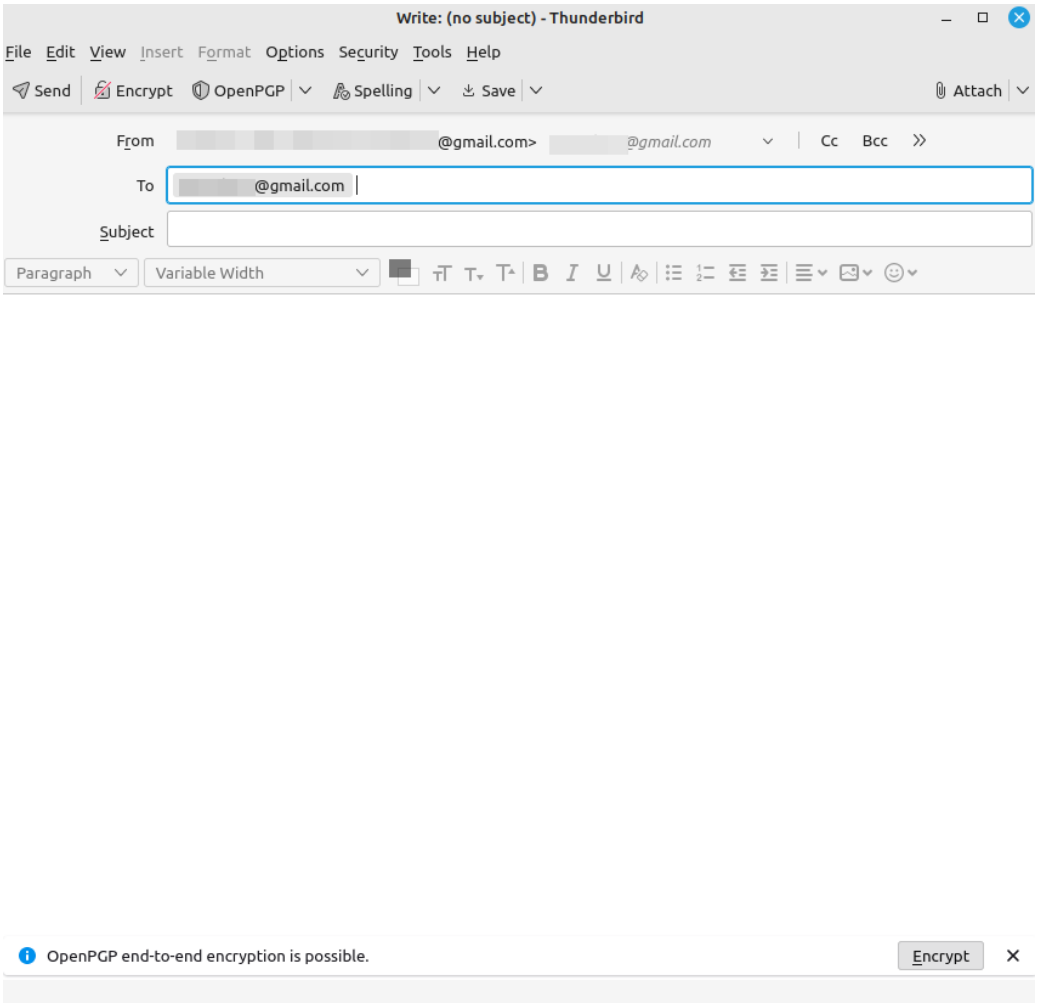

Figure 18. A titkosítás akkor lehetséges, ha rendelkezünk a címzett publikus kulcsával

Tehát ha küldünk magunknak egy üzenetet a “Testing email encryption” tárggyal és a “Hi! Bye!” szöveggel, akkor képesek leszünk megnyitni és elolvasni azt. A képernyő jobb oldalán kattintsunk az “OpenPGP” gombra, hogy információt kapjunk a kulcsról: (PGP által titkosított e-mail küldése és fogadása).

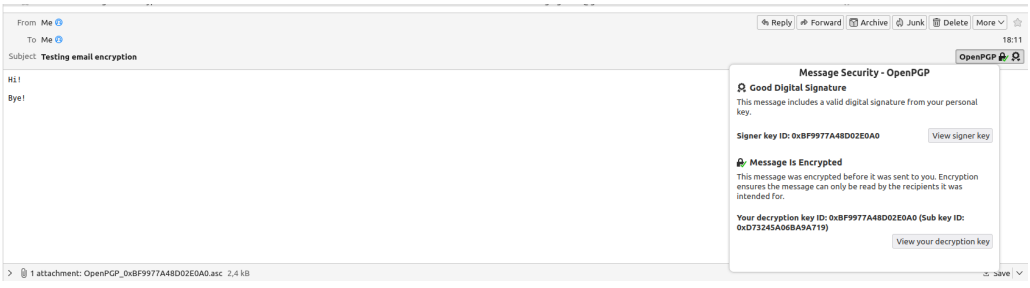

Figure 19. PGP által titkosított e-mail küldése és fogadása

Másrészt, ha olyan címzettnek próbálunk üzenetet küldeni, akinek a publikus kulcsa nincs a kulcstartónkban, akkor egy olyan üzenetet kapunk, amely arra figyelmeztet, hogy a titkosítás nem

lehetséges: (A titkosítás csak akkor lehetséges, ha van használható kulcsunk a címzetthez).

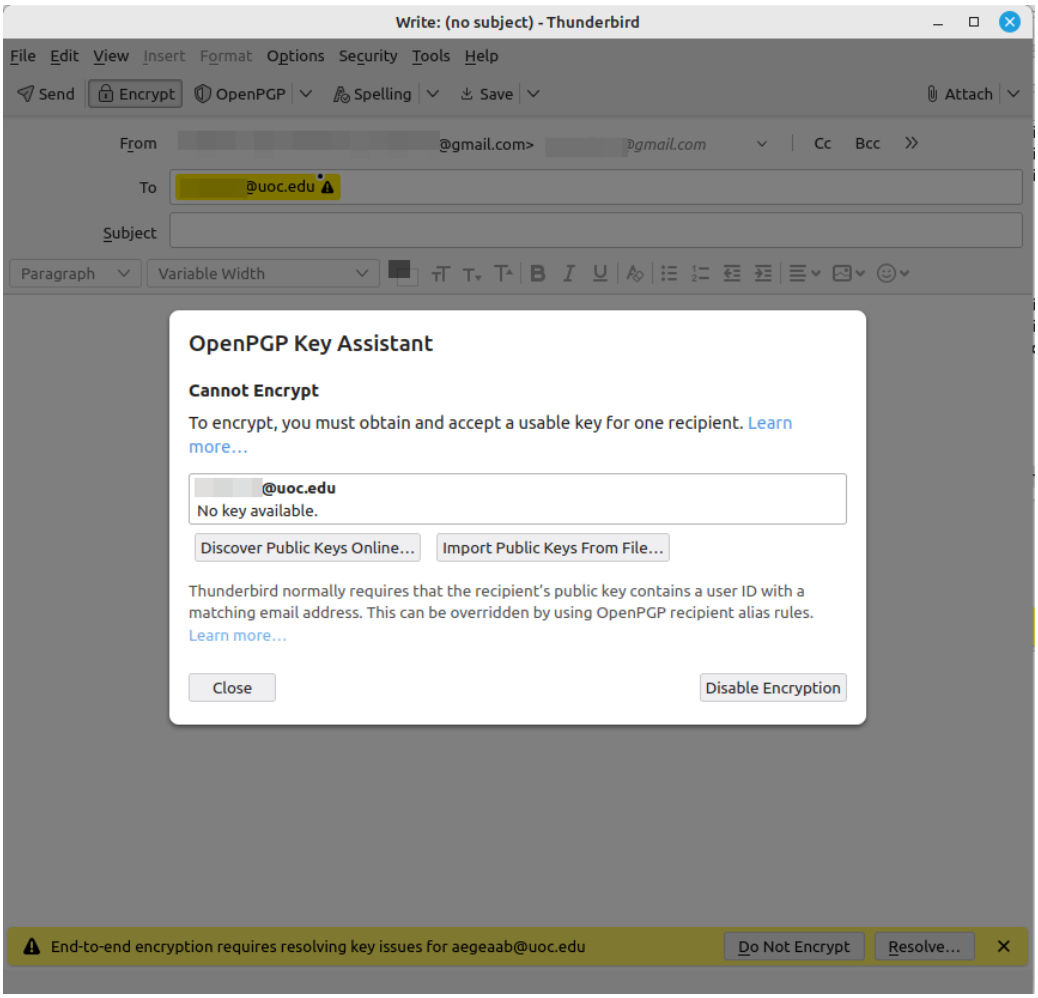

Figure 20. A titkosítás csak akkor lehetséges, ha van használható kulcsunk a címzetthez

Publikus kulcsokat importálhatunk fájlokból, vagy megkereshetjük őket a kulcsszervereken.

Titkosított e-mailek küldése és fogadása S/MIME-vel

Hasonlóan az előző részben látottakhoz, a Thunderbird lehetővé teszi, hogy titkosított e-mailt küldjünk valakinek, akinek rendelkezünk a tanúsítványával: (A titkosítás akkor lehetséges, ha rendelkezünk a címzett érvényes tanúsítványával).

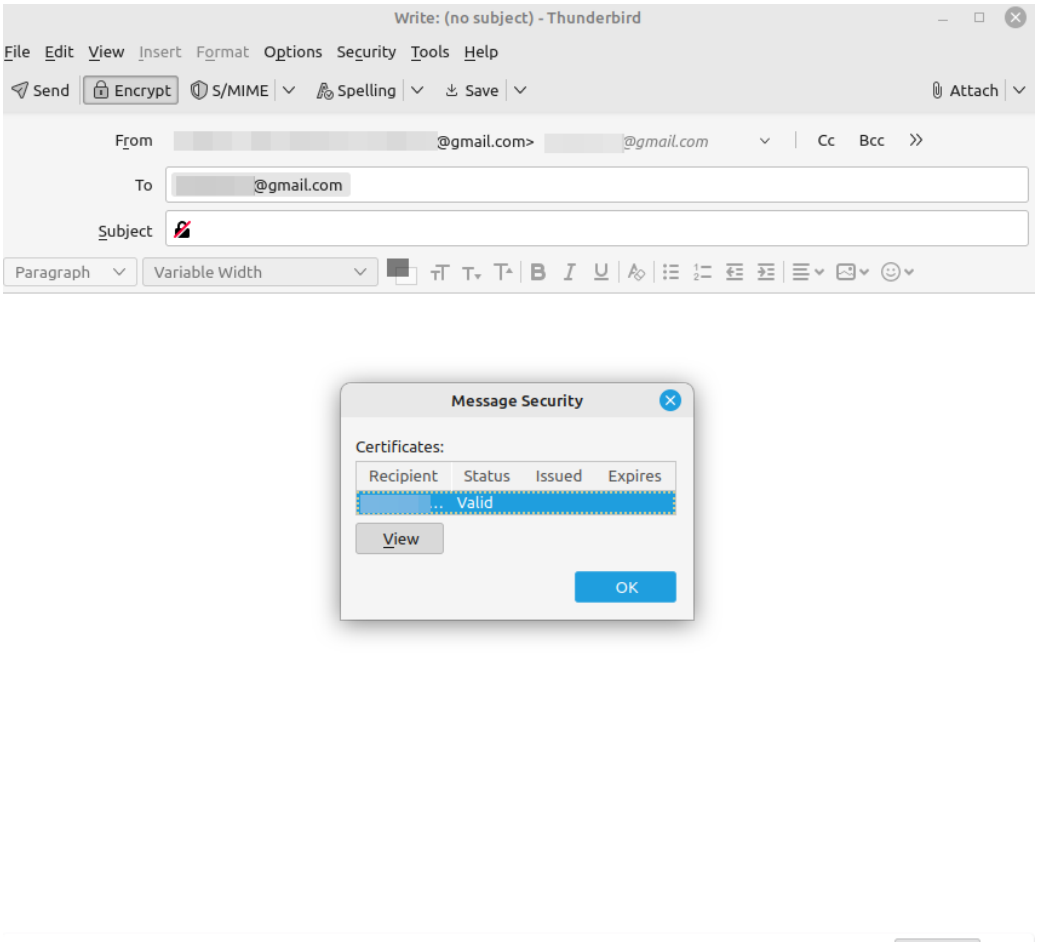

Figure 21. A titkosítás akkor lehetséges, ha rendelkezünk a címzett érvényes tanúsítványával

Küldhetünk magunknak egy üzenetet a “Retesting email encryption” tárggyal és a korábbi szöveggel. Ismét meg tudjuk majd nyitni, el tudjuk olvasni, és a jobb oldali “S/MIME” gombra kattintva láthatjuk az S/MIME biztonsági információkat: (S/MIME által titkosított e-mailek küldése és fogadása).

Figure 22. S/MIME által titkosított e-mailek küldése és fogadása

Ha olyan címzettnek próbálunk üzenetet küldeni, akinek a tanúsítványával nem rendelkezünk, egy figyelmeztető üzenet tájékoztat erről: (A kulcsokkal való problémák megoldása szükséges az end-to-end titkosításhoz).

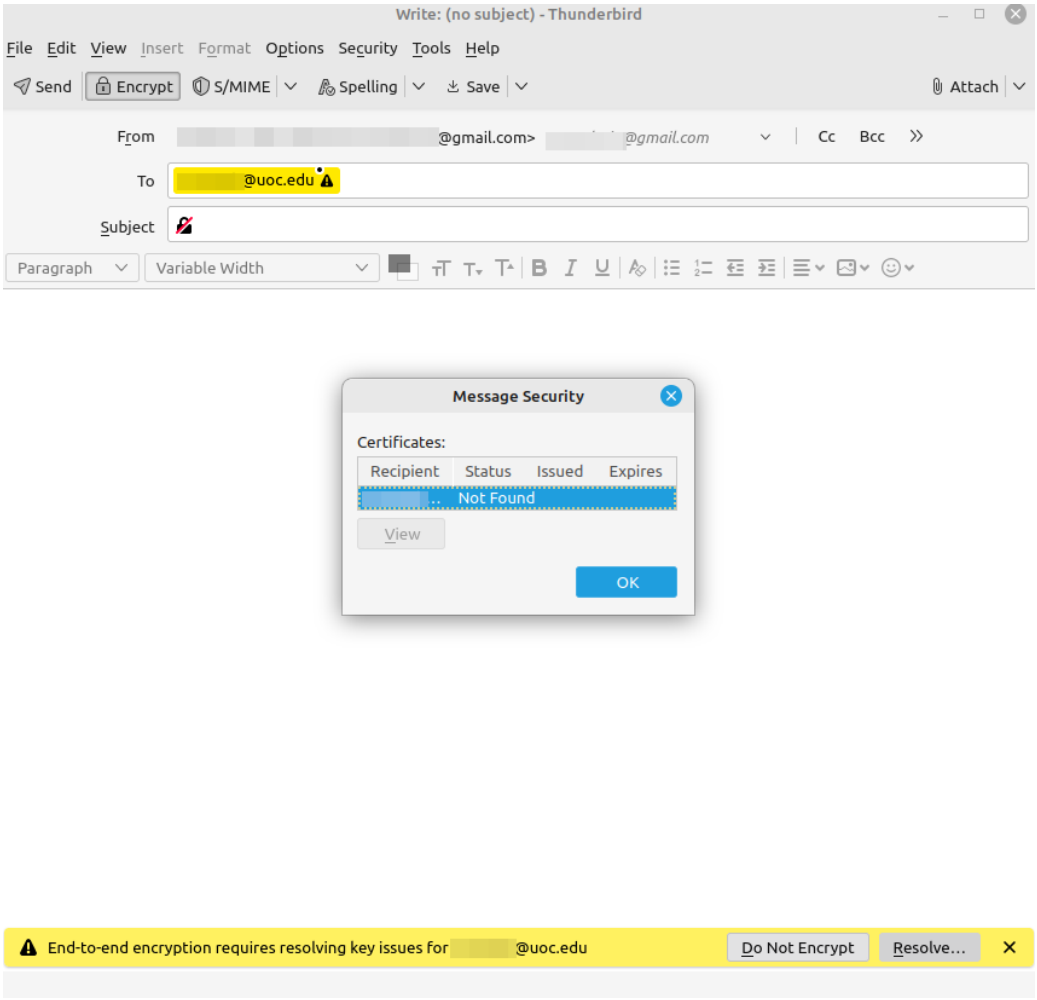

Figure 23. A kulcsokkal való problémák megoldása szükséges az end-to-end titkosításhoz

Gyakorló feladatok

1. A nyilvános kulcsú kriptográfia egy publikus és egy privát kulcsból álló kulcspáron alapul. Jelöljük meg, hogy az alábbi állítások melyik kulcstípusnak felelnek meg:

Állítás	**Publikus vagy privát kulcs?**
Bárki számára elérhető, aki titkosított e-mailt szeretne küldeni	
Nem szabad megosztani senkivel	
Plain text típusú üzenetre alkalmazható, hogy rejtjelezett szöveget kapjunk	
E-mail visszafejtésére használható	
Importálható a kulcstartónkba	

2. Jelöljük meg, hogy az alábbi állítások az alábbi koncepciók közül melyiknek felelnek meg: szimmetrikus kriptográfia, rejtjelezett szöveg (ciphertext), hitelesítésszolgáltatók, digitális aláírás, Mozilla Thunderbird, ECDSA, titkosítás, kulcspár, GPG, S/MIME.

Állítás	**Koncepció**
Egy publikus kulcs és a hozzá tartozó privát kulcs	
A titkosításhoz és a visszafejtéshez is ugyanazt a kulcsot használják	
Megbízható harmadik fél, amely digitális tanúsítványokat állít ki, von vissza és kezel	
Egy digitális dokumentum hitelességének és sértetlenségének ellenőrzésére szolgál	
Az OpenPGP ingyenes implementációja	
Digitális aláírások létrehozására és ellenőrzésére szolgáló kriptográfiai algoritmus	
Érthetetlenné tett üzenet	
Egy biztonsági protokoll, amely garantálja az end-to-end titkosítást	

Állítás	**Koncepció**
Garantálja, hogy az üzenetet csak a címzett olvassa el	
Ingyenes és nyílt forráskódú, többplatformos e-mail kliens, amely támogatja az end-to-end titkosítást	

Gondolkodtató feladatok

1. Az előző szakasz utolsó feladatában megnevezett három felhasználási eset mellett nevezzünk meg két olyan adatcsere-protokollt, amely aszimmetrikus kriptográfiát használ! Magyarázzuk el röviden, hogyan működnek!

2. Milyen protokollok garantálhatják a biztonságos e-mail-váltást?

3. Milyen protokollok garantálhatják a biztonságos webböngészést?

 | |

Összefoglalás

Ez a lecke a mai digitális világban kritikus fontosságú e-mail titkosítást vizsgálja, két széles körben használt protokollra összpontosítva: OpenPGP és S/MIME. Ezek a titkosítási szabványok biztosítják az e-mail kommunikáció titkosságát, integritását és hitelességét, védelmet nyújtva a jogosulatlan hozzáférés ellen. Az OpenPGP egy decentralizált bizalmi modell alapján működik, ahol a felhasználók maguk kezelik a titkosítási kulcsaikat, míg az S/MIME egy központosított bizalmi modellt használ, amely mögött megbízható hitelesítésszolgáltatók (CA-k) által kiadott digitális tanúsítványok állnak. Mindkét protokoll lehetővé teszi a titkosítást, megakadályozva, hogy illetéktelenek elolvashassák az e-mail tartalmát, valamint digitális aláírást kínálnak a feladó személyazonosságának igazolására.

A lecke a népszerű e-mail kliens, Mozilla Thunderbird gyakorlati konfigurációját is tárgyalja, amely támogatja az OpenPGP és az S/MIME end-to-end titkosítást.

Válaszok a gyakorló feladatokra

1. A nyilvános kulcsú kriptográfia egy publikus és egy privát kulcsból álló kulcspáron alapul. Jelöljük meg, hogy az alábbi állítások melyik kulcstípusnak felelnek meg:

Állítás	**Publikus vagy privát kulcs?**
Bárki számára elérhető, aki titkosított e-mailt szeretne küldeni	publikus kulcs
Nem szabad megosztani senkivel	privát kulcs
Plain text típusú üzenetre alkalmazható, hogy rejtjelezett szöveget kapjunk	publikus kulcs
E-mail visszafejtésére használható	privát kulcs
Importálható a kulcstartónkba	publikus kulcs

Jelöljük meg, hogy az alábbi állítások az alábbi koncepciók közül melyiknek felelnek meg: szimmetrikus kriptográfia, rejtjelezett szöveg (ciphertext), hitelesítésszolgáltatók, digitális aláírás, Mozilla Thunderbird, ECDSA, titkosítás, kulcspár, GPG, S/MIME.

+

Állítás	**Koncepció**
Egy publikus kulcs és a hozzá tartozó privát kulcs	kulcspár
A titkosításhoz és a visszafejtéshez is ugyanazt a kulcsot használják	szimmetrikus kriptográfia
Megbízható harmadik fél, amely digitális tanúsítványokat állít ki, von vissza és kezel	hitelesítésszolgáltatók
Egy digitális dokumentum hitelességének és sértetlenségének ellenőrzésére szolgál	digitális aláírás
Az OpenPGP ingyenes implementációja	GPG
Digitális aláírások létrehozására és ellenőrzésére szolgáló kriptográfiai algoritmus	ECDSA
Érthetetlenné tett üzenet	rejtjelezett szöveg (ciphertext)
Egy biztonsági protokoll, amely garantálja az end-to-end titkosítást	S/MIME

Állítás	**Koncepció**
Garantálja, hogy az üzenetet csak a címzett olvassa el	titkosítás
Ingyenes és nyílt forráskódú, többplatformos e-mail kliens, amely támogatja az end-to-end titkosítást	Mozilla Thunderbird

Válaszok a gondolkodtató feladatokra

1. Az előző szakasz utolsó feladatában megnevezett három felhasználási eset mellett nevezzünk meg két olyan adatcsere-protokollt, amely aszimmetrikus kriptográfiát használ! Magyarázzuk el röviden, hogyan működnek!

   A Secure File Transfer Protocol (SFTP) és a Secure Shell (SSH) a fájlátvitelt teszi biztonságossá egy kliens és egy szerver között.

   A virtuális magánhálózat (Virtual Private Network — VPN) biztonságos és hitelesített kommunikációt biztosít távoli eszközök között egy nem biztonságos hálózaton, például az interneten keresztül.

2. Milyen protokollok garantálhatják a biztonságos e-mail-váltást?

   PGP, S/MIME.

3. Milyen protokollok garantálhatják a biztonságos webböngészést?

   SSL, TLS.

022.4 Adattárolás titkosítása

Hivatkozás az LPI célkitűzésre

Security Essentials version 1.0, Exam 020, Objective 022.4

Súlyozás

2

Kulcsfontosságú ismeretek

- Az adatok, fájlok és tárolóeszközök titkosításának megértése
- A VeraCrypt használata az adatok titkosított tárolóban vagy titkosított tárolóeszközökön történő tárolásához
- A BitLocker főbb funkcióinak megértése
- A Cryptomator használata felhőben tárolt fájlok titkosításához

A használt fájlok, kifejezések és segédprogramok részleges listája

- VeraCrypt
- BitLocker
- Cryptomator

Lecke 1

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	022 Titkosítás
Fejezet:	022.4 Adattárolás titkosítása
Lecke:	1/1

Bevezetés

A kiberbiztonság területén a tárolt (inaktív, data at rest) adatok védelme ugyanolyan fontos, mint az adatátvitel biztosítása. A fájlok és a tárolóeszközök titkosítása kulcsfontosságú gyakorlatok, amelyekkel garantálható, hogy az érzékeny információk biztonságban maradjanak, akár helyi eszközökön, akár a felhőben tárolják őket. Ezek a titkosítási módszerek az adatokat olvashatatlan formátumba alakítják át, így a védett adatokhoz csak azok férhetnek hozzá, akik a megfelelő visszafejtési kulcsok birtokában vannak. Ez az eljárás nemcsak az adatokat védi az illetéktelen hozzáféréstől lopás vagy elvesztés esetén, hanem garantálja az adatvédelmi és biztonsági előírásoknak való megfelelést is.

Ez a lecke a fájlok és tárolóeszközök titkosításának alapvető fogalmait vizsgálja, részletezve, hogy hogyan lehet az adatokat biztonságosan tárolni a helyi eszközökön és a felhőben. Emellett a fájlok és a teljes tárolóeszközök titkosításának gyakorlati módszereit is bemutatja, átfogó ismereteket nyújtva az érzékeny információk védelméhez szükséges eszközökről és technikákról a mai, egyre inkább összekapcsolt digitális környezetben.

Adat, fájl és tárolóeszköz titkosítás

Az érzékeny információkat — legyenek azok személyes, pénzügyi vagy üzleti jellegűek --, védeni kell a jogosulatlan hozzáféréstől. Az adattitkosítás az egyik legmegbízhatóbb módszer ennek a védelemnek a biztosítására, mivel az adatokat olyan kódolt formátumba alakítja át, amelyet csak a megfelelő dekódoló kulcsot birtokló, felhatalmazott felhasználók tudnak visszafejteni.

Az *adattitkosítás* (data encryption) az olvasható adatok (*plaintext*) olvashatatlan formátumba (*ciphertext*) történő átalakítását jelenti. Ez biztosítja, hogy még ha az adatokat rosszindulatú szereplők le is hallgatják vagy hozzáférnek hozzájuk, a dekódoló kulcs nélkül nem tudják megfejteni a tartalmukat. A titkosítás különböző szinteken alkalmazható, beleértve az egyes fájlokat, a teljes tárolóeszközöket és még a felhőalapú tárolási szolgáltatásokat is.

A *fájltitkosítás* (file encryption) kifejezetten az egyes fájlok titkosítására utal, így azok biztonságossá válnak még akkor is, ha eszközök között vagy nem biztonságos hálózatokon keresztül továbbítják őket. A fájltitkosításra tervezett eszközök és szoftverek biztosítják, hogy a fájlokhoz csak olyan személyek férhessenek hozzá, akik rendelkeznek a megfelelő titkosítási kulccsal vagy jelszóval. Ez a módszer különösen hasznos az érzékeny dokumentumok vagy bizalmas információk védelmére, amelyeket esetleg meg kell osztani vagy biztonsági másolatként tárolni külső meghajtókon, vagy felhőalapú tárolószolgáltatásokon.

A *tárolóeszköz-titkosítás* (storage device encryption) azonban a teljes tárolóeszközök, például merevlemezek, SSD-k, USB flash meghajtók és külső tárolóeszközök titkosítását jelenti. A titkosítás ezen formája során a tárolóeszközön lévő összes adat automatikusan titkosításra kerül, amikor a meghajtóra írják, és olvasáskor kerül visszafejtésre. Ez a módszer garantálja, hogy ha a fizikai eszköz elveszik vagy ellopják, a rajta lévő adatok biztonságban maradnak. A tárolóeszközök titkosítását általában laptopok, asztali számítógépek és mobileszközök esetében használják, hogy lopás vagy hackerkísérlet esetén védelmet nyújtson az illetéktelen hozzáférés ellen.

A *teljes lemeztitkosítás* (full disk encryption — FDE) a tárolóeszközök titkosításának egy olyan alcsoportja, amely a tárolóeszköz teljes tartalmát titkosítja, beleértve az operációs rendszert is. Ez biztosítja, hogy az eszközön lévő összes adat védve legyen, anélkül, hogy a felhasználónak be kellene avatkoznia az egyes fájlok titkosításába. Az FDE-t általában vállalati környezetben használják, ahol nagy az elveszett vagy ellopott laptopokból eredő adatvesztés kockázata. Az FDE átfogó biztonsági réteget biztosít azáltal, hogy az operációs rendszer indítása előtt hitelesítésre van szükség.

A fájlok és a tárolóeszközök titkosításának egyik kritikus aspektusa az erős titkosítási algoritmusok, például az *Advanced Encryption Standard* (AES) használata, amely biztosítja, hogy a titkosított adatokat a támadók ne tudják könnyen feltörni. Ezek a titkosítási módszerek magas szintű biztonságot nyújtanak, de csak akkor hatékonyak, ha a titkosítási kulcsokat vagy

jelszavakat megfelelően kezelik. A rossz kulcskezelési gyakorlatok, például a gyenge jelszavak vagy a titkosítási kulcsok biztonsági mentésének elmulasztása aláásható a titkosítás hatékonyságát, és adatvesztéshez vezethet.

Mivel az adattárolás egyre inkább a felhőbe költözik, a *felhőalapú tárolás titkosítása* (cloud storage encryption) az adatbiztonság alapvető részévé vált. A felhőalapú tárhelyszolgáltatók gyakran kínálnak beépített titkosítást a felhasználók adatainak védelmére az átvitel során (titkosítás az adatátvitel során) és a felhőalapú szervereken való tárolás során (titkosítás az inaktív állapotban). Egyes felhasználók azonban inkább maguk titkosítják fájljaikat, mielőtt feltöltik azokat a felhőbe, biztosítva, hogy csak ők férjenek hozzá a titkosítási kulcsokhoz.

Annak megértése, hogy hogyan és mikor kell alkalmazni a fájlok és a tárolóeszközök titkosítását, kritikus fontosságú az adatbiztonság fenntartása szempontjából mind a személyes, mind a szakmai környezetben. A titkosítás megfelelő alkalmazása biztosítja, hogy az érzékeny adatok bizalmasak maradjanak, védve legyenek a jogosulatlan hozzáféréstől, és megfeleljenek az adatvédelmi előírásoknak.

Megvizsgáljuk az olyan titkosítási eszközök gyakorlati alkalmazását, mint a *VeraCrypt*, a *BitLocker* és a *Cryptomator*. Ezek az eszközök robusztus megoldásokat kínálnak a fájlok, tárolóeszközök és felhők titkosítására, és mindegyikük egyedi, a konkrét titkosítási igényekre szabott funkciókat kínál.

A VeraCrypt használata az adatok titkosított konténerben vagy titkosított tárolóeszközön történő tárolására

A VeraCrypt keresztplatformos, támogatja a Windows, a macOS és a Linux rendszert, ami sokoldalú megoldást jelent a többféle környezetben működő egyének és szervezetek számára. Az egyik operációs rendszeren titkosított adatok egy másik operációs rendszeren is elérhetők és visszafejthetők, feltéve, hogy a megfelelő visszafejtési hitelesítő adatok rendelkezésre állnak. Ez a rugalmasság elengedhetetlen a biztonságos adattárolás fenntartásához a különböző platformokon és eszközökön.

A VeraCrypt funkcionalitásának középpontjában a *titkosított konténerek* (encrypted containers) létrehozása áll. A titkosított konténer olyan, mint egy virtuális lemez, ahol az adatok biztonságosan tárolhatók. Ez a konténer egyetlen fájlként jelenik meg a rendszerben, de miután a VeraCryptthez csatolják, úgy viselkedik, mint egy hagyományos meghajtó, ahol fájlokat lehet hozzáadni, szerkeszteni és törölni. A módszer legfontosabb előnye, hogy a konténer teljes tartalma titkosítva van, így a megfelelő visszafejtési kulcs vagy jelszó nélkül illetéktelen felhasználók nem férhetnek hozzá az adatokhoz.

Mielőtt bármilyen konténerünk lenne, a VeraCrypt fő képernyője így néz ki: A VeraCrypt fő

képernyője.

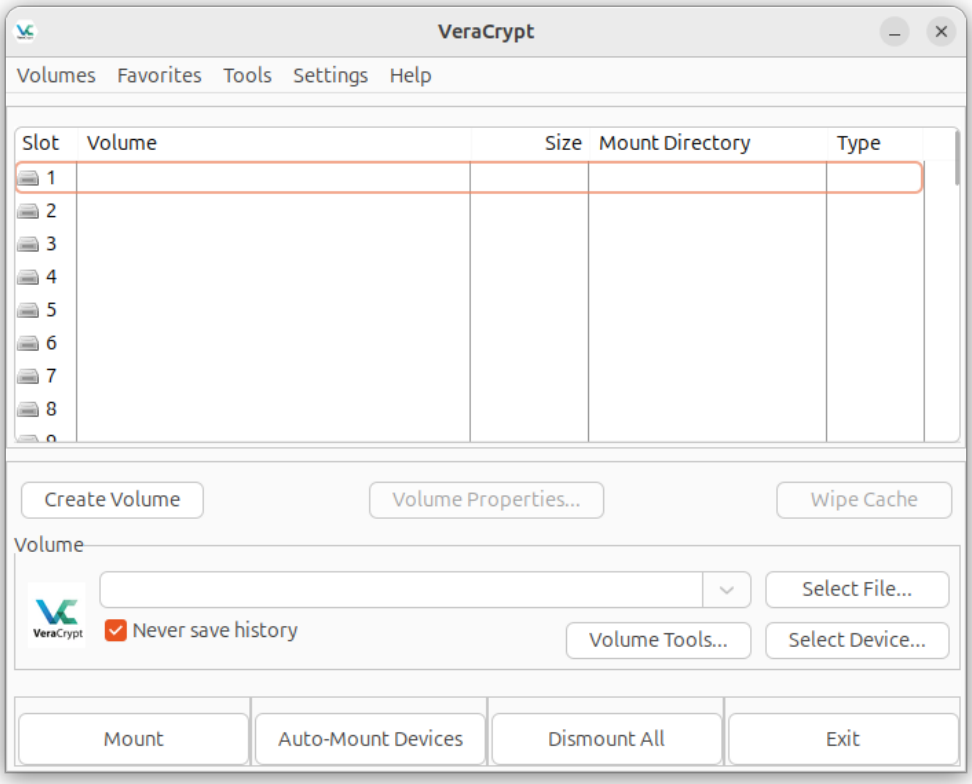

Figure 24. A VeraCrypt fő képernyője

Ha titkosított konténert szeretnénk létrehozni a VeraCrypt-ben, először is válasszuk ki a konténerként szolgáló fájlt vagy partíciót: (A VeraCryptben kiválasztott kötetfájl).

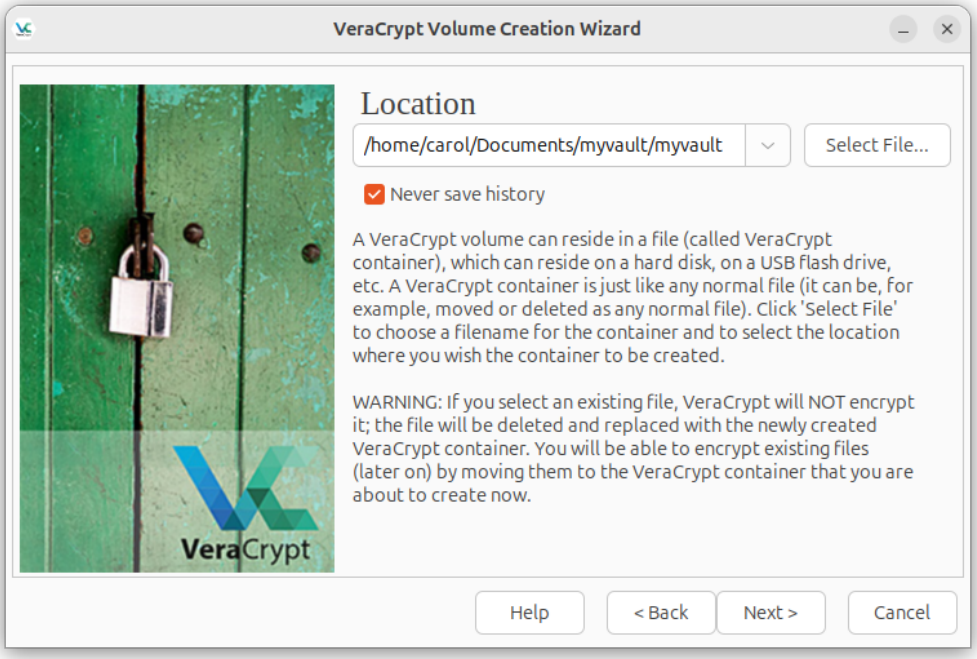

Figure 25. A VeraCryptben kiválasztott kötetfájl

A rendszer megkér minket a titkosítási algoritmus kiválasztására. Az AES a leggyakrabban ajánlott algoritmus, köszönhetően a magas szintű biztonságának: (Az AES kiválasztása a VeraCrypt titkosítási algoritmusaként).

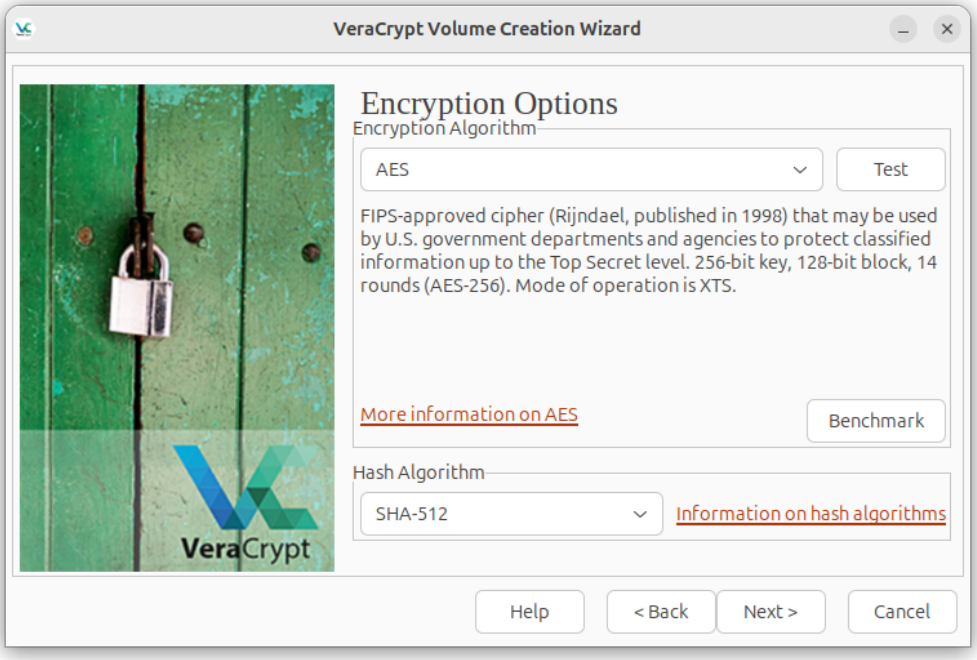

Figure 26. Az AES kiválasztása a VeraCrypt titkosítási algoritmusaként

Majd adjuk meg a meghajtó méretét: (VeraCrypt kötetméret).

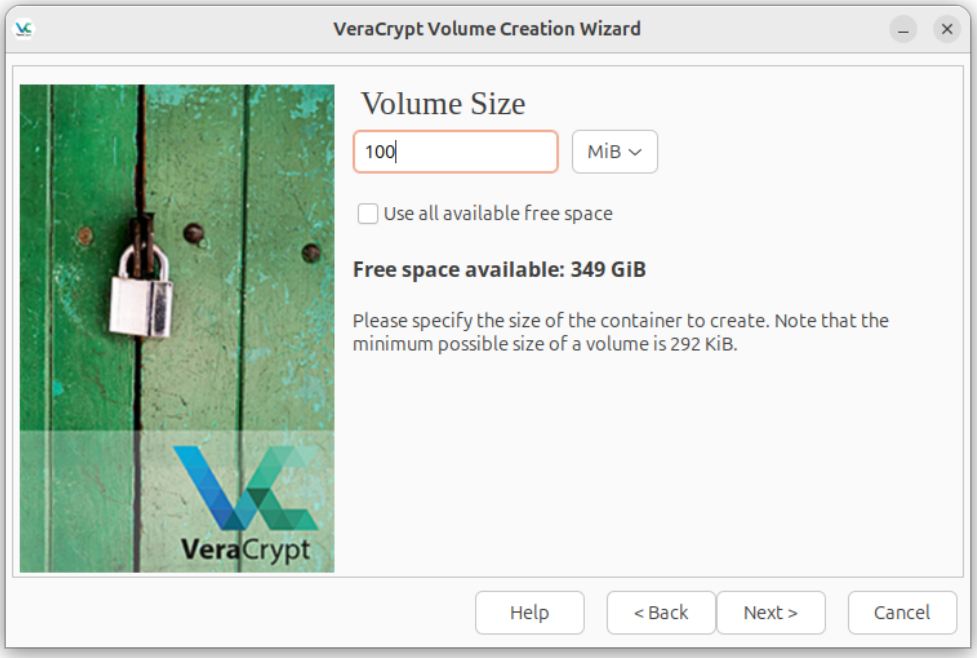

Figure 27. VeraCrypt kötetméret

Az utolsó lépés egy erős jelszó létrehozása: (Jelszó megadása a VeraCryptben).

Figure 28. Jelszó megadása a VeraCryptben

Most már a konténer csatolva van a VeraCryptben és készen áll a használatra: (Titkosított meghajtó a VeraCrpytben felcsatolva). Úgy működik, mint bármely más adathordozó, de a konténerben tárolt összes adatot automatikusan, valós időben titkosítja.

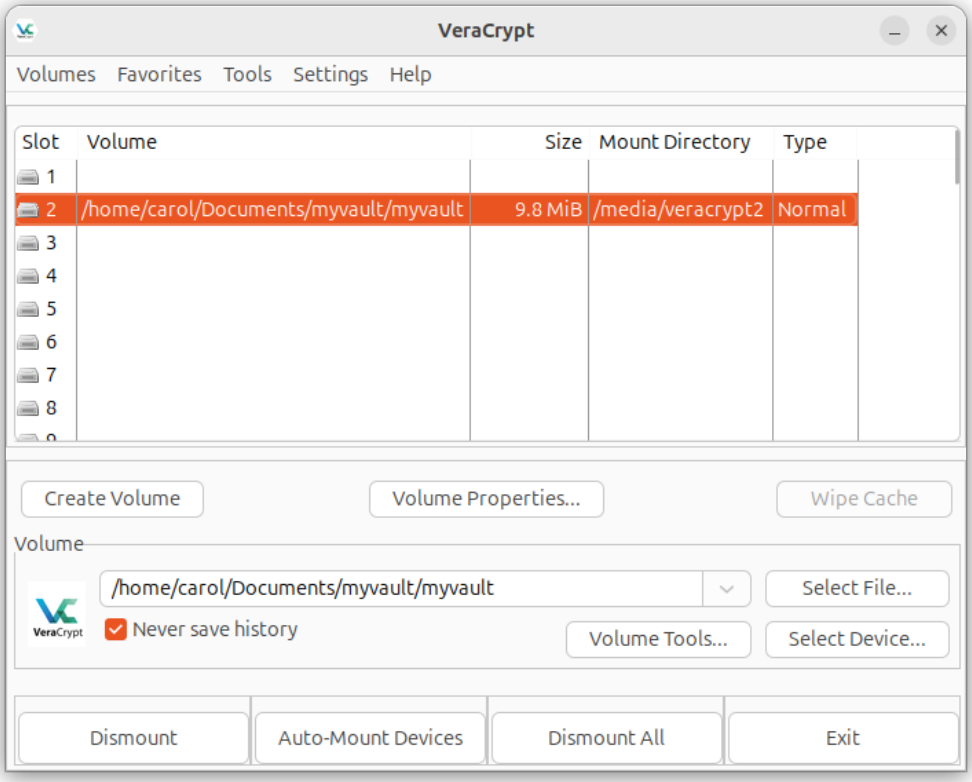

Figure 29. Titkosított meghajtó a VeraCrpytben felcsatolva

A VeraCrypt támogatja a teljes lemeztitkosítását is, így a felhasználók teljes tárolóeszközöket, például külső meghajtókat, USB flash meghajtókat vagy akár belső merevlemezeket is titkosíthatnak. Ez biztosítja, hogy az eszközön lévő összes adat titkosítva legyen, beleértve a rendszerfájlokat és magát az operációs rendszert is, ha szükséges. A teljes lemeztitkosítás különösen hasznos az érzékeny információk védelmére a fizikai eszköz ellopása vagy elvesztése esetén. Teljes lemeztitkosítás használata esetén a felhasználóknak jelszót kell megadniuk vagy egy kulcsfájlt kell használniuk a rendszerindításkor a meghajtó visszafejtéséhez és a tartalmához való hozzáféréshez.

A VeraCrypt segítségével úgy titkosítható a tárolóeszköz, hogy a felhasználó megadja a titkosítandó meghajtót vagy partíciót, és kiválasztja a titkosítási algoritmust. A titkosított tárolókhoz hasonlóan egy erős jelszó vagy kulcsfájl jön létre az adatok biztonságának biztosítása érdekében. A titkosítási folyamat befejezése után az egész eszköz hozzáférhetetlenné válik a megfelelő visszafejtési hitelesítő adatok nélkül. Ez a módszer átfogó védelmet nyújt az olyan hordozható meghajtók számára, amelyek érzékeny információkat tartalmazhatnak.

A Cryptomator használata a fájltárolási felhőszolgáltatásokban tárolt fájlok titkosítására

A Cryptomator egy hatékony eszköz, amelyet kifejezetten arra terveztek, hogy titkosítsa a fájlokat, mielőtt azokat feltöltenénk a felhőalapú tárolószolgáltatásokba. Egyszerűsége és könnyű kezelhetősége ideális megoldássá teszi az érzékeny adatok védelmére olyan platformokon, mint a Google Drive, a Dropbox és a OneDrive. A Cryptomator létrehoz egy titkosított “vaultot” (széfet) a helyi rendszeren, ahol a fájlok biztonságosan tárolhatók a felhővel való szinkronizálás előtt. Ez a vault biztosítja, hogy az adatok titkosítva legyenek az eszközön a feltöltés előtt, így azok olvashatatlanná válnak az illetéktelen felhasználók számára, még akkor is, ha a felhőszolgáltatás veszélybe kerül.

A Cryptomator több platformon is elérhető, többek között Windowson, macOS-en, Linuxon és mobileszközökön, például iOS és Android rendszereken. A telepítés után létrehozhatunk egy titkosított széfet, ahol a fájlokat tároljuk. Ez a vault egy olyan mappában található, amely szinkronizálódik a választott felhőalapú tárolási szolgáltatással, biztosítva, hogy a titkosított fájlok automatikusan feltöltődjenek a normál szinkronizálási folyamat részeként.

Telepítés után indítsuk el a Cryptomatort és hozzunk létre egy új, titkosított széfet az “Add” gombra kattintva: (<<022.4.fig7>).

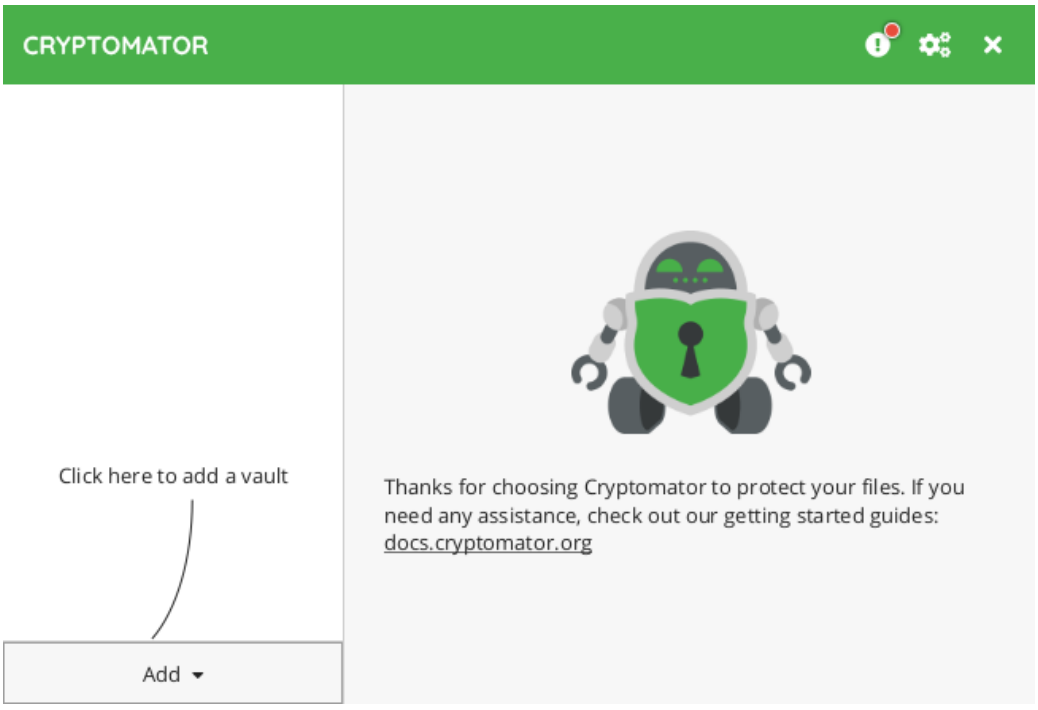

Figure 30. A Cryptomator fő képernyője

Ezután válasszuk a “Creat New Vault” lehetőséget, válasszunk nevet és tárolási helyet a széfnek:

(A vault helyének kiválasztása a Cryptomatorban). Ez a vault elhelyezhető egy olyan mappában, amely szinkronizálva van a felhőalapú tárhelyszolgáltatással (pl. Google Drive vagy Dropbox mappa).

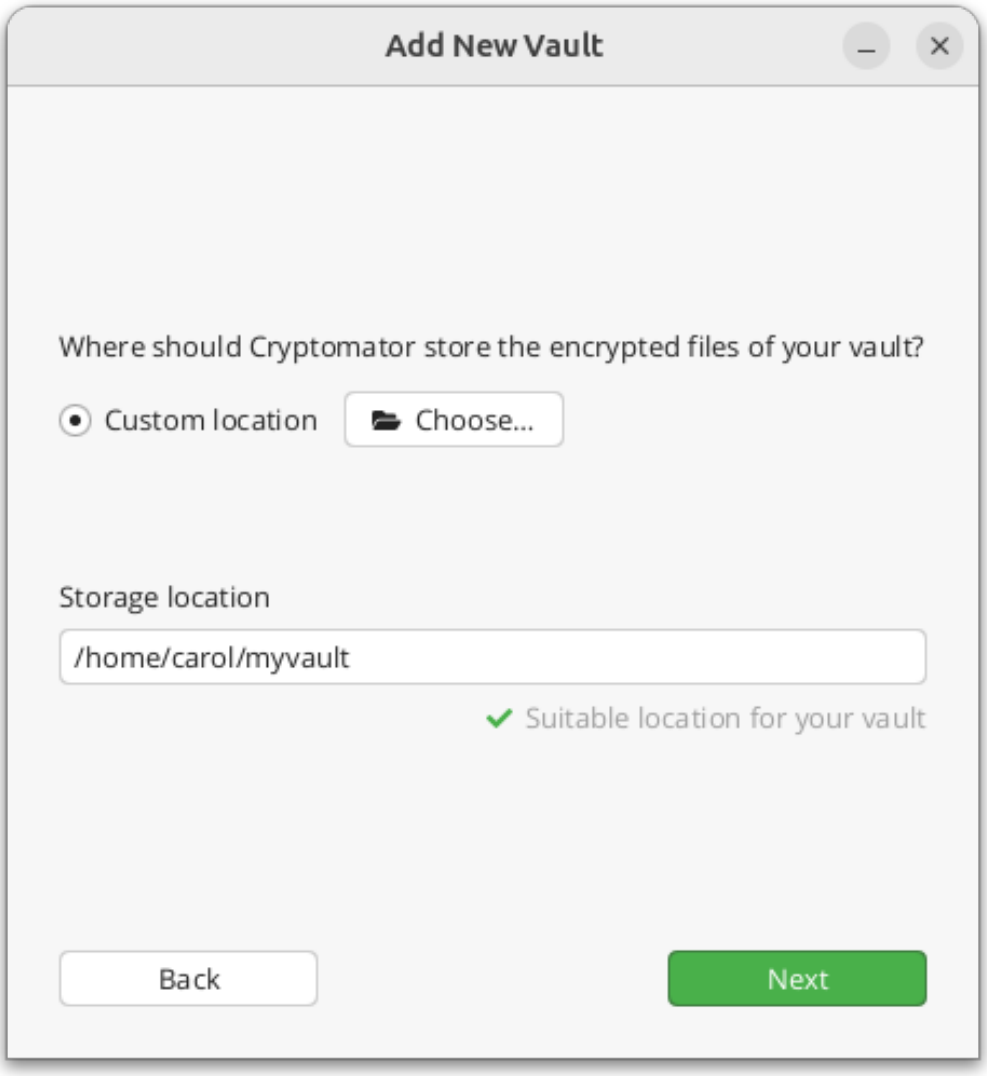

Figure 31. A vault helyének kiválasztása a Cryptomatorban

Eztuán be kell állítanunk egy erős jelszót a széfhez: (Jelszó megadása a Cryptomatorban). Ezzel a jelszóval férhetünk hozzá az összes titkosított fájlhoz.

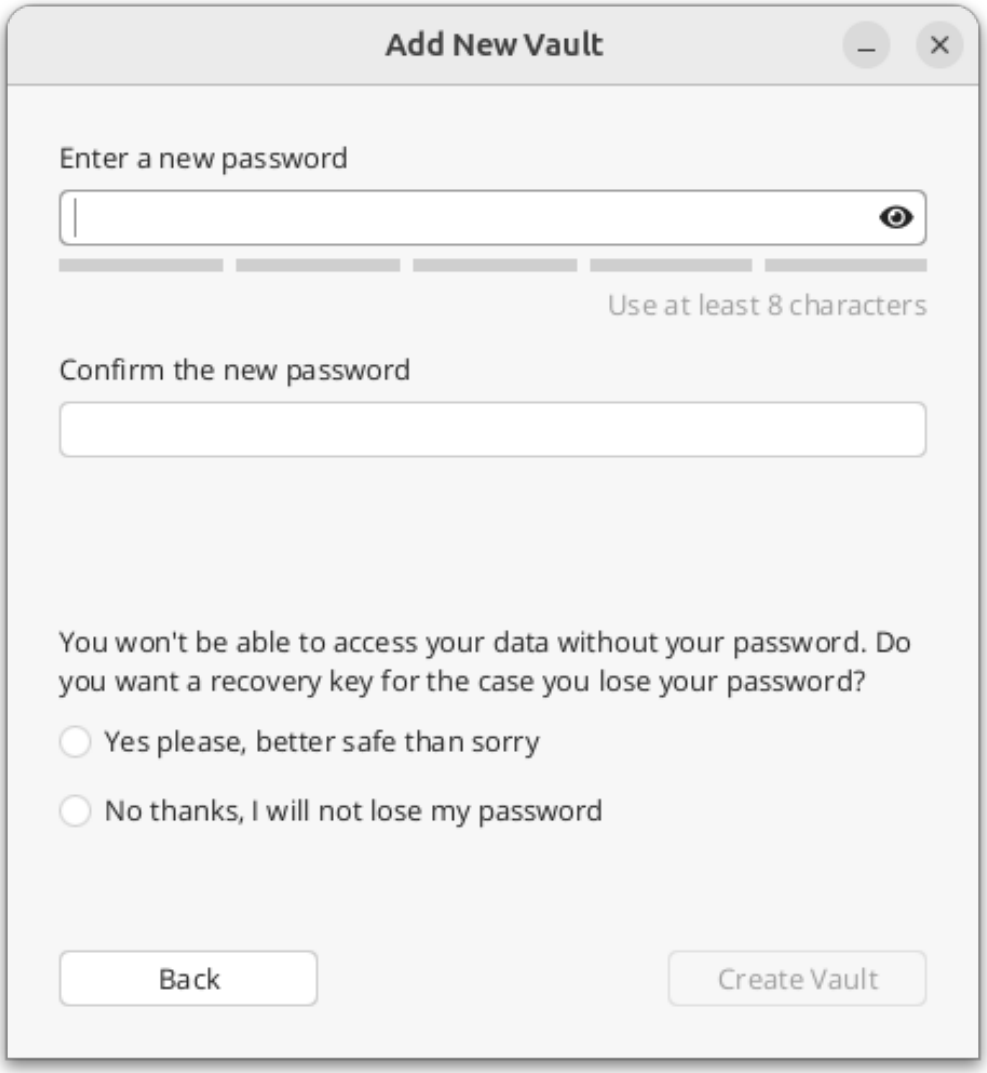

Figure 32. Jelszó megadása a Cryptomatorban

A vault létrehozása után a Cryptomator a vault feloldását (unlock) és csatlakoztatását (mount) fogja kérni. A feloldáskor egy virtuális meghajtó jön létre a rendszeren. Ez a virtuális meghajtó úgy viselkedik, mint egy normál mappa, lehetővé téve, hogy fájlokat mozgassunk bele és ki belőle: (Cryptomator — a vault feloldása és csatlakoztatása).

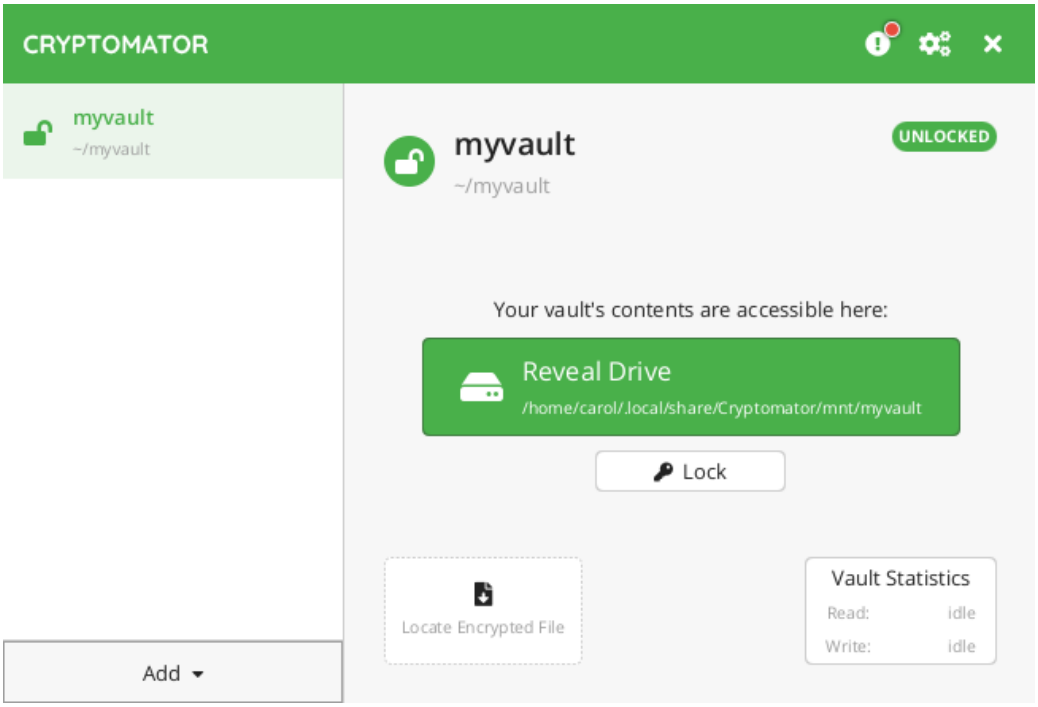

Figure 33. Cryptomator — a vault feloldása és csatlakoztatása

A vault csatlakoztatása után elkezdhetjük a fájlok hozzáadását. Egyszerűen húzzuk vagy másoljuk a fájlokat a vaultba. A fájlok hozzáadásakor a Cryptomator automatikusan titkosítja azokat, így biztosítva a széfben tárolt adatok biztonságát.

Ezek a fájlok titkosítva jelennek meg a szinkronizált felhőalapú mappában (pl. Google Drive, Dropbox vagy OneDrive). A virtuális meghajtóról történő megtekintéskor azonban eredeti, titkosítatlan változatukként jelennek meg.

Mivel a vault egy olyan mappában van tárolva, amely szinkronizálva van egy felhővel, minden titkosított fájl automatikusan feltöltődik a felhőbe. Ezek a fájlok titkosított blobokként jelennek meg a felhőben, így az illetéktelen felhasználók nem tudják elolvasni a tartalmukat.

Miután befejeztük a munkát a fájlokkal, zárolhatjuk a széfet, ami leválasztja a virtuális meghajtót, és biztosítja, hogy a titkosított fájlok biztonságban maradjanak. Amikor legközelebb hozzá kell férnünk a széfhez, egyszerűen feloldjuk a jelszó megadásával, így pedig a virtuális meghajtó újra csatlakoztatva lesz, a visszafejtett fájlokkal együtt.

A Cryptomator zökkenőmentes szinkronizálást kínál a felhőalapú tárolási szolgáltatásokkal, biztosítva, hogy titkosított fájlok biztonságosan kerüljenek tárolásra anélkül, hogy további lépéseket kellene tennünk. Amikor például hozzáadunk vagy módosítunk egy fájlt a széfben, az azonnal titkosítva lesz, és szinkronizálódik a felhőszolgáltatással. Ez biztosítja, hogy az érzékeny adatok mindenkor védve legyenek, még a szinkronizálás során is.

A Cryptomator által használt titkosítási eljárás robusztus, és úgy tervezték, hogy mind a titkosítást, mind az integritást biztosítsa. A széfben tárolt fájlok titkosítása AES-256 algoritmussal történik, és minden egyes fájl külön-külön van titkosítva, ami lehetővé teszi a hatékony szinkronizálást, és biztosítja, hogy csak a módosított fájlok kerüljenek újra feltöltésre a felhőbe.

A titkosítási funkciók mellett a Cryptomator vizuális jelzésekkel is segíti a vault kezelését. A vault virtuális meghajtóként jelenik meg a rendszerben, ahol a titkosított fájlok könnyen elérhetők, a zárolás és a feloldás folyamata pedig egyszerű és intuitív. A Cryptomator továbbá nyílt forráskódú, ami azt jelenti, hogy a kódja nyilvánosan elérhető a felülvizsgálathoz, ami az átláthatóság és az eszköz biztonságába vetett bizalom további rétegét adja.

A BitLocker fő jellemzői

A BitLocker a Microsoft Windows bizonyos kiadásaiba beépített teljes lemeztitkosítási (full-disk encryption) funkció, amely a számítógép merevlemezén lévő teljes kötetek titkosításával védi az adatokat. Erős titkosítási algoritmusok alkalmazásával a BitLocker biztosítja, hogy az eszközön tárolt adatok biztonságban legyenek az illetéktelen hozzáféréstől, még akkor is, ha a fizikai tárolóeszközt ellopják vagy elveszítik. A BitLocker különösen hasznos olyan környezetben, ahol a hordozható eszközökön, például laptopokon vagy külső meghajtókon tárolt adatok biztonsága kritikus fontosságú.

A BitLocker elsődleges funkciója a teljes lemeztitkosítása (full-disk encryption — FDE). A BitLocker az AES algoritmust használja 128 bites vagy 256 bites kulcshosszúsággal, amely erős védelmet nyújt a biztonság megkerülésére irányuló kísérletekkel szemben. A BitLocker a *BitLocker To Go* funkció révén támogatja a külső meghajtók és cserélhető tárolóeszközök titkosítását is.

A BitLocker egyik legfontosabb jellemzője a rendszer *Trusted Platform Module* (TPM) moduljával való integráció, amely egy hardveralapú biztonsági komponens, amely sok modern számítógépbe van beépítve. A TPM további védelmi réteget biztosít azáltal, hogy a titkosítási kulcsokat a fő operációs rendszertől elszigetelt, biztonságos környezetben tárolja.

A BitLocker *indítás előtti hitelesítés* (pre-boot authentication) funkciót kínál, amely növeli a biztonságot azáltal, hogy a felhasználónak a rendszer indítása előtt meg kell adnia egy PIN-kódot vagy egy indítókulccsal (startup key) ellátott USB-kulcsot kell használnia.

A Windows natív funkciójaként a BitLocker szorosan integrálódik az operációs rendszerbe, zökkenőmentes frissítéseket és kompatibilitást biztosít más biztonsági funkciókkal, például a Windows Defenderrel és a Secure Boot-tal. Ez az integráció biztosítja azt, hogy a BitLocker zökkenőmentesen védi az adatokat, miközben fenntartja a rendszer általános stabilitását és használhatóságát.

Gyakorló feladatok

1. Mi a fő különbség a fájl titkosítás és a teljes lemeztitkosítás (full-disk encryption — FDE) között?

2. Mi a Trusted Platform Module (TPM) szerepe a BitLocker titkosításában?

3. Hogyan biztosítja a Cryptomator, hogy a felhőszolgáltatásokban tárolt fájlok biztonságban maradjanak?

4. Hasonlítsuk össze a VeraCrypt és a BitLocker biztonsági jellemzőit! Mik a legfontosabb különbségek a teljes lemez titkosításának kezelésében, és milyen esetekben részesítenénk előnyben az egyiket a másikkal szemben?

Gondolkodtató feladatok

1. A BitLocker titkosítást kínál a Windows-felhasználók számára, de nem minden felhasználó szeretne egy zárt forráskódú megoldást használni. Keressük meg a BitLocker nyílt forráskódú alternatíváit, mint például a Linux rendszerekben általánosan használt LUKS és eCryptfs! Hasonlítsuk össze ezeket az eszközöket a titkosítási erősség, a könnyű használat és a kulcs-visszaállítási mechanizmusok szempontjából! Melyiket ajánlanánk egy rugalmas és átlátható titkosítási megoldást kereső felhasználónak, és miért?

2. Hogyan alkalmazzák a felhőben tárolt fájlok titkosítását a felhőalapú tárhelyszolgáltatók, mint például a Google Drive és a Dropbox? Hasonlítsuk össze ezt a Cryptomator által biztosított titkosítással! Milyen előnyökkel jár a Cryptomator használata e szolgáltatások mellett?

Összefoglalás

Ez a lecke kiemeli az inaktív (data at rest) adatok védelmének fontosságát, hangsúlyozva a fájlok és a tárolóeszközök titkosítását az adatok titkosságának és biztonságának garantálása érdekében. A tananyag a titkosítás alapvető fogalmaival foglalkozik, kitérve a fájlok és a tárolóeszközök titkosítására, valamint a teljes lemeztitkosításra (FDE). A lecke elmagyarázza, hogy ezek a módszerek hogyan alakítják át az olvasható adatokat olvashatatlan formátumokká, amelyekhez csak a megfelelő visszafejtő kulcsokkal rendelkező, felhatalmazott felhasználók férhetnek hozzá. Ez a védelem a helyi eszközökre és a felhőalapú tárolásra egyaránt vonatkozik, így lopás vagy elvesztés esetén is garantálja az adatok biztonságát.

A leckében a VeraCrypt, a titkosított konténerek létrehozására és teljes lemeztitkosításra szolgáló eszköz, valamint a Cryptomator, amely a felhőszolgáltatásokban tárolt fájlokat védi, is bemutatásra kerül. Végül a BitLockerről is beszélünk, kiemelve az olyan funkciókat, mint a teljes lemeztitkosítás és a TPM-mel való integráció a biztonságos kulcstárolás érdekében.

Válaszok a gyakorló feladatokra

1. Mi a fő különbség a fájl titkosítás és a teljes lemeztitkosítás (full-disk encryption — FDE) között?

   A fájltitkosítás az egyes fájlokat védi, biztosítva, hogy csak a megfelelő visszafejtő kulccsal vagy jelszóval rendelkező, felhatalmazott felhasználók férhessenek hozzá. A teljes lemeztitkosítás (FDE) ezzel szemben a teljes tárolóeszközt titkosítja, beleértve az operációs rendszert is, így az eszközön lévő összes adat elérhetetlenné válik hitelesítés nélkül. Az FDE az eszközön lévő összes adatot védi, míg a fájltitkosítás konkrét fájlokat céloz meg.

2. Mi a Trusted Platform Module (TPM) szerepe a BitLocker titkosításában?

   A BitLocker titkosításban a Trusted Platform Module (TPM) egy hardveralapú biztonsági komponens, amely a titkosítási kulcsokat biztonságos környezetben tárolja. Fokozza a biztonságot azáltal, hogy biztosítja a titkosítási kulcsok elszigeteltségét az operációs rendszertől, és képes automatikusan feloldani a titkosított meghajtókat a rendszerindítás során, amennyiben a rendszer integritása nem sérült.

3. Hogyan biztosítja a Cryptomator, hogy a felhőszolgáltatásokban tárolt fájlok biztonságban maradjanak?

   A Cryptomator a fájlokat helyben titkosítja, mielőtt feltöltené őket a felhőalapú tárolószolgáltatásokba. Létrehoz egy titkosított széfet, ahol a fájlokat biztonságosan tárolja, és amint ezeket a fájlok feltöltésre kerülnek, titkosított blobokként jelennek meg a felhőalapú tárhelyen. Ez biztosítja, hogy még ha a felhőszolgáltatás veszélybe is kerül, az illetéktelen felhasználók nem tudják elolvasni a titkosított fájlokat.

4. Hasonlítsuk össze a VeraCrypt és a BitLocker biztonsági jellemzőit! Mik a legfontosabb különbségek a teljes lemez titkosításának kezelésében, és milyen esetekben részesítenénk előnyben az egyiket a másikkal szemben?

   A VeraCrypt egy nyílt forráskódú eszköz, amely platformok közötti teljes lemeztitkosítást kínál, és lehetővé teszi a felhasználók számára titkosított konténerek létrehozását. Több testreszabási lehetőséget és átláthatóságot biztosít, mivel nyílt forráskódú. A BitLocker ezzel szemben a Windowsba integrált, és zökkenőmentes kezelést kínál a Trusted Platform Module (TPM) segítségével, amely hardveralapú biztonságot garantál. A BitLockert általában a vállalati környezetekben preferálják legfőképp az egyszerű integráció és az Active Directory révén történő kezelés miatt, míg a VeraCryptet azok a felhasználók részesíthetik előnyben, akik nyílt forráskódú, szélesebb platformtámogatással rendelkező szoftvert szeretnének.

Válaszok a gondolkodtató feladatokra

1. A BitLocker titkosítást kínál a Windows-felhasználók számára, de nem minden felhasználó szeretne egy zárt forráskódú megoldást használni. Keressük meg a BitLocker nyílt forráskódú alternatíváit, mint például a Linux rendszerekben általánosan használt LUKS és eCryptfs! Hasonlítsuk össze ezeket az eszközöket a titkosítási erősség, a könnyű használat és a kulcs-visszaállítási mechanizmusok szempontjából! Melyiket ajánlanánk egy rugalmas és átlátható titkosítási megoldást kereső felhasználónak, és miért?

   A LUKS (Linux Unified Key Setup) és az eCryptfs egyaránt erős titkosítást kínál. A LUKS, a Linux szabványa, erős titkosítást biztosít, és partíciónként több kulcsot is támogat. Az eCryptfs felhasználóbarátabb, de nem biztos, hogy a lemezszintű titkosításhoz kellően sokoldalú. A kutatások alapján a LUKS lenne az ajánlott eszköz a rugalmassága és a különböző Linux-disztribúciókkal való kompatibilitása, valamint a teljes meghajtók titkosítására való képessége miatt.

2. Hogyan alkalmazzák a felhőben tárolt fájlok titkosítását a felhőalapú tárhelyszolgáltatók, mint például a Google Drive és a Dropbox? Hasonlítsuk össze ezt a Cryptomator által biztosított titkosítással! Milyen előnyökkel jár a Cryptomator használata e szolgáltatások mellett?

   Az olyan felhőalapú tárolási szolgáltatók, mint a Google Drive és a Dropbox, általában szerveroldali titkosítást kínálnak, ahol az adatok titkosítása inaktív állapotban és útközben is a szolgáltató által kezelt kulcsok segítségével történik. A titkosítási kulcsok felett azonban továbbra is ők rendelkeznek, ami azt jelenti, hogy potenciálisan hozzáférhetnek a fájljainkhoz, vagy megoszthatják azokat, ha a törvény előírja. A Cryptomator ezzel szemben kliensoldali titkosítást biztosít, ami azt jelenti, hogy a felhasználó helyben titkosítja a fájlokat, mielőtt feltöltené azokat. A visszafejtési kulcsok csak a felhasználó birtokában vannak, így nagyobb adatvédelmet és biztonságot nyújt. A Cryptomator használatának előnye ezekkel a szolgáltatásokkal az, hogy biztosítja, hogy az adatok olvashatatlanok maradnak akkor is, ha a felhőszolgáltató veszélybe kerül, vagy ha az adatokat harmadik féllel kell megosztania.

Linux Professional Institute

Témakör 023: Eszköz- és tárolóbiztonság

023.1 Hardverbiztonság

Hivatkozás az LPI célkitűzésre

Security Essentials version 1.0, Exam 020, Objective 023.1

Súlyozás

2

Kulcsfontosságú ismeretek

- A számítógép fő alkotóelemeinek megértése
- Az okoseszközök és az Internet of Things (IoT) megértése
- A számítógéphez való fizikai hozzáférés biztonsági vonatkozásainak megértése
- Az USB-eszközök típusainak, csatlakoztatásának és biztonsági szempontjainak megértése
- A Bluetooth-eszközök típusainak, kapcsolatainak és biztonsági szempontjainak megértése
- Az RFID-eszközök típusainak, kapcsolatainak és biztonsági szempontjainak megértése
- A Trusted Computing megértése

A használt fájlok, kifejezések és segédprogramok részleges listája

- Processzorok, memória, tároló, hálózati adapterek
- Tabletek, okostelefonok, okostévék, routerek, nyomtatók intelligens otthon, riasztó, IoT eszközök (pl. izzók, termosztátok, TV-k)
- USB
- Bluetooth
- RFID

Linux Professional Institute

Lecke 1

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	023 Eszköz- és tárolóbiztonság
Fejezet:	023.1 Hardverbiztonság
Lecke:	1/1

Bevezetés

A kiberbiztonság már nem korlátozódik a szoftverek sebezhetőségére vagy a hálózat megsértésére. A hardverbiztonság kritikus szerepet játszik a számítógépes rendszerek általános védelmének biztosításában. A hardverbiztonsággal kapcsolatos alapvető ismeretek elengedhetetlenek a számítógépes rendszerek integritását és titkosságát veszélyeztető kockázatok azonosításához és mérsékléséhez.

A számítógép fő alkatrészei

A számítógép fő alkotóelemeinek megismerése alapvető fontosságú annak megértéséhez, hogy a hardverek szintjén hogyan alakulhatnak ki biztonsági rések. Minden számítógépes rendszer több kulcsfontosságú elemből áll, amelyek együttesen végzik el a feladatokat és kezelik az adatokat, valamint minden egyes komponens saját biztonsági kihívásokat jelent.

Minden számítógép középpontjában a *processzor* (*Central Processing Unit* (központi feldolgozóegység), vagy CPU) áll, amely az utasítások végrehajtásáért és a számítások elvégzéséért felelős. A rendszer agyaként a CPU teljesítménye és biztonsága kulcsfontosságú. A processzor sebezhetőségei olyan kihasználásokhoz vezethetnek, mint például az oldalcsatornás (side-

channel) támadások, amelyek során a támadók a CPU működése közbeni viselkedésének megfigyelésével hozzáférhetnek érzékeny adatokhoz.

A számítógép *memóriája*, amelyet elsősorban *Random Access Memory* (RAM) néven emlegetnek, egy másik kritikus komponens. A RAM ideiglenesen tárolja azokat az adatokat és utasításokat, amelyekhez a CPU-nak gyorsan hozzá kell férnie. Mivel azonban a RAM volatilis, és az áramellátás kikapcsolásakor elveszíti az adatait, célpontjává válhat az olyan támadásoknak, mint például a hidegindítási (cold boot) támadások, amelyek során a támadó a rendszer kikapcsolása után megpróbálhat érzékeny adatokat kinyerni.

A *tárolóeszközök* (storage device), például a merevlemezek és a *solid-state-drive* (SSD) felelősek az adatok állandó megőrzéséért. Az operációs rendszertől és az alkalmazásoktól kezdve a személyes fájlokig és az érzékeny információkig mindent tárolnak. A RAM-mal ellentétben a tárolók a rendszer kikapcsolása után is megőrzik az adatokat, ami a támadások elsődleges célpontjává teszi őket. A tárolóeszközök titkosítása és a biztonságos törlési gyakorlatok elengedhetetlenek az adatok jogosulatlan hozzáféréstől való védelméhez, különösen lopás vagy elvesztés esetén.

Végül a *hálózati adapterek* (network adapter) lehetővé teszik a számítógép számára a helyi hálózatokhoz és az internethez való csatlakozást, megkönnyítve az eszközök közötti adatátvitelt. Ezek az adapterek kulcsfontosságúak a kommunikáció szempontjából, de számos biztonsági rést is nyitnak, például a man-in-the-middle támadásoknak, packet sniffingnek vagy a rosszul védett hálózatokon keresztül történő illetéktelen hozzáférésnek való kitettségnek.

Okoseszközök és az Internet of Things (IoT)

Az intelligens eszközök és az *Internet of Things* (dolgok internete, IoT) megértése kritikus fontosságú az összekapcsolt eszközök gyors elterjedése által jelentett potenciális biztonsági kockázatok felismeréséhez. A hagyományos számítógépekkel ellentétben az IoT-eszközök gyakran beleolvadnak a mindennapi környezetbe, az otthonoktól az irodákon át a közterekig, ami olyan új sebezhetőségeket teremt, amelyeket ki lehet használni, ha az eszközök nincsenek megfelelően biztosítva.

Az intelligens eszközök, például a táblagépek, okostelefonok és okostévék a személyes és szakmai digitális interakciók élvonalába tartoznak. Ezek az eszközök olyan nagy teljesítményű eszközökké fejlődtek, amelyek képesek összetett alkalmazások futtatására, érzékeny adatok tárolására és különféle hálózatokhoz való csatlakozásra. Széles körű használatuk azonban a kibertámadások elsődleges célpontjaivá is teszi őket.

Az IoT elterjedése számos intelligens otthoni eszközt is bevezetett, például termosztátokat, villanykörtéket, kamerákat és hangalapú asszisztenseket. Miközben ezek az eszközök kényelmet és automatizálást kínálnak, egyedi biztonsági kihívásokat is jelentenek. A legtöbb IoT-eszközt úgy

tervezték, hogy “plug and play” legyen, ami azt jelenti, hogy egyszerűen telepíthető, de gyakran nincsenek erős beépített biztonsági protokollok. Például sok IoT-eszközt alapértelmezett felhasználónevekkel és jelszavakkal szállítanak, amelyeket a felhasználók elmulaszthatnak megváltoztatni, így az eszközök sebezhetővé válnak az olyan támadásokkal szemben, mint a botnetek vagy az illetéktelen irányítás. Az IoT-rendszerek és az internet közötti átjáróként szolgáló eszközöket, például a routereket megfelelően kell konfigurálni erős jelszavakkal, titkosítással és hálózati szegmentációval, hogy megakadályozzák az illetéktelen hozzáférést.

Az okostévék, nyomtatók és routerek esetében a kockázatok túlmutatnak az eszközök eltérítésén. A patchek rendszeres telepítése, a nem használt funkciók letiltása és a rendellenes tevékenység figyelése segíthet e kockázatok csökkentésében.

A számítógéphez való fizikai hozzáférés biztonsági vonatkozásai

A kiberbiztonság vizsgálatakor fontos felismerni, hogy a számítógéphez való fizikai hozzáférés még a legstabilabb digitális védelmet is jelentősen alááshatja. Az illetéktelenek számára fizikailag hozzáférhető rendszer számos közvetlen támadásnak van kitéve, amelyek közül sok megkerüli a hagyományos szoftveralapú biztonsági intézkedéseket.

A fizikai hozzáféréssel kapcsolatos egyik legközvetlenebb kockázat a hardverkomponensek manipulálásának lehetősége. A fizikai hozzáféréssel rendelkező támadó manipulálhatja a kulcsfontosságú hardverelemeket, például kicserélheti vagy módosíthatja a rendszer merevlemezét, rosszindulatú eszközöket, például *keyloggereket* vagy jogosulatlan hardvert telepíthet a kommunikáció vagy az adatátvitel lehallgatására.

Egy másik kritikus kockázat a rendszer adataihoz való fizikai hozzáférésből adódik. Még ha az adatok titkosítva is vannak, egy támadó, aki fizikai hozzáférést szerez az eszközhöz, potenciálisan kiveheti vagy lemásolhatja a tárolóeszközöket, hogy később megpróbálja visszafejteni azokat.

A fizikai hozzáférés azt is eredményezheti, hogy a támadó külső adathordozóról, például USB-meghajtóról vagy CD-ről indítja a rendszert. Ezáltal a támadó teljesen megkerülheti az operációs rendszert és biztonsági mechanizmusokat, így pedig hozzáférhet a fájlokhoz, jelszavakhoz és egyéb érzékeny információkhoz anélkül, hogy fel kellene törnie a rendszer meglévő bejelentkezési adatait. Ez a fajta támadás rávilágít a BIOS (Basic Input/Output System) vagy UEFI (Unified Extensible Firmware Interface) beállítások konfigurálásának fontosságára, hogy letiltsuk a külső eszközökről történő rendszerindítást, és biztosítsuk, hogy az ilyen beállítások jelszóval védettek legyenek. Emellett a jelszó beállítása a rendszerindítás-kezelőben (boot manager), például a GRUB-ban, további biztonsági réteget jelent, ami megnehezíti a támadók számára az operációs rendszer biztonsági ellenőrzésének megkerülését.

USB

Az *Universal Serial Bus* (USB) eszközök — típusaik, kapcsolataik és biztonsági szempontjaik — megértése alapvető fontosságú, mivel mindenütt jelen vannak a modern számítástechnikában. Az USB-eszközöket a tárolástól a perifériák csatlakoztatásáig számos célra használják, így a számítógépekkel és hálózatokkal való mindennapi interakciók gyakori részei. Kényelmük azonban biztonsági kockázatokat is jelent, amelyeket gondosan kell kezelni.

Az USB-eszközöknek több típusa létezik, köztük az USB-A, az USB-B és az USB-C, amelyek mindegyike más-más felhasználási esetekre készült. Az USB-A a legelterjedtebb típus, amely a legtöbb számítógépben megtalálható, és olyan perifériák csatlakoztatására szolgál, mint a billentyűzetek, egerek és tárolóeszközök. Az USB-B-t gyakran használják nagyobb eszközökhöz, például nyomtatókhoz vagy külső merevlemezekhez, az USB-C pedig egy újabb szabvány, amely kisebb, megfordítható kialakításáról és gyorsabb adatátviteli sebességéről ismert.

A fizikai csatlakozók mellett különböző USB-verziók is léteznek, amelyek különböző célokat szolgálnak. Az USB 2.0, 3.0 és 3.1 például az adatátviteli sebesség tekintetében különbözik, az USB 3.1 jelentősen gyorsabb teljesítményt nyújt, mint az USB 2.0. A gyorsabb adatátvitel előnyös lehet a teljesítmény szempontjából, de azt is jelenti, hogy a rosszindulatú adatok gyorsabban továbbíthatók, ami biztonsági kockázatot jelent.

Biztonsági szempontból az USB-eszközök számos támadásnak és sebezhetőségnek vannak kitéve. Az egyik leggyakoribb fenyegetés a rosszindulatú (malicious) USB-eszközök használata. A támadók rosszindulatú szoftverekkel telepített USB-meghajtókkal veszélyeztethetik a rendszereket, amikor az eszközt a számítógéphez csatlakoztatják. Ezek a támadások olyan technikákkal történhetnek, mint a rosszindulatú fájlok automatikus futtatása vagy az USB-kapcsolatok operációs rendszer általi kezelésében lévő sebezhetőségek kihasználása.

Az USB-eszközöket gyakran használják *adatkinyerésre* (data exfiltration) is, amikor érzékeny adatokat másolnak egy USB-meghajtóra, majd eltávolítják őket egy biztonságos környezetből. Ezt a fajta támadást rosszindulatú belső vagy külső támadók követhetik el, akik fizikai hozzáférést szereznek a rendszerhez. Az *USB-portok kontrollálásának* bevezetése vagy a portok teljes letiltása általános gyakorlat az illetéktelen eszközök csatlakoztatásának megakadályozására.

Az USB-eszközökkel kapcsolatos biztonsági kockázatok mérséklése érdekében elengedhetetlen számos bevált gyakorlat alkalmazása. Az USB-meghajtókon tárolt adatok titkosítása alapvető fontosságú, különösen, ha érzékeny információkat kezelünk. Emellett a rosszindulatú támadások valószínűségének csökkentésében segít, ha csak megbízható eszközöket használunk, és biztosítjuk, hogy minden USB-eszköz megbízható forrásból származzon. Végezetül a szervezeteknek olyan irányelveket kell bevezetniük, amelyek korlátozzák az USB-eszközök használatát a fokozottan biztonságos környezetekben, és fejleszteniük az alkalmazottak ismereteit az ismeretlen eszközök

csatlakoztatásának lehetséges veszélyeiről.

Bluetooth

A Bluetooth technológia többféle eszköztípust támogat a különböző iparágakban. A Bluetooth-eszközök leggyakoribb típusai közé tartoznak az olyan személyes eszközök, mint az okostelefonok, a táblagépek, a vezeték nélküli fülhallgatók és az okosórák. Ezek az eszközök rövid távolságokon keresztül kommunikálnak egymással, így a Bluetooth alapvető technológia a vezeték nélküli ökoszisztémák létrehozásához mind a személyes, mind a szakmai környezetben. A szórakoztató elektronika mellett a Bluetooth-t orvosi eszközökben, autóipari rendszerekben és ipari berendezésekben is használják, ahol a megbízható vezeték nélküli kommunikáció elengedhetetlen. A Bluetooth-eszközök típusainak és alkalmazásainak megértése fontos a velük járó biztonsági vonatkozások felismeréséhez.

A Bluetooth-eszközök különböző kapcsolatokkal működnek, amelyek elsősorban a *Bluetooth Classic* és a *Bluetooth Low Energy* (BLE) kategóriába sorolhatók. A Bluetooth Classic a folyamatos, nagysebességű kapcsolatot igénylő eszközökhöz használatos, például a vezeték nélküli hangszórókra történő valós idejű hangátvitelhez (streameléshez) vagy a nagyméretű fájlok telefonok és számítógépek közötti átvitelére. A BLE-t viszont olyan eszközökre optimalizálták, amelyeknek időszakos kommunikációra van szükségük alacsony energiafogyasztás mellett, így ideális IoT-eszközök, fitneszkövetők és intelligens otthoni kütyük számára. Mindegyik kapcsolattípus saját biztonsági kihívásokkal jár. A Bluetooth Classic például sérülékenyebb lehet az adatátvitel során történő *lehallgatással* szemben, míg a BLE-eszközök könnyűsúlyúak, így nem rendelkeznek fejlett biztonsági mechanizmusokkal.

Biztonsági szempontból a Bluetooth-eszközök különböző támadásoknak vannak kitéve. Az egyik leggyakoribb fenyegetés a *bluejacking*, amikor a támadó kéretlen üzeneteket vagy fájlokat küld a hatótávolságon belül lévő Bluetooth-kompatibilis eszközre. Bár ez ártalmatlannak tűnhet, adathalász-támadásokhoz vagy rosszindulatú linkek terjesztéséhez vezethet. Egy másik kockázat a *bluesnarfing*, ami egy komolyabb támadás, ekkor a támadó a felhasználó beleegyezése nélkül, jogosulatlanul fér hozzá az eszköz adataihoz, például a névjegyekhez, üzenetekhez vagy más érzékeny információkhoz.

Súlyosabb támadás a *Bluetooth eszköz megszemélyesítése* (impersonation), ami a *man-in-the-middle* támadás egy változata. Ebben a forgatókönyvben a támadó lehallgatja a két Bluetooth-eszköz közötti kommunikációt, és az egyik félnek adja ki magát. Ez lehetővé teszi a támadó számára, hogy hozzáférjen, manipulálja vagy ellopja az eszközök között továbbított adatokat. Mivel a Bluetooth hatótávolsága körülbelül tíz méter, ezek a támadások jellemzően közvetlen közelségben történnek, így jelentős fenyegetést jelentenek nyilvános helyeken, például repülőtereken, kávézókban és irodákban.

A Bluetooth-kapcsolatok másik jelentős sebezhetősége a *párosítással* kapcsolatos. Amikor az eszközök párosítva vannak, biztonsági kulcsokat cserélnek a biztonságos kapcsolat létrehozásához. Ha azonban a párosítási folyamat nincs megfelelően védve, a támadók elfoghatják vagy manipulálhatják ezeket a kulcsokat, és így jogosulatlan hozzáférést szerezhetnek az eszközökhöz. A nyilvános párosítás, amikor az eszközök párosítása nyílt vagy nem biztonságos környezetben történik, különösen sebezhető az ilyen típusú támadással szemben. A védett párosítási módszerek, például a *passkey authentication* (kulcshitelesítés) használatának biztosítása csökkentheti ezt a kockázatot.

Az ilyen kockázatok elleni védelem érdekében fontos, hogy a Bluetooth-eszközök védettségére vonatkozó legjobb gyakorlatokat kövessük! Mindenekelőtt hatékony módja a jogosulatlan hozzáférés megakadályozásának a Bluetooth letiltása, ha nem használjuk.

A szervezetek számára a vállalati eszközök Bluetooth-tevékenységének nyomon követése szükséges lépés az érzékeny adatokhoz való jogosulatlan hozzáférés megakadályozásához. A Bluetooth biztonságos környezetben történő használatának korlátozásával és a vezeték nélküli kommunikációt figyelő eszközök telepítésével a vállalkozások minimalizálhatják a Bluetooth-eszközökkel kapcsolatos potenciális kockázatokat. Hasonlóképpen, az alkalmazottak oktatása a személyes Bluetooth-eszközeik nyilvános helyeken történő védelmének fontosságáról segít csökkenteni a támadásoknak való kitettséget.

RFID

A *Radio Frequency Identification* (RFID) eszközök — típusaik, kapcsolataik és biztonsági szempontjaik — megértése alapvető fontosságú, mivel az RFID-technológiát széles körben használják olyan iparágakban, mint a kiskereskedelem, az egészségügy, a logisztika és a beléptetés-ellenőrzés. Az RFID-eszközök megkönnyítik az adatok vezeték nélküli átvitelét a címkék és az olvasó között, rádióhullámok segítségével azonosítva és nyomon követve tárgyakat vagy személyeket. Miközben az RFID számos előnyt kínál a hatékonyság és az automatizálás tekintetében, biztonsági kockázatokat is jelent, amelyeket kezelni kell.

Az RFID-eszközök három fő típusba sorolhatók: *passzív*, *aktív* és *fél-passzív* (semi-passive). A passzív RFID-címkék nem rendelkeznek belső áramforrással; az RFID-olvasó által továbbított energiára támaszkodnak a bekapcsoláshoz és az adatok visszaküldéséhez. Az RFID ezen típusát általában a készletgazdálkodásban, a kiskereskedelem nyomon követésében és a beléptetés ellenőrzésében használják. Az aktív RFID-címkék belső akkumulátorral rendelkeznek, és nagyobb távolságokra is képesek jeleket továbbítani. Ezeket gyakran ott használják, ahol nagy értékű eszközök vagy járművek valós idejű nyomon követésére van szükség, például logisztikai vagy raktári műveletekben. A félig passzív RFID-címkék szintén rendelkeznek akkumulátorral, de azt csak a belső áramkörök táplálására használják; a kommunikáció továbbra is az RFID-olvasótól függ. Ezt a típust akkor használják, ha megbízhatóbb olvasásra van szükség, különösen olyan

környezetben, ahol sok az interferencia.

Az RFID-eszközök közötti kapcsolatok vezeték nélküliek. Az RFID-olvasó rádióhullámokat bocsát ki, amelyek aktiválják a hatósugarában lévő címkéket. A címke ezután adatokat küld vissza az olvasónak, amely feldolgozza azokat és értelmezésre továbbítja egy számítógépes rendszerbe. Az alkalmazott frekvenciától függően az RFID-kapcsolatok néhány centimétertől több méterig terjedhetnek. A leggyakoribb frekvenciatartományok a következők: *alacsony frekvencia* (LF), *magas frekvencia* (HF) és *ultramagas frekvencia* (UHF). Az LF jellemzően kis hatótávolságú, alacsony adatátviteli igényű alkalmazásokhoz, például állatok nyomon követéséhez használatos, míg a HF-t a proximity kártyák és az NFC-kompatibilis eszközök esetében alkalmazzák. Az UHF a legelterjedtebb típus ipari és logisztikai alkalmazásokban, mivel nagyobb hatótávolsággal rendelkezik és nagyobb mennyiségű adatot képes továbbítani.

Az RFID-eszközök biztonsági szempontjait vizsgálva számos potenciális sebezhetőség merül fel. Az egyik legismertebb kockázat a lehallgatás. Mivel az RFID-kommunikáció vezeték nélkül történik, egy megfelelő vevővel rendelkező támadó lehallgathatja a címke és az olvasó között továbbított jeleket, és így bizalmas információkat, például hitelkártyaszámokat vagy személyazonosító adatokat tudhat meg. Ez különösen az olyan alkalmazásokban aggasztó, mint az érintés nélküli fizetési rendszerek, ahol a pénzügyi információkhoz való jogosulatlan hozzáférés csalást eredményezhet.

Egy másik gyakori biztonsági fenyegetés a *klónozás* (cloning). A klónozási támadás során a támadó lemásolja az RFID-címke adatait, és egy új címkét hoz létre ugyanazzal az információval. Ezt a klónozott címkét ezután arra lehet használni, hogy jogosulatlanul hozzáférjenek korlátozott területekre vagy rendszerekhez, különösen olyan környezetekben, ahol az RFID-t beléptetés-ellenőrzésre használják.

Az *RFID skimming* egy másik támadási módszer, amikor a támadó a tulajdonos tudta vagy beleegyezése nélkül adatokat olvas ki a címkéről. A skimming eszközök gyakran kisméretűek és hordozhatóak, így a támadók az RFID-címkéket zsúfolt helyeken, például tömegközlekedési eszközökön vagy bevásárlóközpontokban is észrevétlenül leolvashatják. Ez a kockázat különösen jelentős az RFID-képes hitelkártyák és személyazonosító okmányok esetében, ami személyazonosság-lopáshoz vagy pénzügyi csaláshoz vezethet.

E kockázatok mérséklése érdekében számos biztonsági intézkedést kell alkalmazni. Az egyik legfontosabb lépés az RFID-címkék és az olvasók között továbbított adatok titkosítása. Ez biztosítja, hogy még ha az adatokat le is hallgatják, a támadó ne tudja könnyen elolvasni vagy felhasználni azokat.

Egy másik hatékony biztonsági intézkedés az RFID-jelek blokkolására szolgáló *RFID-pajzsok* (shield) vagy *Faraday-kalitkák* használata, amikor a címkék nincsenek használatban. Ezeket a

pajzsokat gyakran használják pénztárcákban vagy kártyatartókban, hogy megvédjék az RFID-képes hitelkártyákat vagy személyazonosító okmányokat a skimmingtől.

Végezetül, kritikus fontosságú az RFID-rendszerek rendszeres frissítése és ellenőrzése. Mint minden más technológiát, az RFID-eszközöket és olvasókat is naprakészen kell tartani a legújabb biztonsági javításokkal. Az RFID-tevékenység nyomon követése, különösen az olyan érzékeny környezetekben, mint a raktárak, egészségügyi létesítmények és biztonságos épületek, segít a szokatlan viselkedés vagy az illetéktelen hozzáférési kísérletek valós időben történő észlelésében.

Trusted Computing

A *Trusted Computing* (bizalmi számítástechnika) olyan technológiák és szabványok összessége, amelyek a számítógépes rendszerek biztonságát növelik azáltal, hogy megbízható és kiszámítható működést biztosítanak. A Trusted Computing alapgondolata olyan számítástechnikai környezet létrehozása, amelyben a felhasználók bízhatnak abban, hogy eszközeik biztonságban vannak a manipulációtól, a jogosulatlan hozzáféréstől és a rosszindulatú szoftverektől. Az ezt lehetővé tevő fő technológia a *Trusted Platform Module* (TPM), egy speciális, a modern eszközökbe integrált hardverkomponens, amely kritikus szerepet játszik a rendszer alapját képező védelemben.

A Trusted Computing egyik legfontosabb funkciója a *secure boot* (biztonságos rendszerindítás). Ez biztosítja, hogy a rendszer csak ellenőrzött és megbízható szoftverrel induljon el. A rendszerindítás során a firmware-től az operációs rendszerig minden egyes komponens egy kriptográfiai aláírás alapján kerül ellenőrzésre. Ha a szoftver bármelyik részét manipulálták vagy rosszindulatú kóddal helyettesítették, a rendszer megtagadja a rendszerindítást.

A Trusted Computing lehetővé teszi a *távoli tanúsítást* (remote attestation) is, amely lehetővé teszi, hogy egy eszköz egy távoli fél számára bizonyítsa, hogy megbízható állapotban van. Például egy felhőalapú számítástechnikai környezetben egy távoli kiszolgáló az tanúsítással megerősítheti, hogy egy klienseszköz vagy virtuális gép a szoftver megbízható verzióját futtatja, mielőtt hozzáférést biztosítana az érzékeny erőforrásokhoz.

A rendszer integritásának védelme és a biztonságos rendszerindítási folyamatok biztosítása mellett a Trusted Computing döntő szerepet játszik az érzékeny adatok titkosításon keresztüli védelmében. A TPM képes titkosítási kulcsokat generálni és kezelni, biztosítva, hogy a kulcsok soha ne hagyják el a biztonságos hardverkörnyezetet.

A Trusted Computing a modern számítástechnikai rendszerek védelmének hatékony megközelítése, amely különböző mechanizmusokkal biztosítja, hogy az eszközök és a szoftverek megbízhatóak és manipulációtól mentesek legyenek.

Gyakorló feladatok

1. Mik a processzor, a memória (RAM), a tárolóeszközök és a hálózati adapterek lehetséges biztonsági rései? Nevezzünk meg minden egyes komponens esetében egy valós példát a biztonsági fenyegetésre, és javasoljunk stratégiát vagy megoldást a kockázat csökkentésére!

2. Mutassunk be három gyakori, IoT-eszközökkel kapcsolatos biztonsági kockázatot! Ismertessünk továbbá két legjobb gyakorlatot (best practice) ezen kockázatok csökkentésére! Végül térjünk ki arra, hogy a Trusted Computing és a Trusted Platform Module (TPM) hogyan növelheti az IoT-eszközök biztonságát!

Gondolkodtató feladatok

1. Vizsgáljuk meg, hogy a különböző operációs rendszerek, például a Windows, a Linux és a macOS hogyan valósítják meg a biztonságos rendszerindítási (secure boot) mechanizmusokat!

2. Vizsgáljunk meg egy valós IoT botnet támadást, például a Mirai botnetet!

Összefoglalás

Ez a lecke a hardver- és eszközbiztonság legfontosabb aspektusait emeli ki, a számítógépek, az okoseszközök, az IoT, az USB, a Bluetooth, az RFID és a Trusted Computing főbb komponensire összpontosítva. E technológiák mindegyike egyedi biztonsági kihívásokat jelent, a processzorok sebezhetőségétől és a tárolókhoz való jogosulatlan hozzáféréstől kezdve a gyakran gyengén védett okos- és IoT-eszközökkel kapcsolatos kockázatokig. Az USB- és Bluetooth-eszközök emellett érzékenyek a rosszindulatú programok bejuttatására, a jogosulatlan adatátvitelre és a man-in-the-middle támadásokra, míg az RFID-rendszerek olyan kockázatokkal szembesülnek, mint a klónozás és a skimming. A Trusted Computing olyan technológiák alkalmazásával, mint a Trusted Platform Module (TPM), segít a rendszer integritásának biztosításában, a biztonságos indítási folyamatokban és az adatok védelmében.

Válaszok a gyakorló feladatokra

1. Mik a processzor, a memória (RAM), a tárolóeszközök és a hálózati adapterek lehetséges biztonsági rései? Nevezzünk meg minden egyes komponens esetében egy valós példát a biztonsági fenyegetésre, és javasoljunk stratégiát vagy megoldást a kockázat csökkentésére!

   A processzorok sebezhetőek az oldalcsatornás támadásokkal szemben, amelyek során a támadó a processzor viselkedésének elemzésével érzékeny adatokat nyerhet ki. Ezek a támadások hardveres javítások alkalmazásával és a rendszer firmware frissítésével enyhíthetők. A memóriát (RAM) olyan kockázatok fenyegetik, mint a hidegindítási támadások, amelyek során az adatokat a leállítás után nyerik ki. Ez a probléma a memória titkosításával és a RAM leállításkor történő törlésével csökkenthető. A tárolóeszközök, például a merevlemezek és az SSD-k, érzékenyek az adatlopásra, különösen akkor, ha az adatok nincsenek titkosítva. A teljes lemeztitkosítás és a biztonságos törlési gyakorlatok kulcsfontosságúak a tárolási adatok védelmében. A hálózati adapterek kihasználhatók a man-in-the-middle támadások vagy a packet sniffing révén, amikor a hálózatokon keresztül továbbított adatokat lehallgatják. A kommunikáció titkosítása és a tűzfalak engedélyezése hatékony módszer az ilyen típusú támadások megelőzésére.

2. Mutassunk be három gyakori, IoT-eszközökkel kapcsolatos biztonsági kockázatot! Ismertessünk továbbá két legjobb gyakorlatot (best practice) ezen kockázatok csökkentésére! Végül térjünk ki arra, hogy a Trusted Computing és a Trusted Platform Module (TPM) hogyan növelheti az IoT-eszközök biztonságát!

   Az IoT-eszközök számos biztonsági kockázatoknak vannak kitéve, beleértve az alapértelmezett hitelesítő adatok megőrzése miatti jogosulatlan hozzáférést, a botnet-támadásokat, amelyek a kompromitált eszközöket nagyszabású DDoS-támadásokhoz használják, valamint az adatokhoz való illetéktelen hozzáféréseket, amelyeket nem biztonságos adatátviteli csatornák okoznak. E kockázatok mérséklése érdekében fontos, hogy az IoT-eszközökön megváltoztassuk az alapértelmezett felhasználóneveket és jelszavakat, és rendszeresen frissítsük a firmware-eket a sebezhetőségek javításának érdekében. A Trusted Computing, különösen a Trusted Platform Module (TPM) használata hozzájárul az IoT-eszközök védelméhez, mivel biztosítja, hogy csak megbízható szoftvereket indítsunk el, és biztonságosan tárolja a kriptográfiai kulcsokat, így védve az érzékeny adatokat és lehetővé téve a biztonságos távoli tanúsítást.

Válaszok a gondolkodtató feladatokra

1. Vizsgáljuk meg, hogy a különböző operációs rendszerek, például a Windows, a Linux és a macOS hogyan valósítják meg a biztonságos rendszerindítási mechanizmusokat!

   A biztonságos rendszerindítási (Secure Boot) mechanizmusok operációs rendszerenként eltérőek, de általában hardverkomponensekre, például a TPM-re vagy az UEFI-re támaszkodnak a rendszerindítási folyamat integritásának ellenőrzésére. A Windowsban a Secure Boot az UEFI-t használja annak biztosítására, hogy az indítás során csak megbízható szoftverek töltődjenek be, és a TPM-et alkalmazza a hitelesítéshez szükséges kriptográfiai kulcsok tárolására. Ez a megközelítés különösen hatékony a vállalati környezetekben, mivel védelmet nyújt az illetéktelen bootloaderek és rootkitek ellen. A Linux-disztribúciók, például az Ubuntu, szintén támogatják az UEFI-t használó Secure Bootot, bár a megvalósítás a disztribúciótól függően eltérő lehet. A Linux-felhasználóknak kézzel kell konfigurálniuk a Secure Boot beállításait, hogy bizonyos illesztőprogramokkal vagy egyéni kernelekkel kompatibilis legyen. A macOS hasonló megközelítést használ a Secure Boot funkcióval, amely szorosan integrálva van az Apple T2 biztonsági chipjébe. Ez biztosítja, hogy indításkor csak az Apple által aláírt, megbízható szoftverek tölthetők be, ami egy erős biztonsági réteget jelent a manipuláció vagy a rosszindulatú programok ellen.

2. Vizsgáljunk meg egy valós IoT botnet támadást, például a Mirai botnetet!

   A Mirai botnet jól ismert példája az IoT-alapú kibertámadásnak. Több ezer IoT-eszközt, például kamerákat és routereket tett tönkre a gyenge vagy alapértelmezett jelszavak kihasználásával. A Mirai sebezhető eszközöket keresett az interneten, megfertőzte őket, és egy olyan botnetet hozott létre, amely képes volt tömeges destributed denial-of-service (elosztott szolgáltatásmegtagadásos, DDoS) támadásokat indítani. A botnet megzavarta a főbb webhelyeket és szolgáltatásokat, köztük a Dyn DNS-szolgáltatót, és olyan jelentős platformokat érintett, mint a Twitter, a Netflix és a Reddit.

023.2 Alkalmazásbiztonság

Hivatkozás az LPI célkitűzésre

Security Essentials version 1.0, Exam 020, Objective 023.2

Súlyozás

2

Kulcsfontosságú ismeretek

- A gyakori szoftvertípusok megértése
- Az alkalmazások különböző forrásainak megértése, valamint a szoftverek biztonságos beszerzésének és telepítésének módjai
- A firmware, az operációs rendszerek és az alkalmazások frissítéseinek megértése
- A mobilalkalmazások forrásainak megértése
- A szoftverek gyakori biztonsági réseinek megértése
- A helyi védelmi szoftverek fogalmának megértése

A használt fájlok, kifejezések és segédprogramok részleges listája

- Firmware, operációs rendszerek, alkalmazások
- Alkalmazásboltok
- Helyi csomagszűrők, végponti tűzfalak, alkalmazási réteg tűzfalai
- Puffer túlcsordulások, SQL injection

Linux Professional Institute

Lecke 1

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	023 Eszköz- és tárolóbiztonság
Fejezet:	023.2 Alkalmazásbiztonság
Lecke:	1/1

Bevezetés

A szoftverbiztonság kritikus fontosságú a rendszerek és az adatok integritásának fenntartásához. Ez a szoftverek biztonságos telepítésének biztosításával kezdődik, azáltal, hogy az alkalmazásokat megbízható szolgáltatóktól szerezzük be, és megakadályozzuk a rosszindulatú kódok betolakodását a telepítési folyamat során. A szoftverbeszerzés legjobb gyakorlatainak betartása elengedhetetlen a jogosulatlan hozzáférés vagy a rosszindulatú programok elkerülése érdekében, legyen szó asztali számítógépekről, szerverekről vagy mobil platformokról. Emellett a szoftverfrissítések kezelése is kulcsfontosságú, mivel a rendszeres frissítések és javítások olyan sebezhetőségeket kezelnek, amelyek kihasználhatók, ha nem javítják őket.

Egy másik kulcsfontosságú szempont a szoftverek védelme a nem kívánt hálózati kapcsolatoktól. Ehhez olyan eszközöket kell használni, mint a tűzfalak, packet filterek (csomagszűrők) és végpontvédelem, amelyek biztosítják, hogy a szoftver csak engedélyezett hálózatokkal és entitásokkal kommunikáljon. A telepítések biztonságossá tételével, az időben történő frissítések biztosításával és a hálózati kapcsolatok kezelésével a szervezetek hatékonyan minimalizálhatják a kockázatokat és fenntarthatják a szoftver integritását.

Gyakori szoftvertípusok és frissítéseik

A számítástechnika és a kiberbiztonság területén alapvető fontosságú megérteni azokat a szoftverkategóriákat, amelyek a digitális rendszerek működésének alapját képezik. Ezek a kategóriák a következők: *firmware*, *operációs rendszerek* és *alkalmazások*. Mindegyik típus különálló szerepet tölt be az eszköz vagy rendszer funkcionalitásának, használhatóságának és biztonságának garantálásában.

A firmware közvetlenül a hardvereszközökbe ágyazott alacsony szintű szoftver. A hardverkomponensek és a magasabb szintű szoftverek közötti interfészként szolgál, biztosítva a rendszer hardverének megfelelő működését. A firmwaret általában nem-volatilis memóriában tárolják, és elengedhetetlen a rendszer indításához és az olyan hardverkomponensek kezeléséhez, mint az alaplap, a merevlemezek és a hálózati interfészek.

A firmware-frissítések különösen fontosak, mivel a firmware a hardver és a magasabb szintű szoftverek közötti kommunikációt szabályozza, ezért sebezhetősége veszélyeztetheti az egész eszközt. Ezeket a frissítéseket gyakran a hardvergyártók adják ki biztonsági problémák megoldása, más hardverkomponensekkel való kompatibilitás javítása vagy új funkciók támogatása érdekében. Mivel a firmware szerves része az eszköz működésének, a naprakészen tartása biztosítja a rendszer folyamatos integritását és biztonságát.

Az operációs rendszer (OS) az a központi szoftver, amely a számítógép hardver- és szoftvererőforrásait kezeli. Ilyen szoftver például a Windows, a macOS és a Linux, amelyek felhasználói felületet biztosítanak, és lehetővé teszik az alkalmazások futtatását a rendszerben. Az operációs rendszer felelős a memória, a feldolgozási teljesítmény, a fájlrendszerek és a perifériás eszközök kezeléséért. Az operációs rendszerek biztonsága alapvető fontosságú, mivel ezek jelentik az első védelmi vonalat az illetéktelen hozzáféréssel és a rosszindulatú szoftverekkel szemben.

Az operációs rendszer frissítései gyakran tartalmaznak biztonsági javításokat az ismert sebezhetőségek, például a hálózati protokollokkal, a memóriakezeléssel vagy a hozzáférés-szabályozással kapcsolatos sebezhetőségek kijavítására. Az operációs rendszer naprakészségének biztosításával a felhasználók csökkentik annak kockázatát, hogy rendszerüket rosszindulatú programok vagy más támadások használják ki. Fontos az operációs rendszer életciklusának figyelemmel kísérése is, mivel a régebbi rendszerek már nem biztos, hogy kapnak kritikus biztonsági frissítéseket, és így sebezhetővé válhatnak a támadásokkal szemben.

Az alkalmazások olyan szoftverprogramok, amelyeket arra terveztek, hogy a felhasználó számára meghatározott feladatokat végezzenek el, például a produktivitást segítő eszközök, mint a szövegszerkesztők, vagy a webböngészők és a szórakoztató platformok. Az alkalmazások működése az operációs rendszertől függ, és sokféle funkciót kínálnak. Széles körű használatuk miatt az alkalmazások a kibertámadások gyakori célpontjai.

Az alkalmazásfrissítések a hibák kijavítására, a használhatóság fejlesztésére és a sebezhetőségek patchelésére (foltozására) összpontosítanak azon szoftverekben, amelyeket a felhasználók a legközvetlenebbül használnak. Ezek a frissítések megelőzhetik a biztonsági kockázatokat, például az befecskendezéses támadásokat (injection attack), a puffer túlcsordulását (buffer overflow) vagy az érzékeny adatokhoz való jogosulatlan hozzáférést. Az alkalmazások naprakészen tartása csökkenti a sebezhetőségek kihasználásának valószínűségét.

Szoftverek biztonságos beszerzése és telepítése

A digitális korban a szoftveralkalmazásokat sokféle forrásból szerzik be, ezért kulcsfontosságú, hogy megértsük, hol és hogyan lehet biztonságosan beszerezni és telepíteni a szoftvereket. A források sokfélesége — a hivatalos alkalmazásboltoktól kezdve a harmadik féltől származó webhelyekig — jelentős biztonsági kockázatot jelenthet, ha nem megfelelően kezeljük őket. A rosszindulatú szoftverfertőzések (malware infection), az adatsértés és a jogosulatlan hozzáférés megelőzéséhez elengedhetetlen, hogy tudjuk, hogyan ellenőrizzük egy szoftverforrás legitimitását, és garantáljuk a biztonságos telepítési gyakorlatokat.

Az *alkalmazásboltok* (app store) az egyik legelterjedtebb és legmegbízhatóbb forrásai a szoftveralkalmazásoknak, különösen a mobileszközök számára. Az olyan platformok, mint az Apple App Store, a Google Play Store és a Microsoft Store a felhasználók számára hozzáférést biztosítanak olyan alkalmazások nagy gyűjteményéhez, amelyek a platform szolgáltatója által valamilyen szintű biztonsági ellenőrzésen estek át. Ezek az áruházak gyakran alkalmaznak mechanizmusokat a rosszindulatú kódok ellenőrzésére, és biztosítják, hogy az alkalmazások megfelelnek bizonyos biztonsági előírásoknak, mielőtt a nyilvánosság számára elérhetővé válnak. Bár az alkalmazásboltok biztonságosabb környezetet biztosítanak a szoftverek beszerzéséhez, nem bolondbiztosak. Előfordult, hogy rosszindulatú alkalmazások átcsúsztak az ellenőrzési folyamaton, ezért a felhasználóknak letöltés előtt feltétlenül ellenőrizniük kell az alkalmazások értékeléseit, a róluk írt véleményeket és engedélyeiket.

Az asztali és vállalati környezetek esetében a szoftverek beszerezhetők a gyártók webhelyeiről, harmadik féltől származó disztribútoroktól vagy csomagkezelő rendszerekből (package management systems). A hivatalos szállítói webhelyekről történő letöltéskor fontos ellenőrizni, hogy a forrás legitim-e, gyakran a HTTPS-tanúsítványok és a szoftvercsomagok digitális aláírásának ellenőrzésével. A megbízható csomagkezelők, például Linux rendszerek esetén az APT, vagy a Microsoft Windows csomagkezelője használatával szintén biztosítható, hogy az alkalmazások biztonságos forrásként megbízható tárolókból (repository) származzanak.

A szoftverek biztonságos telepítéséhez a felhasználóknak a best practice-ket kell követniük, például el kell kerülniük a nem megbízható vagy ismeretlen forrásokat, a szoftver integritását hashek vagy digitális aláírások segítségével kell ellenőrizniük, és naprakészen kell tartaniuk rendszereiket és biztonsági szoftvereiket. Ezek a lépések segítenek biztosítani, hogy a

rosszindulatú szoftverek véletlenül se kerüljenek telepítésre, megelőzve ezzel a rendszer esetleges veszélyeztetését.

Mobilalkalmazások forrásai

A mobilalkalmazások mindennapi életünk szerves részévé váltak, a kommunikációs eszközöktől kezdve a produktivitást segítő alkalmazásokon át a szórakoztató platformokig. A mobilalkalmazások széles körű használata azonban jelentős biztonsági problémákat is felvet. Annak érdekében, hogy a mobileszközökre telepített alkalmazások biztonságosak és megbízhatóak legyenek, elengedhetetlen a mobilalkalmazások különböző forrásainak és a kapcsolódó biztonsági kockázatoknak a megértése.

A mobilalkalmazások legelterjedtebb és legbiztonságosabb forrásai a hivatalos alkalmazásboltok, például az Apple App Store és a Google Play Store. Ezek a platformok központosított tárolóként szolgálnak, ahol a fejlesztők terjeszthetik alkalmazásaikat, és mindkét áruház szigorú ellenőrzési folyamatokkal rendelkezik a rosszindulatú szoftverek terjesztésének minimalizálása érdekében. Az Apple különösen az App Store felett tart fenn szigorú ellenőrzést: minden alkalmazásnak át kell esnie egy olyan felülvizsgálati folyamaton, amely ellenőrzi a biztonsági szabványoknak és az adatvédelmi irányelveknek való megfelelést. Hasonlóképpen, a Google Play Store automatizált rendszerek, például a Google Play Protect segítségével vizsgálja az alkalmazásokat rosszindulatú programok és egyéb biztonsági fenyegetések szempontjából. Bár ezek az alkalmazásboltok általában biztonságosak, egyik rendszer sem tévedhetetlen, és a felhasználóknak letöltés előtt mindig ellenőrizniük kell az alkalmazások értékelését, engedélyeit és a fejlesztő hitelességét.

A hivatalos alkalmazásboltok mellett a mobilalkalmazások harmadik féltől származó alkalmazásboltokból vagy weboldalakról is beszerezhetők. Ezek az alternatív platformok olyan alkalmazásokat kínálhatnak, amelyek a hivatalos áruházakban nem érhetők el, de lényegesen nagyobb biztonsági kockázatot jelentenek. A harmadik féltől származó alkalmazások gyakran nem esnek át ugyanolyan szintű ellenőrzésen, mint a hivatalos platformokon találhatóak, ami növeli a rosszindulatú vagy kompromitált alkalmazások letöltésének valószínűségét. Az ilyen forrásokból letöltést választó felhasználóknak tisztában kell lenniük a potenciális veszélyekkel, és további óvintézkedéseket kell tenniük, például vírusirtó szoftverrel ellenőrizni az alkalmazásokat, és megbizonyosodni a forrás jogszerűségéről.

A mobilalkalmazások terjesztésének másik módja a vállalati alkalmazásboltok (enterprise app stores). Ezek olyan privát alkalmazásboltok, amelyeket jellemzően a szervezeteken belül használnak belső használatra kifejlesztett egyedi alkalmazások terjesztésére. Bár a vállalati alkalmazásboltok biztonságos hozzáférést biztosíthatnak az üzletspecifikus alkalmazásokhoz, gondos kezelést igényelnek annak biztosítása érdekében, hogy az alkalmazásokat biztonságosan fejlesszék, teszteljék és terjesszék. Annak érdekében, hogy elkerüljék a véletlen kompromittálódást, az alkalmazottakat is oktatni kell arról, hogy hogyan töltsék le és telepítsék

biztonságosan ezeket az alkalmazásokat.

Gyakori biztonsági rések a szoftverekben

A szoftversebezhetőségek olyan hibák vagy gyenge pontok a kódban, amelyeket a támadók kihasználva veszélyeztethetik a rendszer biztonságát. A két leggyakoribb és legveszélyesebb sebezhetőség a *buffer overflow* (puffer túlcsordulás) és az *SQL injection* (SQL-injekció). Ezeket a sebezhetőségeket széles körben kihasználják, és súlyos következményekkel járhatnak, beleértve a jogosulatlan hozzáférést, az adatsértéseket és a rendszer összeomlását.

A buffer overflow akkor következik be, amikor egy program több adatot ír egy pufferbe — egy ideiglenes adattároló területre --, mint amennyit az a terület elbír. Ilyenkor a többletadatok felülírhatják a szomszédos memóriát, ami megváltoztathatja a program végrehajtási folyamatát. A támadók ezt kihasználva rosszindulatú kódot juttatnak be, irányítást szereznek a rendszer felett, vagy a program összeomlását idézik elő. Ez a sebezhetőség gyakran a nem megfelelő bemeneti érvényesítés (input validation) vagy a kódban lévő határellenőrzések (boundary check) hiánya miatt alakul ki. A buffer overflow sebezhetőségek mérséklése érdekében a fejlesztőknek biztonságos kódolási gyakorlatokat kell alkalmazniuk, például a határok ellenőrzését és a bemeneti validálást, valamint olyan modern biztonsági funkciókat, mint a stack canaries és az *Address Space Layout Randomization* (ASLR).

```
Az SQL-injection egy másik gyakori biztonsági sebezhetőség, amely az adatbázisokkal
együttműködő alkalmazásokban fordul elő. Az ilyen típusú támadás során a támadó
rosszindulatú SQL-kódot juttat be egy beviteli mezőbe, manipulálva az alkalmazás
adatbázishoz intézett lekérdezését. Ha a bemenet nincs megfelelően ellenőrizve, a támadó
jogosulatlanul hozzáférhet az adatbázishoz, érzékeny adatokat kérhet le vagy módosíthat, de
akár adminisztrációs műveleteket is végezhet. Az SQL injection támadások a nem megfelelő
bemeneti ellenőrzés és az előkészített utasítások (prepared statement) vagy paraméterezett
lekérdezések nem megfelelő használatának következményei. Az SQL injection elleni védekezés
érdekében a fejlesztőknek mindig ellenőrizniük kell a felhasználói bemenetet, paraméterezett
lekérdezéseket kell használniuk, és kerülniük kell a közvetlen felhasználói bemenetből
származó SQL-kifejezések felépítését.
```

Helyi védelmi szoftverek

A helyi védelmi szoftverek létfontosságú szerepet játszanak a rendszerek védelmében sokféle biztonsági fenyegetéstől, a bejövő és kimenő hálózati forgalom ellenőrzésével és a rosszindulatú tevékenységek szűrésével. Ezt a védelmet jellemzően olyan eszközök biztosítják, mint a *local packet filter*-ek (lokális csomagszűrők), *endpoint firewall*-ok (végponti tűzfalak) és *application layer firewall*-ok (alkalmazási réteg tűzfalai), amelyek mindegyike a rendszer egyedi igényeihez

igazodva különböző szintű biztonságot nyújt.

A helyi csomagszűrők hálózati szinten működnek, és a rendszerbe vagy a rendszerből továbbított egyes adatcsomagokat vizsgálják. Ezek a szűrők előre meghatározott szabályok, például IP-címek, portszámok vagy protokollok alapján döntenek a csomagok engedélyezéséről vagy blokkolásáról. A csomagszűrés a tűzfalfunkciók alapvető része, és segít megakadályozni a jogosulatlan hozzáférést azáltal, hogy megállítja a rosszindulatú csomagokat, mielőtt azok elérnék a célállomásukat. Bár az alapvető forgalomszabályozásban hatékony, a csomagszűrők nem képesek a kommunikáció magasabb szintjein előforduló, kifinomultabb támadások felismerésére.

Az endpoint tűzfalakat úgy tervezték, hogy az egyes eszközök, például laptopok vagy asztali számítógépek védelmére szolgálnak, mivel az eszköz és a hálózat közötti akadályként működnek. Az endpoint tűzfalak az egyszerű csomagszűrőknél átfogóbb védelmet nyújtanak, mivel az eszközre belépő és onnan kilépő összes forgalmat figyelik, blokkolják a rosszindulatú tevékenységet és megakadályozzák az illetéktelen hozzáférést. Emellett biztonsági házirendeket is érvényesíthetnek, például megakadályozhatják, hogy bizonyos alkalmazások hozzáférjenek a hálózathoz, vagy megakadályozhatják a külső eszközök csatlakoztatását.

A helyi védelmi szoftverek esetében a helyi csomagszűrő és az endpoint tűzfal funkcióit általában együttesen valósítják meg, és a hálózati forgalom szűrésével, valamint a biztonsági irányelvek közvetlenül az egyes eszközökön történő érvényesítésével biztosítva átfogó védelmi réteget.

Mind a Windows, mind a macOS integrált tűzfalakkal rendelkezik, amelyek csomagszűrést és endpoint tűzfalat is biztosítanak az általános biztonsági képességek részeként. Ez a kettős funkció biztosítja, hogy a jogosulatlan hozzáférés és a rosszindulatú tevékenységek effektíven blokkolva legyenek, és így hatékony védelmet nyújtsanak.

A *Windows Defender Firewall* például a hálózati szinten figyeli és ellenőrzi a forgalmat, és eszközszinten érvényesíti a biztonsági házirendeket, hogy megakadályozza, hogy az alkalmazások a házirendeket sértő műveleteket hajtsanak végre.

A macOS hasonlóképpen beépített tűzfallal rendelkezik, amely kombinálja a csomagszűrést a végponti tűzfal képességekkel, lehetővé téve a felhasználók számára, hogy szabályokat állítsanak be a bejövő és kimenő forgalom szabályozására. A macOS olyan fejlett lehetőségeket is biztosít, mint a naplózás és a lopakodó üzemmód, amely segít megakadályozni, hogy a rendszert észleljék a hálózaton, tovább növelve a biztonságot az eszköz szintjén. Ezek a funkciók nagyobb ellenőrzést biztosítanak a felhasználóknak az eszközök hálózattal való interakciója felett, így biztosítva az átfogó védelmet.

A Linux rendszerekben széles körben használt *iptables* csomagszűrő eszközként működik, amely lehetővé teszi a felhasználók számára, hogy szabályokat határozzanak meg a bejövő és kimenő hálózati forgalom kezelésére. A hálózati szinten működő eszköz lehetővé teszi a felhasználók

számára, hogy a forgalmat olyan kritériumok alapján blokkolják vagy engedélyezzék, mint IP-címek, portszámok és protokollok. Az iptables rendkívül testreszabható, és fejlett lehetőségeket biztosít a hálózati biztonság kezeléséhez, de a megfelelő konfigurációhoz a hálózati fogalmak alapos ismerete szükséges.

Ezenkívül a *SELinux* (Security-Enhanced Linux) kritikus szerepet játszik Linux-környezetek esetén a végpontok védelmében. Bár nem hagyományos tűzfal, a SELinux olyan *kötelező hozzáférés-szabályozást* (mandatory access controls — MAC) hajt végre, amely korlátozza a folyamatok által végezhető műveleteket. Ez egy extra biztonsági réteget ad hozzá úgy, hogy ellenőrzi, hogyan lépnek kapcsolatba az alkalmazások a rendszerrel. A jogosultságok szigorú kezelésével a SELinux segít megakadályozni, hogy a jogosulatlan folyamatok veszélyeztessék a rendszert, így a rendszer integritásának biztosításában értékes kiegészítője a tűzfalaknak és más biztonsági eszközöknek.

Az *alkalmazásrétegbeli tűzfalak* magasabb szinten működnek, mint a csomagszűrők vagy az enpoint tűzfalak, és az egyes alkalmazásokhoz vagy szolgáltatásokhoz kapcsolódó forgalmat vizsgálják. Ezek a tűzfalak az alkalmazási rétegben kicserélt adatokat figyelik, ahol olyan létfontosságú protokollok működnek, mint a HTTP, az FTP vagy az SMTP. Az alkalmazásrétegbeli tűzfalak mélyebb ellenőrzést és irányítást biztosítanak, lehetővé téve a rendszergazdák számára, hogy a forgalmat az alkalmazás típusa vagy a továbbított adatok tartalma alapján blokkolják. Ez teszi őket rendkívül hatékonnyá az olyan támadások ellen, amelyek az alkalmazások sebezhetőségeit célozzák, mint például az *cross-site scripting* (XSS), az SQL injection és a buffer overflow.

Egy példa az alkalmazásrétegbeli tűzfalra a *ModSecurity*, egy nyílt forráskódú webes alkalmazás tűzfal (web application firewall — WAF), amely védelmet nyújt az olyan webes alapú fenyegetések ellen, mint az SQL injection és a cross-site scripting. Egy másik példa a *F5 BIG-IP*, amely fejlett funkciókat tartalmaz az alkalmazásszintű forgalom kezelésére és annak biztosítására, hogy az érzékeny alkalmazások védve legyenek a célzott támadásoktól.

Számos felhőszolgáltató kínál *felhőalapú alkalmazás-tűzfalakat* (cloud-based application firewall) a platformjukon elhelyezett alkalmazások védelmére.

Ilyen például az AWS esetén az *AWS Web Application Firewall* (AWS WAF) szolgáltatás, amely védelmet nyújt a gyakori webes exploitok ellen, lehetővé téve a felhasználók számára, hogy egyéni szabályokat határozzanak meg a forgalom bizonyos típusainak blokkolására. A Google Cloud hasonló szolgáltatást nyújt a *Cloud Armor* révén, amely segít az alkalmazások sebezhetőségének mérséklésében, és védelmet biztosít a DDoS és az alkalmazásrétegbeli támadások ellen. Hasonlóképpen a Microsoft Azure szolgáltatása az *Azure Web Application Firewall* (Azure WAF), amely központosított védelmet nyújt a felhőplatformján hosztolt alkalmazások számára, kiszűrve a rosszindulatú forgalmat, mielőtt az elérné az alkalmazást. Ezek a felhőalapú tűzfalak nagymértékben skálázhatók, könnyen integrálhatók, és átfogó védelmet

nyújtanak a felhőkörnyezetekben lévő webes alkalmazások számára.

Gyakorló feladatok

1. Miért fontos a biztonságos szoftvertelepítés?

2. Miért fontos a biztonság szempontjából a rendszeres szoftverfrissítés?

3. Hogyan védi a fenyegetésektől a hálózati kapcsolatok kezelése a szoftvert?

Gondolkodtató feladatok

1. Mi történik a buffer overflow során?

2. Hogyan használják ki a támadók az SQL injection sebezhetőségeket?

3. Mi a különbség a végponti tűzfal (endpoint firewall) és a csomagszűrő (packet filter) között?

 | |

Összefoglalás

Ez a lecke a szoftverbiztonság fenntartásának alapvető gyakorlatait ismerteti, a biztonságos telepítésre, a rendszeres frissítésekre és a hálózati kapcsolatok kezelésére összpontosítva. Kiemeli annak fontosságát, hogy a rosszindulatú szoftverek elkerülése érdekében megbízható forrásból szerezzünk be szoftvereket, és biztosítsuk, hogy minden szoftver, beleértve a firmwaret, az operációs rendszereket és az alkalmazásokat is, naprakész legyen a sebezhetőségek javítása érdekében. A lecke emellett elmagyarázza, hogyan használhatják ki a támadók az olyan gyakori szoftveres sebezhetőségeket, mint a buffer overflow és az SQL injection, és azt is, hogy hogyan csökkenthetik ezeket a kockázatokat a biztonságos kódolási gyakorlatok és a bemeneti validálás.

A lecke a helyi védelmi szoftvereket is megvizsgálja, különbséget téve a helyi csomagszűrők (local packet filter), a végponti tűzfalak (endpoint firewall) és az alkalmazási szintű tűzfalak (application layer firewall) között, amelyek mindegyike különböző szintű védelmet nyújt. Az olyan példák, mint az iptables, a Windows Defender tűzfal és a ModSecurity bemutatják, hogy ezek az eszközök hogyan védik a rendszereket a hálózati forgalom szűrésével és az alkalmazásspecifikus támadások megakadályozásával. A felhőalapú tűzfalak — például az AWS, a Google Cloud és a Microsoft Azure által biztosított tűzfalak — szerepét is tárgyaljuk, mivel ezek elengedhetetlenek a felhőben tárolt alkalmazások fejlett fenyegetésekkel szembeni védelméhez.

Válaszok a gyakorló feladatokra

1. Miért fontos a biztonságos szoftvertelepítés?

   A megbízható forrásból származó szoftverek telepítésének biztosítása segít megelőzni a rosszindulatú kódok bejutását. Ez a folyamat biztosítja, hogy a telepített szoftverek legitimek és mentesek a biztonsági fenyegetésektől, csökkentve ezzel a jogosulatlan hozzáférés vagy a rosszindulatú szoftverek (malware) fertőzésének kockázatát.

2. Miért fontos a biztonság szempontjából a rendszeres szoftverfrissítés?

   A szoftverfrissítések és javítások (patchek) létfontosságúak, mivel olyan sebezhetőségeket kezelnek, amelyeket a támadók kihasználhatnak. A rendszeres frissítések biztosítják, hogy a biztonsági hibák kijavításra kerüljenek, így segítve a rendszerek védelmét az ismert fenyegetésekkel szemben.

3. Hogyan védi a fenyegetésektől a hálózati kapcsolatok kezelése a szoftvert?

   A tűzfalak, csomagszűrők és végpontvédelem biztosítják, hogy a szoftverek csak az engedélyezett hálózatokkal kommunikálhassanak. Ez megakadályozza a jogosulatlan hozzáférést, és megvédi a szoftvert a nem szándékos kapcsolatok, például a rosszindulatú bejövő forgalom általi veszélyeztetéstől.

Válaszok a gondolkodtató feladatokra

1. Mi történik a buffer overflow során?

   A buffer overflow akkor következik be, amikor több adat kerül a pufferbe, mint amennyit az elbír, ami a szomszédos memória felülírásához vezet. Ez lehetővé teheti a támadók számára, hogy rosszindulatú kódot juttassanak be, vagy összeomlasszák a rendszert. Ennek megelőzése érdekében a fejlesztőknek biztonságos kódolási gyakorlatokat kell alkalmazniuk, mint például a bemeneti érvényesítés és a határérték-ellenőrzések, valamint olyan biztonsági funkciókat, mint a stack canaries és az ASLR.

2. Hogyan használják ki a támadók az SQL injection sebezhetőségeket?

   SQL-injekcióról akkor beszélünk, amikor a támadók rosszindulatú SQL-kódot illesztenek be egy webes alkalmazás beviteli mezőibe, manipulálva az adatbázist, hogy jogosulatlan hozzáférést szerezzenek érzékeny adatokhoz vagy kártyékony műveleteket hajtsanak végre. Ez a probléma enyhíthető a felhasználói bemenetek ellenőrzésével és paraméterezett lekérdezések használatával, amelyek megakadályozzák az SQL utasítások közvetlen manipulálását.

3. Mi a különbség a végponti tűzfal (endpoint firewall) és a csomagszűrő (packet filter) között?

   A végponti tűzfal abban különbözik a csomagszűrőtől, hogy átfogóbb védelmet nyújt az egyes eszközök számára. Míg a csomagszűrő csak ellenőrzi és szűri az adatcsomagokat előre meghatározott hálózati rétegbeli szabályok (pl. IP-címek, portok vagy protokollok) alapján, a végponti tűzfal ennél tovább megy, mivel az eszközre jellemzően az összes bejövő és kimenő forgalmat felügyeli és ellenőrzi. A végponti tűzfalak összetettebb biztonsági házirendeket is érvényesíthetnek, például blokkolhatják az illetéktelen alkalmazásokat, megakadályozhatják a külső eszközök csatlakoztatását, és szabályozhatják, hogy bizonyos programok milyen adatokhoz férhetnek hozzá. A forgalom ellenőrzésének és a házirendek érvényesítésének ez a mélyebb szintje hatékonyabbá teszi a végponti tűzfalakat az egyes rendszerek védelmében, szemben a csomagszűrők egyszerűbb forgalomszabályozásával. A végponti tűzfalakra példa a Windows Defender Firewall és a macOS beépített tűzfala.

023.3 Malware

Hivatkozás az LPI célkitűzésre

Security Essentials version 1.0, Exam 020, Objective 023.3

Súlyozás

3

Kulcsfontosságú ismeretek

- A rosszindulatú szoftverek gyakori típusainak megértése
- A rootkit és a távoli hozzáférés fogalmának megértése
- A vírus- és malwareszkennerek megértése
- A kémkedésre, adatszivárgásra és a címjegyzékek másolására használt rosszindulatú programok kockázatának ismerete

A használt fájlok, kifejezések és segédprogramok részleges listája

- Vírusok, zsarolóprogramok, trójai programok, reklámprogramok, cryptominerek
- Backdoorok és távoli hozzáférés
- Fájlmásolás, billentyűzetnaplózás, kamera, mikrofon eltérítés

Lecke 1

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	023 Eszköz- és tárolóbiztonság
Fejezet:	023.3 Malware
Lecke:	1/1

Bevezetés

A *malware* kifejezés a *mal*-icious (rosszindulatú) és a soft-*ware* szavak szótagjaiból áll össze. Szoftvertípusok széles skáláját foglalja magában, amelyek végső soron a számítógépes rendszer vagy hálózat veszélyeztetésére irányulnak: vírusok, trójai programok, zsarolóprogramok, reklámprogramok stb. A legtöbb — ha nem is mindegyik — típusnak vannak altípusai is. A támadások gyakran akkor lesznek a legpusztítóbbak, ha e rosszindulatú szoftverek (malware) különböző kombinációit tartalmazzák.

A malware mögötti okok sokrétűek és változatosak — beleértve a csínytevéseket és az aktivizmust, de a kémkedést, az internetes lopást és más súlyos bűncselekményeket is. A malware programok túlnyomó többségét mindenesetre arra tervezték, hogy etikátlanul és illegálisan pénzt keressenek. A rosszindulatú programok többféle módon is bejuthatnak a számítógépbe vagy a hálózatba: fájlletöltések, gyanús mellékleteket vagy hivatkozásokat tartalmazó e-mailek, vagy fertőzött webhely meglátogatása — hogy csak néhányat említsünk.

Ez a lecke bemutatja a különböző típusú rosszindulatú programok alapelveit (a *modus uperandi* -t — munkamódszerüket), a lehetséges károk mértékét, és azt, hogy hogyan védhetjük meg a számítógépét ellenük.

A malwarek gyakori típusai

A következő alfejezetek a leggyakoribb malwarek néhány típusát mutatják be.

Vírusok

A biológiai és a számítógépes *vírusoknak* egyaránt szükségük van gazdatestre ahhoz, hogy kárt okozzanak. A számítógépes vírus tehát egy rosszindulatú futtatható kód, amely települ a számítógépre és képes önmagát terjeszteni. A terjedés gyakran úgy történik, hogy a vírust tartalmazó kezdeti rosszindulatú e-mailt elküldik az áldozat címjegyzékében szereplő összes kapcsolatnak. Ahhoz, hogy pusztítást végezzen, a vírusnak emberi beavatkozásra van szüksége. Tehát amikor a gyanútlan felhasználó lefuttatja a fertőzött gazdafájlt, a vírus programok módosításával szaporodik, vagy más számítógépekre is átterjed, és így akár egy egész hálózatot is megfertőzhet.

A vírusok által okozott károk mértéke igen pusztító lehet, mivel általában olyan kellemetlen gyakorlatokra tervezték őket, mint a hálózat forgalommal való elárasztása, a programok korruptálása vagy a fájlok (vagy akár a merevlemez) törlése.

NOTE A vírusokkal ellentétben a *férgeknek* (worm) nincs szükségük sem fertőzött gazdafájlra, sem emberi beavatkozásra a terjedéshez. Önálló vírusfajtaként definiálhatók.

Ransomware (zsarolóvírus)

Amint a neve is mutatja, ez a fajta malware a felhasználói adatokat váltságdíjért (ransom) tartja fogva. Ezek a rosszindulatú szoftverek általában úgy működnek, hogy a váltságdíj kifizetéséig korlátozzák a felhasználók hozzáférését bizonyos fájlokhoz (vagy a számítógép egyes részeihez). A vírusokkal ellentétben a kiberbűnözők egy *ransomware* támadás során egyértelműek és világosak, elmagyarázzák az áldozatnak, hogy mi történt, valamint azt is, hogy milyen lépésekeet kell tennie az elveszett információk visszaszerzéséhez.

A zsarolóprogramok gyakran nyilvános kulcsú kriptográfiát és szimmetrikus kulcsot használnak a kompromitált fájlok titkosításához. Ezek a fájlok ezután elérhetetlenné válnak a jogos tulajdonosok számára; a fájlokat csak a támadó privát kulcsával lehet visszafejteni. Az áldozat üzenetet kap a váltságdíj kifizetésére vonatkozó utasításokkal. A támadók tehát állítólag csak akkor adják át a felhasználónak a privát kulcsot, ha az kifizeti a váltságdíjat. A vírusokhoz hasonlóan a zsarolóvírusok is gyorsan terjedhetnek, és egész szervezeteket tehetnek tönkre azáltal, hogy a hálózatokon keresztül terjednek, és fájl- és adatbázis-szervereket vesznek célba.

NOTE A zsarolóvírus-bűnözők személyazonosságuk védelme érdekében általában

virtuális valuta (pl. Bitcoin) formájában kérik a fizetséget.

Cryptominerek / Cryptojacking

A rosszindulatú *cryptominereket* (cryptobányász) úgy tervezték, hogy titokban kihasználják a CPU (vagy GPU) üresjáratát. Mivel a háttérben futnak, nehéz lehet őket felismerni. Így a rosszindulatú szoftver titokban települ a számítógépre (vagy webböngészőbe), és elkezd kriptovalutákat bányászni. Bár a bányászat az áldozatok számára észrevétlenül zajlik, általában fokozott ventilátor-tevékenységről vagy a processzor intenzív munkájának más jeleiről, például túlmelegedésről vagy teljesítménycsökkenésről számolnak be.

Rootkitek és távoli hozzáférés

A *rootkitek* olyan különféle rosszindulatú szoftvereket jelentik, amelyek célja, hogy a kiberbűnözők számára távoli hozzáférést (remote access) és irányítást biztosítsanak, miközben az áldozat számára észrevétlenek maradnak. A rootkitek általában jelszavak, valamint banki és személyes adatok ellopására szolgáló eszközökkel rendelkeznek. Innen ered a kifejezés: *root* (a támadók root hozzáférést kapnak) és *kit* (eszközkészletet) használnak.

A rootkitek különböző típusai a számítógép különböző részeit támadják meg: a kernelt, az alkalmazásokat, a firmwaret, a boot rendszert (bootkitek) vagy akár a RAM-ot.

Spyware

A *spyware* (kémprogram) egy általános kifejezés minden olyan rosszindulatú szoftverre, amelyet arra terveztek, hogy megfigyelje a számítógépes tevékenységünket, és — a legtöbbször — személyes vagy bizalmas információkat is ellopjon: hitelesítő vagy fizetési adatainkat, navigációs előzményeinket és így tovább. A kémprogramok tipikus változatai közé tartoznak a reklámprogramok (adware), a billentyűzetnaplózás (keylogging) valamint a kamera és a mikrofon eltérítése.

Adware

A *adware* (reklámprogram) általában a webböngészőn belül jelenik meg, és a malwarek egy olyan típusa, amely arra szolgál, hogy reklámokkal bombázza a képernyőt. A legtöbb fejlett adware az online viselkedésünket kémleli, hogy specifikus hirdetésekkel célozzon meg minket. A reklámprogramok törvényes szoftvernek álcázhatják magukat, hogy rávegyenek minket a telepítésükre, de a böngésző sebezhetőségén keresztül is telepíthetőek.

A rendszerre történő telepítés után az adware jellemzően az alábbi jelekről ismerhetők fel: Új eszköztárak jelennek meg a böngészőben, a weboldal linkjei rossz weboldalra vezetnek, a

böngésző lassabbá válik, a böngésző kezdőlapja megváltozik stb.

Keylogging

A *keylogging* (billentyűzetnaplózás) kifejezés magától értetődő. A keylogger tehát egy olyan típusú malware, amely a billentyűleütéseket egy fájlba rögzíti; a fájlt ezután elküldi egy harmadik félnek az interneten keresztül. Nyilvánvaló, hogy a kiberbűnözők komoly károkat okozhatnak az áldozatnak azáltal, hogy lehallgatnak olyan sebezhető információkat, mint a jelszavak, PIN-kódok vagy bankszámlaszámok.

A keyloggerek lényege, hogy elkerüljék a felfedezést és észrevétlenek maradjanak az áldozat számára, mielőtt a kár bekövetkezne.

NOTE A keyloggerek lehetnek hardveralapúak és szoftveralapúak is. Használhatók legitim felügyeleti eszközként is.

Kamera és mikrofon eltérítés

Ez a fajta *hijacking* (eltérítés) malware arra szolgál, hogy jogosulatlanul hozzáférjen mind a beépített, mind a külső mikrofonjainkhoz és kameráinkhoz. Így a kameraképünk és beszélgetéseink a beleegyezésünk nélkül rögzíthetők. Ez számos rosszindulatú cél miatt lehet és nagyon kellemetlen következményekkel járhat: Érzékeny adatok lehallgatása a hangfelvételeken keresztül, videók rögzítése és eladása gyanús weboldalaknak stb.

Trójai vírusok

Homérosz *Odüsszeia* vagy Vergilius *Aeneis* műve szerint a görögök a trójai háborút a ravaszságnak és a csalásnak köszönhetően nyerték meg: Ahelyett, hogy lerombolták volna Trója városfalait, kitalálták, hogy egy óriási fából készült lovat hagynak a város kapujában. A hiszékeny trójaiak behozták a lovat, és — legnagyobb meglepetésükre — felfedezték, hogy a görög katonák egész idő alatt benne rejtőztek. A görög mitológia analógiájára a trójai vírus (trojan horse vagy egyszerűen csak trójai) olyan malware, amely törvényes szoftver vagy tartalom, például video- vagy hangfájlok (vagy bármilyen más tartalom) álcája alatt észrevétlenül terjed. Valójában a trójaiakat inkább úgy lehet definiálni, mint a kiberbűnözők által használni kívánt bármilyen típusú rosszindulatú szoftver (vírusok, férgek, zsarolóprogramok stb.) többcélú terjedési stratégiáját.

A kiberbűnözők általi pusztításhoz használt gyakori módszerek

A következő alfejezetek bemutatnak néhány módszert, amelyet a kiberbűnözők az előző fejezetekben ismertetett malwarek némelyikének — ha nem mindegyikének — végrehajtására

vagy telepítésére használnak.

Backdoor

A *backdoor*-t (hátsó ajtó) úgy definiálhatjuk, mint a számítógépes rendszerhez való hozzáférés olyan módját, amely megkerüli az erre a célra tervezett legális, előre meghatározott protokollt (hasonlóan ahhoz, ahogyan az emberek néha valódi hátsó ajtókat használnak, hogy elkerüljék, hogy a valós épületekbe való belépésüket észleljék). Más szóval: A rendszerhez olyan behatoló fér hozzá, aki minden biztonsági intézkedést megkerül. De vajon a hátsó ajtókat szándékosan vagy egyszerűen véletlenül hozzák létre? Nos, mindkettő; nézzük meg.

Először is, ne feledjük, hogy a szoftverek általában — különösen a távoli hozzáférést feltételező szoftverek — sebezhetőek, ezért a kiberbűnözők keményen dolgoznak az úgynevezett *nulla napos sebezhetőségek* (zero-day vulnerability) felfedezésén. Ahogy a nevük is mutatja, ezeket a sebezhetőségeket még a szoftver megjelenésének napján felfedezik, és azért igazán veszélyesek, mert még nincsenek aktuális javítások vagy megoldások a potenciális károk ellensúlyozására. Így például egy portot véletlenül védtelenül hagyhatnak, és — ha felfedezésre kerül --, ezzel hátsó ajtót biztosíthatnak a behatolóknak.

Másodszor, a kiberbűnözők megpróbálhatnak saját maguk létrehozni egy hátsó ajtót. Ehhez például a social engineering módszerét alkalmazhatják, és megpróbálhatják meggyőzni az áldozatot, hogy telepítsen egy látszólag hasznosnak tűnő szoftvert, amely tartalmazza a hátsó ajtót létrehozó malwaret (például alagutat (tunnel) hozva létre a saját és az áldozat számítógépe között).

Végül, de nem utolsósorban, a gyártók és a fejlesztők maguk is létrehozhatnak és elhelyezhetnek hátsó ajtókat a termékeiken különböző okokból (az egyik ilyen ok a rendszerhez való hozzáférés biztosítása bármikor!).

A leggyakoribb kellemetlen dolgok közül, amelyekre a hátsó ajtók felhasználhatók, a következőket említhetjük:

- Rosszindulatú programok szállítása: trójaiak, keyloggerek stb.
- Kémkedés, azaz érzékeny információk ellopása, ami személyazonosság-lopáshoz vagy csalárd tranzakciók végrehajtásához vezethet stb.
- Szerverek eltérítése
- Weboldalak eltorzítása (defacing)

NOTE

A *Website defacement* (vagy *web defacement*) egy weboldal elleni támadás, amelynek során a kiberbűnözők a weboldal tartalmának egy részét a saját

tartalmukkal helyettesítik (pl. a honlapot egy olyan üzenettel helyettesítik, amely azt írja: “Ezt a weboldalt feltörték”).

Data Exfiltration

A data exfiltration (adatkinyerés) az adatoknak egy információs rendszerből történő jogosulatlan átvitelére utal. A data exfiltration egyik leggyakoribb formája a DNS-resolver feltörése. Egy ilyen forgatókönyv esetén a lépések a következők:

1. Adathalász-támadást (phishing attack) hajtanak végre: Egy e-mailt küldenek, amely egy dokumentumba ágyazott malwaret tartalmaz.
2. Az áldozat megnyitja az e-mailt. A rosszindulatú kód végrehajtásra kerül, és a DNS-resolveren keresztül parancs- és vezérlésicsatorna jön létre.
3. A malware elkezd szaporodni, amíg nem talál bizalmas adatokat, amelyeket kinyerhet. Az adatokat ezután egy külső szerverre küldi.

NOTE

A DNS a *Domain Name System* rövidítése, és nagyon fontos szerepet tölt be az interneten, mivel ez a rendszer felelős a hostnevek IP-címekre történő lefordításáért.

Hogyan jutnak be a malwarek a számítógépbe, és mit tehetünk ellenük?

Mint már láttuk, a malwarek többféle módon is bejuthatnak a számítógépünkre: amikor a felhasználó megtévesztő e-mailekben vagy weboldalakon felugró ablakokban található linkekre kattint, mellékleteket nyit meg, USB-meghajtót helyez be stb. A cryptominereket például egyszerűen egy weboldal meglátogatásával is el lehet juttatni! Ebben az esetben a rosszindulatú JavaScript egy darabját már korábban beágyazták a weboldalba, így minden látogató hoston elindul a cryptomining (cryptobányászat). Hasonlóképpen, a vírusok — és más típusú rosszindulatú programok — másolatokat készíthetnek a rendszerben lévő kritikus fájlokról, hogy ezzel elkerüljék az azonosítást.

A trójaiakat általában valamilyen social engineering módszerrel juttatják célba. Általában az áldozat egy adathalász e-mail üzenetet kap, amelynek melléklete tartalmazza a rosszindulatú kódot. Amint rákattint, lefut a tartalma.

NOTE

A *social engineering* egy gyűjtőfogalom, amely a bizalmas információk megszerzésére irányuló törvénytelen társadalmi gyakorlatokra utal. A *phishing* (adathalászat) egyfajta social engineering technika, amikor a támadó hamisított e-

mail üzenetet küld az áldozatnak, hogy rávegye őket bizalmas vagy érzékeny információk felfedésére. Az adathalászaton belül találunk specifikusabb támadásokat, mint például a *spear phising* (egy adott személyt céloz meg) vagy a *whaling* (egy vállalat magas rangú embereit célozza meg).

A malwarek elleni védelemnek több módja is van:

- Használjunk vírusirtó és antimalware szoftvereket (szkennerek stb.)!
- Tartsuk folyamatosan frissítve az összes szoftvert (antimalware és egyéb)!
- Korlátozzuk az adathozzáférést!
- Futtassunk programokat virtuális környezetben (*sandboxing*)!
- Ellenőrizzük, hogy tartalmaznak-e az e-mailek és a csatolmányok rosszindulatú programokat!
- Ne töltsünk le vagy telepítsünk futtatható fájlokat nem megbízható forrásból!
- Figyeljünk az adathalász e-mailekre utaló jelekre (furcsa tartománynevek, nyelvtani és gépelési hibák stb.)!
- Rendszeresen készítsünk biztonsági mentést az eszközökről és a fontos adatokról!
- Erősítsük meg a hitelesítési rendszereinket!

NOTE

A Linux kernelhez egy nagy teljesítményű tűzfal, az *iptables* tartozik, és néhány disztribúció saját, felhasználóbarát front-endet is tartalmaz hozzá (az Ubuntu például a *Gufw*-t). Hasonlóképpen, az *nmap* (egy hálózati szkenner) minden nagyobb GNU/Linux disztribúció repositoryjában megtalálható, és a rosszindulatú programok bizonyos típusai ellen használható a hálózatok védelmére. Sok más malware elleni megoldás is elérhető Linuxhoz, de ez nem tartozik ennek a leckének a tárgykörébe.

Gyakorló feladatok

1. Tekintsük át a következő tüneteket, és határozzuk meg, hogy legvalószínűbben melyik malware típushoz tartoznak:

Tünet	Malware típusa
A számítógép túlmelegszik, amikor egyszerűen csak szörfözünk az interneten.	
Észreveszünk egy általunk nem telepített, új eszköztárat a böngészőjében.	
Egy nem általunk írt e-mailt elküldenek mindenkinek a címjegyzékből.	
Nem tudunk hozzáférni a fájljainkhoz, mert azok titkosítva vannak.	
Nem engedélyezett fényképeket találunk magunkról a világhálón.	

2. Jelöljük meg, hogy az alábbi tevékenységek kockázatos gyakorlatnak vagy védőintézkedésnek minősülnek-e:

Intézkedés	Kockázatos gyakorlat vagy védőintézkedés
Az adathozzáférés korlátozása	
Futtatható fájl telepítése nem megbízható forrásból	
Felugró ablakra kattintás	
A legújabb rendszerfrissítések telepítése	
Gyanús USB-kulcs behelyezése a számítógépbe	
Rendszeres biztonsági mentés	
Hitelkártyaadatok elküldése e-mailben	

3. Milyen típusú támadás esetén kapunk csalárd e-mailt, amely látszólag megbízható forrásból (bank, közösségi média, rokonok vagy ismerősök, cégen belüli felettes) érkezik?

4. Milyen kifejezés határozza meg azokat a malwareket, amelyek legitim szoftvernek (vagy

tartalomnak) adják ki magukat?

5. Milyen típusú rosszindulatú szoftver rögzíti titokban a billentyűzeten lenyomott billentyűket?

Gondolkodtató feladatok

1. Tegyük fel, hogy a készülék mikrofonját eltérítették, és a kiberbűnözők elkapnak néhány személyes információt rólunk. Hogyan használhatnák fel ezeket az információkat arra, hogy hozzáférjenek az online szolgáltatásainkhoz?

2. A szignatúra-alapú felismerést a vírusirtó szoftverek használják a rosszindulatú programok azonosítására. Mit értünk a *vírus szignatúrája* (virus signature) vagy *vírusdefiníció* (virus definition) kifejezések alatt?

3. Keressünk rá az interneten a következő kifejezésekre, és magyarázzuk el jelentésüket:
   a. Kétfaktoros (vagy többfaktoros) autentikáció:
   b. Botnet:

Összefoglalás

Ebben a leckében megtudhattuk, hogy mi a malware, mik a malware különböző típusai és hogyan működnek. Azt is megtanultuk, hogy a rosszindulatú programok milyen különböző módon tudnak beszivárogni a számítógépre, és hogyan védhetjük meg hatékonyan a rendszert a malwarek támadásaitól.

Válaszok a gyakorló feladatokra

1. Tekintsük át a következő tüneteket, és határozzuk meg, hogy legvalószínűbben melyik kártevőtípushoz tartoznak:

Tünet	**Malware típusa**
A számítógép túlmelegszik, amikor egyszerűen csak szörfözünk az interneten.	Cryptomining
Észreveszünk egy általunk nem telepített, új eszköztárat a böngészőjében.	Adware (reklámprogram)
Egy nem általunk írt e-mailt elküldenek mindenkinek a címjegyzékből.	Vírus
Nem tudunk hozzáférni a fájljainkhoz, mert azok titkosítva vannak.	Ransomware (zsarolóvírus)
Nem engedélyezett fényképeket találunk magunkról a világhálón.	Camera hijacking (a kamera eltérítése)

2. Jelöljük meg, hogy az alábbi tevékenységek kockázatos gyakorlatnak vagy védőintézkedésnek minősülnek-e:

Intézkedés	**Kockázatos gyakorlat vagy védőintézkedés**
Az adathozzáférés korlátozása	Védőintézkedés
Futtatható fájl telepítése nem megbízható forrásból	Kockázatos gyakorlat
Felugró ablakra kattintás	Kockázatos gyakorlat
A legújabb rendszerfrissítések telepítése	Védőintézkedés
Gyanús USB-kulcs behelyezése a számítógépbe	Kockázatos gyakorlat
Rendszeres biztonsági mentés	Védőintézkedés
Hitelkártyaadatok elküldése e-mailben	Kockázatos gyakorlat

3. Milyen típusú támadás esetén kapunk csalárd e-mailt, amely látszólag megbízható forrásból (bank, közösségi média, rokonok vagy ismerősök, cégen belüli felettes) érkezik?

   Phishing támadás

4. Milyen kifejezés határozza meg azokat a malwareket, amelyek legitim szoftvernek (vagy

tartalomnak) adják ki magukat?

Trójai vírusok (trojan horse)

5. Milyen típusú rosszindulatú szoftver rögzíti titokban a billentyűzeten lenyomott billentyűket?

Keyloggerek

Válaszok a gondolkodtató feladatokra

1. Tegyük fel, hogy a készülék mikrofonját eltérítették, és a kiberbűnözők elkapnak néhány személyes információt rólunk. Hogyan használhatnák fel ezeket az információkat arra, hogy hozzáférjenek az online szolgáltatásainkhoz?

   Ne feledjük, hogy egyes online szolgáltatások *biztonsági kérdéseket* használnak arra az esetre, ha elfelejtettük a jelszavunkat. Így a kiberbűnözők bejelentkezhetnek a szolgáltatásba, ha helyesen válaszolnak például az olyan kérdésekre, hogy mi a háziállatunk neve vagy milyen színű a szeme.

2. A szignatúra-alapú felismerést a vírusirtó szoftverek használják a rosszindulatú programok azonosítására. Mit értünk a *vírus szignatúrája* (virus signature) vagy *vírusdefiníció* (virus definition) kifejezések alatt?

   A vírus szignatúrája vagy a vírusdefiníció a vírus ujjlenyomatára utal, vagyis azon egyedi adatok összességére, amelyek lehetővé teszik a vírusirtó szoftverek számára a vírus azonosítását.

3. Keressünk rá az interneten a következő kifejezésekre, és magyarázzuk el jelentésüket:

   a. Kétfaktoros (vagy többfaktoros) autentikáció:

      A kétfaktoros hitelesítés (Two-Factor Authentication, 2FA) vagy a többfaktoros hitelesítés (Multifactor Authentication, MFA) a felhasználói fiókok védelme során további biztonsági rétegeket biztosít.

   b. Botnet:

      A botnetet fertőzött számítógépek (“botok”) hálózataként definiálhatjuk, amelyeket tömeges támadások, például elosztott szolgáltatásmegtagadás (DDOS) stb. végrehajtására használnak.

023.4 Adatelérhetőség

Hivatkozás az LPI célkitűzésre

Security Essentials version 1.0, Exam 020, Objective 023.4

Súlyozás

2

Kulcsfontosságú ismeretek

- A biztonsági mentések fontosságának megértése
- A gyakori biztonsági mentési típusok és stratégiák megértése
- A biztonsági mentések biztonsági vonatkozásainak megértése
- Biztonsági mentések létrehozása és biztonságos tárolása
- Az adattárolás, az adathozzáférés és -megosztás megértése a felhőszolgáltatásokban
- A felhőalapú tárolás és a felhőben történő megosztott hozzáférés biztonsági vonatkozásainak megértése
- Az internetkapcsolattól való függőség és az adatok felhőszolgáltatások és a helyi tárolók közötti szinkronizálásának ismerete

A használt fájlok, kifejezések és segédprogramok részleges listája

- Teljes, differenciális és inkrementális biztonsági mentések
- A biztonsági mentés megőrzése
- Fájlmegosztó felhőszolgáltatások

Lecke 1

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	023 Eszköz- és tárolóbiztonság
Fejezet:	023.4 Adatelérhetőség
Lecke:	1/1

Bevezetés

Napjaink digitális világában az adatok számos tevékenység éltető elemei, legyen szó személyes, tudományos vagy üzleti célú területről. Az adatok rendelkezésre állásának biztosítása kulcsfontosságú, mivel az adatvesztés katasztrofális következményekkel járhat. Ez a lecke végigvezet minket az adatelérhetőség alapvető fogalmain, beleértve a biztonsági mentéseket és a felhőalapú tárolást.

A biztonsági mentések (backup) fontossága

Az adatvesztés különböző okok miatt következhet be, például hardverhibák, szoftverhibák, emberi hibák vagy akár kibertámadások. A biztonsági másolatok az adatok másolatai, amelyekkel azok veszteség vagy sérülés esetén visszaállíthatók. Íme néhány fő ok, amiért a biztonsági mentések nélkülözhetetlenek.

A biztonsági mentések lehetővé teszik az adatok gyors és hatékony helyreállítását váratlan események, például hardverhibák, balesetek vagy kibertámadások esetén. A biztonsági mentések biztonsági hálót jelentenek az adataink számára.

A biztonsági mentések segítenek megőrizni az adatok integritását, biztosítva, hogy azok sértetlenek és sérülésmentesek maradjanak.

Az üzletmenet folytonossága szempontjából a biztonsági mentések kritikus fontosságúak a működés fenntartása és a leállások megelőzése szempontjából. Az ügyfél- vagy leltáradatok elvesztése végzetes lehet egy vállalkozás számára, ezért a biztonsági mentések elengedhetetlenek.

Egy szervezet számára elengedhetetlen, hogy rendelkezzen egy jó biztonsági mentési tervvel (backup plan). A biztonsági mentési tervet úgy kell kidolgozni, hogy meghatározzák, milyen adatokat fontos megtartani, valamint azt, hogy milyen gyakran kell másolni a fontos adatokat.

Gyakori biztonsági mentési típusok és stratégiák

A biztonsági mentési terv hatékony végrehajtásához elengedhetetlen, hogy az adatok kritikusságán és a változások gyakoriságán alapuló következetes ütemezés kialakítása mellett többféle biztonsági mentési típust és stratégiát is figyelembe vegyünk.

A *teljes biztonsági mentés* (full backup) egy adott időpontban az összes adatot másolja. Teljes körű adatvisszaállítást biztosít. Általában egy rendszerben az első biztonsági mentés teljes biztonsági mentés. Bár ez a módszer biztosítja a legátfogóbb helyreállítási lehetőséget, időigényes és jelentős tárhelyet igényel. A teljes biztonsági mentéseket az idő- és erőforrásigényük miatt jellemzően ritkábban végzik el, de gyakran használják őket más típusú biztonsági mentések alapjául.

Az *inkrementális biztonsági mentések* (incremental backup) csak azokat az adatokat másolják, amelyek az utolsó biztonsági mentés óta megváltoztak, függetlenül attól, hogy az teljes vagy inkrementális biztonsági mentés volt. Ez a módszer hatékony a tárolás és az idő szempontjából, mivel kevesebb helyet igényel és gyorsabb a feldolgozása. A helyreállítás során azonban szükség van az utolsó teljes és minden további inkrementális biztonsági mentésre, ami bonyolultabbá teheti a helyreállítást.

A *differenciális biztonsági mentés* (differential backup) az utolsó teljes biztonsági mentés óta végrehajtott összes változtatást elmenti, függetlenül attól, hogy készültek-e korábbi differenciális biztonsági mentések. Ez a módszer több helyet igényel, mint az inkrementális biztonsági mentés, de egyszerűsíti a visszaállítási folyamatot, mivel csak az utolsó teljes biztonsági mentésre és a legutóbbi differenciális biztonsági mentésre van szükség.

A *snapshot biztonsági mentések* (snapshop backup) egy adott időpontban rögzítik a rendszer állapotát. A hagyományos fájlalapú biztonsági mentésekkel ellentétben a pillanatfelvételek (snapshot) gyorsan elkészíthetők, és szinte azonnali helyreállítást tesznek lehetővé a rendszer korábbi állapotba történő visszaállításával. A snapshotok azonban fejlettebb tárolórendszereket igényelnek, és nem biztos, hogy ugyanolyan részletes helyreállítási lehetőségeket kínálnak, mint

más módszerek.

Példa-forgatókönyvek

A backup plan fontos szempontja, hogy megértsük, mikor kell differenciális vagy inkrementális mentést használni a teljes mentés után. A differenciális és inkrementális biztonsági mentések közötti különbségek szemléltetésére hasonlítsuk össze a következő két példát!

Adatok visszaállítása teljes és inkrementális biztonsági mentésekből

Képzeljünk el egy Emma nevű informatikai rendszergazdát, aki egy közepes méretű e-kereskedelmi vállalatnál dolgozik. A vállalat adatbázisa kritikus fontosságú vásárlói rendelési információkat tartalmaz, és az adatok rendelkezésre állásának biztosítása érdekében rendszeres biztonsági mentéseket végeznek.

Vasárnap este Emma kezdeményezi a teljes adatbázis teljes biztonsági mentését, rögzítve az összes ügyfélmegrendelést és termékkészlet-adatot.

Hétfőtől szombatig naponta inkrementális biztonsági mentések készülnek. Ezek a biztonsági mentések csak azokat az adatokat rögzítik, amelyek az utolsó biztonsági mentés óta megváltoztak. Az adatbázisban minden nap történnek kisebb frissítések az új megrendelések és termékbővítések miatt.

Szerdán hardverhiba történik, és az adatbázisban lévő adatok egy része megsérül. A szerda reggel leadott megrendelések elvesznek.

Az elveszett adatok visszaállításához Emma a legutóbbi, vasárnap készült teljes biztonsági mentést használja. Ez a biztonsági mentés tartalmazza az alapadatokat. Ezután az Emma a hétfői, keddi és szerdai inkrementális biztonsági mentéseket alkalmazza. Ez a folyamat biztosítja, hogy naprakészre hozza az adatbázist, miközben minimalizálja az átvitt adatok mennyiségét és a helyreállításhoz szükséges időt.

A teljes biztonsági mentésből történő visszaállítással és az inkrementális biztonsági mentések alkalmazásával az Emma sikeresen helyreállítja az elveszett adatokat, biztosítva, hogy az összes megrendelés és termékinformáció sértetlen marad a szerdai hardverhiba pillanatáig.

Adatok visszaállítása teljes és differenciális biztonsági mentésekből

Most tekintsünk át egy másik forgatókönyvet, amelyben a résztvevők ugyanaz az e-kereskedelmi vállalat és Emma, az IT-adminisztrátor, de ezúttal differenciális biztonsági mentési stratégiát használnak.

Vasárnap este Emma kezdeményezi a teljes adatbázis teljes biztonsági mentését, rögzítve az összes megrendelést és termékkészlet-adatot.

Emma a hét folyamán naponta ütemezi a differenciális biztonsági mentéseket. Ezek a biztonsági mentések az utolsó teljes biztonsági mentés óta bekövetkezett összes adatváltozást rögzítik.

Szerdán egy szoftverhiba miatt adatbázis-sérülés következik be, ami adatvesztéshez vezet.

Az elveszett adatok visszaállításához Emma a vasárnap este készített legutóbbi teljes biztonsági mentést használja. Ez a teljes biztonsági mentés tartalmazza az alapadatokat. Ezután az Emma csak a legutóbbi, szerdai differenciális biztonsági mentést alkalmazza. Mivel a differenciális biztonsági mentések a legutóbbi teljes biztonsági mentés óta bekövetkezett összes változást rögzítik, csak a legfrissebb differenciális biztonsági mentésre van szükség.

A teljes biztonsági mentésből történő visszaállítással és a legfrissebb differenciális biztonsági mentés alkalmazásával az Emma sikeresen helyreállítja az elveszett adatokat, biztosítva, hogy az összes megrendelés és termékinformáció a szerdai szoftverhiba időpontjáig helyreálljon. Ez a módszer leegyszerűsíti a helyreállítási folyamatot, mivel csak a teljes biztonsági mentést és a legutóbbi differenciális biztonsági mentést kell visszaállítani, ellentétben az inkrementális biztonsági mentésekkel, amelyeknél több biztonsági mentést kell egymás után alkalmazni.

A biztonsági mentés megőrzése

A hatékony adatkezeléshez és a katasztrófa utáni helyreállítási tervezéshez elengedhetetlen a megfelelő *biztonsági mentés-megőrzési irányelv* (backup retention policy). Ez határozza meg, hogy a biztonsági mentéseket mennyi ideig kell megőrizni, és milyen feltételek mellett lehet törölni őket. A jól megtervezett megőrzési irányelv célja az adatok rendelkezésre állásának, a megfelelési követelményeknek, a tárolási költségeknek és a működési hatékonyságnak az egyensúlyban tartása. Íme a jó biztonsági mentés-megőrzési irányelv néhány kulcsfontosságú eleme.

Először is az adatokat fontosságuk alapján osztályozzák, és a különböző adatkategóriákhoz felhasználási és megőrzési időszakokat határoznak meg (pl. a napi biztonsági mentéseket 7-30 napig kellhet megőrizni az operatív helyreállításhoz, a heti biztonsági mentéseket 4-12 hétig a rövid távú helyreállításhoz, és a havi vagy éves biztonsági mentéseket hosszú távú archiválási célokra).

Az adatmegőrzési időszakokat előíró ágazatspecifikus szabályozásoknak (pl. GDPR, HIPAA) való megfelelés biztosítása érdekében konzultálni kell a jogi és megfelelőségi (compliance) csapatokkal, hogy a megőrzési (retention) irányelveket összhangba hozzák a jogi követelményekkel.

Egy másik szempont a megőrzendő biztonsági mentések granularitása. Például lehet, hogy az elmúlt 24 órára vonatkozó óránkénti, az előző hétre vonatkozó napi és az előző évre vonatkozó

heti biztonsági mentéseket is megőrizzük.

Egy szervezet a biztonsági mentések több változatát is tárolhatja, különösen a kritikus adatok esetében, hogy ezzel lehetővé tegye a pontos helyreállítást.

Tekintettel a legtöbb biztonsági mentés korlátozott élettartamára, az automatizált folyamatok megkönnyíthetik a biztonsági másolatok törlését, amint elérik a megadott megőrzési időszakot. Ez segít elkerülni a manuális hibákat és biztosítja a megfelelőséget.

A hosszú távú biztonsági mentések külső tárolása védelmet nyújt az olyan katasztrófák ellen, mint a tűz, árvíz és hardverhiba.

Fontos, hogy rendszeresen teszteljük a helyreállítási folyamatot a különböző megőrzési időszakokkal rendelkező biztonsági mentések esetében, hogy az adatok sikeresen helyreállíthatók legyenek.

A biztonsági másolatok megőrzési irányelveit egyértelműen közölni kell az összes érintett féllel, beleértve az informatikai személyzetet, az adattulajdonosokat és a vezetőséget.

Az érdekelt feleknek rendszeresen felül kell vizsgálniuk és módosítaniuk kell a megőrzési irányelveket, hogy az igazodjon a változó üzleti igényekhez, a megfelelési követelményekhez és a technológiai fejlődéshez.

A biztonsági mentések megőrzési irányelveinek alapos dokumentációját kell létrehozni és fenntartani, beleértve a megőrzési időszakok részleteit, az adatok osztályozását és a megfelelőségi szempontokat.

A biztonsági mentési irányelveknek is szükségük van eljárásokra a kivételek kezelésére, például a jogi vizsgálatok vagy peres ügyek miatt bizonyos adatok megőrzési idejének meghosszabbítására.

A felügyeleti és jelentési mechanizmusok biztosíthatják a szabályzatnak való megfelelést, és figyelmeztethetik a rendszergazdákat a lehetséges problémákra vagy jogsértésekre.

A jó biztonsági mentési megőrzési irányelveknek egyensúlyt kell teremteniük az adatok rendelkezésre állása és a tárolási költségek között, miközben betartják a jogi és megfelelőségi követelményeket. Az irányelvek rendszeres felülvizsgálata és frissítése biztosítja, hogy az továbbra is hatékonyan megfeleljen a szervezet változó igényeinek.

A mentések biztonsági vonatkozásai

A biztonsági mentéseket ugyanolyan biztonsági szinten kell kezelni, mint az elsődleges adatokat.

Ezért ezeket titkosítani kell, hogy védettek legyenek a jogosulatlan hozzáféréssel szemben.

A hozzáférés-szabályozás biztosítja, hogy csak az arra jogosult személyek férjenek hozzá a biztonsági mentésekhez. Erről a szervezettől függően hasznos lehet naplót vezetni arról. Ezt a naplófájlt rendszeresen auditálni kell a biztonsági mentési irányelvek betartásának biztosítása érdekében.

További rugalmasságot teremt a biztonsági másolatok külön helyen történő tárolása, amely védelmet nyújt az olyan fizikai katasztrófák ellen, mint a tűz vagy a lopás. Harmadik félként cégek állnak rendelkezésre, amelyek átveszik a fizikai biztonsági mentéseket (általában szalagra írva), és egy korlátozott hozzáféréssel rendelkező, klimatizált külső helyszínen tárolják azokat. Az ilyen szolgáltatás drága lehet, és jellemzően nagyvállalatok veszik igénybe. Az adatlopás elleni óvintézkedésként minden külső helyszínen tárolt adatot titkosítani kell.

A felhőalapú vagy offsite biztonsági mentéseknek szigorú biztonsági protokollokat kell követniük, beleértve a titkosítást, a hozzáférés ellenőrzését és az adatvédelmi előírások betartását.

A zsarolóvírus-támadásokkal szemben ellenálló biztonsági mentési stratégiák közé tartozik a megváltoztathatatlan (immutable) tárolás vagy a légréses (air-gapped) mentések használata, amelyek biztosítják, hogy az adatok biztonságban maradjanak fertőzés esetén.

Biztonsági mentések létrehozása és biztonságos tárolása

A következő gyakorlatok segítenek a biztonsági mentések létrehozásában és biztonságos tárolásukban.

A biztonsági mentési szoftver vagy szolgáltatás kiválasztásakor figyelembe veendő tényezők közé tartozik a menthető rendszerek számossága és a biztonsági mentések visszaállításának egyszerűsége. Egyes biztonsági mentési megoldások *verziózást* (versioning) biztosítanak, amely lehetővé teszi a fájlok vagy adatok korábbi verzióinak elérését és visszaállítását. A szinkronizálás segít a változások előzményeinek megőrzésében, így szükség esetén visszaléphetünk egy adott időpontra. Ez hasznos a véletlen törlések vagy adatsérülések utáni helyreállításkor.

A rendszeresen ütemezett biztonsági mentések biztosítják, hogy adataink naprakészek legyenek. Monitorozzuk a biztonsági mentési megoldást, hogy megbizonyosodjunk arról, hogy az ütemterv betartásra kerül, valamint arról, hogy a biztonsági mentéshez rendelkezésre állnak az erőforrások.

A megbízható és biztonságos tárolóeszközök vagy szolgáltatások külső merevlemezeket, hálózati tárolókat (NAS) vagy felhőalapú tárolókat használnak a redundancia érdekében. Mágnesszalagot gyakran használnak külső helyszínen (offsite) történő archiválásra.

A biztonsági másolat sértetlenségét ellenőrizni kell a helyreállíthatóság biztosítása érdekében. Állítsunk fel egy ütemtervet, amelyben tesztelhetjük a biztonsági mentéseket az adatok és a

rendszerek visszaállítására egy felkészülési (staging) környezetben.

Adattárolás, hozzáférés és megosztás a felhőszolgáltatásokban

A felhőszolgáltatások kényelmes módot kínálnak az adatok tárolására, elérésére és megosztására. A legfontosabb fogalmak az alábbiak.

Ebben a biztonsági mentési modellben az adatokat a felhőszolgáltatók által fenntartott távoli szervereken tárolják. E szolgáltatások ára gyakran számos tényezőtől függ, például a biztonsági másolatokhoz szükséges tárhely mennyiségétől, a biztonsági másolatok megőrzési idejétől és az adatátvitel sebességétől, ha a biztonsági másolatot a rendszer helyreállításához kell felhasználni. Ne feledjük, hogy egyes internetszolgáltatók díjat számíthatnak fel a hálózatukon áthaladó nagy mennyiségű adatért.

A felhőszolgáltatások részletes ellenőrzést biztosítanak arra vonatkozóan, hogy ki férhet hozzá az adatainkhoz. A rendszergazda a felhőszolgáltató által biztosított eszközökkel kezelheti ezeket az ellenőrzéseket, jellemzően webes felületen vagy parancssori programon keresztül.

Az olyan tárhelyszolgáltatások, mint a Dropbox, a Google Drive és a OneDrive lehetővé teszik a fájlok egyszerű megosztását másokkal. Ne feledjük, hogy ezek a szolgáltatások nem feltétlenül biztonsági mentési megoldások, hanem a szervezeten belüli fájlokhoz való hozzáférés biztosításának eszközei. Amikor egy felhasználó szándékosan vagy véletlenül töröl egy fájlt, attól függően, hogy a többi felhasználó kliense hogy van beállítva, valószínűleg ugyanezt a fájl törlődik az ő rendszerükből. Az ilyen módon eltávolított fájl visszaállításához szükség lehet a felhőszolgáltatóval való kapcsolatfelvételre és a fájl visszaállításának kérésére. Ez szintén további költségekkel járhat.

A felhőalapú tárolás és a megosztott hozzáférés biztonsági vonatkozásai

Fontos megérteni, hogy a felhőmegoldások voltaképpen “valaki más számítógépei”. Ezt szem előtt tartva a felhőalapú tárhelyszolgáltatónak bizonyos szintű megbízhatóságot kell sugároznia az ügyfél felé, tekintettel arra, hogy rendszereikben az ügyfél legfontosabb adatainak másolatait fogják tárolni. Ennek a bizalomnak az előterében a következő megfontolások állnak.

A rendszergazdáknak fel kell mérniük a felhőszolgáltató által biztosított biztonsági intézkedéseket, és szükség esetén további titkosítást kell alkalmazniuk.

Az adatok megosztásakor is óvatosságra van szükség annak biztosítása érdekében, hogy csak az arra jogosult személyek férjenek hozzá. Logoljuk (naplózzuk), hogy ki fér hozzá a biztonsági másolatokhoz, valamint azt, hogy mikor történt a hozzáférés a biztonsági másolatokhoz.

Az internetkapcsolattól és az adatszinkronizációtól való függőség

Ha offsite vagy felhőalapú biztonsági mentési megoldásokkal foglalkozunk, tartsuk szem előtt a következőket:

A felhőalapú tárolás internetkapcsolattól függ. A kapcsolat hiánya befolyásolhatja az adatokhoz való hozzáférést. Amint azt korábban említettük, egyes internetszolgáltatók magasabb díjat számíthatnak fel a sávszélesség nagymértékű használatáért. Ne feledkezzünk meg az internetkapcsolattal járó biztonsági aggályokról sem!

A *szinkronizáció* biztosítja, hogy a felhőben tárolt adatok megegyeznek a helyi rendszereken tárolt adatokkal. Segít fenntartani az adatok konzisztenciáját azáltal, hogy a biztonsági másolatot naprakészen tartja a forrásadatokon végrehajtott változtatásokkal. Megfelelő szinkronizálás nélkül elavult vagy hiányos biztonsági mentéseink lehetnek, ami problémás lehet az adatok helyreállítása során.

Gyakorló feladatok

1. Mi a biztonsági mentés elsődleges célja?

2. Melyik biztonsági mentéstípus a leghatékonyabb a tárhely szempontjából, de lehet lassabb az adatok visszaállítása során?

3. Mi a célja a biztonsági mentések megőrzési irányelvének?

 | |

Gondolkodtató feladatok

1. Készítsünk biztonsági mentési tervet személyes vagy munkahelyi adatainkhoz, figyelembe véve az adatok típusát, a biztonsági mentések gyakoriságát és a tárolási lehetőségeket!

2. Vizsgáljunk meg egy népszerű felhőalapú tárolási szolgáltatást és annak biztonsági jellemzőit!

Összefoglalás

Ebben a leckében az adatmentések fontosságát, a gyakori mentési típusokat és stratégiákat, a biztonsági mentésekkel kapcsolatos biztonsági vonatkozásokat, valamint a felhőszolgáltatások adattárolásának alapjait tekintettük át. Az adatkezelés és a biztonsági mentési stratégiák legjobb gyakorlatainak követésével biztosíthatjuk értékes adataink rendelkezésre állását és biztonságát. Ha a biztonsági mentésekhez külső tárolóhelyet használunk (beleértve a felhőt is), az adatok biztonsága és sértetlensége érdekében mindenképpen titkosítani kell azokat.

Válaszok a gyakorló feladatokra

1. Mi a biztonsági mentés elsődleges célja?

   Az adatok helyreállítása adatvesztés vagy sérülés esetén.

2. Melyik biztonsági mentéstípus a leghatékonyabb a tárhely szempontjából, de lehet lassabb az adatok visszaállítása során?

   Inkrementális biztonsági mentések.

3. Mi a célja a biztonsági mentések megőrzési irányelvének?

   Annak meghatározása, hogy a biztonsági mentések mennyi ideig maradjanak meg és mikor törlődjenek.

Válaszok a gondolkodtató feladatokra

1. Készítsünk biztonsági mentési tervet személyes vagy munkahelyi adatainkhoz, figyelembe véve az adatok típusát, a biztonsági mentések gyakoriságát és a tárolási lehetőségeket!

   A feladat megoldása a mentésre kerülő rendszertől függően változik. A Linux-felhasználók a Déjà Dup és a duplicity segítségével könnyedén kezelhetik a biztonsági mentéseket, az Apple-felhasználók a Time Machine és az iCloud biztonsági mentéseket, a Windows-felhasználók pedig a Windows Backup segédprogramot használhatják. E segédprogramok közül sok kínál módot a biztonsági mentési feladatok ütemezésére, hogy lépést tartsanak az adatok változásával.

2. Vizsgáljunk meg egy népszerű felhőalapú tárolási szolgáltatást és annak biztonsági jellemzőit!

   A figyelembe veendő tényezők közé tartozik az egyes szolgáltatási csomagokhoz rendelkezésre álló tárhely mennyisége, az alkalmazott titkosítási módszerek, az adathozzáférési korlátozások és az adatátviteli díjak.

Linux Professional Institute

Témakör 024: Hálózat- és szolgáltatásbiztonság

024.1 Hálózatok, hálózati szolgáltatások és az internet

Hivatkozás az LPI célkitűzésre

Security Essentials version 1.0, Exam 020, Objective 024.1

Súlyozás

4

Kulcsfontosságú ismeretek

- A különböző hálózati médiumok és hálózati eszközök megértése
- Az IP-hálózatok és az internet fogalmának megértése
- Az útválasztás és az internetszolgáltatók (ISP-k) fogalmának megértése
- A MAC- és adatkapcsolati rétegbeli címek, az IP-címek, a TCP- és UDP-portok, valamint a DNS fogalmának megértése
- A felhőalapú számítástechnika fogalmainak megértése

A használt fájlok, kifejezések és segédprogramok részleges listája

- Vezetékes hálózatok, WiFi hálózatok, mobilhálózatok
- Switchek, Routerek, Access Point
- Default Router
- Internet Service Provider
- IPv4, IPv6
- TCP, UDP, ICMP, DHCP
- DNS, DNS hostnevek, forward DNS, reverse DNS
- Felhőalapú számítástechnika
- Infrastructure as a Service (IaaS)

- Platform as a Service (PaaS)
- Software as a Service (SaaS)

Linux Professional Institute

Lecke 1

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	024 Hálózat- és szolgáltatásbiztonság
Fejezet:	024.1 Hálózatok, hálózati szolgáltatások és az internet
Lecke:	1/2

Bevezetés

A mai digitális világban a számítógépes hálózatok és az internet alapvető ismerete minden informatikai szakember számára elengedhetetlen. Ez magában foglalja a hálózati médiatípusok, például a vezetékes és vezeték nélküli kapcsolatok alapvető fogalmainak megértését, valamint azt, hogy az adatok hogyan kerülnek továbbításra ezeken a hálózatokon keresztül. Szükséges az olyan címzési sémák, mint az IP-címek, az útválasztás (routing) és a csomagtovábbítás (packet forwarding) folyamata, valamint az olyan kulcsfontosságú internetes protokollok ismerete, mint a TCP/IP, a HTTP és a DNS. Ezek az elemek alkotják a hálózati kommunikáció gerincét, lehetővé téve a zökkenőmentes adatcserét.

Hálózati média és hálózati eszközök

A kiberbiztonság és a hálózatépítés területén kulcsfontosságú a hálózati médiumok alapvető típusainak és a hálózatokat összekötő eszközöknek a megértése. A *vezetékes*, a *vezeték nélküli* és a *celluláris* hálózatok mindegyike egyedi jellemzőkkel rendelkezik, és működésükhöz sajátos eszközökre van szükség. Ez a lecke a hálózati médiumok különböző típusait, a kezelésükhöz használt eszközöket és a hálózatok közötti kommunikáció lehetővé tételében betöltött szerepüket

vizsgálja.

Mielőtt belemerülnénk az internetbe és a funkcionalitását biztosító nagy teljesítményű protokollokba, fontos, hogy először az alapokat vizsgáljuk meg: a helyi hálózatokat. Ahhoz, hogy valóban megértsük, hogyan kapcsolódik össze minden, az alapokkal kell kezdenünk - -a hálózati médiatípusokkal és az ezeket a kapcsolatokat lehetővé tevő eszközökkel.

Hálózati médiatípusok

A *vezetékes hálózatok* fizikai kábeleket használnak az eszközök összekapcsolására, hasonlóan ahhoz, ahogyan a töltő csatlakoztatja a telefont a konnektorhoz. A vezetékes kapcsolatok leggyakoribb típusai az *Ethernet* és az *optikai szál* (fiber optic).

Az Ethernet széles körben elterjedt az otthonokban és az irodákban, mivel gyorsan tud adatokat küldeni, hasonlóan ahhoz, ahogyan egy vízsugár nagy nyomáson szállítja a vizet. Mind rövid távolságokon, például a számítógép és egy közeli router között, mind pedig az épületen belüli nagyobb távolságokon jól működik.

Az üvegszálas kábelek (fiber optic cable) viszont olyanok, mint az internet szupersztrádái. Az Ethernethez hasonló elektromos jelek helyett fényt használnak az adatátvitelhez, így sokkal gyorsabbak és sokkal nagyobb távolságokon is képesek az adatátvitelre — gondoljunk az optikai szálra úgy, mintha az információt fénysebességgel továbbítanák. Azonban, ahogyan egy autópálya építése is drágább, mint egy hagyományos út lefektetése, úgy az optikai szálak telepítése is költségesebb és bonyolultabb, ezért leggyakrabban nagyvállalatoknál vagy városok közötti internetkapcsolatoknál használják.

Ezzel szemben a *Wi-Fi hálózatok* rádióhullámokat használnak az adatátvitelhez, hasonlóan ahhoz, ahogyan az autórádió fogja a zenét egy állomásról, vezetékek nélkül. A Wi-Fi hihetetlenül népszerű, mivel lehetővé teszi, hogy az eszközök, például az okostelefonok és a laptopok, kábelek nélkül csatlakozhassanak az internethez. Ez a rugalmasság nagyszerű lehetőség arra, hogy úgy mozogjunk egy házban, hogy közben folyamatosan kapcsolatban maradunk.

A Wi-Fi általában két “csatornán” vagy frekvenciasávon működik: 2,4 GHz és 5 GHz. Gondoljunk ezekre úgy, mint a sávokra az úton. A 2,4 GHz-es sáv olyan, mint egy szélesebb út, amely messzebbre ér — így még a routertől távoli helyiségekben is csatlakozhatunk rá --, de a sebesség lassabb, mintha egy forgalmas autópályán vezetnénk. Ezzel szemben az 5 GHz-es sáv olyan, mint egy gyorsabb, de keskenyebb sáv. Gyorsabb sebességet biztosít olyan dolgokhoz, mint a streaming vagy a játék, de közelebb kell lennünk a routerhez, ahogyan gyorsan hajtani is könnyebb egy rövid, tiszta úton.

Azonban, bár a Wi-Fi szuper kényelmes, könnyebben megzavarható, hasonlóan ahhoz, ahogyan a rádiójeleket is befolyásolhatják a falak vagy más elektronikus eszközök. Biztonsági kockázatoknak

is jobban ki van téve, ezért fontosak az olyan intézkedések, mint az erős jelszavak és a titkosítás használata, hogy a hálózat biztonságban legyen a nem kívánt látogatóktól.

A *mobilhálózatok* (cell network), beleértve a 3G-t, a 4G-t és most már az 5G-t is, magas mobiltornyokat használnak az adatok küldésére és fogadására a mobiltelefonról. Ezek a tornyok jeleket küldenek, amelyeket a telefonunk vesz, így Wi-Fi vagy bármilyen kábel nélkül is hozzáférhetünk az internethez. Ezeknek a hálózatoknak köszönhetően használhatunk alkalmazásokat, böngészhetünk az interneten, vagy streamelhetünk zenét, miközben úton vagyunk, még akkor is, ha távol az otthonunktól.

Minden egyes generáció — 3G, 4G és 5G — ugrásszerűen növeli a hálózatok sebességét és teljesítményét. A 3G olyan, mint egy régi, lassabb út, amely korábban nagyszerű volt az olyan egyszerű tevékenységekhez, mint az üzenetküldés vagy az alapvető weboldalak betöltése. A 4G jött, és mindent felgyorsított, lehetővé téve az olyan tevékenységeket, mint a videostreaming és a gyorsabb letöltések. Az 5G a legújabb és leggyorsabb, olyan, mint egy nagy sebességű gyorsvonat, amely még több adatot képes egyszerre kezelni, így ideális az olyan tevékenységekhez, mint a virtuális valóság és az intelligens eszközök használata.

Azonban ahogy egyes területeken jobbak az útviszonyok, mint máshol, úgy a mobilhálózat sebessége és erőssége is attól függ, hogy hol tartózkodunk. Egyes helyeken nagyszerű 4G vagy 5G lefedettséggel rendelkezhetünk, ami gyors sebességet biztosít, míg más területeken a jel gyengébb lehet, ami lassabb internetkapcsolatot eredményez.

Hálózati eszközök

Ahhoz, hogy megértsük, hogyan kommunikálnak a hálózati eszközök, elengedhetetlen, hogy tisztában legyünk azzal, hogy hogyan azonosítják és ismerik fel egymást a különböző típusú hálózati médiumokon: Wi-Fi, Ethernet, optikai vagy mobilhálózatok.

Ez az azonosítás azért lényeges, mert amikor az egyik eszköz kérést intéz egy másikhoz, meg kell tudni állapítani, hogy honnan származik az adatcsomag, és melyik számítógépen van a címzett.

Helyi hálózati szinten ezt a címzést a *MAC-cím* (*Media Access Control*) néven ismert konvenció kezeli. A MAC-cím olyan, mint a hálózaton lévő minden egyes eszköz egyedi “ujjlenyomata”, amely biztosítja, hogy az adatokat megfelelően irányítsák és juttassák el a megfelelő eszközhöz. Ilyen típusú címzés nélkül lehetetlen lenne kezelni a több csatlakoztatott eszköz közötti adatforgalmat, ami zűrzavarhoz és adatvesztéshez vezetne.

Minden hálózathoz csatlakozó eszköznek saját MAC-címe van, így a címek elengedhetetlenek a hálózaton belüli kommunikációhoz. Minden MAC-cím hat pár hexadecimális karakterből vagy bájtból áll, ahol az első három pár általában az eszköz gyártóját azonosítja, az utolsó három pár pedig az adott eszközre specifikus.

A MAC-címek szabványát az *Institute of Electrical and Electronics Engineers* (IEEE) tartja fenn. A szabvány meghatározza, hogy az első három bájt, az úgynevezett *Organizationally Unique Identifier* (OUI) azonosítja a gyártót — Cisco, Intel stb. Az OUI-kat az IEEE jelöli ki a gyártóknak. A fennmaradó három bájtot a gyártó határozza meg, aki felelős az általa gyártott eszközök számozásának kezeléséért.

A MAC-címre egy példa:

```
00:1A:2B:3C:4D:5E**
```

A `00:1A:2B` azonosítja a gyártót. Ez az OUI egy kommunikációs termékeket gyártó kis vállalatra vonatkozik. A `3C:4D:5E`` a gyártó által gyártott adott eszköz egyedi azonosítója.

Bár a MAC-cím egyedi és a hardverbe ágyazott, különböző technikákkal módosítható, így szükség esetén megváltoztatható.

A hálózatokon belüli adatáramlás kezelésére és irányítására számos fontos eszközt használnak, amelyek mindegyike meghatározott szerepet tölt be. Ezeket a következő szakaszok ismertetik.

Switch

A *switch* olyan az ugyanazon a hálózaton belüli eszközök számára, mint egy közlekedési rendőr, aki biztosítja, hogy hatékonyan tudjanak egymással kommunikálni. Képzeljük el, hogy egy irodában több számítógép, nyomtató és egyéb eszköz van, amelyeknek mind meg kell osztaniuk egymással az információkat. A switch összekapcsolja őket, és gondoskodik arról, hogy a megfelelő adatok a megfelelő eszközhöz jussanak. Ezt a feladatot az *Open Systems Interconnection* (OSI) modell úgynevezett *adatkapcsolati rétegén* (data link layer, 2. réteg) végzi. Ezen a rétegen használják a fizikai címeket, azaz a MAC-címeket.

Amikor egy eszköz adatot küld, a switch a MAC-cím alapján megnézi, hogy melyik eszköznek szánták az adatot. Ahelyett, hogy az adatokat a hálózat minden eszközének elküldené, a switch csak a megfelelő MAC-címmel rendelkező eszközhöz irányítja azokat. Ez gyorsabbá és hatékonyabbá teszi a kommunikációt, megakadályozza a torlódást a hálózaton, és biztosítja, hogy az adatok oda jussanak el, ahová kell.

A switcheknek két fajtája van. A *managed switchek* olyan testreszabható eszközök, amelyeket hálózati rendszergazdák irányíthatnak, finomhangolhatják az adatáramlást, felügyelhetik a forgalmat, és szabályokat alkalmazhatnak a jobb teljesítmény és biztonság érdekében. Másrészt az *unmanaged switchek* egyszerűbbek, és automatikusan, beállítás vagy felügyelet nélkül működnek, úgy, mint egy egyszerű plug-and-play eszköz, amely egyszerűen csak elvégzi a munkát.

Router

A *router* (útválasztó) felelőssége szélesebb körű, mivel különböző hálózatokat köt össze. Az OSI-modell *hálózati rétegén* (network layer, 3. réteg) működik, ahol az IP-címek segítségével irányítják az adatokat a hálózatok között. Gondoljunk úgy egy routerre, mint egy postai szolgálatra, amely tudja, hogyan kell egy csomagot eljuttatni az egyik városból (hálózatból) a másikba. Otthoni környezetben a router csatlakoztatja az összes helyi eszközt — például telefonokat, laptopokat és okostévéket — a szélesebb internethez az *internetszolgáltatón* (Internet Service Provider — ISP) keresztül. A routerek alapvető fontosságúak annak biztosításában, hogy az adatok tudják, hová kell menniük, akár a helyi eszközök között, akár az interneten.

A routerek nemcsak a helyi hálózaton belüli adatforgalom kezeléséhez (az olyan eszközök, mint a telefonok és számítógépek között), hanem az otthoni hálózat és a tágabb értelemben vett internet közötti forgalom kezeléséhez is elengedhetetlenek. Router nélkül az eszközök nem tudnának kommunikálni a helyi környezetükön kívül és nem férnének hozzá az online erőforrásokhoz.

Access Point

Az *access point* (hozzáférési pont, AP) különösen fontos a vezeték nélküli hálózatok esetében. Ez egy olyan eszköz, amely Wi-Fi jelet sugároz, lehetővé téve az olyan eszközök, mint az okostelefonok, táblagépek és laptopok számára, hogy fizikai kábelek nélkül csatlakozzanak a hálózathoz. A hozzáférési pontot képzeljük el úgy, mint egy Wi-Fi jeladót, amely lehetővé teszi, hogy a vezeték nélküli eszközök kommunikáljanak a vezetékes hálózattal. Nagyobb területeken, például irodákban vagy iskolákban több hozzáférési pont is telepíthető a zökkenőmentes Wi-Fi lefedettség biztosítása érdekében, így az eszközök az épület különböző részein való mozgás közben is összeköttetésben maradhatnak anélkül, hogy elveszítenék a kapcsolatukat.

Sok otthonban gyakori, hogy a hozzáférési pont routerként is funkcionál. A legtöbb modern Wi-Fi router mindkét funkciót egyetlen eszközben egyesíti. Ez azt jelenti, hogy az eszköz nemcsak azt teszi lehetővé, hogy telefonjaink, laptopjaink és más vezeték nélküli eszközeink Wi-Fi segítségével csatlakozhassanak a hálózathoz, hanem az otthoni hálózat és az internet közötti forgalmat is kezeli. Ez a kettős funkció azért kényelmes, mert leegyszerűsíti a beállítást: Egyetlen eszköz képes gondoskodni mindenről, az eszközök közötti helyi forgalom kezelésétől az internet-hozzáférés biztosításáig.

IP hálózatok és az internet

A modern hálózatépítés középpontjában az *IP-hálózatok* és az *internet* állnak, két alapvető komponens, amelyek lehetővé teszik az eszközök számára, hogy hatalmas távolságokon keresztül kommunikáljanak és cseréljenek adatokat. E fogalmak működésének megértése alapvető fontosságú mindenki számára, aki a kiberbiztonsággal foglalkozik, mivel ezek alkotják az

adatátvitel és így a hálózati biztonság gerincét.

IP-hálózatok: A kommunikáció alapja

Az IP-hálózat olyan hálózat, amely az *Internet Protocol* (IP) protokollt használja az eszközök közötti adatátvitelre. Az IP-hálózat minden eszköze — legyen az számítógép, okostelefon vagy szerver — egyedi azonosítóval, úgynevezett *IP-címmel* rendelkezik. Ez a cím olyan, mint az eszköz otthoni címe, amely lehetővé teszi, hogy az adatok megtalálják az utat a megfelelő célállomáshoz.

Az IP-címeknek két elsődleges változata létezik, mindegyiknek megvan a maga formátuma és célja.

Az *Internet Protocol 4-es verziója* (IPv4) az IP-címzés legelterjedtebb változata. Négy számcsoportból áll, amelyek mindegyike 0-tól 255-ig terjed, és pontokkal vannak elválasztva (pl. `192.168.1.1.1`). A rendelkezésre álló IPv4-címek száma összesen körülbelül 4,3 milliárd, ami soknak tűnhet, de az internetre csatlakoztatott eszközök (okostelefonok, számítógépek, IoT-eszközök stb.) exponenciális növekedése miatt az IPv4-címek egyre szűkösebbé váltak. E hiány kezelésére olyan technikákat vezettek be, mint a *Network Address Translation* (NAT), hogy meghosszabbítsák az IPv4 használhatóságát, de ez csak ideiglenes megoldás volt.

Az *Internet Protocol 6-os verziója* (IPv6) megoldja az IPv4 korlátait. Ez a verzió sokkal hosszabb és összetettebb formátumot használ, amely nyolc, négy hexadecimális számjegyből álló, kettősponttal elválasztott csoportból áll (pl. `2001:0db8:85a3:0000:0000:8a2e:0370:7334`). Az IPv6 szinte korlátlan mennyiségű — körülbelül 340 decillió — címet biztosít, ami elegendő ahhoz, hogy az internetre csatlakoztatott eszközök iránti növekvő igényt még a jövőben is kielégítse. A több cím biztosításán túl az IPv6 javítja a hatékonyságot, egyszerűsíti az útválasztást (routing), és olyan funkciókkal növeli a biztonságot, mint a beépített titkosítás és a jobb eszközhitelesítés.

Az IP-hálózatok hihetetlenül rugalmasak. Lehetnek kicsik, mint például egy otthoni vagy irodai eszközöket összekötő *Local Area Network* (LAN), vagy lehetnek hatalmasak és összetettek, mint például egy több várost vagy országot átfogó *Wide Area Network* (WAN). A címzés és a csomagtovábbítás azonban minden IP-hálózat működésekor ugyanazokra az alapelvekre támaszkodnak.

Amikor az adatokat egy IP-hálózaton keresztül küldik, azokat kis egységekre, úgynevezett *csomagokra* (packet) bontják. Minden csomagot megjelölnek a forrás és a cél IP-címével, majd továbbítják a hálózaton. A korábban tárgyalt routerek felelősek azért, hogy ezeket a csomagokat az IP-címek segítségével megfelelő célállomásra irányítsák.

Az internet: egy globális IP-hálózat

Az internet lényegében a világ legnagyobb IP-hálózata, amely eszközök milliárdjait köti össze világszerte. Úgy működik, hogy több kisebb hálózatot kapcsol össze, lehetővé téve számukra az egymással való kommunikációt. Amikor meglátogatunk egy webhelyet, e-mailt küldünk vagy videót streamelünk, eszközünk az interneten keresztül kommunikál a világ minden táján található szerverekkel.

Az internet protokollok gyűjteményén alapul, amelyek közül a legfontosabb a *Transmission Control Protocol/Internet Protocol* (TCP/IP). Ez a protokollcsomag biztosítja az adatok megbízható továbbítását a különböző hálózatokon keresztül. A már tárgyalt IP-rész kezeli a címzést és az útválasztást, míg a TCP-rész biztosítja, hogy az adatok sértetlenül és a megfelelő sorrendben érkezzenek meg, még akkor is, ha több csomagban küldik őket.

Az internet egyik legfontosabb eleme a decentralizáció. Nem egyetlen szervezet irányítja az egész internetet, hanem számos összekapcsolt hálózatból áll, amelyeket különböző szervezetek, vállalatok és kormányok kezelnek. Ez a decentralizált struktúra teszi az internetet rendkívül ellenállóvá, ugyanakkor kihívásokat is jelent a szabályozás, a biztonság és a magánélet védelme terén.

Útválasztás és az internetszolgáltatók (ISP-k)

A hálózatépítésben a *routing* (útválasztás) és az internetszolgáltatók (Internet Service Provider, ISP-k) szerepe olyan alapvető fogalmak, amelyek segítenek megérteni, hogyan terjednek az adatok az interneten, és hogyan kommunikálnak az eszközök a különböző hálózatokon. Ezeknek a fogalmaknak a megértése kulcsfontosságú, különösen akkor, ha figyelembe vesszük a nyilvános és magánhálózatokon keresztüli adatátvitel biztonsági vonatkozásait.

Útválasztás: Hogyan találják meg az adatok az útjukat

Az internetes kommunikáció középpontjában az útválasztás (routing) áll — az a folyamat, amely meghatározza az adatok legjobb útvonalát az egyik eszközről a másikra történő továbbításához a különböző hálózatokon keresztül. Gondoljunk erre úgy, mint az internet GPS-ére. Amikor egy weboldal betöltésére irányuló kérést küldünk, az adatok kis csomagokra bontódnak, amelyeknek meg kell találniuk az utat a készülékünktől a weboldalnak otthont adó szerverig. Mint már említettük, a routerek olyan speciális eszközök, amelyek a hálózatok közötti forgalmat irányítják, és meghatározzák a leghatékonyabb útvonalat ezeknek a csomagoknak.

Az útválasztók IP-címek alapján hoznak döntéseket. Az adatokat a cél IP-cím alapján továbbítják, egyik hálózatról a másikra ugrálva, amíg az adatok el nem érik a végső célállomást. Ahogyan egy postai csomag is több elosztóközponton halad át, mielőtt megkapnánk, az adatcsomagok is több

routeren keresztül haladnak a különböző hálózatokon keresztül.

Az útválasztás az OSI-modell hálózati rétegén (network layer, 3. réteg) történik, és az útválasztók olyan protokollokat használnak a csomagok irányítására, mint például az IP.

Az útválasztás egyik fontos fogalma a *default router*, amelyet gyakran *default gateway*-nek (alapértelmezett átjáró) is neveznek, és amely döntő szerepet játszik abban, hogy az eszközök hogyan kommunikálnak mind a helyi hálózaton belül, mind a tágabb értelemben vett internettel. Egyszerűen fogalmazva, az alapértelmezett router hídként működik a helyi hálózat (például az otthoni hálózat) és a külső hálózatok, leggyakrabban az internet között.

Az alapértelmezett router az az eszköz, amelyet a számítógép vagy más eszközök használnak a külső hálózatok eléréséhez. Amikor egy helyi hálózaton lévő eszköznek adatokat kell küldenie egy másik, nem ugyanahhoz a hálózathoz tartozó eszköznek — például egy weboldalhoz való hozzáférés vagy egy felhőszolgáltatáshoz való csatlakozás --, az adatokat az alapértelmezett routerhez küldi. A router ezt követően továbbítja az adatokat a megfelelő célállomásra az interneten vagy egy másik külső hálózaton.

A legtöbb otthoni vagy kis irodai beállításban az alapértelmezett router ugyanaz az eszköz, mint a vezeték nélküli router, amely az internetszolgáltatón keresztül csatlakoztatja otthonunkat az internethez.

Internetszolgáltatók (ISP-k): Átjárók az internethez

Az internethez való kapcsolódást az internetszolgáltatók (ISPk) teszik lehetővé — ezek olyan vállalatok, amelyek otthoni, üzleti és szervezeti internet-hozzáférést biztosítanak. Ezek a cégek routerekből, kábelekből és szerverekből álló nagy hálózatokat üzemeltetnek, amelyek összekötik a kisebb helyi hálózatokat (például az otthoni Wi-Fi-t) a globális internettel.

Az internetszolgáltató egyedi *nyilvános IP-címet* rendel az otthonunkhoz vagy vállalkozásunkhoz, amely lehetővé teszi, hogy a router kommunikáljon az interneten lévő más eszközökkel. Amikor beírunk egy webcímet, a készülék először az internetszolgáltatóval veszi fel a kapcsolatot, aki a kérést a megfelelő internetes helyre irányítja. Az internetszolgáltató “közvetítőként” (middleman) működik, az adatokat a célállomásra irányítja, a válaszokat pedig visszaküldi nekünk.

Gyakorló feladatok

1. Mik a *vezetékes* és *vezeték nélküli* hálózatok közötti különbségek? Adjunk példákat mindegyikre, és magyarázzuk el, hogyan működnek!

2. Mi az a *MAC-cím*, és hogyan segíti az eszközök kommunikációját a helyi hálózaton? Adjunk példát arra, hogyan nézhet ki egy MAC-cím, és magyarázzuk el a felépítését!

3. Mik az *IPv4* és az *IPv6* címek közötti különbségek? Miért fejlesztették ki az IPv6-ot, és hogyan javít az IPv4 képességein?

Gondolkodtató feladatok

1. Vizsgáljuk meg, hogy hogyan használják a MAC-cím meghamisítását hálózati támadások esetén! Milyen potenciális biztonsági kockázatokkal járhat a MAC-spoofing, és milyen technikákkal lehet megelőzni az ilyen támadásokat?

2. Nézzünk utána, hogy milyen az IPv6 bevezetésének jelenlegi helyzete szerte a világon. Milyen kihívásokkal szembesültek a szervezetek az IPv4-ről az IPv6-ra való átállás során, és melyek az IPv6 használatának legfontosabb előnyei az IPv4-el szemben?

Összefoglalás

Ez a lecke a modern hálózatépítés kulcsfogalmait mutatja be, kezdve a helyi hálózatok alapjaival és azzal, hogy az eszközök hogyan kommunikálnak a különböző típusú hálózati médiumok, például vezetékes, vezeték nélküli és mobilhálózatok segítségével. Minden egyes hálózattípust ismertetünk, beleértve az Ethernet, az optikai szálak, a Wi-Fi és a celluláris technológiák, például a 3G, 4G és 5G szerepét.

A lecke elmagyarázza, hogyan kezelik az adatforgalmat a hálózati eszközök, például a switchek, routerek és hozzáférési pontok. A MAC-címek a helyi hálózaton lévő eszközök azonosítójaként kerülnek bemutatásra, lehetővé téve közöttük a hatékony kommunikációt. A tananyag elmagyarázza a switch szerepét a helyi forgalom kezelésében, valamint a router szerepét a különböző hálózatok összekapcsolásában, különösen az internet-hozzáférésben. Emellett a hozzáférési pont fogalmát is tárgyaljuk, kiemelve, hogy hogyan sugározza a Wi-Fi jelet a vezeték nélküli eszközöknek.

A lecke az IP-hálózatokkal és az internettel foglalkozik, kitérve arra, hogy hogyan használják az IP-címeket (mind az IPv4-et, mind az IPv6-ot) az eszközök azonosítására a globális hálózatokban. Bemutatja az Internet Protocolt (IP), mint a hálózatok közötti adatátvitel módszerét, és elmagyarázza az IP-címek két változata közötti különbséget. Az útválasztás az adatok legjobb útvonalának megtalálása, az alapértelmezett router és az internetszolgáltatók (ISP-k) szerepének ismertetése a szélesebb internethez való hozzáférés kulcsfontosságú elemei.

Végül kitér az internet decentralizált jellegére és a TCP/IP protokollok fontosságára a megbízható és biztonságos kommunikáció biztosításában. Olyan fogalmakról is szó esik, mint a csomagtovábbítás, az alapértelmezett átjárók és az internetszolgáltatók szerepe az internet-hozzáférés biztosításában.

Válaszok a gyakorló feladatokra

1. Mik a *vezetékes* és *vezeték nélküli* hálózatok közötti különbségek? Adjunk példákat mindegyikre, és magyarázzuk el, hogyan működnek!

   A vezetékes hálózatok az eszközök közötti adatátvitelhez fizikai kábelekre, például Ethernetre vagy optikai szálakra támaszkodnak. Az Ethernet-kábelek gyakoriak az otthoni és irodai beállításoknál a rövidebb távolságokon átívelő stabil kapcsolatokhoz, míg az optikai szálak fényt használnak az adatok sokkal nagyobb sebességű, nagyobb távolságokon történő továbbítására, gyakran városok között vagy nagy szervezeteknél. A vezeték nélküli hálózatok, például a Wi-Fi, rádióhullámokat használnak az adatátvitelhez, ami lehetővé teszi, hogy az olyan eszközök, mint a telefonok vagy a laptopok kábelek nélkül csatlakozzanak. A Wi-Fi különböző frekvenciasávokon működik, a 2,4 GHz-es frekvencia nagyobb hatótávolságot, de lassabb sebességet, az 5 GHz-es pedig nagyobb sebességet, de rövidebb távolságot biztosít.

2. Mi az a *MAC-cím*, és hogyan segíti az eszközök kommunikációját a helyi hálózaton? Adjunk példát arra, hogyan nézhet ki egy MAC-cím, és magyarázzuk el a felépítését!

   A MAC-cím az egyes eszközök hálózati kártyájához rendelt egyedi hardverazonosító, amely lehetővé teszi az eszközök számára, hogy ugyanazon a hálózaton belül kommunikáljanak. Biztosítja, hogy az adatok a hálózaton belül a megfelelő eszközhöz érkezzenek. A cím hat hexadecimális karakterpárból áll, amelyek közül az első három az eszköz gyártóját, az utolsó három pedig az adott eszközre jellemző. A MAC-címre példa a `00:1A:2B:3C:4D:5E`, ahol a `00:1A:2B` azonosítja a gyártót és a `3C:4D:5E` pedig a gyártó katalógusában szereplő adott eszközre jellemző.

3. Mik az *IPv4* és az *IPv6* címek közötti különbségek? Miért fejlesztették ki az IPv6-ot, és hogyan javít az IPv4 képességein?

   Az IPv4-címek négy, ponttal elválasztott számból állnak, például `192.168.1.1`, és korlátozott számú egyedi címet biztosítanak, ami az internethez csatlakozó eszközök számának növekedésével egyre kevésbé elegendő. Az IPv6-ot ennek a hiánynak a kezelésére hozták létre, sokkal hosszabb formátumot használva, több lehetséges kombinációval, például `2001:0db8:85a3:0000:0000:8a2e:0370:7334`. Az IPv6 szinte korlátlan mennyiségű címet kínál, valamint javítja az útválasztás hatékonyságát és a biztonságot olyan funkciókkal, mint a beépített titkosítás és a fokozott hitelesítés.

Válaszok a gondolkodtató feladatokra

1. Vizsgáljuk meg, hogy hogyan használják a MAC-cím meghamisítását hálózati támadások esetén! Milyen potenciális biztonsági kockázatokkal járhat a MAC-spoofing, és milyen technikákkal lehet megelőzni az ilyen támadásokat?

   MAC-cím hamisításról akkor beszélünk, ha egy eszközt szándékosan úgy konfigurálnak, hogy egy másik eszköz MAC-címét utánozza. A támadók ezt a technikát a hálózati szűrők megkerülésére, jogosulatlan hozzáférés megszerzésére vagy a hálózaton belüli identitásuk álcázására használják. Nyilvános Wi-Fi hálózatok esetén például egy támadó meghamisíthatja egy engedélyezett eszköz MAC-címét, hogy hozzáférjen a korlátozott területekhez.

   A kockázatok közé tartozik az érzékeny adatokhoz való jogosulatlan hozzáférés, a hálózati szolgáltatások megszakítása és a rosszindulatú tevékenységek nyomon követésének megnehezítése. A MAC-cím hamisítás megakadályozására a rendszergazdák olyan technikákat alkalmazhatnak, mint a portbiztonság a switcheken, amely portonként korlátozza a MAC-címek számát, valamint a MAC-címszűrés a routereken és a tűzfalakon. Emellett a hálózati titkosítás (pl. WPA3 a Wi-Fi esetében) és a szokatlan MAC-aktivitás figyelése segíthet a hálózatok védelmében az ilyen támadások ellen.

2. Nézzünk utána, hogy milyen az IPv6 bevezetésének jelenlegi helyzete szerte a világon. Milyen kihívásokkal szembesültek a szervezetek az IPv4-ről az IPv6-ra való átállás során, és melyek az IPv6 használatának legfontosabb előnyei az IPv4-el szemben?

   Globálisan az IPv6 fokozatosan terjedt el, egyes régiók és iparágak gyorsabban fejlődtek, mint mások. Az egyik fő kihívás az infrastruktúra IPv4-ről IPv6-ra való átállításának költsége és bonyolultsága volt, mivel számos régi rendszer nem teljesen kompatibilis az IPv6-al. Emellett néhány szervezetnek nincs közvetlen szüksége az IPv6 által biztosított hatalmas címtartományra, ami lassította az átállást.

   E kihívások ellenére az IPv6 jelentős előnyöket kínál az IPv4-el szemben, többek között exponenciálisan nagyobb címtartományt, egyszerűsített hálózati konfigurációt az olyan funkciókkal, mint az állapotmentes automatikus címkonfiguráció (stateless address autoconfiguration — SLAAC), és jobb hatékonyságot az útválasztásban. Az IPv6 jobb biztonsági funkciókat is tartalmaz, mint például a protokollba épített IPsec a titkosított kommunikációhoz.

Linux Professional Institute

Lecke 2

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	024 Hálózat- és szolgáltatásbiztonság
Fejezet:	024.1 Hálózatok, hálózati szolgáltatások és az internet
Lecke:	2/2

Bevezetés

Az informatikai szakemberek számára a hálózati kommunikáció és a felhőalapú számítástechnika megértése kulcsfontosságú. Ez a lecke az alapvető hálózati komponensekkel foglalkozik, és elmagyarázza, hogyan fordítja le a DNS a tartományneveket IP-címekre. A DHCP-t is feltárjuk és bemutatjuk a felhőalapú számítástechnikai modelleket, kiemelve, hogy ezek hogyan nyújtanak skálázható és rugalmas megoldásokat az IT-erőforrások kezelésére.

A TCP/IP és szerepük a hálózati kommunikációban

A TCP/IP modell lényege, hogy lehetővé teszi az adatok megbízható és hatékony továbbítását a hálózaton lévő eszközök között. A TCP/IP-modellben működő fő protokollok közé tartozik a TCP, az UDP, az ICMP és a DHCP, amelyek mindegyike külön szerepkörrel és jellemzőkkel rendelkezik.

Transmission Control Protocol (TCP)

A TCP egy *kapcsolat-orientált protokoll* (connection-orinted protocol), amely garantálja a megbízható, rendezett és hibaellenőrzött adatküldést a hálózaton keresztül. Ezt úgy éri el, hogy

két eszköz között kapcsolatot hoz létre a *háromirányú kézfogás* (three-way handshake) néven ismert folyamat segítségével. A kézfogás során az eszközök vezérlő üzeneteket (SYN, SYN-ACK és ACK) cserélnek, hogy szinkronizálják szekvenciaszámaikat és megállapodjanak a kommunikációs paraméterekben, mielőtt a tényleges adatátvitel megkezdődne.

A TCP kézfogás olyan, mint amikor a postás egy fontos, ajánlott levelet kézbesít. Először a postás (kliens) kopogtat az ajtón (SYN-kérést küld), hogy a címzett tudja, hogy levele érkezik. A címzett (szerver) kinyitja az ajtót, és egy aláírt nyugtát (SYN-ACK) ad vissza a levél megérkezésének visszaigazolásaként. Végül a postás a nyugta aláírásával (ACK) megerősíti a cserét, és távozik, biztosítva mindkét fél számára, hogy az üzenet sikeresen kézbesítve lett. Ez a megbízható csere garantálja, hogy a kommunikáció létrejön és megerősítést nyer, hasonlóan a postai kézbesítéshez, melynek során a kézbesítésről visszaigazolást kapunk.

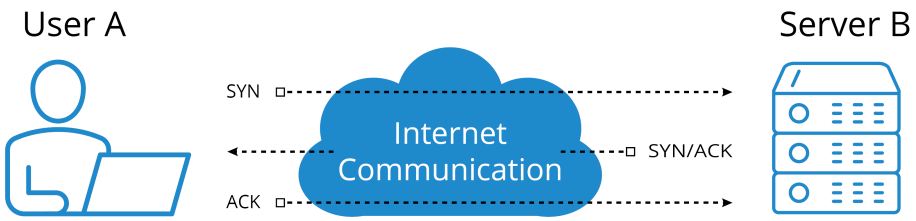

Figure 34. TCP/IP háromirányú kézfogás

Miután a kapcsolat létrejött, a TCP *szekvenciaszámokat* (sequence number) használ az egyes adatsegmensek nyomon követésére. Ezek a sorszámok biztosítják, hogy még akkor is, ha a csomagok a hálózati útvonalak vagy késések miatt nem a megfelelő sorrendben érkeznek, a fogadó rendszer helyesen tudja összerakni az adatokat. A TCP a csúszóablakok (sliding window) használatával *flow control* (adatfolyam-szabályozási) mechanizmusokat is tartalmaz, amelyek lehetővé teszik a vevő számára, hogy az adatátvitel ütemét úgy szabályozza, hogy az ne terhelje túl a feldolgozási képességeit vagy a pufferkapacitását.

A TCP szekvenciaszámok és az adatfolyam-szabályozás egy postáséhoz hasonlítható, aki meghatározott sorrendben kézbesít egy sor csomagot. Minden csomagot (adatszegmenst) egy számmal (szekvenciaszámmal) jelölnek, így mind a postás (kliens), mind a címzett (szerver) nyomon tudja követni a sorrendet. Ha egy csomag elvész vagy késik, a címzett értesítheti a postást, hogy csak az adott csomagot küldje újra.

A szekvenálás mellett a TCP az adatok kézhezvételének megerősítésére *visszaigazoló* (acknowledgement ACK) csomagokat is használ. A célállomás minden egyes fogadott szegmensre visszaigazolást küld, amely megerősíti az adatok sikeres megérkezését a szekvencia egy bizonyos bájtjáig. Ha egy bizonyos időn belül nem érkezik visszaigazolás, a TCP csomagvesztést feltételez,

és a vissza nem igazolt adatok *újraközvetítését* indítja el. Ez teszi a TCP-t rendkívül megbízhatóvá, mivel garantálja, hogy az adatok nem vesznek el útközben, még a torlódásra vagy csomagkiesésre hajlamos hálózatokban sem.

Ezek a megbízhatósági mechanizmusok teszik a TCP-t a legmegfelelőbb protokollá a garantált kézbesítést és adatintegritást igénylő alkalmazások számára. A webszolgáltatások (HTTP/HTTPS használatával), az e-mail átvitel (SMTP/IMAP) és a fájlátvitel (FTP/SCP) esetén mind a TCP-től függ, hogy az adatok sérülés és veszteség nélkül érkezzenek meg. Amikor például egy webböngésző megnyit egy weboldalt, a TCP biztosítja, hogy az oldal minden eleme (beleértve a HTML, CSS, JavaScript és képeket) megbízhatóan eljusson a szervertől a klienshez. Ha az adatfolyam bármely része megszakad, a TCP újraküldi a hiányzó szegmenseket, biztosítva ezzel, hogy az oldal teljes mértékben és helyesen töltődjön be.

User Datagram Protocol (UDP)

Az UDP egy *kapcsolat nélküli protokoll* (connectionless protocol), ami azt jelenti, hogy az adattovábbítás előtt nem szükséges kapcsolatot létesíteni az eszközök között. Ehelyett az UDP egyszerűen csak adatokat küld *datagramoknak* nevezett különálló egységekben, mindenféle formális beállítási folyamat nélkül. A TCP-vel ellentétben az UDP nem garantálja ezen adatküldemények kézbesítését, sorrendjét vagy integritását. Ez azt jelenti, hogy a csomagok érkezhetnek rendezetlenül, duplikálódhatnak, vagy teljesen elveszhetnek, és az UDP nem próbálja meg helyreállítani vagy újraküldeni őket.

A kapcsolatépítési és újraküldési mechanizmusok hiánya jelentősen csökkenti az overheadet, így az UDP a TCP-nél sokkal gyorsabb és hatékonyabb olyan helyzetekben, ahol előnyben részesítik a sebességet a megbízhatósággal szemben. Ez a tulajdonság kritikus az olyan alkalmazások esetében, ahol az adatokat gyorsan és valós időben kell átadni, még akkor is, ha néhány csomag elvész. Például a videostreaming esetében egy hiányzó csomag a videó minőségének enyhe romlását vagy rövid vizuális zavarokat okozhat, de a teljes adatfolyam zavartalanul, megszakítás nélkül folytatódik.

Hasonlóképpen, a *Voice over IP* (VoIP) alkalmazások UDP-t használnak a hangadatok továbbítására, ahol az enyhe csomagvesztés vagy jitter észrevétlen maradhat a felhasználó számára, de a késedelmek észrevehető problémákat okozhatnának a hívás minőségében.

Az online játékok számára előnyös az UDP alacsony késleltetése, mivel lehetővé teszi az adatok minimális késleltetéssel történő továbbítását, ami gyors és reszponzív játékot tesz lehetővé. Még akkor is, ha időnként csomagok vesznek el vagy késnek, a játék akkor is működőképes marad, anélkül, hogy lefagyna vagy megakadna.

Az UDP másik gyakori felhasználási területe a *DNS-lekérdezések*, amikor a kliens kérést küld egy

domainnév IP-címre való feloldására. Az UDP ideális erre a célra, mivel a DNS-lekérdezések jellemzően kis méretűek, és gyorsan kell megoldani őket. Ha nem érkezik válasz, a kliens egyszerűen újra elküldheti a kérést anélkül, hogy a TCP-kapcsolat létrehozásával és fenntartásával járó többletköltséget kellene viselnie.

Általánosságban tehát az UDP feláldozza a megbízhatóságot a sebességért, de valós idejű környezetben néhány elveszett csomag gyakran előnyösebb, mint az újraküldéssel járó késedelem.

Internet Control Message Protocol (ICMP)

Az ICMP-t elsősorban diagnosztikai és hibajelentő funkciókra használják a hálózatokban. A TCP-től vagy az UDP-től eltérően az ICMP nem szállítási protokoll, és nem az alkalmazási adatok továbbítására tervezték. Ehelyett vezérlő protokollként szolgál, amely lehetővé teszi a hálózati eszközök számára a hálózati feltételekről és hibákról szóló információk cseréjét, biztosítva az IP-alapú kommunikáció zavartalan működését.

Az ICMP egyik fő célja a hálózati problémák, például elérhetetlen állomás, hálózati torlódás vagy útválasztási problémák jelentése. Ha például egy router nem tud továbbítani egy csomagot, mert a célhálózat elérhetetlen, ICMP üzenetet küld vissza a kiindulási ponton lévő eszköznek, tájékoztatva azt a problémáról. Hasonlóképpen, ha egy router túlterhelt vagy torlódásos, az ICMP üzeneteket küldhet, amelyek jelzik, hogy a csomagok kiesnek vagy késnek.

Az ICMP-n alapuló, jól ismert és széles körben használt eszköz a `ping` parancs. A ping egy egyszerű, de hatékony diagnosztikai segédprogram, amely egy állomás elérhetőségét teszteli a hálózaton. A `ping` futtatásakor a rendszer ICMP *echo request* üzeneteket küld a célállomásnak, és az állomás ICMP *echo replies* üzenetekkel válaszol. A kérés elküldése és a válasz fogadása között eltelt idő segít meghatározni az eszköz és a célállomás közötti késleltetést és kapcsolódást. Ha nem érkezik válasz, az azt jelzi, hogy az állomás hálózati probléma miatt leállt vagy elérhetetlen.

TCP és UDP portok

A TCP és az UDP is *portokat* használ az egy eszközön lévő különböző szolgáltatások megkülönböztetésére. A port a kommunikáció logikai végpontja, amely biztosítja, hogy az adatok a megfelelő alkalmazáshoz kerüljenek. A portok számozása 0-tól 65535-ig terjed, a 0-1023-as portok a *well-known portok* (közismert portok) széles körben használt protokollok számára, például a HTTP (80-as port), a HTTPS (443-as port) és a DNS (53-as port). Az 1024-49151 közötti portok a *regisztrált portok*, a 49152 és 65535 közötti portok pedig a *dinamikus* vagy *privát portok*, amelyeket általában ideiglenes vagy belső kapcsolatokhoz használnak.

A szerveren minden egyes szolgáltatás vagy alkalmazás egy adott *portszámon* figyel, így amikor

egy TCP vagy UDP csomag érkezik, a célport alapján a megfelelő szolgáltatáshoz irányítják. Például egy weboldal böngészőn keresztüli látogatása a 80-as portra (HTTP esetén) vagy a 443-as portra (HTTPS esetén) küldi a kérést. Hasonlóképpen, egy DNS-lekérdezés az UDP 53-as portra kerül.

A hálózati biztonság szempontjából kulcsfontosságú a protokollok közötti különbségek és a portok használatának megértése, mivel a támadók gyakran kihasználják az ezeken a területeken található sebezhetőségeket. A biztonsági szakembereknek figyelemmel kell kísérniük a hálózati forgalmat, biztosítaniuk kell a szolgáltatások megfelelő konfigurációját, és védeniük kell a kritikus portokat a gyakori fenyegetések elleni védekezéshez.

DHCP: Hogyan kap egy eszköz IP-címet

Amikor egy eszköz, például egy számítógép vagy okostelefon csatlakozik egy hálózathoz, IP-címre van szüksége a többi eszközzel való kommunikációhoz. Ezt a folyamatot általában a *Dynamic Host Configuration Protocol* (DHCP) nevű szolgáltatás végzi. A DHCP automatikusan osztja ki az IP-címeket az eszközöknek, megkönnyítve ezzel a csatlakozást anélkül, hogy kézi beállításra lenne szükség.

Így működik: Amikor egy eszköz először csatlakozik egy hálózathoz, még nem rendelkezik IP-címmel. Ahhoz, hogy IP-címet kérjen, az eszköz egy speciális üzenetet, az úgynevezett *DHCP discover* üzenetet küld, amelyben IP-címet kér. Ezt az üzenetet a hálózat összes eszköze megkapja, mivel az eszköz nem ismeri a *DHCP-szerver* konkrét helyét. A DHCP-szerver egy olyan rendszer, amely az IP-címek elosztását kezeli.

Amint a DHCP-szerver megkapja ezt a kérést, egy *DHCP offer* a válasza, amely tartalmazza az eszköz által használható IP-címet, valamint az egyéb szükséges beállításokat, például az alhálózati maszkot és az alapértelmezett átjárót. Ezek a beállítások azért fontosak, mert ezek segítségével az eszköz tudja, hogyan kommunikáljon a hálózaton lévő többi eszközzel, és hogyan férjen hozzá az internethez.

Az ajánlat fogadása után az egy *DHCP request* nevű üzenetet küld vissza, amelyben jelzi, hogy elfogadja a javasolt IP-címet. Ez biztosítja, hogy a DHCP-szerver tudja, hogy az eszköz az általa felajánlott IP-címet kívánja használni. Végül a DHCP-szerver egy visszaigazolás, az úgynevezett *DHCP acknowledgment* (ACK) elküldésével megerősíti a hozzárendelést. Ekkor az eszköz elkezdheti használni az új IP-címét a hálózaton keresztül történő adatküldésre és fogadásra.

A DHCP-kiszolgáló által kiosztott IP-cím nem állandó; az eszköz egy meghatározott időszakra bérli azt. Amikor a bérlet lejár, az eszköz megújíthatja azt, hogy megőrizze ugyanazt az IP-címet.

A DHCP az IP-címek kiosztásának automatizálásával egyszerűsíti a hálózathoz való csatlakozás

folyamatát. DHCP nélkül a hálózati rendszergazdáknak minden eszközhöz kézzel kellene egyedi IP-címet rendelniük, ami időigényes és hibalehetőségekkel teli lenne, különösen nagy hálózatok esetén.

A DNS szerepe

Amikor az internetet használjuk, gyakran támaszkodunk domainnevekre, például az `lpi.org`-ra, hogy elérjük a weboldalakat. A számítógépek azonban nem értik közvetlenül ezeket a neveket, hanem IP-címek segítségével kommunikálnak. A felhasználóbarát domainneveket IP-címekre fordító rendszert a *Domain Name System* (DNS) nevű rendszernek hívják.

A DNS úgy működik, mint az internet telefonkönyve. Amikor beírjuk egy weboldal címet (például `learning.lpi.org`) a böngészőbe, a DNS felelős a domainnévhez tartozó IP-cím megtalálásáért, hogy a böngésző meg tudja találni a megfelelő webszervert, és csatlakozni tudjon hozzá.

A számítógép terminálján az `nslookup` vagy a `dig` parancs segítségével tájékozódhatunk arról, hogy milyen IP-cím tartozik egy domainnévhez, vagy fordítva:

```
$ nslookup learning.lpi.org
Server: 127.0.0.1
Address: 127.0.0.1#53

Non-authoritative answer:
Name: learning.lpi.org
Server: 208.94.166.201
```

DNS hostnevek

A hálózathoz csatlakoztatott minden eszközhöz hozzárendelhető egy *DNS hostnév*, amely egy ember által olvasható címke, amely az IP-címhez kapcsolódik. Például egy szervernek lehet a `webserver1.example.com` hostneve. Ezt a hostnevet az emberek könnyebben megjegyzik, mint a számítógépek által használt numerikus IP-címet. A hostnevek a szélesebb körű DNS-rendszer részét képezik, segítve a felhasználók és a rendszergazdák számára a hálózaton lévő eszközök kényelmesebb kezelését és azonosítását.

Forward DNS Lookup

A *forward DNS lookup* (előremutató névfeloldás) a DNS leggyakoribb használata. Ennek során a domainnevet a megfelelő IP-címre alakítják át. Amikor egy URL-címet írunk be a böngészőnkbe, egy forward DNS lekérdezés történik, a domainnév IP-címre való feloldásához. Ha például a

böngészőbe beírjuk a `www.example.com` címet, a DNS-rendszer forward lookupot végez a hozzá tartozó IP-cím, például a `192.0.2.1` keresésére, és a böngészőt a megfelelő szerverre irányítja.

A DNS-rendszer DNS-szerverek sorát használja a lookup elvégzésére. Eszközünk először egy helyi DNS *resolver*-rel veszi fel a kapcsolatot, amely a folyamat felgyorsítása érdekében gyorsítótárba (cache) helyezheti a korábbi lekérdezéseket. Ha az IP-cím nem található a gyorsítótárban, a feloldó más DNS-szerverekkel, köztük a tartomány *authoritatív DNS-szerverével* lép kapcsolatba a helyes IP-cím megtalálása érdekében. Ha az IP-cím megvan, visszaküldi a böngészőnek, és létrejön a kapcsolat a webszerverrel.

Reverse DNS Lookup

A *reverse DNS lookup* (fordított névfeloldás) éppen ellenkezőleg működik. Ahelyett, hogy egy domainnevet IP-címre alakítana át, egy IP-címet alakít vissza domainnévvé. Ez hasznos egy állomás identitásának ellenőrzésére, és gyakran használják e-mail szervereknél és hálózati hibaelhárításnál. Ha például egy szerver kérést kap egy IP-címről, és meg akarja erősíteni az állomás identitását, akkor reverse DNS lookupot végezhet, hogy megnézze az adott IP-címhez tartozó domainnevet. Ez segít megelőzni a rosszindulatú tevékenységet.

Míg a forward DNS lookup elengedhetetlen a mindennapi internethasználathoz, a reverse DNS lookupot a hálózati rendszergazdák, a biztonsági rendszerek és az e-mail szerverek használják a kapcsolatok integritásának biztosítására.

A DNS az internet működésének kritikus eleme, amely lehetővé teszi az emberbarát domainnevek gépileg olvasható IP-címekké történő lefordítását. A DNS biztosítja, hogy az eszközök és az emberek hatékonyan kommunikálhassanak az interneten, legyen szó akár forward DNS lookupról, amely lehetővé teszi a felhasználók számára, hogy domainnév alapján érjenek el weboldalakat, akár az identitás ellenőrzésére és a biztonság fenntartására használt reverse DNS lookupról. DNS nélkül az interneten való navigálás sokkal bonyolultabb lenne, mivel a felhasználóknak minden egyes weboldal és szolgáltatás esetében bonyolult IP-címeket kellene megjegyezniük.

A Cloud Computing koncepciói

A felhőalapú számítástechnika (cloud computing) olyan modell, amely lehetővé teszi a felhasználók számára, hogy a helyi hardverre és infrastruktúrára való támaszkodás helyett az interneten keresztül férjenek hozzá és kezeljenek az olyan számítástechnikai erőforrásokat, mint a szerverek, tárhelyek, adatbázisok és szoftverek. Ez a modell rugalmasságot, skálázhatóságot és költségmegtakarítást biztosít, mivel nem kell drága fizikai infrastruktúrába beruházni. A felhőalapú számítástechnikát jellemzően három fő szolgáltatási modellbe sorolják: *Infrastruktúra mint szolgáltatás* (Infrastructure as a Service — IaaS), *Platform mint szolgáltatás* (Platform as a

Service — PaaS) és *Szoftver mint szolgáltatás* (Software as a Service — SaaS). Mindegyik modell különböző szintű irányítást és menedzsmentet kínál, különböző igényeket és felhasználási eseteket szolgálva ki.

Infrastructure as a Service (IaaS)

Az IaaS a felhőalapú számítástechnikai szolgáltatások legalapvetőbb szintje. Az interneten keresztül virtualizált számítástechnikai erőforrásokat, például virtuális gépeket, tárhelyet és hálózatot biztosít. Az IaaS segítségével a felhasználók igény szerint bérelhetik ezeket az erőforrásokat, és felfelé vagy lefelé skálázhatják őket. Ez a szolgáltatási modell kínálja a felhasználók számára a legmagasabb szintű ellenőrzést, mivel a felhasználók felelősek saját operációs rendszereik, alkalmazásaik és adataik kezeléséért, a felhőszolgáltató pedig kezeli a mögöttes fizikai infrastruktúrát.

Az IaaS ideális olyan vállalkozások számára, amelyeknek rugalmas, skálázható erőforrásokra van szükségük, de a saját hardver megvásárlásával és karbantartásával járó költségek nélkül. Egy vállalat például használhatja az IaaS-t virtuális szerverek gyors felállítására új alkalmazások teszteléséhez, vagy infrastruktúrája méretének növelésére, hogy kezelni tudja a forgalom átmeneti növekedését egy marketingkampány során. Népszerű IaaS szolgáltató például az Amazon Web Services (AWS), a Microsoft Azure és a Google Cloud.

Platform as a Service (PaaS)

A PaaS egy olyan felhőszolgáltatási modell, amely platformot biztosít a fejlesztők számára az alkalmazások létrehozásához, telepítéséhez és kezeléséhez anélkül, hogy a mögöttes infrastruktúrával kellene törődniük. A PaaS magában foglal mindent, amire a fejlesztőnek szüksége van az alkalmazások létrehozásához és futtatásához, például fejlesztőeszközöket, middleware szoftvereket, adatbázisokat és operációs rendszereket. A PaaS segítségével a felhasználók a kódírásra és a funkciók létrehozására összpontosíthatnak, míg a felhőszolgáltató gondoskodik a szerverek, a tárolás, a hálózat és más backend szolgáltatások kezeléséről.

A PaaS ideális olyan fejlesztők és vállalkozások számára, amelyek egyszerűsíteni szeretnék a fejlesztési folyamatot, és csökkenteni az infrastruktúra kezelésének bonyolultságát. Egy fejlesztőcsapat például a PaaS segítségével gyorsan telepíthet egy új webes alkalmazást anélkül, hogy szervereket kellene konfigurálnia vagy adatbázisokat kellene karbantartania. Népszerű PaaS szolgáltatás például a Google App Engine, a Microsoft Azure App Service és a Heroku.

Software as a Service (SaaS)

A SaaS a leginkább felhasználóbarátabb és széles körben alkalmazott felhőszolgáltatási modell. A SaaS segítségével a felhasználók webböngészőn vagy kliensalkalmazáson keresztül férnek hozzá a

felhőben tárolt szoftveralkalmazásokhoz, anélkül, hogy a szoftvert helyben telepíteni vagy kezelni kellene. A felhőszolgáltató kezeli a szoftver kezelésének minden aspektusát, beleértve a frissítéseket, a biztonságot és az infrastruktúrát, így a felhasználók magára az alkalmazás használatára összpontosíthatnak.

A SaaS ideális olyan vállalkozások és magánszemélyek számára, akik a karbantartás, a frissítések vagy a technikai részletek miatt való aggódás nélkül szeretnének szoftvert használni. A SaaS gyakori példái közé tartoznak az olyan e-mail szolgáltatások, mint a Gmail, az olyan együttműködési eszközök, mint a Slack, és az olyan ügyfélkapcsolat-kezelő (CRM) rendszerek, mint a Salesforce. A SaaS-alkalmazásokat jellemzően előfizetéses alapon kínálják, így minden méretű vállalkozás számára elérhetővé és megfizethetővé válnak.

A felhőalapú számítástechnika forradalmasította a vállalkozások és a magánszemélyek technológiához való hozzáférését és annak használatát, rugalmasságot, skálázhatóságot és költséghatékonyságot kínálva. A három fő felhőszolgáltatási modell — IaaS, PaaS és SaaS — mindegyike különböző szintű ellenőrzést és kezelést kínál, lehetővé téve a felhasználók számára, hogy az igényeiknek leginkább megfelelő modellt válasszák. Legyen szó akár virtuális infrastruktúra bérléséről az IaaS, akár alkalmazások fejlesztéséről a PaaS, akár teljesen menedzselt szoftverek használatáról a SaaS segítségével, a felhőalapú számítástechnika hatékony keretet biztosít a modern IT-műveletekhez és az innovációhoz.

Gyakorló feladatok

1. Hogyan alakít át a Domain Name System (DNS) IP-címmé egy olyan domainnevet, mint a `www.example.com`? Mi a szerepe a forward DNS-nek és a reverse DNS-nek, és miben különböznek egymástól?

2. Mi a különbség az Infrastructure as a Service (IaaS), a Platform as a Service (PaaS) és a Software as a Service (SaaS) között? Mondjunk példát mindegyikre, és fejtsük ki, hogy az egyes modellekben a felhasználó milyen szintű ellenőrzést gyakorol!

Gondolkodtató feladatok

1. Keressük meg és fejtsük ki el a DNS-sel kapcsolatos leggyakoribb biztonsági kockázatokat, mint például a DNS spoofing (hamisítás) vagy a cache poisoning (mérgezés)! Hogyan működnek ezek a támadások, és milyen intézkedésekkel lehet védekezni ellenük?

2. Hasonlítsunk össze három nagy felhőszolgáltatót — Amazon Web Services (AWS), Microsoft Azure és Google Cloud — az IaaS, PaaS és SaaS kínálatuk szempontjából! Melyek a fő különbségek az árképzési modelljeik, szolgáltatásaik és célközönségeik között?

Összefoglalás

Ebben a leckében az alapvető hálózati protokollok és a felhőalapú számítástechnikai fogalmak mélyreható feltárásáról van szó. A legfontosabb protokollok, például a TCP, az UDP, az ICMP és a DHCP ismertetésével kezdődik, a hálózati kommunikációban betöltött szerepükre összpontosítva. A szöveg ezután részletezi a DNS működését, amely a domainneveket IP-címekké fordítja le a forward és reverse lookupokon keresztül. Emellett hangsúlyozza a TCP/UDP portok fontosságát a hálózati forgalom megfelelő szolgáltatásokhoz és alkalmazásokhoz való irányításában.

A lecke végül áttér a felhőalapú számítástechnikai modellekre, és elmagyarázza az infrastruktúra mint szolgáltatás (Infrastructure as a Service — IaaS), a platform mint szolgáltatás (Platfrom as a Service — PaaS) és a szoftver mint szolgáltatás (Software as a Service — SaaS) közötti különbségeket. Ezek a modellek különböző szintű ellenőrzést és rugalmasságot kínálnak a vállalkozások és a fejlesztők számára, az IaaS segítségével történő virtuális infrastruktúra kezelésétől kezdve az alkalmazások PaaS segítségével történő építésén és telepítésén át a SaaS segítségével történő, teljesen menedzselt alkalmazások használatáig.

Válaszok a gyakorló feladatokra

1. Hogyan alakít át a Domain Name System (DNS) IP-címmé egy olyan domainnevet, mint a `www.example.com`? Mi a szerepe a forward DNS-nek és a reverse DNS-nek, és miben különböznek egymástól?

   A Domain Name System (DNS) az ember által olvasható domainneveket, mint például a `www.example.com`, IP-címekre fordítja, mint például a `192.0.2.1`, lehetővé téve az eszközök számára az internetes kommunikációt. A forward DNS lookup során a domainnév a megfelelő IP-címre alakítódik át, így az eszköz meg tudja találni a megfelelő webszervert. Ezzel szemben a reverse DNS lookup során az IP-címet a hozzá tartozó domainnévre oldja fel. Ezt gyakran használják egy állomás identitásának ellenőrzésére, például az e-mail rendszerekben vagy a hálózati diagnosztikában. Mindkét folyamat elengedhetetlen a zökkenőmentes kommunikáció és az internetes biztonság biztosításához.

2. Mi a különbség az Infrastructure as a Service (IaaS), a Platform as a Service (PaaS) és a Software as a Service (SaaS) között? Mondjunk példát mindegyikre, és fejtsük ki, hogy az egyes modellekben a felhasználó milyen szintű ellenőrzést gyakorol!

   Az IaaS virtualizált erőforrásokat, például szervereket és tárhelyet biztosít, a felhasználóknak pedig teljes ellenőrzést az operációs rendszer és az alkalmazások felett. Az AWS EC2 az IaaS egyik vezető példája.

   A PaaS platformot kínál a fejlesztők számára az alkalmazások létrehozásához és telepítéséhez az infrastruktúra kezelése nélkül, ahol az ellenőrzés az alkalmazási rétegre korlátozódik. A Google App Engine a PaaS vezető példája.

   A SaaS teljesen menedzselt szoftvert biztosít az interneten keresztül, a felhasználók egyszerűen hozzáférnek az alkalmazáshoz, és nem ellenőrzik az infrastruktúrát vagy a szoftverek kezelését. A Gmail a SaaS egyik vezető példája.

Válaszok a gondolkodtató feladatokra

1. Keressük meg és fejtsük ki el a DNS-sel kapcsolatos leggyakoribb biztonsági kockázatokat, mint például a DNS spoofing (hamisítás) vagy a cache poisoning (mérgezés)! Hogyan működnek ezek a támadások, és milyen intézkedésekkel lehet védekezni ellenük?

   A DNS biztonsági kockázatai, mint például a DNS spoofing és a cache poisoning, akkor jelentkeznek, amikor a támadók a DNS-válaszokat manipulálva rosszindulatú webhelyekre irányítják át a felhasználókat. A DNS spoofing során a támadó DNS-válaszokat hamisít, hogy az áldozat eszköze azt higgye, hogy egy legitim domainhez csatlakozik, miközben valójában egy káros szerverre kerül átirányításra. A cache poisoning úgy működik, hogy a támadó manipulálja a DNS gyorsítótárat a szerveren, ami miatt a szerver helytelen IP-címeket tárol és ad a domainnevekhez. Az ilyen támadások elleni védelem érdekében olyan technikákat lehet alkalmazni, mint a DNSSEC (DNS Security Extensions) a DNS-válaszok hitelességének ellenőrzésére. A gyorsítótár rendszeres kiürítése segíthet a cache poisoning kockázatának minimalizálásában. Segíthet megelőzni a DNS-forgalom lehallgatását és manipulálását ezek mellett a titkosított DNS-lekérdezések használata olyan protokollok segítségével, mint a DNS over HTTPS (DoH).

2. Hasonlítsunk össze három nagy felhőszolgáltatót — Amazon Web Services (AWS), Microsoft Azure és Google Cloud — az IaaS, PaaS és SaaS kínálatuk szempontjából! Melyek a fő különbségek az árképzési modelljeik, szolgáltatásaik és célközönségeik között?

   Az Amazon Web Services (AWS), a Microsoft Azure és a Google Cloud a három vezető felhőszolgáltató, amelyek mindegyike IaaS, PaaS és SaaS megoldásokat is kínál. Az AWS a kiterjedt globális infrastruktúrájáról és a szolgáltatások széles skálájáról ismert, ezért népszerű a nagyvállalatok körében. Árképzési modellje rendkívül rugalmas, és pay-as-you-go opciókat kínál. A Microsoft Azure szorosan integrálódik a Microsoft más termékeivel és szolgáltatásaival, így a Windows-alapú infrastruktúrát már használó vállalkozások számára is jó választás. Az árazása szintén pay-as-you-go modellt követ, de különösen versenyképes a Microsoft-szoftvereket használó vállalkozások számára. A Google Cloud ezzel szemben az adatelemzésre és a gépi tanulásra helyezi a hangsúlyt.

024.2 Hálózat- és internetbiztonság

Hivatkozás az LPI célkitűzésre

Security Essentials version 1.0, Exam 020, Objective 024.2

Súlyozás

3

Kulcsfontosságú ismeretek

- Az adatkapcsolati rétegbeli hozzáférés következményeinek megértése
- A WiFi hálózatok kockázatainak és biztonságos használatának megértése
- A forgalom lehallgatásával kapcsolatos fogalmak megértése
- Az internet gyakori biztonsági fenyegetéseinek megértése, valamint az azok elhárítására irányuló megközelítések ismerete

A használt fájlok, kifejezések és segédprogramok részleges listája

- Adatkapcsolati réteg
- Titkosítatlan és nyilvános WiFi
- WiFi biztonság és titkosítás
- WEP, WPA, WPA2
- Forgalomlehallgatás
- Man in the Middle támadások
- DoS és DDoS támadások
- Botnetek
- Csomagszűrők

Lecke 1

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	024 Hálózat- és szolgáltatásbiztonság
Fejezet:	024.2 Hálózat- és internetbiztonság
Lecke:	1/1

Bevezetés

Napjaink összekapcsolt világában a hálózati biztonság alapvető szempontjainak megértése elengedhetetlen az adatok védelme és a kommunikáció integritásának fenntartása szempontjából. Az egyik kulcsfontosságú terület, amelyet figyelembe kell venni, az adatkapcsolati réteghez való hozzáférés következményei, amely a hálózat legalacsonyabb rétegének sebezhetőségét tárhatja fel, valamint potenciálisan lehetővé teszi a támadók számára a forgalom lehallgatását vagy manipulálását. Hasonlóképpen, a Wi-Fi hálózatok kockázatai és biztonságos használata egyre nagyobb jelentőséggel bírnak, mivel a vezeték nélküli kapcsolat mindenütt jelen van, és a rosszul konfigurált vagy nem védett hálózatok lehetőséget nyújtanak az illetéktelen hozzáférésre.

Egy másik kritikus terület a forgalom lehallgatása (traffic interception), ahol a támadók lehallgatják vagy módosítják a hálózati forgalmat, ami jelentős kockázatot jelent az adatok titkosságára és integritására. Végezetül az informatikai szakemberek számára létfontosságú az olyan gyakori internetes biztonsági fenyegetések, mint a denial-of-service (szolgáltatásmegtagadási) vagy a man-in-the-middle támadások és a botnetek megértése, valamint a megfelelő elhárítási stratégiák, hogy megvédjék a rendszereket a fejlődő kiberfenyegetésekkel szemben. Ezek a témakörök együttesen alkotják a hálózatbiztonság gerincét, segítve a jogosulatlan hozzáférés megakadályozását és a biztonságos kommunikáció biztosítását a digitális

környezetekben.

Hozzáférés az adatkapcsolati réteghez

Az *adatkapcsolati réteg* (link layer) az OSI hálózati modelljének második rétege. A hálózati kommunikáció fizikai és adatkapcsolati szempontjait kezeli. Ez a réteg felelős az adatok helyi hálózati szegmensen keresztüli továbbításáért, és olyan dolgokat kezel, mint a keretátvitel (frame transmission), a hibadetektálás és az adatfolyam-szabályozás (flow control). A hálózatban lévő eszközök az adatkapcsolati rétegen keresztül kommunikálnak egymással olyan protokollok segítségével, mint az Ethernet vagy a Wi-Fi. Az ehhez a réteghez való hozzáférés kritikus fontosságú az ugyanazon a helyi hálózaton lévő eszközök közötti adatátvitel vezérléséhez.

Az adatkapcsolati réteghez való illetéktelen hozzáférés azonban jelentős biztonsági kockázatot jelenthet. Egy támadó, aki hozzáférést szerez ehhez a réteghez, potenciálisan elfoghatja, manipulálhatja vagy bejuttathatja a forgalmat a hálózatba. Ez lehetővé teszi számára, hogy különféle támadásokat hajtson végre, például *packet sniffing*-et, amikor a támadó adatcsomagokat rögzít és elemez, vagy *man-in-the-middle támadást*, amikor a felek tudta nélkül elfogja és esetleg megváltoztatja a két eszköz közötti kommunikációt. Ezek a támadások adatsértéshez, érzékeny információkhoz való jogosulatlan hozzáféréshez vagy akár a hálózati szolgáltatások megszakításához vezethetnek.

Az adatkapcsolati réteghez való hozzáféréssel kapcsolatos kockázatok csökkentése a fizikai hálózati infrastruktúra biztosítását, erős hitelesítési mechanizmusok bevezetését és titkosítás alkalmazását igényli. A switcheken például engedélyezhető a *port security*, amivel a hozzáférést az engedélyezett eszközökre korlátozzuk, a lehetséges támadások körének korlátozására pedig *hálózati szegmentálás* (network segmentation) alkalmazható.

Egy eredendő kockázat továbbra is fennáll az *adatkapcsolati rétegen*, mégpedig az ARP (Address Resolution Protocol) mérgezése (poisoning). Az ARP-t az IP-címek MAC-címekhez való hozzárendelésére használják a helyi hálózaton, egy támadó pedig kihasználhatja ezt hamisított ARP-üzenetek küldésével, hogy MAC-címét egy másik eszköz IP-címéhez társítsa. Ez lehetővé teszi a támadó számára, hogy az adott eszköznek szánt forgalmat elfogja vagy megváltoztassa.

A Wi-Fi hálózatokban az adatkapcsolati réteg biztosításának kihívásai még nagyobbak a vezeték nélküli kommunikáció fizikája miatt, ahol az adatok továbbítása nyílt léghullámokon keresztül történik.

Wi-Fi hálózatok

A Wi-Fi hálózatok kényelmet és rugalmasságot kínálnak, lehetővé téve az eszközök vezeték nélküli csatlakoztatását az internethez. Ugyanakkor jelentős biztonsági kockázatot is jelentenek,

különösen, ha nem megfelelően vannak biztosítva. Az egyik fő probléma a titkosítatlan és nyilvános Wi-Fi hálózatokkal kapcsolatban merül fel, amelyek általában nyilvános helyeken, például kávézókban, repülőtereken és szállodákban találhatók. Ezek a hálózatok gyakran nyílt hozzáférést biztosítanak bárki számára, aki a hatótávolságukban van, és mivel nincs titkosításuk, a rajtuk keresztül továbbított adatok lehallgathatók. A támadók könnyen megfigyelhetik a hálózati forgalmat, és olyan technikákkal, mint a packet sniffing, érzékeny információkat, például bejelentkezési adatokat, személyes adatokat vagy pénzügyi adatokat szerezhetnek. A nyilvános Wi-Fi hálózatok elsődleges célpontot jelentenek a kiberbűnözők számára, akik ki akarják használni ezeket a sebezhetőségeket.

E kockázatok mérséklése érdekében Wi-Fi biztonságot és titkosítást kell bevezetni, hogy az eszközök és a hálózat között továbbított adatok védve legyenek. A titkosítás kódolja az adatokat, így azok a megfelelő visszafejtési kulcs nélkül még akkor sem olvashatók vagy értelmezhetők, ha azokat elfogják. Az idők során különböző titkosítási szabványokat fejlesztettek ki a Wi-Fi hálózatok biztonságának javítása érdekében. Az egyik legkorábbi a *Wired Equivalent Privacy* (WEP) volt, de hamar kiderült, hogy nem biztonságos, mivel a támadók könnyen feltörhették a titkosítást. Ennek eredményeképpen a WEP ma már elavultnak számít, és nem szabad használni.

A *Wi-Fi Protected Access* (WPA) bevezetése a WEP számos gyengeségének kiküszöbölésével javította a biztonságot. A WPA a *Temporal Key Integrity Protocol* (TKIP) protokollt használta a titkosítási kulcs dinamikus megváltoztatására minden egyes csomag esetén, ami megnehezítette a támadók számára a titkosítás feltörését. A WPA azonban még mindig rendelkezett sebezhetőségekkel, ami a ma legszélesebb körben használt titkosítási szabvány, a *WPA2* kifejlesztéséhez vezetett. A WPA2 az *Advanced Encryption Standard* (AES) szabványt használja, amely sokkal erősebb titkosítási szintet kínál, mint elődei, és továbbra is a Wi-Fi biztonságának ipari szabványa.

A WPA2 robosztussága ellenére sem teljesen védett a támadásokkal szemben, és a kifinomultabb kiberfenyegetések megjelenésével újabb szabványok, például a *WPA3* kerültek bevezetésre. A WPA3 még erősebb titkosítást és jobb védelmet nyújt a brute-force támadásokkal szemben. Biztonságos környezetben a legújabb titkosítási szabvány és az erős jelszavak használata elengedhetetlen a Wi-Fi hálózatokon keresztül továbbított adatok titkosságának és sértetlenségének biztosításához. A routerek és hálózati berendezések rendszeres frissítése a legújabb biztonsági protokollok támogatása érdekében szintén segít a felmerülő fenyegetések elleni védelemben, így biztosítva, hogy a vezeték nélküli hálózatok továbbra is biztonságosak maradjanak az illetéktelen hozzáféréstől.

A forgalom lehallgatása

A forgalom lehallgatása (traffic interception) akkor következik be, amikor egy illetéktelen felhasználó, akit támadónak nevezünk, behatol a hálózat csomópontjainak kommunikációs

pontjai közé. Ezt nevezhetjük *man-in-the-middle* támadásnak is. A forgalom lehallgatásának formái lehetnek passzív vagy aktív támadások a hálózat célzott állomásai ellen.

A forgalom passzív lehallgatása

A *passzív támadás* vagy *passzív forgalomlehallgatás* akkor történik, amikor a támadó lehallgatja a hálózaton lévő hostok közötti hálózati tranzakciókat. A támadó valószínűleg észrevétlen marad, mert a hostok közötti információ zavartalannak tűnik, de azt egy ember a középen figyeli és elemzi.

A passzív adatforgalom lehallgatójának indítékai eltérőek lehetnek, beleértve az értékesítési célú információlopást vagy az interneten versenyelőnyre szert tenni kívánó riválisi cégeket. A passzív forgalomlehallgatást viszonylag nehéz felderíteni, mivel nem változtatja meg a hálózaton keresztül továbbított adatokat, az információk küldése és fogadása pedig normális módon történik. Az egyik lehetséges megoldás nem a felderítés, hanem az ilyen típusú támadások megelőzése a hálózati pontokon keresztül közlekedő információk titkosításával. A kommunikációs minták és a továbbított kommunikáció típusának ismerete azonban bizonyos helyzetekben értékes információkkal szolgálhat a támadó számára.

TIP A hálózat forgalmának megfigyelésére és elemzésére a `tcpdump` vagy a `wireshark` parancsok használhatók.

A forgalom aktív lehallgatása

A forgalom lehallgatása akkor tekinthető *aktív* támadásnak, ha az a hálózaton keresztülhaladó adatok módosításával jár. Lényegében ez nem csak lehallgatást jelent, mint a passzív esetben, hanem olyan támadásokat is magában foglalhat, mint az *ARP spoofing* egy kapcsolt LAN-kapcsolaton, vagy a rögzített, érvényes hitelesítési adatok visszajátszása cross-site scripting segítségével (főként azért, hogy a hálózaton egy másik felhasználó szerepét töltse be, és így az ilyen felhasználó jogosultságait bitorolja).

Az adatforgalom aktív lehallgatása olyan aktív támadás, amely magában foglalhatja a hálózat küldő és fogadó állomásai között átmenő üzenetek módosítását, átirányítását vagy késleltetését is. Ilyen például, amikor egy elküldött üzenet a következő volt: “Engedélyezze Jane Smith számára a profilfiók szerkesztését”, de a fogadott üzenet a következő volt: “Engedélyezze John Doe számára a profilfiók szerkesztését”, ezáltal megváltoztatva az információ integritását. A fő gondolat az, hogy a támadó úgy módosítsa az üzenetet, hogy az megfeleljen a saját szándékainak, ami finom kísérlet lehet magasabb jogosultságok megszerzésére.

A passzív és aktív forgalomlehallgatási támadások bizonyos mértékig ellentétes védelmet igényelnek. Míg a rendszergazdáknak és a felhasználóknak a passzív támadást inkább

megelőzniük kell, mint észlelniük, addig az aktív támadást észlelniük kell, és a lehető leggyorsabban intézkedniük kell a helyzet orvoslása és a hálózat további károsodásának megelőzése érdekében.

TIP Az `arp` vagy `nmap` parancsok segítségével információt kaphatunk a hálózat szomszédos hostjairól.

DoS és DDoS támadások

A *szolgáltatásmegtagadás* (Denial of service — DoS) az aktív támadás egyik formája, amikor az arra jogosult felhasználók nem férhetnek hozzá egy számítógépes rendszerhez, hálózathoz vagy bizonyos információkhoz. Ezt a hálózat vagy egy adott rendszer elleni támadás okozza. A támadás végrehajtásához a támadó kihasználhatja a rendszer egy adott alkalmazásában vagy a hoston futó operációs rendszerben lévő ismert sebezhetőséget. A kihasználás gyakran úgy történik, hogy a támadó olyan sok kéréssel árasztja el a rendszert, hogy a gépet túlterheli, és összeomlik a rendszer, ezáltal offline állapotba kerül, vagy használhatatlanná válik az arra jogosult felhasználók számára.

Amikor szolgáltatásmegtagadásos támadást indítanak egy célzott host ellen, a cél lehet a hosthoz való hozzáférés akadályozása, vagy más akciókkal kombinálva a számítógépes rendszer veszélyeztetése. Arra is felhasználható, hogy jogosulatlan hozzáférést szerezzenek a számítógépes rendszerhez vagy a hálózathoz. A DoS-támadásokra példa a *SYN flooding* és a *Ping of Death*.

A SYN flooding során a támadás kihasználja a két host közötti kommunikációhoz használt TCP/IP protokoll háromirányú kézfogását. A támadás lényege, hogy a hostot kérésekkel árasztja el, így annak nincs ideje a SYN, SYN/ACK és ACK kommunikáció sorrendjében a meg nem válaszolt kéréseket eldobni. Az ACK-kérés befejezi a 3-utas kézfogást, de mivel a kezdeti kapcsolat egy hamis IP-címről érkezik, a host nem ad ACK-választ, és tovább várakozik. Hamarosan újabb és újabb kérések halmozódnak fel, amíg a host már nem képes több kérést kezelni, és ezzel akadályozza az engedélyezett felhasználók valódi kéréseinek feldolgozását az adott gépről.

A Ping of Death egy másik DoS-támadás, amely nagyméretű *Internet Control Message Protocol* (ICMP) csomagokat küld a célzott állomásnak. Az adatcsomagoknak általában 65 536 bájtnál (vagy 64 kilobájtnál) kisebbnek kell lenniük, de ha a csomag mérete ennél nagyobb, és olyan hostnak küldik, amely nem képes ekkora csomagméretet kezelni, a rendszer lefagy vagy összeomlik, és elérhetetlenné válik az engedélyezett felhasználók számára.

A DoS-támadásokat általában egyetlen támadó rendszer hajtja végre. Ha azonban több rendszert is bevetnek a célpont megtámadására, akkor az *elosztott szolgáltatásmegtagadás* (Distributed Denial of Service — DDoS) néven ismert. A DDoS során a támadó több más rendszert is megfertőz, és ráveszi őket, hogy a nevében rosszindulatú funkciókat hajtsanak végre. Ez akkor fordulhat elő,

ha a felhasználókat esetleg megtévesztették, hogy olyan szoftvert telepítsenek a számítógépükre, amely egy ideig észrevétlenül szunnyad. A támadás olyan rendszereket is kihasználhat, amelyeket nem patcheltek vagy nem frissítettek a legújabb ismert sebezhetőségek ellen. Amint elég sok gépet megfertőztek, a támadás elindul. Ez a támadás lehet egy SYN-áradat, amelynek során több fertőzött host hamis kommunikációs kéréseket küld a célzott szervernek, amíg az túl nem terhelődik.

A SYN flooding DoS-támadás megelőzésének egyik módja az, hogy módosítjuk a host várakozási idejét, mielőtt a fel nem használt kéréseket eldobja. Az is jó biztonsági gyakorlat, ha a rendszereket patchelik a legújabb biztonsági frissítésekkel. Egyes kémprogram- vagy vírusirtó csomagok részeként léteznek olyan eszközök, amelyek képesek felismerni és eltávolítani a szunnyadó “zombi” szoftvereket. Bár az ICMP protokoll blokkolása segíthet a Ping of Death megelőzésében, egyúttal akadályozhatja a legitim és hasznos hibaelhárító eszközöket is.

Botok és botnetek

A *bot* olyan szoftver, amely egy másik program irányítása alatt hajt végre feladatokat. A hálózaton keresztül működtetett és irányított botok csoportját *botnetnek* nevezzük. Egy botnetet arra lehet használni, hogy a hálózaton keresztül legitim, szükséges és törvényes műveleteket hajtsanak végre — például a számítási munkaterhek (workload) elosztásakor. Egy botnet azonban a hálózaton belüli fondorlatos és káros műveletekre is használható, mint például az előző szakaszban tárgyalt DDoS-támadások. A botnetek kémszoftverként is felhasználhatók arra, hogy a hálózaton keresztül keyloggerek segítségével információkat lopjanak. A botneteket használhaatják e-mail spammelésre, azaz kéretlen üzenetek küldésére a célpontnak.

Általában, amikor egy számítógépet megfertőz a bot malware, a felhasználó nem tud róla, a fertőzés pedig akár át is terjedhet a hálózat más hostjaira is. Ez egy nagy botnetet hozhat létre, amelyet később egy adott célpont elleni tömeges támadás indítására használnak fel. A botfejlesztők képesek arra is, hogy botjaikat úgy módosítsák, hogy kikerüljék a biztonsági intézkedéseket, például az IP-feketelistákat (blacklist) és a hozzáférés-ellenőrzési méréseket, azáltal, hogy lakott területek IP-címeit lefoglalják, és különböző alkalmakkor használják őket a felderítés elkerülése érdekében. Minden internetezőnek célzott biztonsági szoftvereket, például kémprogram- és vírusirtó csomagokat kell telepítenie, és rendszeresen frissítenie. Ezeknek az eszközöknek ezután rutinellenőrzéseket kell végezniük, hogy segítsenek megelőzni a fertőzést vagy támadást. Szintén jó biztonsági gyakorlat, ha nem kattintunk nem egyértelmű, ismeretlen vagy megbízhatatlan forrásból származó linkekre, illetve nem nyitunk meg ilyen e-maileket sem.

Csomagszűrők és egyéb védekezési stratégiák hálózati támadások ellen

A *csomagszűrők* (packet filter) döntő szerepet játszhatnak a különböző hálózati támadások, például a SYN flood, a Denial of Service (DoS), a Distributed Denial of Service (DDoS), a botnetek és a man-in-the-middle támadások mérséklésében. A csomagszűrő egy olyan tűzfalmechanizmus, amely a bejövő és kimenő csomagokat a hálózati szinten vizsgálja, elemezve azok fejlécét (header), hogy előre meghatározott biztonsági szabályok alapján meghatározza, hogy engedélyezni vagy blokkolni kell-e azokat.

A csomagszűrők a bejövő SYN-kérések számának korlátozásával vagy a *SYN sütik* (cookie) bevezetésével, amelyek lehetővé teszik a szerver számára, hogy több kapcsolatot kezeljen az erőforrások túlterhelése nélkül, enyhíthetik a SYN flood támadásokat, amikor a támadó a szervert túlterheli azzal, hogy nagyszámú hiányos kapcsolati kérést küld. A csomagszűrők az ismert támadók IP-címeit is felismerhetik és blokkolhatják, megakadályozva, hogy forgalmuk elérje a szervert.

A DoS- és DDoS-támadások megelőzése érdekében a csomagszűrők képesek azonosítani a rendellenes forgalmi mintákat (pattern) — például egy IP-címről érkező szokatlanul sok kérés vagy DDoS-forgatókönyv esetén több forrásból érkező kérés --, és blokkolni vagy korlátozni a forgalmat. Ez megakadályozza, hogy a szervert túlterhelje a rosszindulatú forgalom, miközben folytatódik a valódi kérések feldolgozása.

Botnetek esetében, amelyek összehangolt támadások indítására használt, kompromittált eszközök hálózatai, a csomagszűrők képesek észlelni az ismert botnet IP-címekről érkező forgalmat, vagy blokkolni a gyanúsan viselkedő eszközök kommunikációját. A botnet-üzemeltetők által a fertőzött eszközök kezelésére használt parancs- és vezérlési (C2) forgalom blokkolásával a csomagszűrők jelentősen csökkenthetik a botnet-támadások hatékonyságát.

Végül a csomagszűrők megakadályozhatják a man-in-the-middle támadásokat (amikor egy támadó lehallgatja a két eszköz közötti kommunikációt), azáltal, hogy biztonságos kapcsolatokat kényszerítenek ki, például HTTPS vagy SSL/TLS protokollok használatával, amelyek titkosítják a forgalmat. A szűrők úgy is beállíthatók, hogy eldobják a gyanús csomagokat, amelyek úgy tűnnek, mintha egy man-in-the-middle támadás részei lennének, például módosított fejlécük van vagy nem megbízható forrásból származnak.

A csomagszűrők megfelelő konfigurálásával a szervezetek jelentősen csökkenthetik a különböző típusú támadások kockázatát, javítva hálózataik biztonságát és integritását.

Gyakorló feladatok

1. Mi a különbség a DoS és a DDoS támadás között?

2. Milyen potenciális kockázatokat rejt magában a hálózat adatkapcsolati rétegéhez való illetéktelen hozzáférés, és milyen konkrét támadási módszerek alkalmazhatók ezen a rétegen?

3. Mi a különbség a WEP, WPA és WPA2 titkosítási szabványok között, és miért fontos a legújabb titkosítási protokollok használata a Wi-Fi hálózatok esetén?

4. Hogyan segíthetnek a csomagszűrők a DoS- és DDoS-támadások enyhítésében, és milyen konkrét technikákat használnak az ilyen típusú támadások megelőzésére?

Gondolkodtató feladatok

1. Miközben Henry a számítógépén dolgozik, egy gyors felugró parancssor megjelenik, majd eltűnik, és utána minden más normálisnak tűnik a számítógépen. A számítógépen futó folyamatok ellenőrzése közben azonban egy furcsa folyamatot is lát, amely szintén fut. Mi lehet ez, és mit tehet azonnal?

2. Henry megpróbálja lehallgatni a Dave és Carol közötti hálózati forgalmat, bár a kommunikáció titkosított. Lehetséges ez?

3. Milyen típusú forgalomlehallgatás az előző feladatban leírt támadás?

Összefoglalás

Ez a lecke a hálózati biztonságot tárgyalja, kezdve a kapcsolatszintű hozzáférés kockázataival, kiemelve az olyan támadásokat, mint a packet sniffing, a man-in-the-middle támadások és az ARP poisoning. Hangsúlyt fektet a fizikai infrastruktúra biztosítására és az erős hitelesítés használatára.

A lecke kitér a titkosítatlan nyilvános Wi-Fi biztonsági kockázataira és a Wi-Fi titkosítási szabványok fejlődésére is, a WEP-től a WPA2-n át a WPA3-ig. Elmagyarázza továbbá a forgalom lehallgatását, különbséget téve a passzív és az aktív támadások között. Végül a DoS-, DDoS- és botnet-támadásokkal foglalkozik, valamint azzal, hogy a csomagszűrők hogyan segíthetnek enyhíteni ezeket a fenyegetéseket a gyanús forgalom blokkolásával.

Válaszok a gyakorló feladatokra

1. Mi a különbség a DoS és DDoS támadás között?

   Míg a szolgáltatásmegtagadás (DoS) egyetlen rendszerrel támadja a célpontot, az elosztott szolgáltatásmegtagadás (DDoS) több számítógépet használ a támadás végrehajtásához.

2. Milyen potenciális kockázatokat rejt magában a hálózat adatkapcsolati rétegéhez való illetéktelen hozzáférés, és milyen konkrét támadási módszerek alkalmazhatók ezen a rétegen?

   Az adatkapcsolati réteghez való illetéktelen hozzáférés jelentős biztonsági kockázatot jelent, mivel a támadók elfoghatják, manipulálhatják vagy bejuttathatják a forgalmat a hálózatba. A konkrét támadási módszerek közé tartozik a packet sniffing, amikor a támadó rögzíti és elemzi a hálózaton keresztül továbbított adatokat, valamint a man-in-the-middle támadások, amikor a támadó lehallgatja és esetleg módosítja az eszközök közötti kommunikációt. Az ARP poisoning egy másik gyakori támadásforma, amikor a támadó meghamisítja az ARP-üzeneteket, hogy MAC-címét egy másik eszköz IP-címéhez társítsa, így lehetővé téve, hogy az adott eszköznek szánt forgalmat elfogja vagy módosítsa.

3. Mi a különbség a WEP, WPA és WPA2 titkosítási szabványok között, és miért fontos a legújabb titkosítási protokollok használata a Wi-Fi hálózatok esetén?

   A WEP a legrégebbi Wi-Fi titkosítási szabvány, amelyet ma már nem tartanak biztonságosnak a titkosítás könnyű feltörését lehetővé tevő hibák miatt. A WPA javította a biztonságot a TKIP használatával, amely dinamikusan változtatja a titkosítási kulcsokat, de még mindig vannak sebezhető pontjai. A WPA2 ma a legszélesebb körben használt szabvány, amely az AES titkosítás használatával erősebb biztonságot nyújt. Fontos a legújabb titkosítási protokollok, például a WPA3 használata, mivel ezek fokozott védelmet nyújtanak a nyers erővel (brute-force) végrehajtott támadások és más fejlett fenyegetések ellen, biztosítva a Wi-Fi hálózatokon az adatok titkosságát és sértetlenségét.

4. Hogyan segíthetnek a csomagszűrők a DoS- és DDoS-támadások enyhítésében, és milyen konkrét technikákat használnak az ilyen típusú támadások megelőzésére?

   A csomagszűrők a DoS- és DDoS-támadásokat a bejövő és kimenő csomagok hálózati szintű elemzésével és a gyanús mintának megfelelő forgalom — például egyetlen IP-címről vagy több forrásból érkező nagy mennyiségű kérés — blokkolásával vagy korlátozásával mérséklik. A SYN flooding támadások enyhítése érdekében a csomagszűrők korlátozhatják a SYN-kérések számát, vagy SYN-sütiket használhatnak, hogy több kapcsolatot kezeljenek a szerver túlterhelése nélkül. A DDoS-támadások kezelésében a csomagszűrők a rendellenes forgalmi minták azonosításával és a rosszindulatú forgalom sebességének korlátozásával vagy

blokkolásával segítenek, miközben a valós forgalmat átengedik.

Válaszok a gondolkodtató feladatokra

1. Miközben Henry a számítógépén dolgozik, egy gyors felugró parancssor megjelenik, majd eltűnik, és utána minden más normálisnak tűnik a számítógépen. A számítógépen futó folyamatok ellenőrzése közben azonban egy furcsa folyamatot is lát, amely szintén fut. Mi lehet ez, és mit tehet azonnal?

   Ez valószínűleg egy bot. A számítógépet vírusirtó szoftverrel kell átvizsgálni.

2. Henry megpróbálja lehallgatni a Dave és Carol közötti hálózati forgalmat, bár a kommunikáció titkosított. Lehetséges ez?

   Igen, az üzenet mintájából, a protokoll típusából és a forgalom időzítéséből akkor is lehet információt szerezni, ha az üzenet tartalma titkosított.

3. Milyen típusú forgalomlehallgatás az előző feladatban leírt támadás?

   A hálózati forgalom lehallgatása passzív forgalomlehallgatási támadás.

024.3 Hálózati titkosítás és anonimitás

Hivatkozás az LPI célkitűzésre

Security Essentials version 1.0, Exam 020, Objective 024.3

Súlyozás

3

Kulcsfontosságú ismeretek

- A virtuális magánhálózatok (VPN) megértése
- Az end-to-end titkosítás fogalmának megértése
- Az anonimitás és a felismerhetőség az interneten megértése
- Azonosítás az adatkapcsolati rétegbeli címek és az IP-címek által
- A proxy-szerverek fogalmának megértése
- A TOR fogalmának megértése
- A Darknet ismerete
- A kriptovaluták és az anonimitási szempontjaik ismerete

A használt fájlok, kifejezések és segédprogramok részleges listája

- Virtual Private Network (VPN)
- Publikus VPN szolgáltatók
- Szervezet-specifikus VPN (pl. céges vagy egyetemi VPN)
- End-to-end titkosítás
- Szállítási titkosítás
- Anonimitás

- Proxy szerverek
- TOR
- Rejtett szolgáltatás
- .onion
- Blockchain

Linux Professional Institute

Lecke 1

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	024 Hálózat- és szolgáltatásbiztonság
Fejezet:	024.3 Hálózati titkosítás és anonimitás
Lecke:	1/2

Bevezetés

Napjaink összekapcsolt világában a biztonságos és privát kommunikáció szükségessége fontosabbá vált, mint valaha. Az adatvédelmet és a kiberbiztonságot fenyegető növekvő fenyegetések miatt az egyének és a szervezetek megbízható megoldásokat keresnek érzékeny információik védelmére és a titoktartás (confidentiality) megőrzésére. A nyilvános hálózatokon keresztüli biztonságos kommunikációt lehetővé tevő egyik kulcsfontosságú technológia a virtuális magánhálózat (VPN). A VPN a felhasználó eszköze és a célhálózat közötti titkosított alagút (tunnel) létrehozásával biztosítja, hogy az adatok biztonságban maradjanak a lehallgatástól és a jogosulatlan hozzáféréstől. Ez teszi a VPN-eket alapvető eszközzé azok számára, akik online tevékenységeiket szeretnék megvédeni, vagy távolról szeretnének hozzáférni korlátozott erőforrásokhoz.

A VPN-technológia sokoldalúsága és alkalmazkodóképessége miatt mind az egyéni felhasználók, mind a vállalatok körében népszerűvé vált, és a személyes adatvédelemtől a vállalati biztonságig sokféle felhasználási esetet szolgál ki.

Előnyeik ellenére a VPN-ek nem jelentenek mindenre egyformán alkalmas megoldást. A VPN-ek különböző típusainak, felhasználási eseteinek és korlátaiknak a megértése kulcsfontosságú az

egyedi igényeinknek megfelelő szolgáltatás kiválasztásához. Ez a lecke a következőket mutatja be: a VPN-ek különböző aspektusait, beleértve a funkcióikat, felhasználási módjaikat és az őket megalapozó technológiákat, átfogó áttekintést nyújtva arról, hogyan járulnak hozzá a modern digitális biztonsághoz.

Bevezetés a virtuális magánhálózatokba (VPN)

A *virtuális magánhálózat* (Virtual Private Network — VPN) biztonságos és titkosított kapcsolatot hoz létre egy kevésbé biztonságos hálózaton, például az interneten keresztül. A VPN-ek védik az érzékeny adatokat, fenntartják az adatvédelmet, és hozzáférést biztosítanak a földrajzi elhelyezkedés vagy hálózati szegmentáció alapján korlátozott erőforrásokhoz. A VPN lényegében egy biztonságos alagutat hoz létre a felhasználó eszköze és a célhálózat között, biztosítva, hogy az ezen az alagúton keresztül továbbított adatok védve legyenek a lehallgatástól és az illetéktelen hozzáféréstől.

A VPN alapvető funkciója az adatok sértetlenségét és titkosságát biztosító titkosítási protokollok használatán alapul. A biztonságos kapcsolatok létrehozására általában olyan protokollokat használnak, mint az *IPsec* (Internet Protocol Security), az *OpenVPN* és a *WireGuard*. Ezek a protokollok az alagút egyik végén titkosítják az adatokat, a másik végén pedig visszafejtik azokat, így megakadályozzák, hogy a lehallgatott adatok olvashatók legyenek.

A VPN-ek két fő kategóriába sorolhatók: publikus VPN-ek és szervezet-specifikus VPN-ek. Mindegyik egyedi célt szolgál, és a felhasználó vagy a szervezet igényeitől függően különböző felhasználási esetekre szabott.

Publikus VPN-szolgáltatók

A publikus VPN-szolgáltatók olyan egyéni felhasználóknak kínálnak szolgáltatásokat, akik meg akarják védeni internetes forgalmukat, el akarják rejteni IP-címüket, vagy meg akarják kerülni a földrajzi elhelyezkedésükre vonatkozó korlátozásokat. Ezek a szolgáltatók világszerte szerverhálózatokat tartanak fenn, és lehetővé teszik a felhasználók számára, hogy különböző földrajzi helyeken keresztül csatlakozzanak, hatékonyan elrejtve valódi tartózkodási helyüket. Ez különösen hasznos az egyes országokra korlátozott tartalmak eléréséhez vagy a korlátozó régiókban a cenzúra elkerülésére.

A nyilvános VPN-ek a nyilvános Wi-Fi hálózatokon való internetkapcsolatok biztosításához is hasznosak. Ha egy nem biztonságos Wi-Fi hotspothoz csatlakoznak, a felhasználók különböző támadásoknak vannak kitéve, például man-in-the-middle támadásoknak, amelyek során a támadó lehallgathatja és potenciálisan megváltoztathatja a továbbított adatokat. Nyilvános VPN használata esetén a felhasználó és a VPN-szerver közötti teljes forgalom titkosítva van, ami jelentősen csökkenti az adatok veszélyeztetésének kockázatát.

Bár a nyilvános VPN-ek kényelmet és biztonságot nyújtanak a személyes használathoz, nem veszélytelenek. A felhasználóknak óvatosnak kell lenniük a VPN-szolgáltató kiválasztásakor, mivel egyesek naplózhatják a felhasználói tevékenységeket, adatokat adhatnak el harmadik félnek, vagy akár kompromittáltak lehetnek. Alapvető fontosságú, hogy olyan jó hírű szolgáltatót válasszunk, amely egyértelmű és szigorú naplózást tiltó irányelvekkel rendelkezik, erős titkosítási szabványokat használ, valamint a működőse és az irányelvei átláthatóak.

Szervezet-specifikus VPN-ek

A szervezet-specifikus VPN-eket úgy tervezték, hogy megfeleljenek a vállalkozások, oktatási intézmények és más, belső hálózataikhoz távoli hozzáférést igénylő szervezetek biztonsági és csatlakozási igényeinek. Ezek a VPN-ek lehetővé teszik az alkalmazottak, a diákok és az arra jogosult személyzet számára, hogy távoli helyekről biztonságosan csatlakozhassanak a szervezet hálózatához. Ez különösen fontos az olyan érzékeny erőforrások, mint a belső adatbázisok, intranetek vagy saját alkalmazások eléréséhez, anélkül, hogy azokat a szélesebb internet számára elérhetővé tennék.

A vállalati és egyetemi VPN-ek általában felhasználói hitelesítő adatokkal, tanúsítványokkal vagy többfaktoros hitelesítéssel (multi-factor authentication, MFA) történő azonosítást igényelnek a csatlakozó felhasználó identitásának ellenőrzéséhez. A felhasználó hitelesítését követően a VPN biztonságos alagutat hoz létre a felhasználó eszköze és a szervezet hálózata között, biztosítva, hogy minden továbbított adat védve legyen a lehallgatástól és a manipulációtól.

A biztonságos hozzáférés biztosítása mellett a szervezetspecifikus VPN-ek biztonsági irányelveket is érvényesíthetnek, például a hozzáférés korlátozását a felhasználó szerepe, tartózkodási helye vagy az eszköz megfelelősége alapján. Egy vállalati VPN például csak olyan menedzselt eszközökről engedélyezhet kapcsolatot, amelyek naprakész vírusirtó szoftverrel rendelkeznek, és megfelelnek a szervezet biztonsági szabványainak.

A vállalati VPN gyakran *távoli hozzáférésű VPN* (remote access VPN), amely lehetővé teszi a távoli felhasználók számára, hogy biztonságosan csatlakozzanak a szervezet hálózatához, úgy, mintha fizikailag az irodában lennének (Távoli hozzáférésű VPN). Ezt a fajta extranet-alapú VPN-t általában az otthonról dolgozó vagy úton lévő alkalmazottak használják, lehetővé téve számukra a belső erőforrások elérését. Egy alkalmazott például egy távoli hozzáférésű VPN segítségével csatlakozhat a vállalat intranetjéhez, miközben egy kávézóból dolgozik, így biztosítva, hogy az érzékeny információk titkosítva és védve maradnak még a nem biztonságos nyilvános Wi-Fi hálózatokon keresztül is.

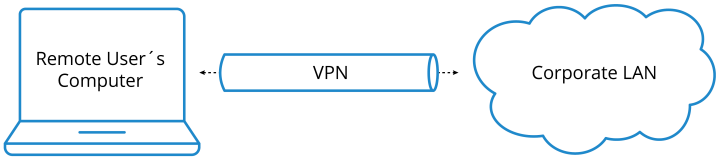

Figure 35. Távoli hozzáférésű VPN

A *site-to-site VPN* ezzel szemben különböző fizikai helyszíneken lévő teljes hálózatokat köt össze, biztonságos kommunikációs csatornát biztosítva közöttük (Site-to-site VPN). Ez a fajta intranet-alapú VPN jellemzően a fiókirodákat vagy partnerhálózatokat köti össze a fő vállalati hálózattal. Egy multinacionális vállalat például használhat site-to-site VPN-t a különböző országokban lévő irodáinak összekapcsolására, lehetővé téve a zökkenőmentes kommunikációt és adatmegosztást közöttük anélkül, hogy a belső forgalmat elérhetővé tenné a nyilvános interneten. A site-to-site VPN-ek használatával a szervezetek egységes és biztonságos hálózati infrastruktúrát hozhatnak létre, megkönnyítve az együttműködést és az erőforrások megosztását a földrajzilag szétszórt helyszíneken.

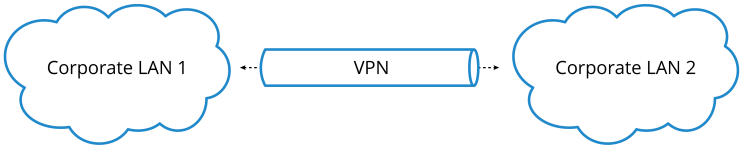

Figure 36. Site-to-site VPN

Az End-to-End titkosítás és az átviteli titkosítás koncepciói

A *végponttól-végpontig titkosítás* (end-to-end encryption — E2EE) és az *átviteli titkosítás* (transfer encryption) szerves részét képezik a VPN-ekben alkalmazott biztonsági mechanizmusoknak, mivel mindkettő a titkosításra támaszkodik az adatok átvitel közbeni védelmében. A VPN-ek biztonságos alagutat hoznak létre a felhasználó eszköze és egy távoli szerver között, biztosítva, hogy az ezen az alagúton áthaladó összes adat titkosított maradjon. Általában az átviteli titkosítás védi az adatokat, miközben azok a felhasználó eszköze és a VPN-kiszolgáló között haladnak.

Átviteli titkosítás

Az átviteli titkosítás (transfer encryption), más néven *encryption in transit*, az adatok védelmére összpontosít, amikor azok a rendszerek között haladnak, például a felhasználó böngészője és egy webszerver között, vagy egy hálózaton belül két szerver között. Az átviteli titkosítás biztosítja, hogy az adatokat ne lehessen illetéktelenek által lehallgatni és elolvasni a továbbítás során.

Amikor például egy felhasználó egy vállalati VPN-hez csatlakozik, az IPsec vagy OpenVPN protokollok jellemzően arra szolgálnak, hogy az adatokat a forrásnál titkosítsák, és csak a VPN-

szerverhez való megérkezéskor dekódolják azokat. Ez a titkosítás megakadályozza, hogy harmadik fél lehallgassa és hozzáférjen a felhasználó és a VPN-szerver közötti kommunikáció tartalmához. Amint azonban az adatok elérik a VPN-szervert, az adatok visszafejtésre és továbbításra kerülnek a rendeltetési helyükre. Ez azt jelenti, hogy a VPN titkosítást kínál az adatok számára a VPN-szerverhez vezető út során, de nem nyújt végponttól végpontig tartó titkosítást a teljes kommunikációs útvonalon. Amikor például egy felhasználó egy VPN-en keresztül kérést küld egy webhelyre vagy egy távoli alkalmazásnak, csak a felhasználó és a VPN-szerver közötti adatforgalom titkosítása történik, így az adatok a VPN-szerveren túl is sebezhetőek a lehallgatással szemben.

Egy másik lehetséges eset, amikor a látogató egy biztonságos weboldalra lép (ezt az URL-ben az `https` jelzi), az átviteli titkosítás biztosítja, hogy a látogató böngészője és a weboldal szervere között kicserélt adatok titkosítva és védve legyenek a lehallgatástól vagy a manipulációtól. Ez alapvető fontosságú az érzékeny információk, például a bejelentkezési adatok vagy a fizetési adatok védelme érdekében, hogy a támadók az átvitel során ne tudják elfogni őket. A HTTPS esetében az adatok titkosítva vannak a látogató böngészője és a szerver között, de a szerver továbbra is hozzáfér a titkosítatlan adatokhoz, ha azok megérkeznek. Ennek oka, hogy a szerver rendelkezik a dekódolási kulcsokkal. Ezért, bár a HTTPS védi az adatokat a lehallgatókkal szemben az útjuk során, magától a szervertől nem védi azokat.

Az adattovábbítás titkosítását gyakran kombinálják más biztonsági intézkedésekkel, hogy összetett hálózati környezetekben többszintű védelmet biztosítsanak az adatok számára.

End-to-end titkosítás

Az end-to-end titkosítás (E2EE) magasabb szintű biztonságot nyújt, mivel biztosítja, hogy az adatok titkosítása a feladó eszközén történik, és csak a címzett eszközén kerül visszafejtésre, anélkül, hogy közvetítők hozzáférnének a titkosítatlan információkhoz. Ez a megközelítés különösen hatékonyan akadályozza meg, hogy harmadik felek, például szolgáltatók vagy hackerek megnézhessék vagy megváltoztathassák a továbbított adatokat. Az E2EE-t széles körben használják a biztonságos üzenetküldő alkalmazásokban, az e-mail szolgáltatásokban és a fájlmegosztó platformokon. Egy biztonságos üzenetküldő alkalmazásban például az üzenet titkosítása a feladó eszközén történik, és a teljes út során titkosított marad, amíg el nem éri a címzettet, ahol végül visszafejtik. Még ha az üzenetet az átvitel során le is hallgatják, az olvashatatlan lenne a speciális visszafejtési kulcsok nélkül, amelyeket csak a kommunikáló eszközökön tárolnak.

Az E2EE egyik legnagyobb előnye, hogy az adatokat mind a szállítás során, mind pedig inaktív állapotukban (a céleszközön tárolva) védi. Ez azt jelenti, hogy még akkor is, ha a szolgáltató szervere veszélybe kerül, az adatok illetéktelenek számára hozzáférhetetlenek maradnak.

Bár a VPN-ek megbízható titkosítást biztosítanak a tranzitadatok számára, nem nyújtanak olyan átfogó védelmet, mint az E2EE, mivel nem fedik le a teljes kommunikációs láncot. A maximális biztonság érdekében ajánlott a VPN-eket end-to-end titkosított szolgáltatásokkal együtt használni. Ez a többszintű megközelítés biztosítja, hogy az adatok nem csak a VPN-alagúton való áthaladás során, hanem a végső célállomás elérésekor is védettek maradnak.

Névtelenség és azonosítás az interneten

Az anonimitás és az azonosítás az interneten (anonymity and recognition) összetett fogalmak, amelyek jelentése a felhasználók azonosítása vagy rejtve maradása a világhálón való navigálás során. Az internetet eredetileg nem az anonimitást szem előtt tartva tervezték; ehelyett az alapvető protokollok a csatlakoztathatóságra és az adatátvitelre összpontosítanak. Ez azt jelenti, hogy minden, az internethez csatlakozó eszközhöz azonosítót, például IP-címet vagy adakapcsolati réteg címet rendelnek, amely alapján nyomon követhető a tevékenysége és az interakciói. E fogalmak megértése alapvető fontosságú annak megértéséhez, hogy hogyan sérülhet az anonimitás, és milyen intézkedésekkel lehet megőrizni azt.

Adatkapcsolati réteg címek és IP-címek

A hálózathoz csatlakoztatott eszközöket a kommunikáció különböző szintjein egyedi címek segítségével azonosítják. Az *adatkapcsolati rétegben* minden *hálózati interfész kártya* (Network Interface Card — NIC) egyedi *Media Access Control* (MAC) címmel rendelkezik. Ez a cím a helyi hálózaton belüli kommunikációra szolgál, valamint egy adott eszköz azonosítására használható a hálózaton belül. Bár a MAC-cím általában nem kerül továbbításra a helyi hálózaton kívül, a hálózati rendszergazdák vagy rosszindulatú szereplők ugyanabban a hálózati szegmensben mégis felhasználhatják az eszköz tevékenységének nyomon követésére és ellenőrzésére.

A *hálózati rétegben* az eszközökhöz *Internet Protocol* (IP) címeket rendelnek, amelyek lehetnek statikusak vagy dinamikusak. Az IP-címek kritikus fontosságúak az adatok interneten keresztüli útválasztásához, de az eszközök digitális azonosítójaként is szolgálnak. Amikor meglátogatunk egy webhelyet, a szerver naplózza az IP-címünket, ahol a cím alapján megközelítőleg meghatározható a földrajzi elhelyezkedésünk, az internetszolgáltatónk és nyomon követhető az online viselkedésünk.

Bár az IP-címek önmagukban nem árulják el személyazonosságunkat, további adatpontok, például fiókbejelentkezések, böngészési szokások vagy más weboldalakkal való interakciók révén összekapcsolhatók velük. Az IP-címek egyénekhez kapcsolása veszélyezteti az anonimitást, és lehetővé teszi a felhasználók felismerését és a profilalkotást.

Anonimitás az interneten

Az anonimitás az interneten azt jelenti, hogy úgy használjuk a világhálót, hogy nem fedjük fel valódi személyazonosságunkat, és nem vagyunk könnyen lenyomozhatók. Az anonimitás eléréséhez el kell rejteni vagy zavarossá kell tenni (obfuszkálni) azokat az azonosítókat, amelyeket általában a felhasználók nyomon követésére használnak, mint például az IP-címeket és az adatkapcsolati réteg címeit. Az anonimitás elérésének egyik gyakori módszere az olyan anonimitási hálózatok használata, mint a Tor (The Onion Router), amely az internetes forgalmat önkéntesek által üzemeltetett szervereken keresztül vezeti, elrejtve az IP-címet, és megnehezítve a tevékenységek visszakövetését.

Egy másik megközelítés a virtuális magánhálózat (VPN) használata, amely egy biztonságos szerveren keresztül irányítja át a forgalmat, és így elrejti az IP-címet. Bár a VPN bizonyos szintű anonimitást biztosít azáltal, hogy elrejti az IP-címet a meglátogatott webhelyek elől, nem teljesen bolondbiztos. A VPN-szolgáltató maga is láthatja a valódi IP-címünket, és nyomon követheti a tevékenységünket, ezért fontos, hogy megbízható szolgáltatót válasszunk, amely szigorú naplózást tiltó irányelvekkel rendelkezik.

A proxy-szerverek is használhatók bizonyos fokú anonimitás elérésére. Proxy használata esetén a saját IP-címünk helyébe a proxy-kiszolgáló IP-címe lép, így elrejtve a valódi tartózkodási helyünket és identitásunkat. Ez különösen hasznos lehet a földrajzi korlátozások megkerüléséhez vagy az egyes régiókban blokkolt tartalmak eléréséhez. A VPN-ekhez hasonlóan azonban a proxyk sem nyújtanak teljes anonimitást, mivel a proxy-szerver naplózhatja és potenciálisan nyilvánosságra hozhatja a felhasználói tevékenységet. A magasabb szintű adatvédelem fenntartásához elengedhetetlen, hogy olyan proxykat használjunk, amelyek nem vezetnek naplót, és kombináljuk őket más adatvédelmi eszközökkel, például a Torral vagy VPN-ekkel.

Az anonimitás fenntartása magában foglalja az adatvédelemre összpontosító eszközök és gyakorlatok használatát is, például a webes tevékenységeket nyomon követő sütik letiltását, az olyan anonim böngészők használatát, mint a Tor, és az olyan bejelentkezési adatok elkerülését, amelyek összekapcsolhatók a valódi személyazonosságunkkal. Ezen intézkedések ellenére a valódi anonimitást az interneten nehéz elérni, mivel a különböző technológiák és technikák, például a böngésző ujjlenyomata és a metaadatok elemzése továbbra is felhasználhatók a felhasználók azonosítására.

Proxy-szerverek

A *proxy-szerver* közvetítőként működik a felhasználó eszköze és az internet között. Amikor a felhasználó egy proxy-szerveren keresztül csatlakozik az internethez, minden kérés és válasz a proxyn keresztül kerül átirányításra, mielőtt eléri a kívánt célállomást. Ez számos célt szolgálhat, többek között a biztonság növelését, a teljesítmény javítását és az anonimitás fenntartását. Amikor

a forgalom proxyn keresztül halad, a felhasználó IP-címe rejtve marad a meglátogatott webhelyek előtt, és helyette a proxy IP-címe jelenik meg, ami hatékonyan elrejti a felhasználó identitását és tartózkodási helyét.

A proxy-szerverek különböző szintű anonimitásra és funkcionalitásra konfigurálhatók. Egyes proxyk egyszerűen csak továbbítják a kéréseket mindenféle módosítás nélkül, míg mások tartalmat szűrnek, gyakran használt adatokat gyorsítótárba helyeznek, vagy akár módosítják a kimenő és bejövő adatokat. Ez a rugalmasság teszi a proxykat népszerű eszközzé különböző felhasználási esetekben, például a földrajzi korlátozások megkerülése, az internetes forgalom szűrése és a hálózati erőforrásokhoz való felhasználói hozzáférés ellenőrzése során.

Proxy-szerverek típusai

A proxy-szerverek különböző formákban léteznek, amelyek mindegyike egyedi igényekre és felhasználási esetekre szabott. A *forward proxy* a legelterjedtebb típus, ahol a proxy-szerver kezeli a kliens (például a webböngésző) internetre irányuló kéréseit. Ezt a proxy-típust gyakran használják vállalati környezetben az alkalmazottak internethasználatának ellenőrzésére és felügyeletére, illetve a tartalomkorlátozások megkerülésére. Egy szervezet például forward proxyt használhat arra, hogy munkaidőben korlátozza a közösségi oldalakhoz való hozzáférést.

A *reverse proxy* (fordított proxy) ezzel szemben a webszerverek előtt helyezkedik el, és a kliensek kéréseit kezeli a szerverek nevében. Ezt általában *terheléselosztásra* (load balancing) használják: a bejövő forgalom elosztása több szerver között azért, hogy egyetlen szerver se legyen túlterhelt. A fordított proxyk további biztonságot is nyújthatnak azáltal, hogy elrejtik a szerverhálózat belső struktúráját a külső felhasználók elől. Például egy fordított proxyt használó weboldal megvédheti az eredeti szervereit a közvetlen támadásoktól, mivel a proxy pajzsként működik.

Az *anonim proxyk* (anonymous proxy) és a *magas anonimitású proxyk* (high anonymity proxy) különböző szintű felhasználói adatvédelmet biztosítanak. Az anonim proxyk elrejtik a felhasználó IP-címét, de továbbra is proxyként azonosítják magukat, míg a magas anonimitású proxyk, más néven *elite proxyk* nem fedik fel, hogy proxyszerverek, így a weboldalak számára nehézséget jelent felismerni és blokkolni őket.

Felhasználási esetek

A proxy-szervereket széles körben használják különböző forgatókönyvekben a biztonság, az adatvédelem és az internetes forgalom feletti ellenőrzés fokozására. Vállalati környezetben a proxyk a nem megfelelő vagy nem produktív weboldalakhoz való hozzáférés blokkolásával érvényesíthetik az elfogadható használatra vonatkozó irányelveket. Megfelelőségi és biztonsági célokból a felhasználói tevékenység megfigyelésére és naplózására is használhatók. Ezzel szemben a magánszemélyek proxy-szervereket használhatnak az internetes cenzúra

megkerülésére, a régióhoz kötött tartalmak elérésére, vagy az anonimitás megőrzésére az internetes böngészés során.

Ezenkívül használják még a proxykat *web scraping* és *adataggregációs* célokra is. Több proxy IP-címet váltogatva a felhasználók elkerülhetik a detektálást és megkerülhetik a weboldalak által előírt sebességkorlátozásokat. Ez különösen hasznos nagy mennyiségű adat gyűjtéséhez anélkül, hogy a céloldalak blokkolnák vagy korlátoznák őket.

Korlátozások és kockázatok

Bár a proxy-szervereknek számos előnyük van, nem korlátlanok és kockázatmentesek. Egy rosszul konfigurált vagy megbízhatatlan proxy veszélyeztetheti a felhasználók adatvédelmét és biztonságát, és potenciálisan érzékeny információkat hozhat nyilvánosságra. A felhasználóknak óvatosnak kell lenniük, ha ingyenes vagy megbízhatatlan proxykat használnak, mivel ezek naplózhatják az adatokat vagy visszaélhetnek velük, hirdetéseket jeleníthetnek meg, vagy akár rosszindulatú tevékenységeket is végezhetnek.

A proxy-k nem titkosítják a felhasználó és a proxy-szerver közötti forgalmat, ami azt jelenti, hogy az adatokat harmadik felek lehallgathatják vagy megfigyelhetik. A magasabb szintű biztonság érdekében a proxykat más technológiákkal, például VPN-ekkel vagy end-to-end terjedő titkosítással együtt kell használni az adatok titkosságának és sértetlenségének biztosítása érdekében.

Összefoglalva, a proxy-szerverek sokoldalú eszközök, amelyek számos előnnyel járnak, az adatvédelem és a biztonság fokozásától kezdve a hálózati teljesítmény és ellenőrzés javításáig. Ugyanakkor elengedhetetlen, hogy tisztában legyünk a képességeikkel és korlátaikkal, és felelősségteljesen használjuk őket a lehetséges kockázatok csökkentése érdekében.

Gyakorló feladatok

1. Mik a legfontosabb tények a site-to-site VPN-ek két típusáról?

2. Mitől lesz egy VPN-kapcsolat privát?

Gondolkodtató feladatok

1. Mik a következő VPN protokollok közötti különbségek: IPsec, OpenVPN és WireGuard? Ismertessük a tipikus felhasználási eseteiket, erősségeiket és gyengeségeiket!

2. Képzeljük el, hogy megbíztak minket meg egy távoli hozzáférésű VPN konfigurálásával egy vállalat alkalmazottai számára. Milyen lépéseket tehetünk a biztonságos és hatékony beállítás érdekében? Adjunk meg legalább három olyan biztonsági intézkedést, amelyet végrehajtanánk!

Összefoglalás

Ez a lecke áttekintést nyújt a virtuális magánhálózatokról (VPN), és elmagyarázza, hogy milyen szerepet játszanak a nyilvános hálózatokon keresztüli biztonságos, titkosított kapcsolatok létrehozásában. A tananyag a VPN-technológia alapjainak ismertetésével kezdődik, beleértve az olyan alagút- és titkosítási protokollokat, mint az IPsec, az OpenVPN és a WireGuard, majd különbséget tesz a személyes adatvédelemre használt nyilvános VPN-ek és a biztonságos távoli hozzáféréshez és a telephelyek közötti kapcsolathoz tervezett szervezet-specifikus VPN-ek között. A szöveg foglalkozik a VPN-ekkel kapcsolatos korlátozásokkal és kockázatokkal is, útmutatást nyújt a jó hírű szolgáltatók kiválasztásához, és kiemeli a VPN-ek más titkosítási módszerekkel való kombinálásának fontosságát az átfogó adatvédelem biztosítása érdekében.

A lecke emellett az online anonimitás és azonosítás fogalmait is vizsgálja, részletezve, hogy az olyan azonosítók, mint az IP-címek hogyan veszélyeztethetik a felhasználók magánéletét. Különböző eszközöket és technikákat tárgyal, beleértve a proxy-szerverek, az anonimitási hálózatok és az adatvédelemre összpontosító gyakorlatok használatát, amelyek segítségével a felhasználók nagyobb anonimitást érhetnek el.

Válaszok a gyakorló feladatokra

1. Mik a legfontosabb tények a site-to-site VPN-ek két típusáról?

   Ha két távoli vállalati LAN között privát kapcsolat áll fenn, akkor site-to-site VPN-ről beszélünk. Ha a két távoli LAN ugyanazon szervezet fióktelepei, akkor intranet alapú site-to-site VPN-ről van szó. Ha a két távoli LAN két különböző, együttműködő félhez tartozik, akkor extranet alapú site-to-site VPN-ről van szó.

2. Mitől lesz egy VPN-kapcsolat privát?

   A kommunikálni kívánó két távoli fél között először egy privát csatornát kell létrehozni. A privát csatornán keresztül küldött adatok egységbezárásra és titkosításra kerül. Ez egy privát VPN-kapcsolatot eredményez. Bárki, aki a privát csatornán keresztül próbál hallgatózni, nem lesz képes hasznos információkat szerezni.

Válaszok a gondolkodtató feladatokra

1. Mik a következő VPN protokollok közötti különbségek: IPsec, OpenVPN és WireGuard? Ismertessük a tipikus felhasználási eseteiket, erősségeiket és gyengeségeiket!

   Az IPsec egy protokollcsomag, amelyet az IP-kommunikáció biztonságossá tételére terveztek az egyes IP-csomagok hitelesítésével és titkosításával. A hálózati rétegen működik, így használható mind a site-to-site, mind a távoli hozzáférésű VPN-ek számára. Erősségei közé tartoznak a robusztus biztonsági funkciók és a legtöbb hálózati eszközzel való kompatibilitás. A konfigurálása azonban bonyolult lehet, és a nagy titkosítási többletköltség miatt teljesítményproblémák merülhetnek fel.

   Az OpenVPN egy nyílt forráskódú VPN protokoll, amely SSL/TLS titkosítást használ, így rendkívül jól konfigurálható és biztonságos. Támogatja a TCP és az UDP szállítási protokollokat is, ami rugalmasságot biztosít a különböző hálózati környezetekben. Az OpenVPN-t széles körben használják távoli hozzáférésű VPN-ek esetében, erős biztonsági jellemzői és a tűzfalak megkerülésére való képessége miatt. Elsődleges gyengesége, hogy kliensszoftvert igényel, és a kiterjedt titkosítás miatt lassabb lehet, mint más protokollok.

   A WireGuard egy viszonylag új, könnyűsúlyú (lightweight) VPN protokoll, amelynek célja, hogy gyorsabb és egyszerűbb legyen, mint az IPsec és az OpenVPN. A legmodernebb kriptográfiát használja, és úgy tervezték, hogy minimális kódbázissal rendelkezzen, így csökkentve a biztonsági sebezhetőségek lehetőségét. A WireGuard erősségei közé tartozik a nagy teljesítmény és az egyszerű konfigurálhatóság. Ugyanakkor még mindig folyamatban van az egyes rendszerekbe való integrálása, és a dinamikus IP-címváltások támogatása korlátozott lehet az érettebb protokollokhoz képest.

2. Képzeljük el, hogy megbíztak minket meg egy távoli hozzáférésű VPN konfigurálásával egy vállalat alkalmazottai számára. Milyen lépéseket tehetünk a biztonságos és hatékony beállítás érdekében? Adjunk meg legalább három olyan biztonsági intézkedést, amelyet végrehajtanánk!

   Válasszunk egy biztonságos és megbízható VPN protokollt, például az OpenVPN vagy IPsec protokollt a VPN beállításához! Ez biztosítja, hogy az alkalmazottak és a vállalati hálózat között továbbított összes adat titkosítva legyen, valamint védve a lehallgatástól.

   Legyen elvárás az alkalmazottak felé, hogy a VPN-hez való csatlakozáskor többfaktoros hitelesítést (MFA) használjanak! Ez egy további biztonsági réteget ad a puszta felhasználóneveken és jelszavakon túl, megnehezítve az illetéktelen felhasználók számára a hozzáférést.

   Konfiguráljuk a VPN-t úgy, hogy a felhasználói szerepkörök és az eszköz megfelelősége alapján

érvényesíthessük a hozzáférés-szabályozási irányelveket. Például csak olyan felhasználók számára engedélyezzük az érzékeny erőforrásokhoz való hozzáférést, akik átmentek az eszközellenőrzésen, például frissített vírusirtó szoftverrel és a legújabb biztonsági javítások telepítésével rendelkeznek! Ez segít megelőzni a jogosulatlan hozzáférést, és korlátozza a kompromitált fiókok vagy eszközök potenciális hatását.

Linux Professional Institute

Lecke 2

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	024 Hálózat- és szolgáltatásbiztonság
Fejezet:	024.3 Hálózati titkosítás és anonimitás
Lecke:	2/2

Bevezetés

Egy olyan korszakban, amikor a digitális magánélet és az anonimitás egyre nagyobb veszélyben van, az olyan technológiák, mint a Tor, a kriptovaluták és a darknet kulcsfontosságú eszközökké váltak azok számára, akik meg akarják védeni online tevékenységeiket. A Tor vagy The Onion Router egy olyan hálózat, amely az internetes forgalom több szerveren keresztül történő átirányításával biztosítja az anonimitást, így elfedve a felhasználók személyazonosságát és megnehezítve tevékenységük nyomon követését. Ez a technológia létfontosságúvá vált az adatvédelem hívei, az újságírók és az elnyomó rezsimekben élő egyének számára, akiknek szabadon kell hozzáférniük az információkhoz és biztonságosan kell kommunikálniuk.

Az anonimitás fogalma túlmutat az egyszerű böngészési szokásokon, és olyan összetettebb rendszerekre is kiterjed, mint a *darknet*, az internet egy olyan rejtett része, amely csak olyan speciális szoftverekkel érhető el, mint a Tor. A darknet a legkülönbözőbb tartalmaknak ad otthont, a törvényes, az adatvédelemre összpontosító fórumoktól és a whistleblower platformoktól a tiltott online piacterekig. Bár a médiában gyakran negatív színben tüntetik fel, egyben kritikus fontosságú tér azok számára, akiknek tevékenységükhöz nagyfokú titoktartásra és anonimitásra van szükségük.

A kriptovaluták, különösen a Bitcoin és más blokklánc-alapú (blockchain-based) eszközök új dimenziót hoztak az anonimitásról szóló beszélgetésbe. Bár a legtöbb blockchainen a tranzakciók átláthatóak és nyomon követhetőek, az pszeudonim címek használata az anonimitás egy olyan rétegét biztosítja, amelyet a hagyományos pénzügyi rendszerek nem kínálnak. Ez a vélt anonimitás azonban megtévesztő lehet, mivel a fejlett elemzési technikák egyre inkább képesek a blockchain tranzakciók anonimitásának megszüntetésére. E technológiák árnyalatainak és korlátainak megértése alapvető fontosságú mindazok számára, akik a digitális anonimitás és a magánélet összetettségében szeretnének eligazodni.

Tor

A *Tor*, a *The Onion Router* rövidítése, egy decentralizált hálózat, amelyet az online adatvédelem és anonimitás fokozására terveztek. Lehetővé teszi a felhasználók számára, hogy anélkül böngészhessenek az interneten, hogy IP-címüket vagy személyes adataikat felfednék harmadik felek előtt. A Tor ezt úgy éri el, hogy az internetes forgalmat egy sor önkéntesek által üzemeltetett szerveren, azaz *csomóponton* (node) keresztül irányítja, amelyek mindegyike saját titkosítási réteget alkalmaz.

Ez a folyamat egy hagyma rétegeihez hasonlít, innen származik az “onion router” elnevezés is. Mivel a forgalom több csomóponton halad át, az adatok eredeti forrása és rendeltetési helye elrejthetővé válik, így bárki, beleértve a kormányzati szerveket vagy a hackereket is, nehezen tudja visszavezetni a tevékenységet a felhasználóig.

A Tor-t eredetileg az 1990-es évek közepén fejlesztette ki az Egyesült Államok Haditengerészeti Kutatási Laboratóriuma az amerikai hírszerzés online kommunikációjának védelmére. A cél egy olyan rendszer létrehozása volt, amely lehetővé teszi a felhasználók számára, hogy névtelenül böngészhessenek az interneten anélkül, hogy felfednék tartózkodási helyüket vagy identitásukat. 2002-ben a Tor forráskódját szabad licenc alatt adták ki, és a Tor nyilvánosan elérhető eszközzé vált mindenki számára, aki fokozott magánéletet és biztonságot keres az interneten.

A projekt 2004-ben további lendületet kapott, amikor az Electronic Frontier Foundation (EFF) támogatni kezdte a fejlesztését. Azóta a Tor világszerte létfontosságú forrássá vált az újságírók, aktivisták és a magánélet védelmére törekvő személyek számára. Lehetővé teszi a felhasználók számára, hogy megkerüljék a cenzúrát, megvédjék online identitásukat és szabadon hozzáférjenek az információkhoz, ami a digitális magánéletért és a véleménynyilvánítás szabadságáért folytatott küzdelemben alapvető eszközzé teszi.

A Tor különböző célokra használatos, a felhasználói adatvédelemtől kezdve a megfigyelés és a nyomon követés elleni védekezésen át a cenzúra megkerüléséig és az információhoz való hozzáférésig olyan régiókban, ahol korlátozott az internet-hozzáférés. Erős anonimitási jellemzői miatt azonban a Tor-t néha illegális tevékenységekkel hozzák összefüggésbe. Ennek ellenére

újságírók, aktivisták és magánszemélyek, akik elnyomó környezetben élve szeretnék megvédeni a magánéletüket, széles körben használják. A Tor a *Tor Browser*, a Mozilla Firefox módosított változata révén érhető el, amely megkönnyíti a felhasználók számára a Tor-hálózathoz való csatlakozást és a biztonságos internetezést (Tor Browser).

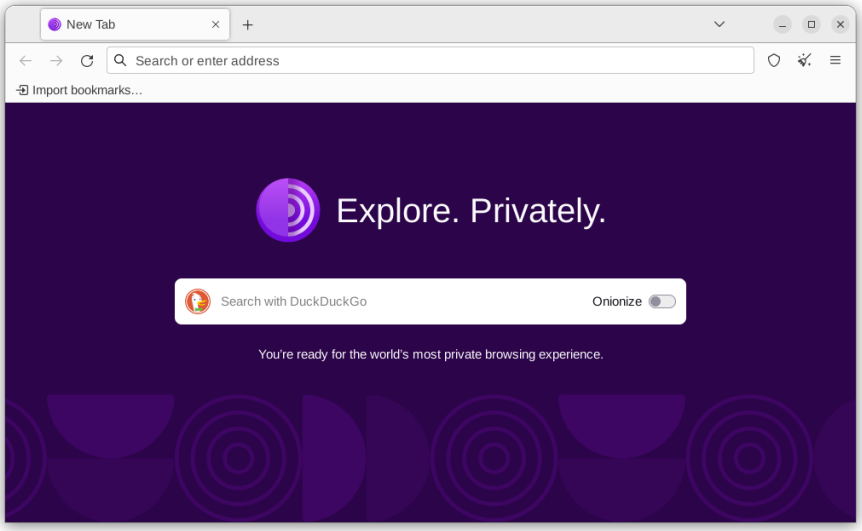

Figure 37. Tor Browser

Rejtett szolgáltatások és .onion domainek

A Tor amellett, hogy anonimitást biztosít az interneten való böngészéshez, támogatja a *rejtett szolgáltatásokat* (hidden service). Ezek lehetővé teszik, hogy a weboldalak és szerverek névtelenül működjenek a Tor-hálózaton belül, így mind a felhasználó, mind a szerver nehezen követhetővé válik. Ezek a szolgáltatások ".onion" domaineket használnak, amelyek a hagyományos webböngészőkön vagy keresőmotorokon keresztül nem, csak a Tor böngészőn vagy hasonló, a Tor-hálózathoz való csatlakozásra konfigurált szoftveren keresztül érhetők el.

A .onion domain a webcímek egy speciális típusa, amely `.onion`-ra végződik, és egy rejtett szolgáltatást képvisel a Tor hálózaton belül. Ezeket a domaineket kriptográfiai algoritmusok segítségével generálják, így biztosítva, hogy mind a szerver, mind a felhasználók névtelenek maradjanak. A rejtett szolgáltatásokat különböző törvényes célokra használják, például biztonságos kommunikációs platformok, informátoroldalak és névtelen fórumok, ahol a magánélet és a titoktartás a legfontosabb. Például az olyan médiaszervezetek, mint a The New York Times, és a SecureDrophoz hasonló whistleblower platformok .onion címeket használnak, hogy lehetővé tegyék a forrásokkal való anonim kommunikációt.

Ezeket a .onion domaineket egy kriptográfiai folyamat során hozzák létre, amely egy egyedi publikus és privát kulcspárt hoz létre. A nyilvános kulcsot a .onion-cím kialakításához használják, míg a privát a szerveren marad, garantálva, hogy csak a megfelelő privát kulccsal rendelkező

kijelölt szerver hostolhatja az adott .onion-szolgáltatást.

Amikor egy felhasználó megpróbál hozzáférni egy .onion oldalhoz, a kérése több Tor-csomóponton keresztül kerül átirányításra, amelyek proxy-szerverként működnek, ezáltal elrejtve a felhasználó identitását és tartózkodási helyét a szolgáltatás elől. Ez a többrétegű útválasztás biztosítja, hogy a felhasználó IP-címe rejtve marad a webhely előtt, így megőrizve a felhasználó magánszféráját. Emellett a felhasználó és a .onion szolgáltatás közötti kommunikáció végponttól végpontig titkosított, ami azt jelenti, hogy az adatok biztonságosan továbbítódnak a felhasználó eszközéről a szerverre anélkül, hogy harmadik felek lehallgatnák vagy manipulálnák azokat.

A .onion oldalak meglátogatásához a felhasználóknak a Tor-hálózathoz konfigurált böngészőt kell használniuk, ilyen például a Tor Browser. A hagyományos webböngészők nem tudják feloldani a .onion címeket, mivel ezek a domainek nem részei a hagyományos DNS-rendszernek. Ez a speciális hozzáférés biztonságos és anonim módszert biztosít a tartalmak tárolására és látogatására, így a .onion oldalak alapvető eszközzé válnak az adatvédelemre összpontosító szolgáltatások, a biztonságos kommunikáció és a korlátozó környezetben történő információmegosztás számára.

Biztonságos navigálás a .onion oldalakon

Az Onion hálózaton való keresés eltér a hagyományos internetes böngészéstől, mivel a .onion oldalakat nem indexelik az olyan hagyományos keresőmotorok, mint a Google. Ehelyett speciális keresőmotorok segítenek megtalálni a Tor-hálózaton belül a .onion oldalakon található tartalmakat. Az Onion hálózat egyik legnépszerűbb keresőmotorja a DuckDuckGo, amelynek Onion változata tiszteletben tartja a felhasználók magánszféráját, és nem követi őket nyomon. Támogatja a .onion oldalak indexelését is.

Egy másik lehetőség az Ahmia, egy olyan keresőmotor, amely .onion oldalakat indexel, és arra összpontosít, hogy hozzáférést biztosítson a törvényes és biztonságos tartalmakhoz, miközben kiszűri a potenciálisan káros anyagokat. Ez egy megbízható forrás a Tor-hálózaton található tartalmak kereséséhez. Emellett a Torch az egyik legrégebbi keresőmotor az Onion-hálózat számára, és nagy mennyiségű .onion oldalt indexel. Egyszerű kezelőfelülete ellenére hatékony a Tor-hálózaton található tartalmak széles körének felkutatásában.

Ahhoz, hogy használhassuk ezeket a keresőmotorokat, a Tor böngészőn keresztül kell elérnünk őket, amely lehetővé teszi az anonim böngészést a Tor-hálózaton. Fontos, hogy óvatosak legyünk, amikor az Onion-hálózat bármelyik keresőmotorját használjuk, mivel illegális vagy rosszindulatú tartalmakkal találkozhatunk! Mindig legyünk éberek, és győződjünk meg arról, hogy megbízható és törvényes forrásokhoz férünk hozzá!

Gyakorlati szempontok és kockázatok

Bár a Tor magas szintű anonimitást biztosít, nem teljesen bolondbiztos. A felhasználóknak tisztában kell lenniük a Tor használatával kapcsolatos lehetséges kockázatokkal, például a rosszindulatú kilépési csomópontokkal, amelyek képesek figyelni a Tor-hálózatot elhagyó titkosítatlan forgalmat. Emellett a személyes adatokat felfedő tevékenységek, például a személyes fiókokba való bejelentkezés vagy a fájlok letöltése még a Tor használata esetén is veszélyeztetheti az anonimitást. Az adatvédelem maximalizálása érdekében a felhasználóknak a Tort más, az adatvédelemre összpontosító eszközökkel, például végponttól végpontig titkosított üzenetküldéssel és biztonságos böngészési gyakorlatokkal kell kombinálniuk.

Összességében a Tor egy hatékony eszköz azok számára, akiknek meg kell védeniük a magánszférájukat és szabadon hozzá szeretnének férni az információkhoz, de úgy kell használniuk, hogy tisztában vannak a képességeivel és korlátaival.

A darknet

A *darknet* az internet egy olyan részét jelenti, amely szándékosan rejtve van, és a hozzáféréshez speciális szoftver, konfiguráció vagy engedély szükséges. A felszíni webtől eltérően, amelyet a hagyományos keresőmotorok, például a Google indexel, és a hagyományos böngészőkkel elérhető, a darknet olyan titkosított hálózatokon belül működik, mint a Tor, az I2P és a Freenet. Ezek a hálózatok anonimitást biztosítanak mind a felhasználók, mind a webhelyek üzemeltetői számára, így a darknet olyan térré válik, ahol a magánszféra és a szólásszabadság megmarad, de illegális tevékenységek is előfordulhatnak.

A darknetet az anonimitási tulajdonságai miatt gyakran hozzák összefüggésbe illegális piacterekkel és bűncselekményekkel. Olyan platformoknak ad otthont, ahol a felhasználók illegális árukat és szolgáltatásokat, például kábítószert, hamisított dokumentumokat és lopott adatokat vásárolhatnak és adhatnak el olyan kriptovaluták segítségével, mint a Bitcoin és a Monero. A darknet azonban nem kizárólag az illegális tevékenységek központja. Az olyan újságírók, aktivisták és informátorok számára is létfontosságú erőforrás, akik elnyomó rezsimekben vagy olyan körülmények között tevékenykednek, ahol a nyílt kommunikáció súlyos következményekkel járhat. A biztonságos kommunikációs platformok, az anonim fórumok és a SecureDrop-hoz hasonló, whistleblower oldalak mind a darknet részét képezik, és biztonságos teret biztosítanak a bizalmasságra vágyók számára.

A darknet eléréséhez általában speciális szoftvereket kell használni, mint például a Tor Browser. A csatlakozást követően a felhasználók olyan .onion oldalakra vagy más rejtett szolgáltatásokra navigálhatnak, amelyek a hagyományos webböngészőkkel nem érhetők el. Annak ellenére, hogy a darknetet veszélyes helyként tartják számon, ez egyúttal a digitális magánélet védelmének és a szabad véleménynyilvánításnak az eszköze is olyan környezetben, ahol ezek a jogok

korlátozottak. Mint minden eszköz esetében, a darknet értéke és a károkozás lehetősége is attól függ, hogy hogyan használják. A felelősségteljes navigáció alapvető fontosságú mindazok számára, akik az internet e rejtett részébe merészkednek.

Kriptovaluták — A blockchain megértése

A *kriptovaluták* (cryptocurrency), mint például a Bitcoin és a Monero, azért váltak népszerűvé, mert olyan mértékű pénzügyi magánszférát és anonimitást kínálnak, amely a hagyományos bankrendszerekben jellemzően nem áll rendelkezésre.

Ezek a digitális valuták decentralizált hálózatokon működnek, a *blockchain* (blokklánc) technológiát használva, amely a tranzakciók rögzítésére és ellenőrzésére szolgáló alapstruktúraként szolgál, anélkül, hogy központi hatóságra, például bankra vagy kormányra lenne szükség. A blokklánc lényegében egy elosztott főkönyv, amelyet a hálózatban részt vevő *csomópontok* (node, számítógépek) hálózata oszt meg és tart fenn. Minden egyes csomópont tartalmazza a teljes blockchain egy példányát, és az új tranzakciókat egy konszenzusmechanizmus, például a *Proof of Work* (PoW) vagy a *Proof of Stake* (PoS) segítségével hitelesítik. Ez a folyamat biztosítja, hogy minden csomópont egyetért a blockchain állapotával, így az ellenállóvá válik a csalással és a manipulációval szemben.

Amikor egy felhasználó tranzakciót kezdeményez, azt más tranzakciókkal együtt egy *blokkba* csoportosítja. Ezt a blokkot ezután továbbítják a hálózatnak, ahol a csomópontok a blockchain protokoll szabályai szerint érvényesítik azt. Például a Bitcoin esetében ez a folyamat egy összetett matematikai rejtvény megoldását jelenti — ez a folyamat a *mining* (bányászás). Miután a blokkot validálták, az hozzáadódik a korábban validált blokkok láncához, így létrehozva egy állandó és megváltoztathatatlan feljegyzést az adott tranzakcióról. Ez a blokkok lánca, vagy blokklánc, a hálózaton valaha történt összes tranzakció átfogó és kronologikus történetét alkotja.

Bár a blockchain átláthatósága lehetővé teszi, hogy bárki megtekinthesse a tranzakciók teljes történetét, nem feltétlenül köti ezeket a tranzakciókat valós személyazonosságokhoz. Ehelyett a felhasználókat egyedi alfanumerikus címek, úgynevezett *nyilvános kulcsok* képviselik. Ezeket a nyilvános kulcsokat kriptográfiai algoritmusok segítségével generálják, és pszeudonim (álnevesített) azonosítóként szolgálnak. Például ahelyett, hogy a blockchain azt mutatná, hogy "Carol Doe 1 Bitcoint küldött Dave Smithnek", a blokklánc azt rögzíti, hogy egy adott cím (pl. `1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa`) 1 Bitcoint küldött egy másik címnek. Ez egyfajta *pszeudonimitást* teremt, mivel a címek nem fedik fel közvetlenül a mögöttük álló személyek személyazonosságát.

Az anonimitás mértéke azonban jelentősen eltér a blokklánc kialakításától függően. Az olyan kriptovaluták esetében, mint a Bitcoin, minden tranzakció nyilvánosan látható, ami azt jelenti, hogy bárki nyomon követheti az egyik címről a másikra történő pénzmozgást. Ha egy személy

személyazonossága egy adott címhez kapcsolódik az információk kiszivárgása, egy ismert tőzsdén való használat vagy véletlen nyilvánosságra hozatal révén, akkor lehetővé válik a teljes tranzakciós előzmények nyomon követése. Ezért a Bitcoin inkább tekinthető pszeudonimnak, mint anonimnak.

Ezzel szemben az olyan, az adatvédelemre összpontosító kriptovaluták, mint a Monero és a Zcash további funkciókat alkalmaznak a tranzakció részleteinek elfedésére. A Monero például gyűrűs aláírásokat és gyűrűs bizalmas tranzakciókat (RingCT) használ, hogy a feladó tranzakcióját több másikkal keverje, így gyakorlatilag lehetetlenné teszi a pénzeszközök eredetének vagy rendeltetési helyének meghatározását. Emellett lopakodó (stealth) címeket is használ, amelyek minden egyes tranzakcióhoz egyedi, egyszeri címet generálnak. Ez azt jelenti, hogy még ha valaki ismer is egy Monero címet, nem láthatja a blokkláncon az adott címre érkező összes tranzakciót.

A Zcash viszont lehetőséget biztosít a felhasználóknak, hogy válasszanak az átlátható (transparent) és a védett (shielded) tranzakciók között. A védett tranzakciók egy kifinomult kriptográfiai technikát használnak, amelyet zk-SNARK-nak (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) neveznek. Ez lehetővé teszi a hálózat számára, hogy ellenőrizze, hogy egy tranzakció érvényes-e anélkül, hogy bármilyen részletet felfedne a feladóról, a címzettről vagy a tranzakció összegéről. Ez magas szintű adatvédelmet biztosít, de több számítási erőforrást igényel, ami ronthatja a skálázhatóságot és a hatékonyságot.

Ezen túlmenően a kriptovaluták vélt anonimitását alááshatja a központosított szolgáltatások, például a tőzsdék használata, amelyek gyakran megkövetelik a személyazonosság ellenőrzését a *Know Your Customer* (KYC) folyamatokon keresztül. Amint egy felhasználó személyazonossága egy tőzsdén keresztül egy címhez kapcsolódik, a tranzakciós előzményei nyomon követhetők és elemezhetők. Ez olyan fejlett blockchain-elemző eszközök kifejlesztéséhez vezetett, amelyek képesek a minták azonosítására, a pénzmozgások nyomon követésére, sőt bizonyos feltételek mellett akár a felhasználók anonimitásának megszüntetésére is.

Ennek leküzdésére az adatvédelmet előtérbe helyező felhasználók gyakran alkalmaznak további intézkedéseket, például adatvédelmi érméket (privacy coin), mixelt szolgáltatásokat (tumblers) vagy a tranzakciós útvonalakat obfuszkáló, az adatvédelmet fokozó pénztárcákat. A mixelt szolgáltatások például különböző felhasználóktól származó több tranzakciót egyesítenek, megnehezítve ezzel az egyes tranzakciók eredetének nyomon követését. Ezek a szolgáltatások azonban a szabályozó hatóságok ellenőrzése alá kerültek, mivel tiltott pénzek tisztára mosására használhatók.

Míg a blockchain technológia átlátható és biztonságos módot biztosít a tranzakciók rögzítésére, az általa kínált adatvédelem és anonimitás szintje nagymértékben eltér a blockchain kialakításától és a felhasználók által a személyazonosságuk védelme érdekében tett intézkedésektől függően. Ezeknek az árnyalatoknak a megértése kulcsfontosságú mindazok számára, akik kriptovalutákkal

kívánnak foglalkozni, akár adatvédelmi, akár biztonsági, akár pénzügyi célokból.

Gyakorló feladatok

1. Hogyan növeli a Tor a felhasználók anonimitását az interneten? Milyen folyamat révén fedi el a Tor a felhasználó identitását, és mi a fejlesztés történelmi háttere?

2. Mik az elsődleges különbségek a Bitcoin és a Monero között az anonimitás szempontjából? Fejtsük ki, hogy az egyes kriptopénzek milyen technikákat alkalmaznak a felhasználók adatainak védelmére!

3. Milyen szerepet játszik a darknet az anonimitással összefüggésben, és hogyan lehet hozzáférni? Magyarázzuk meg mind a pozitív, mind a negatív aspektusait!

 | |

Gondolkodtató feladatok

1. Vizsgáljuk meg a bűnüldöző szervek által a Tor-felhasználók de-anonimizálására használt különböző módszereket! Határozzunk meg legalább két konkrét technikát vagy technológiát, amelyet az ilyen nyomozások során alkalmaznak, és mutassunk be olyan esettanulmányokat, amelyekben ezeket a módszereket sikeresen alkalmazták a Tor-t használó személyek személyazonosságának feltárására! Elemezzük ezeknek a módszereknek a hatékonyságát és a Tor-hálózat által biztosítottnak vélt anonimitásra gyakorolt hatásukat!

Összefoglalás

Ez a lecke a digitális adatvédelem, az anonimitás és az ezeket a fogalmakat támogató technológiák, például a Tor, a darknet és a kriptovaluták közötti kölcsönhatást vizsgálja. A Tor vagy The Onion Router egy olyan hálózat, amely anonimitást biztosít azáltal, hogy az internetes forgalmat több szerveren keresztül irányítja, megnehezítve ezzel a felhasználói tevékenységek nyomon követését. A darknet, az internet egy rejtett része, amely csak olyan speciális szoftvereken keresztül érhető el, mint a Tor, mind a törvényes, a magánélet védelmét célzó tevékenységek, mind az illegális piacok számára menedékként szolgál, ami tükrözi ezen anonimitási technológiák kettős természetét.

A kriptovaluták, bár gyakran anonimnak tekintik őket, blockchain technológiával működnek, ahol a tranzakciókat egy nyilvános főkönyvben rögzítik. Ez az átláthatóság alááshatja az anonimitást, különösen az olyan kriptovaluták esetében, mint a Bitcoin, amelyek inkább pszeudonimak, mint teljesen névtelenek. A fejlett analitika néha képes összekapcsolni a tranzakciókat a valós személyazonosságokkal. Ezzel szemben az olyan, az adatvédelemre összpontosító kriptovaluták, mint a Monero és a Zcash, fokozott anonimitási funkciókat kínálnak a felhasználói személyazonosság és a tranzakciók részleteinek elfedésére. E képességek ellenére a teljes anonimitás fenntartása a kriptovaluták esetében továbbra is kihívást jelent a szabályozási ellenőrzés és a blockchain-elemzés változó terepe miatt.

Válaszok a gyakorló feladatokra

1. Hogyan növeli a Tor a felhasználók anonimitását az interneten? Milyen folyamat révén fedi el a Tor a felhasználó identitását, és mi a fejlesztés történelmi háttere?

   A Tor úgy növeli a felhasználók anonimitását, hogy az internetes forgalmat önkéntesek által üzemeltetett szerverek hálózatán keresztül irányítja, amelyek mindegyike egy-egy titkosítási réteget alkalmaz, ami hasonlít a hagyma rétegeihez. Mivel a forgalom több csomóponton halad át, az adatok eredeti forrása és célállomása elfedhetővé válik, így rendkívül nehéz bárki számára visszakövetni a felhasználó tevékenységét. A Tor-t eredetileg az 1990-es évek közepén fejlesztette ki az Egyesült Államok Haditengerészeti Kutatási Laboratóriuma az amerikai hírszerzési kommunikáció védelmére. A forráskódot 2002-ben szabad licenc alatt adták ki, és így nyilvánosan elérhető eszközzé vált mindenki számára, aki fokozott magánszférát és biztonságot keres az interneten. Azóta az újságírók, aktivisták és a privátszféra védelmét szem előtt tartó magánszemélyek számára létfontosságú forrássá fejlődött.

2. Mik az elsődleges különbségek a Bitcoin és a Monero között az anonimitás szempontjából? Fejtsük ki, hogy az egyes kriptopénzek milyen technikákat alkalmaznak a felhasználók adatainak védelmére!

   Az elsődleges különbség a Bitcoin és a Monero között az anonimitás szempontjából az, hogy a Bitcoin pszeudonim, míg a Monero célja a valódi anonimitás biztosítása. A Bitcoin minden tranzakciót egy nyilvános főkönyvben rögzít, és bár a felhasználókat alfanumerikus címek képviselik, elegendő adat és elemzés segítségével lehetséges ezeket a címeket egyénekre visszavezetni. A Monero ezzel szemben olyan fejlett adatvédelmi technikákat használ, mint a gyűrűs aláírás, a lopakodó címek és a bizalmas tranzakciók, hogy elrejtse a feladó és a címzett adatait, valamint a tranzakció összegét. Ezáltal sokkal nehezebb a Monero tranzakciókat nyomon követni és konkrét személyekhez kötni, és ez magasabb szintű adatvédelmet biztosít, mint a Bitcoin.

3. Milyen szerepet játszik a darknet az anonimitással összefüggésben, és hogyan lehet hozzáférni? Magyarázzuk meg mind a pozitív, mind a negatív aspektusait!

   A darknet az internet egy olyan része, amely fokozott anonimitást biztosít azáltal, hogy a tartalmak eléréséhez speciális szoftverre, például a Tor böngészőre van szükség. Lehetővé teszi a felhasználók számára, hogy olyan rejtett szolgáltatásokban és .onion oldalakon navigáljanak, amelyeket a hagyományos keresőmotorok nem indexelnek, és amelyek a hagyományos böngészőkkel nem érhetők el. A darknet létfontosságú erőforrás lehet az újságírók, aktivisták és informátorok számára, akik biztonságosan kommunikálhatnak és információhoz juthatnak anélkül, hogy a megfigyeléstől vagy cenzúrától tartanának. Ugyanakkor illegális tevékenységekkel is összefüggésbe hozható, mivel anonimitási jellemzőit kihasználják illegális

piacterek működtetésére és illegális tartalmak terjesztésére. A darknet tehát, bár a digitális magánélet védelmének és a szabad véleménynyilvánításnak a korlátozó környezetben való lehetővé tételének alapvető eszköze, jelentős etikai és jogi kihívásokat is jelent.

 | |

Válaszok a godolkodtató feladatokra

1. Vizsgáljuk meg a bűnüldöző szervek által a Tor-felhasználók de-anonimizálására használt különböző módszereket! Határozzunk meg legalább két konkrét technikát vagy technológiát, amelyet az ilyen nyomozások során alkalmaznak, és mutassunk be olyan esettanulmányokat, amelyekben ezeket a módszereket sikeresen alkalmazták a Tor-t használó személyek személyazonosságának feltárására! Elemezzük ezeknek a módszereknek a hatékonyságát és a Tor-hálózat által biztosítottnak vélt anonimitásra gyakorolt hatásukat!

   A bűnüldöző szervek által a Tor-felhasználók anonimitásának megszüntetésére használt egyik gyakori technika a forgalomelemzés. Ez magában foglalja a Tor-hálózatba belépő és onnan kilépő forgalom megfigyelését, és olyan minták azonosítását, amelyeket konkrét felhasználókhoz lehet rendelni. A “Silk Road” felszámolásakor a bűnüldöző szervek figyelték a forgalmi mintákat, és más nyomozati technikákkal kombinálva azonosították Ross Ulbrichtot, az oldal üzemeltetőjét, mint “Dread Pirate Roberts”-et. Ez az eset megmutatta, hogy bár a Tor jelentős szintű anonimitást biztosít, ez veszélybe kerülhet, ha más adatforrásokkal és megfigyelési technikákkal kombinálják.

   Egy másik technika a rosszindulatú Tor kilépési csomópontok használatát jelenti. Ezek olyan csomópontok, amelyeket a bűnüldöző szervek vagy más szervezetek üzemeltetnek, és amelyek elfogják és naplózzák a rajtuk áthaladó forgalmat. Például 2014-ben az FBI és az Europol közös, “Onymous” művelete több darknetes piac lefülelését eredményezte. A gyanú szerint a művelet során rosszindulatú kilépési csomópontokat használtak a titkosítatlan forgalom rögzítésére és ezen oldalak adminisztrátorainak és felhasználóinak azonosítására. Ez a módszer rávilágított a Tor-hálózat egyik kulcsfontosságú sebezhetőségére, ahol a Tor-hálózatot elhagyó titkosítatlan adatok lehallgathatók és felhasználhatók a felhasználók azonosítására.

Linux Professional Institute

Témakör 025: Identitás és magánélet

 | |

025.1 Identitás és autentikáció

Hivatkozás az LPI célkitűzésre

Security Essentials version 1.0, Exam 020, Objective 025.1

Súlyozás

3

Kulcsfontosságú ismeretek

- A digitális identitás fogalmának megértése
- Az autentikáció, az authorizáció és a nyilvántartás fogalmainak megértése
- A biztonságos jelszavak jellemzőinek megértése (pl. hosszúság, speciális karakterek, változtatási gyakoriság, összetettség)
- Jelszókezelő használata
- A biztonsági kérdések és a fiókvisszaállítási eszközök fogalmainak megértése
- A többfaktoros hitelesítés (MFA) fogalmainak megértése, beleértve a közös tényezőket is
- Az egyszeri bejelentkezés (SSO) és a közösségi média bejelentkezések fogalmának megértése
- Az e-mail fiókok szerepének megértése az informatikai biztonság szempontjából
- A jelszavak online szolgáltatásokban történő tárolásának megértése
- A jelszavak elleni gyakori támadások megértése
- A személyes fiókok figyelése jelszószivárgások szempontjából (pl. keresőmotorok figyelmeztetései a felhasználónevekre és jelszószivárgás-ellenőrzők)
- Az online banki szolgáltatások és hitelkártyák biztonsági szempontjainak megértése

A használt fájlok, kifejezések és segédprogramok részleges listája

- Online és offline jelszókezelők

- keepass2
- Single sign-on (SSO)
- Kétfaktoros hitelesítés (2FA) és többfaktoros hitelesítés (MFA)
- Egyszeri jelszavak (OTP), időalapú egyszeri jelszavak (TOTP)
- Hitelesítő alkalmazások
- Jelszó hashelés és sózás
- Brute force-támadások, directory támadások, szivárványtábla-támadások

Linux Professional Institute

Lecke 1

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	025 Identitás és magánélet
Fejezet:	025.1 Identitás és autentikáció
Lecke:	1/1

Bevezetés

Az *identitás* kérdése arra fut ki, hogy “Ki vagy te?”. Ha beugrunk egy barátunk partijára, a barátunk felismerhet minket az arcunkról. De ha egy konferenciára megyünk, a személyzet esetleg ellenőrizni akarja a személyi igazolványunkat (amelyen valószínűleg szerepel egy fénykép az arcunkról), mielőtt beengednek. Tehát még a mindennapi életben sem mindig egyszerű dolog az identitás.

Az *autentikáció* (hitelesítés) a személyazonosság megállapításának módja. A konferencián a személyzet a fényképes igazolványon keresztül hitelesít minket. Amikor átvesszük a ruháinkat a tisztítóban, nem kell igazolnunk a személyazonosságukat — de jobb, ha elhozzuk a nyugtát, amelyen listázva vannak a ruhák. Ez az autentikáció egy másik formája.

Ez a lecke a *digitális identitással* foglalkozik, vagyis azzal, ahogyan a számítógépes programok és online szolgáltatások azonosítanak minket, azért, hogy hozzáférést biztosítsanak nekünk. Olyan kapcsolódó témákat fogunk megvizsgálni, mint a jelszókezelés, a többfaktoros hitelesítés és az egyszeri bejelentkezés. Elmondjuk, hogyan maximalizálhatjuk ezeknek a technológiáknak a biztonságos használatát, hogy a támadók nehezen tudják ellopni az identitásunkat.

Az identitás és az autentikáció koncepciói

Az évszázadok során az autentikáció számos formáját fejlesztették ki. A szeszfőzdékben (az alkohol illegális árusítóhelyei, amelyek a szesztilalom idején léteztek az Egyesült Államokban) az emberek a személyzet által ismert jelszó (a híres “Joe sent me”) kimondásával hitelesítették magukat, és így nyertek bebocsátást. A jelszavak — vagy általánosabban a *titkos kulcsok* — ma már a számítógépes hitelesítés központi elemei.

A biztonsági szakértők a hitelesítési típusokat néhány kategóriába sorolják: “valami amit tudsz” (something you know — egy jelszó), “valami, amivel rendelkezel” (something you have — személyi igazolvány, bankkártya) és “valami, ami vagy” (something you are — ujjlenyomat, retinascan).

A személyazonosság és a hitelesítés kritikus fontosságú a számítógépes interakciókban. Azonosítanunk kell magunkat és hitelesítenünk kell magunkat az iskolákban, vállalkozásokban, bankokban, kiskereskedőknél, kormányhivatalokban, közösségi média fiókokban és még sok más helyen.

A hitelesítés során elkövetett hiba súlyos következményekkel járhat. Emberek vesztették el megtakarításaikat személyazonossági csalás vagy olyan támadók által okozott csalások miatt, akik hamisan megbízható intézménynek adták ki magukat.

Az azonosítás lépései: autentikáció, authorizáció és nyilvántartás

Amikor használunk egy szolgáltatást, az identitásunk a következő alapvető módokon kerül felhasználásra.

Az *autentikáció* (authentication, hitelesítés), mint láttuk, csak azt igazolja, hogy Julie Julie, és nem George vagy Ahmed.

Az *authorizáció* (authorization, engedélyezés) a hitelesített személyazonosságot használja annak megállapítására, hogy jogosultak vagyunk-e hozzáférni valamely erőforráshoz. Például lehet, hogy jogosultak vagyunk a számítógépen lévő fájlok olvasására és írására, de a biztonsági beállítások módosítására nem.

A *nyilvántartás* (accounting, más néven *logging*, naplózás, logolás) nyilvántartást vezet arról, hogy mit csináltunk, így a rendszergazda ellenőrizheti, hogy történt-e gyanús dolog a múltban. Ha például úgy tűnik, hogy adatokat loptak, a rendszergazdát érdekelheti, hogy az egyik alkalmazottról naplózásra került, hogy hajnali 3-kor lépett be a rendszerbe. Ez a bejelentkezés akár egy rosszindulatú behatoló is lehetett, aki ellopta a munkatárs hitelesítő adatait.

Jelszóbiztonság

A jelszavak központi szerepet játszanak a számítástechnikai identitás és biztonság szempontjából. Bár sok szó esik a jelszavak alternatíváiról, ezek az alternatívák még mindig ugyanazon a “valami, amit tudsz” koncepción alapulnak, és egy nehezen kitalálható szöveges karakterlánc kiválasztását igénylik.

Ha fizikai azonosítókat és biometrikus azonosítókat használnak, akkor azokat általában jelszóval vagy valamilyen más biztonságos kulccsal együtt használják.

Jó jelszó választás

Kevés internetfelhasználó tart jó jelszóbiztonságot. Ebben a részben a jelszavak biztonságára vonatkozó irányelveket tekintjük át, majd később rátérünk azokra az eszközökre, amelyek segíthetnek nekünk.

Amikor regisztrálunk egy online fiókra, a jó jelszó kiválasztásához általában kapunk néhány iránymutatást, például egy minimális (és néha maximális) hosszúságot, valamint egy szabályt, hogy a szöveget nagybetűk, számjegyek és írásjelek használatával variáljuk (néha korlátozott számú karakterek közül választhatunk).

A komplexitás fontos, de a hosszúság még fontosabb. Ennek oka, hogy a támadók gyakran úgy találják ki a jelszavakat, hogy véletlenszerű karakterkombinációkat próbálnak ki, ezt a módszert nevezik *brute force támadásnak* (nyers erő). Ha tehát összetett, de rövid jelszavunk van, mint például a `H*z-6d`, egy brute force támadás véletlenszerűen próbálkozhat ezzel a hat karakterből álló kombinációval a bejelentkezési kísérletek során.

Ha olyan hosszú jelszót szeretnénk választani, amelyet könnyen be tudunk gépelni, kezdjük egy véletlenszerű, megjegyezhető szavakból álló jelszósor kialakításával. Például kezdhetjük azzal, hogy “ruha vacsora alma kutya okos”, majd keverjünk bele speciális karaktereket, hogy a jelszó `ruha\vacsora5alma(kutya,okos` legyen.

Ha sikerül egy nehéz jelszót választani, vajon ki tudja-e találni egy behatoló? Erre mindig van egy kis esély. Valaki láthatja, ahogy beírjuk a jelszót, és kitalálhat néhány karaktert. Rosszindulatú szoftverek kerülhetnek a számítógépünkre, és megfigyelhetik a billentyűleütéseket. Egy webhely, ahová bejelentkezünk, esetleg nem biztonságos módon tárolja a jelszót, és így feltörhetik.

Ezért használjunk különböző jelszavakat minden webhelyen, ahová bejelentkezünk. A támadók sok népszerű internetes szolgáltatásnál a felhasználónév és a jelszó kombinációját próbálják ki a *credential stuffing* nevű eljárás során. Ez gyakran azért működik, mert sokan ugyanazt a jelszót használják több webhelyen is. Ha egyedi jelszavakat használunk, akkor egy támadó, aki megszerzi a közösségi oldalunkhoz tartozó jelszót, megzavarhatja a azt, de legalább a bankszámlánkhoz nem

juthat hozzá.

Jó ötlet, ha körülbelül évente megváltoztatjuk a jelszavainkat. Egyes webhelyek megkövetelik a jelszó gyakori megváltoztatását. Ne próbálkozzunk trükkökkel, például két jelszó váltogatásával: Minden alkalommal használjunk újat! Mindenképpen változtassuk meg a jelszót, ha hallottuk, hogy az adott szolgáltatás adatszivárgás áldozata lett.

Soha ne osszuk meg a jelszót senkivel! Semmi okunk nincs arra, hogy egy munkáltató, egy rendszergazda vagy egy véletlenszerűen felhívó, magát a bankunk képviselőjének kiadó személy ismerje a jelszavunkat!

A jelszavakat soha nem szabad titkosítatlan csatornákon, például e-mailben vagy sms-ben elküldeni! Mint láttuk, a jelszavakat egyáltalán nem kell megosztani!

Biztonsági kérdések és fiók-visszaállítási eszközök

A jelszó mellett a szolgáltatások gyakran személyes kérdéseket is feltesznek, például “Hol születtél?”, és tárolják a válaszokat. Ezeket a biztonsági kérdéseket néha arra használják, hogy a felhasználónév és a jelszó megadásakor további ellenőrzéseket végezzenek. Ha kizár minket az oldal, és elfelejtettük a jelszavunkat, keressünk a bejelentkezési képernyőn egy olyan linket, mint például az “Elfelejtett a jelszó?”. Ez a link egy olyan oldalra vezet, amelyen a korábban megválaszolt biztonsági kérdések szerepelnek.

Miután pontosan válaszoltunk a kérdésekre, a szolgáltatás általában még egy lépést kér a további biztonság érdekében: Egyszeri használatra egy speciális linket küld az e-mail címünkre. Ezt a linket használva kell bejelentkeznünk egy meghatározott időn belül. Ott visszaállíthatjuk a jelszavunkat. Ez a plusz lépés biztosítja, hogy még ha egy rosszindulatú behatolónak sikerül is helyesen megválaszolnia a biztonsági kérdéseket, nem tud betörni a szolgáltatásba, hacsak nem fér hozzá az e-mail címünkhöz is.

A biztonsági kérdésekkel az a probléma, hogy valaki kitalálhatja a válaszokat. Egy támadónak valószínűleg nem nehéz kitalálni, hogy hol születünk. Még egy homályosabb tényt, például a “Milyen volt az első autód?” kérdésre is tudhatja valaki a választ.

Ezért a legjobb, ha kitalált válaszokat adunk meg a biztonsági kérdésekre, és ezeket észben tartjuk.

Jelszókezelők

Felvázoltunk néhány részletes jelszókezelési szabályt. Szerencsére rendelkezésünkre állnak olyan eszközök, amelyek segítik ezt a folyamatot.

Sokan papíralapú listát vezetnek a jelszavakról, és bizonyos körülmények között ez ésszerű módja a jelszavak kezelésének. Ha otthonról dolgozunk, és senki sem megy be az irodánkba, a papíron vezetett lista biztonságos lehet. (Egy tolvaj azonban ezt is megtalálhatja.)

Ha pedig papíralapú listánk van, akkor is minden egyes jelszót be kell gépelnünk, ami nehézkes és hibalehetőségekkel jár. Sok webhely néhány bejelentkezési kísérlet után kizár minket, hogy meghiúsítsa a brute force támadásokat. A papíralapú lista tehát sosem ideális.

A számítógépen lévő, egyszerű szöveges (plain-text) lista még kevésbé biztonságos, mivel a rosszindulatú programok telepíthetnek egy olyan eszközt, amely megtalálja a listát.

A legnagyobb biztonság érdekében ezért használjunk *jelszókezelőt* (password manager). Ez a program futhat akár a saját számítógépünkön (asztali számítógép, laptop vagy mobileszköz), akár a felhőben. Kezdjük azzal, hogy a jelszókezelőbe minden egyes használt szolgáltatás vagy program releváns bejelentkezési adatait beírja: az e-mail címünket vagy felhasználónevünket, a jelszavunkat és a biztonsági kérdésekre adott válaszainkat.

A jelszókezelő titkosítja a bejelentkezési adatokat, így egy behatoló nem tudja felhasználni azokat, ha az adatfájlt ellopják. Ha a jelszókezelő a felhőben fut, akkor titkosítást használ az adatoknak a számítógép és a felhőben lévő szerver közötti továbbítása során is.

Csak egy jelszót kell megjegyeznünk, az úgynevezett *mesterjelszót* (master password), amely a jelszókezelőbe való belépéshez szükséges. Ezután utasíthatjuk a jelszókezelőt, hogy jelentkezzen be az összes ott tárolt programba és szolgáltatásba. A jelszavak megváltoztatása is egyszerű.

Vannak kompromisszumok a számítógépen lévő *offline jelszókezelő* és a *felhőalapú jelszókezelő* használata között. Nem használhatjuk a helyi jelszókezelőt, ha be szeretnénk jelentkezni egy családtag vagy barát számítógépére, ha a saját rendszerünk leáll, vagy ha meglátogatunk valakit. A felhőalapú jelszókezelő mindenhol elérhető, és egyértelműen hasznos, amikor úton vagyunk.

Az offline jelszókezelők a jelszóadatokat helyben, a felhasználó eszközén tárolják, ami magasabb szintű biztonságot nyújt, mivel az adatok nem a felhőben tárolódnak, és nincsenek kitéve az online támadásoknak. Ez a típusú jelszókezelő ideális azon felhasználók számára, akik a biztonságot részesítik a kényelemmel szemben előnyben, és nincs szükségük arra, hogy jelszavaikhoz több eszközön keresztül is hozzáférjenek. Az offline jelszókezelők, mint például a *KeePass2*, robusztus biztonsági funkciókat kínálnak, beleértve a helyi titkosítást és a jelszavak internetkapcsolat nélküli kezelésének lehetőségét. A fő hátrány, hogy a felhasználóknak kell gondoskodniuk az adataik biztonsági mentéséről, és kevésbé találhatják kényelmesnek a jelszavak kézi szinkronizálását az eszközök között.

Az online jelszókezelők a jelszóadatokat titkosítva tárolják a felhőben, így a felhasználók bármilyen, internetre csatlakoztatott eszközről hozzáférhetnek jelszavaikhoz. Ez a szinkronizálási

funkció különösen hasznos azoknak a felhasználóknak, akiknek több eszközön, például okostelefonokon, táblagépeken és számítógépeken keresztül kell hozzáférniük jelszavaikhoz. Népszerű példák erre a LastPass, az 1Password és a Dashlane. A jelszavak felhőben való tárolása azonban bizonyos biztonsági kockázatokat rejt magában, mivel potenciálisan hozzáférhetnek az adatokhoz, ha a szolgáltatás veszélybe kerül. Maga a felhőalapú jelszókezelő is leállhat, vagy elveszítheti az internet-hozzáférést. A vállalkozás emelheti az árait is, megszűnhet, vagy más módon cserbenhagyhat minket.

Egyes webböngészők is rendelkeznek jelszókezelőkkel. Ezek addig kényelmesek, amíg mindig ugyanazt a böngészőt használjuk, de az egyik böngésző jelszókezelője nem érhető el egy másik böngészőből.

A KeePass2 egy népszerű, ingyenes jelszókezelő, amely minden népszerű operációs rendszeren fut. A weboldalról a rendszerek széles skálájára — Windows, macOS, GNU/Linux, népszerű mobileszközök — letölthetjük, a nyílt forráskód pedig a GNU General Public License alatt érhető el.

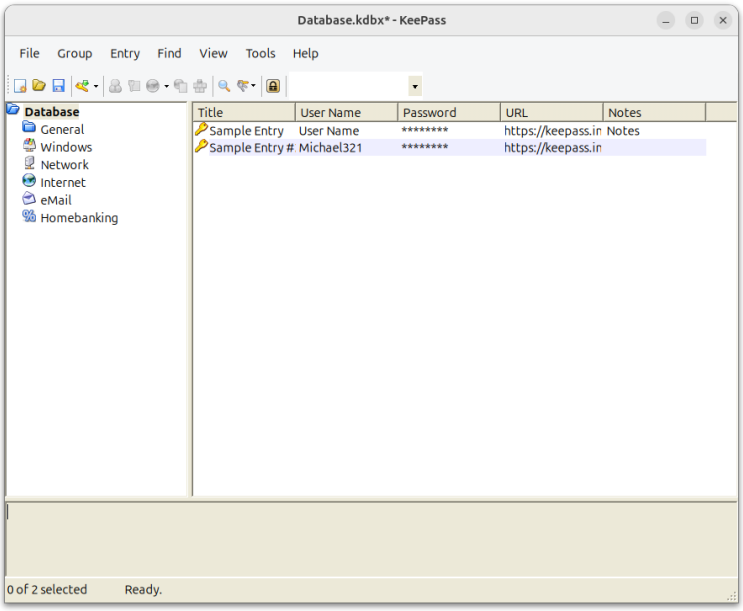

Figure 38. Keepass2 főképernyő

Single sign-on

A *Single sign-on* (egyszeri bejelentkezés, SSO) lehetővé teszi, hogy bejelentkezzünk egy szolgáltatásba, majd úgy használjunk más szolgáltatásokat, hogy azokba külön-külön be kellene jelentkeznünk. Tegyük fel például, hogy a Facebookot állandóan megnyitva tartjuk a számítógépünkön. Amikor meglátogatunk egy másik szolgáltatást, akkor megjelenhet egy párbeszédpanel, amely lehetővé teszi, hogy a Facebook-fiókunkkal jelentkezzeünk be. A Google például egy másik népszerű szolgáltatás, amelyet gyakran használnak egyszeri bejelentkezésre.

A színfalak mögött bonyolult adatcserék zajlanak az egyszeri bejelentkezés lehetővé tétele érdekében. Az alapötlet az, hogy miután rákattintunk a második szolgáltatás által megjelenített ikonra, az üzenetet küld a Facebooknak, és visszakap egy tokent (egy véletlenszerű, titkosított üzenetet), amely hitelesít minket.

Ha egyszeri bejelentkezést (SSO-t) szeretnénk használni, előfordulhat, hogy a használni kívánt szolgáltatás nem ugyanabban a böngészőben fut. Lehet, hogy például a Facebookról már kijelentkeztünk, vagy egy másik böngészőben fut. Ilyen esetben a második szolgáltatás hatására a Facebook megnyit egy párbeszédpanelt, és megkér minket, hogy jelentkezzünk be a Facebookra. Ebben az esetben az egyszeri bejelentkezés használata első alkalommal ugyanannyi gondot jelent, mint egy másik fiókkal történő bejelentkezés, de az SSO későbbi használata egyszerű lesz, mivel a Facebook továbbra is fut.

Az online jelszókezelőhöz hasonlóan az egyszeri bejelentkezési szolgáltatásra való hagyatkozás is kockázatot rejt magában: Ha elveszítjük a fiókunkhoz való hozzáférést, vagy a szolgáltatás megszűnik, elveszítjük a hozzáférést az összes többi olyan szolgáltatáshoz, amely lekérdezte a bejelentkezési adatainkat.

Továbbá, amikor egy új szolgáltatás hozzáférést kér egy másiktól, az új szolgáltatás sok olyan adatot kérhet rólunk, amely nem szükséges a bejelentkezéshez: például a tartózkodási helyet és a születési dátumot. Ha jóvá kell hagynunk az adatok átvitelét az egyik szolgáltatásból a másikba, alaposan gondoljuk át, hogy szeretnénk-e, hogy az új szolgáltatás is ismerje ezeket az adatokat.

Többfaktoros autentikáció

Egyre több internetfelhasználót kérnek arra, hogy mielőtt bejelentkezik egy szolgáltatásba, írjon be egy, a telefonjára küldött számsorozatot, vagy hajtson végre valamilyen más feladatot. A jelszavakkal kapcsolatos kockázatok kiküszöbölése érdekében a szolgáltatások két vagy többféle azonosítást igényelnek, amit *többfaktoros autentikációnak* (multi-factor authentication — MFA) neveznek. A korábban leírt forgatókönyv, amikor a jelszót úgy állítjuk vissza, hogy küldenek az e-mail címünkre egy linket, az MFA egy másik formája. Ezek az eljárások megakadályozzák, hogy valaki a világ másik végéről, vagy akár a szomszédos irodából is megszemélyesítsen minket.

Az MFA minden formája extra erőfeszítést igényel a felhasználó részéről (mivel két vagy többféle módon kell azonosítanunk magunkat), de megéri a fáradságot, mert kiküszöböl számos gyakori támadást. Ma már szinte minden számítógép-felhasználónak van mobiltelefonja, így ésszerű azt MFA-ra használni. Sok szolgáltatás képes a kódot a telefon helyett az e-mail címre küldeni, így a kódot az asztali számítógépünkről vagy laptopunkról is használhatjuk.

A legtöbb MFA jelszót és egy másik faktort kér, ezért nevezhetjük *kétfaktoros hitelesítésnek* (two-factor authentication — 2FA).

Az MFA számos más formája már egy ideje használatban van. A bankkártya egy négyjegyű PIN-kóddal kombinálva egyszerű és hatékony módja annak, hogy bankunk azonosítson minket, bárhol is járjunk a világban. Sok ATM-ben kamera is található, így csalárd pénzfelvétel esetén az ügyintéző láthatja, hogy ki volt az elkövető.

Vannak olyan speciális eszközök, amelyek a munkahelyi számítógépekhez csatlakoztathatók, és lehetővé teszik a hitelesítést egy olyan csíkkal ellátott kártya felmutatásával, mint amilyen a bankautomaták esetében is van.

Az *egyszeri jelszavakat* (one-time password) jóval a digitális számítástechnika előtt fejlesztették ki. Azok az emberek, akik telefonon vagy rádión keresztül akarták igazolni magukat, egy "egyszer használatos jegyzettömböt" (one-time pad) vittek magukkal, amelynek minden egyes lapján egy véletlenszerű kód szerepelt. Az egyik személy kimondta a kódot, a másik hitelesítette azt, majd mindketten letépték a lapot.

A számítástechnikában futtathatunk egy olyan programot vagy eszközt, amely egyszeri jelszót generál, és ezzel hitelesíthetjük magunkat.

Az autentikáció egyik kapcsolódó fajtája az *időalapú egyszeri jelszó* (time-based one-time password — TOTP). Ez a szolgáltatás körülbelül 30 másodpercenként generál egy véletlenszerű kódot. Amikor be akarunk jelentkezni a munkahelyünkre vagy más szolgáltatásba, megnyomhatunk egy gombot a szolgáltatásban a kód generálásához, és beírhatja ezt a kódot, amikor szolgáltatás, ahova be szeretnénk jelentkezni, kéri. A szerver ezzel egyidejűleg ugyanezt a kódot generálja a szolgáltatásból. Ha a kódok egyeznek, akkor bejelentkezhetünk.

Sok mobileszközön már ujjlenyomattal is be lehet jelentkezni. Az ezekben az eszközökben található ujjlenyomat-olvasók csak részben pontosak, és az ujjlenyomatok sem teljesen egyediek. Ezért a legjobb, ha az ujjlenyomatot jelszóval vagy más hitelesítési formával együtt használjuk.

Bár az MFA fárasztó lehet, ajánlott minden programhoz és szolgáltatáshoz használni, amelyhez hozzáférünk. Valószínűleg naponta úgyis csak néhányszor jelentkezünk be a szolgáltatásokba. Egy *autentikátor alkalmazás* (authenticator app) telepítésével beállíthatjük az MFA használatát a szolgáltatásainkhoz, ezzel pedig számos támadást megállíthatunk.

Jelszavak védelme online szolgáltatások esetén

Megbeszéltük, hogyan kell biztonságosan kezelni a jelszavakat. De mi a helyzet a szerverrel? Annak fel kell ismernie a jelszavunkat. Ha azonban a felhasználók és jelszavak adatbázisát tárolja, akkor rendkívül sebezhető a rosszindulatú behatolással szemben.

A jelszó védelmének két fő módja a *hashing* (hashelés) és a *salting* (sózás). Ezek a technikák már évtizedek óta ismertek, és minden szervernek ezeket kellene használnia.

A titkosítás azt jelenti, hogy a jelszó karaktereit valamilyen egyszerű matematikai függvényen futtatjuk le, amely gyakran összeadásból, szorzásból és osztásból áll. A jó hash egy véletlenszerű karakterekből álló, rögzített hosszúságú karakterláncot eredményez. Mivel a hashelés során információ vész el, senki sem tudja rekonstruálni az eredeti jelszót a hashből.

Amikor bejelentkezünk, és beírjuk a jelszót, a szerver hasheli azt, és ellenőrzi, hogy az eredmény megegyezik-e az adatbázisban lévővel.

Az elszánt és jól finanszírozott támadók megtalálták a módját a hashek megtámadásának: Hatalmas adatbázist hoznak létre a karakterláncokból és a hozzájuk tartozó hashekből (amiből azt feltételezhetjük, hogy meg tudják határozni, milyen hash-funkció van használatban). Ezt az adatbázist *szivárványtáblának* (rainbow table) nevezik. Ha a támadó betör egy szerverre, és megszerzi a hasheket, minden egyes hasht megnéz a szivárványtáblában, és kipróbálja a különböző olyan karakterláncokat, amelyek egyeznek.

Ezért a hashinget ki kell egészíteni a sózással (salting). Ez azt jelenti, hogy a felhasználó jelszavához egy rövid, egyedi stringet — úgynevezett *salt* vagy *nonce* — adunk hozzá. Ezután a jelszó és a só kombinációja hashelésre kerül.

E-mail fiókok és az IT biztonság

Az e-mail fiókok gyakran a digitális identitásunk kapuját jelentik, és központi csomópontként szolgálnak a különböző online szolgáltatásokhoz való hozzáférés kezeléséhez, beleértve a közösségi médiát, az e-kereskedelmet, a banki szolgáltatásokat és még a munkával kapcsolatos platformokat is. Emiatt az e-mail fiókok védelme az informatikai biztonság egyik legkritikusabb szempontja. Egy kompromitált e-mail fiók biztonsági rések sorozatához vezethet, mivel a támadók azt jelszavak visszaállítására és más kapcsolódó szolgáltatásokhoz való jogosulatlan hozzáférés megszerzésére használhatják.

Az e-mail fiókok védelméhez elengedhetetlen az erős biztonsági intézkedések bevezetése. Az egyik leghatékonyabb stratégia a többfaktoros hitelesítés alkalmazása.

Az e-mail fiók tevékenységének rendszeres monitorozása szintén fontos gyakorlat. Figyeljünk a szokatlan bejelentkezési kísérletekre vagy a beállítások megváltoztatására, például olyan továbbítási szabályokra, amelyeket nem mi állítottunk be. Ezek arra utalhatnak, hogy valaki illetéktelenül próbál hozzáférni a fiókunkhoz.

Személyes fiókok monitorozása

A személyes fiókok jelszószivárgás elleni monitorozása alapvető fontosságú a digitális biztonság fenntartásában és az online identitás védelmében. Jelszószivárgás akkor történik, amikor a

hackerek jogosulatlanul hozzáférnek a felhasználói hitelesítő adatokat tartalmazó adatbázisokhoz, amelyeket aztán nyilvánosságra hozhatnak vagy eladhatnak a darkweben.

A jelszó kiszivárgásával kapcsolatos kockázatok csökkentése érdekében elengedhetetlen, hogy proaktívan figyeljük a kompromittálódás jeleit a fiókjainkban. Az egyik hatékony módszer a keresőmotorok figyelmeztetéseinek beállítása a felhasználónevekre vagy e-mail címekre.

Emellett a jelszószivárgás-ellenőrzők felbecsülhetetlen értékűek a kompromittált hitelesítő adatok azonosításában. Az olyan webhelyek és szolgáltatások, mint a *Have I Been Pwned* és a *Google's Password Checkup* képesek az e-mail címünket vagy jelszavunkat az ismert jogsértések adatbázisai alapján átvizsgálni, hogy megállapítsák, kiszivárogtak-e az adataink.

Ha értesítést kapunk arról, hogy a jelszavunk kompromittálódott, fontos, hogy gyorsan cselekedjünk. Azonnal változtassuk meg jelszavunkat az érintett webhelyen és mindenhol, ahol ugyanazt a jelszót használtuk.

A modern webböngészők, például a Google Chrome, a Firefox és a Safari beépített biztonsági funkciókkal rendelkeznek, amelyek figyelmeztetik a felhasználókat, ha jelszavaikat egy adatvédelmi incidens során veszélyeztetik. Ezek a böngészők képesek felismerni, ha az elmentett jelszavak már nem biztonságosak, és értesítik a felhasználókat arról, hogy mely fiókok érintettek, így ösztönözve őket, hogy tegyenek lépéseket az adataik védelme érdekében.

Ha a böngésző beépített jelszókezelőjét használjuk, az biztonságosan tárolja a különböző weboldalak bejelentkezési adatait. Ha a tárolt jelszavak bármelyike egyezik egy ismert adatvédelmi incidenssel, a böngésző biztonsági figyelmeztetést jelenít meg.

Az online banki szolgáltatások és hitelkártyák biztonsági szempontjai

Az online bankolás és a hitelkártyák használata kényelmet és elérhetőséget biztosít a felhasználók számára, hogy bárhonnan kezelhessék pénzügyeiket. Ez a kényelem azonban jelentős biztonsági kockázatokkal jár, mivel ezek a szolgáltatások elsődleges célpontjai a személyes adatok és pénzügyi eszközök ellopására törekvő kiberbűnözőknek.

Az online banki biztonság egyik alapja a biztonságos kapcsolat használata, amelyet jellemzően a `https://` kezdetű URL-cím és a böngésző címsorában megjelenő lakat ikon jelez. A személyes adatok megadása előtt mindig győződjünk meg arról, hogy a bank legitim weboldalán vagyunk. Az adathalász-támadások, amelyek során a csalárd weboldalak legitim weboldalakat utánoznak, gyakori fenyegetést jelentenek. Egy másik kritikus biztonsági szempont a többfaktoros hitelesítés (MFA), amelyet a legtöbb bank ma már megkövetel vagy opcionálisan kínál.

Kerüljük a nyilvános vagy megosztott számítógépek használatát, mivel ezek olyan rosszindulatú szoftverekkel lehetnek fertőzöttek, amelyek rögzíthetik a billentyűleütéseket vagy ellophatják a bejelentkezési adatokat. Hasonlóképpen, a nyilvános Wi-Fi hálózatok gyakran nem biztonságosak, és a támadók felhasználhatják őket adataink lehallgatására. Ha muszáj nyilvános Wi-Fi-t használnunk, fontoljuk meg egy virtuális magánhálózat (VPN) használatát a kapcsolat titkosítása és az adatok védelme érdekében.

Gyakorló feladatok

1. Miért fontos, hogy egy jelszó hosszú legyen?

2. Mit tegyünk, ha valaki a Microsofttól telefonál, és elkéri a jelszavunk, hogy kijavíthasson egy biztonsági problémát a Windows rendszerünkön?

3. Milyen előnyei vannak egy jelszókezelő használatának?

 | |

Gondolkodtató feladatok

1. A kórházakban a klinikusok általában egyik emeletről a másikra járnak, és gyakran be kell jelentkezniük, hogy ellenőrizzék a betegeket és beírják a feljegyzéseiket. Milyen hitelesítési formát lenne jó használni egy kórházban?

2. Egyes szakemberek a közösségi médiában a posztolást egy olyan szolgáltatásra bízzák, amely a tervezett időpontokban közzéteszi a bejegyzéseket. Ki kell adnunk a jelszavunkat ennek a szolgáltatásnak, és lehetővé kell tennünk, hogy a szolgáltatás teljes hozzáférést kapjon a fiókunkhoz?

Összefoglalás

Ez a lecke az identitás igazolásának módjait mutatja be, hogy biztonságosan hozzáférhessünk az interneten keresztül elérhető erőforrásokhoz. A lecke tárgyalja a jelszavak védelmét, amelyeket mind nekünk, mind a felhasználónak, mind pedig a bejelentkező szervernek használnia kell. Bemutatásra kerülnek a többfaktoros hitelesítés különböző típusai, valamint a jelszókezelők és az egyszeri bejelentkezés.

Válaszok a gyakorló feladatokra

1. Miért fontos, hogy egy jelszó hosszú legyen?

   A hosszú jelszavak (20 karakter, ideális esetben még több) a leginkább ellenállóak a brute force támadásoknak.

2. Mit tegyünk, ha valaki a Microsofttól telefonál, és elkéri a jelszavunk, hogy kijavíthasson egy biztonsági problémát a Windows rendszerünkön?

   Szakítsuk meg a hívást. Gyakoriak a magukat Microsoftnak kiadó csalók. De bárki, aki a jelszavunkat kéri, csaló. Hasznos lehet, ha felhívjuk a vállalatot, amelyet állítólag képvisel, és figyelmeztetjük őket, hogy valaki át akarja verni az ügyfeleiket.

3. Milyen előnyei vannak egy jelszókezelő használatának?

   Jelszavaink biztonságos, titkosított módon kerülnek tárolásra, így nem kell azokat egyszerű szövegként tárolnunk. Nekünk csak a mesterjelszót kell megjegyeznünk. Hosszú, összetett jelszavakat hozhatunk létre anélkül, hogy megpróbálnánk begépelni őket.

Válaszok a gondolkodtató feladatokra

1. A kórházakban a klinikusok általában egyik emeletről a másikra járnak, és gyakran be kell jelentkezniük, hogy ellenőrizzék a betegeket és beírják a feljegyzéseiket. Milyen hitelesítési formát lenne jó használni egy kórházban?

   A kártyaolvasók jó megoldást jelentenek egy ilyen környezetben. Minden klinikus visel egy kártyát (jelvényt), amelyen egy olyan csík van, ami tartalmazza az azonosító adatokat. Minden nővérállomáson van egy számítógép egy kártyaolvasóval. Az elektronikus nyilvántartásokhoz való hozzáféréshez minden orvos vagy nővér a kártyáját a kártyaolvasó elé tartja, és esetleg egy jelszót is megad a kétfaktoros hitelesítéshez. Ha kijelentkezés nélkül távoznak, a fiók bizonyos idő elteltével automatikusan kijelentkezik.

2. Egyes szakemberek a közösségi médiában a posztolást egy olyan szolgáltatásra bízzák, amely a tervezett időpontokban közzéteszi a bejegyzéseket. Ki kell adnunk a jelszavunkat ennek a szolgáltatásnak, és lehetővé kell tennünk, hogy a szolgáltatás teljes hozzáférést kapjon a fiókunkhoz?

   Nem. Ezeknek a szolgáltatásoknak nagyon korlátozott hozzáférésük van a fiókunkhoz. A szolgáltatás a közösségi média alkalmazásprogramozási felületét (API) használja a bejegyzések közzétételéhez. A szolgáltatásnak saját API-jelszava van, így bármikor visszavonhatjuk a hozzáférést. A szolgáltatás számára engedélyezett műveletek is korlátozottak lehetnek.

025.2 Információk bizalmas kezelése és biztonságos kommunikáció

Hivatkozás az LPI célkitűzésre

Security Essentials version 1.0, Exam 020, Objective 025.2

Súlyozás

2

Kulcsfontosságú ismeretek

- Az adatszivárgás és a lehallgatott kommunikáció következményeinek és kockázatainak megértése
- Az adathalászat, a social engineering és a scam megértése
- Az e-mail spamszűrők fogalmainak megértése
- A kapott e-mail mellékletek biztonságos kezelése
- Az információk biztonságos és felelősségteljes megosztása az e-mail felhőmegosztó és üzenetküldő szolgáltatások használatával
- Titkosított azonnali üzenetküldés használata

A használt fájlok, kifejezések és segédprogramok részleges listája

- Adathalászat és social engineering
- Személyazonosság-lopás
- Scamming és scareware
- E-mail spam, e-mail spam-szűrés
- Titoktartási megállapodások (NDA)
- Információosztályozás

Linux Professional Institute

Lesson 1

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	025 Identitás és magánélet
Fejezet:	025.2 Információk bizalmas kezelése és biztonságos kommunikáció
Lecke:	1/1

Bevezetés

A mai összekapcsolt világban, ahol az érzékeny adatokat gyakran osztják meg online, fontos tudni, hogyan lehet megőrizni a digitális kommunikáció titkosságát. Ez magában foglalja a személyes és szakmai információk védelmét, valamint az olyan fenyegetések felismerését, mint az adathalászat (phishing) és a social engineering, amelyek az emberi pszichológiát használják ki az érzékeny adatokhoz való hozzáférés megszerzésére. Ezeknek a kísérleteknek az azonosítása kulcsfontosságú a jogosulatlan hozzáférés megakadályozásához. Az adatszivárgás és a lehallgatott kommunikáció pénzügyi veszteséghez, a jó hírnév sérüléséhez és jogi problémákhoz vezethet. Ez a lecke az adatszivárgás hatásait, a titoktartási megállapodások (non-disclosure agreement — NDA) fontosságát és az információosztályozás szerepét tárgyalja a bizalmas adatok védelmében.

Adatszivárgás és lehallgatott kommunikáció

Az adatszivárgás (data leak) akkor következik be, amikor érzékeny információk kerülnek nyilvánosságra, akár véletlenül, akár rosszindulatú szándékkal. Ez történhet nem megfelelő biztonsági intézkedések, emberi hiba vagy kiberbűnözők szándékos támadásai miatt. Az

adatszivárgás következményei pusztítóak lehetnek. A vállalkozások számára a kiszivárgott védett információk versenyelőny elvesztését, szellemi tulajdon ellopását és pénzügyi szankciókat eredményezhetnek. A magánszemélyek esetében a személyes adatok, például a társadalombiztosítási számok vagy a hitelkártyaadatok kiszivárgása személyazonosság-lopáshoz és csaláshoz vezethet.

Ezen túlmenően a vállalatoknak jogi következményekkel kell szembenézniük, ha nem felelnek meg az adatvédelmi szabályoknak, mint például az európai *általános adatvédelmi rendelet* (General Data Protection Regulation — GDPR) vagy az Egyesült Államokban a *kaliforniai fogyasztóvédelmi törvény* (California Consumer Privacy Act — CCPA). A megfelelés elmulasztásáért kiszabott bírságok és szankciók jelentősek lehetnek, ami tovább súlyosbítja az adatvédelmi incidensek hatásait.

A lehallgatott kommunikáció hasonló fenyegetést jelent. Ha az érzékeny információkat nem biztonságos csatornákon keresztül továbbítják, azokat illetéktelen felek lehallgathatják. Ez különösen veszélyes üzleti környezetben, ahol a stratégiákról, pénzügyi tervekről vagy termékfejlesztésről folytatott bizalmas megbeszéléseket kihasználhatják a versenytársak vagy rosszindulatú szereplők.

A phishing és social engineering

A *phishing* és a *social engineering* olyan megtévesztő taktikák, amelyeket a kiberbűnözők arra használnak, hogy manipulálják az egyéneket, hogy bizalmas információkat adjanak ki, vagy olyan műveleteket hajtsanak végre, amelyek veszélyeztetik a biztonságot. Ezek a támadások gyakran inkább az emberi pszichológiát használják ki, mint a technikai sebezhetőségeket, ami megnehezíti a felderítésüket és az ellenük való védekezést. A phishing jellemzően csalárd e-maileket, szöveges üzeneteket vagy legitimnek tűnő weboldalakat jelent, amelyekkel az áldozatokat érzékeny információk, például felhasználónevek, jelszavak vagy hitelkártyaadatok felfedésére csábítják. Egy e-mail például úgy tűnhet, hogy megbízható forrásból, például egy bankból vagy online szolgáltatásból érkezik, és arra kéri a címzettet, hogy kattintson egy linkre a számlainformációk frissítéséhez. Miután az áldozat megadja a hitelesítő adatait a hamis webhelyen, a támadó megszerzi ezeket az adatokat, és rosszindulatú célokra használja fel.

A social engineering viszont az adathalászaton túli taktikák szélesebb körét foglalja magában. Ez az egyének manipulálását jelenti, hogy megszegjék a szokásos biztonsági eljárásokat, gyakran úgy, hogy megbízható vagy hivatalos személynek adják ki magukat. Gyakori példa erre a magát az informatikai részlegnek kiadó támadó telefonhívása, aki arra kéri a célpontot, hogy adja meg a bejelentkezési adatokat “egy technikai probléma megoldásához”.

Személyazonosság-lopás

Személyazonosság-lopásról (identity theft) akkor beszélünk, amikor egy támadó jogosulatlanul hozzáfér valakinek a személyes adataihoz, és azt arra használja fel, hogy az áldozatnak adja ki magát, gyakran csalás vagy más bűncselekmények elkövetésére. Ez magában foglalhatja személyes adatok, például társadalombiztosítási számok, hitelkártyaadatok vagy online fiókok hitelesítő adatainak ellopását. Ha ezek az információk a birtokukban vannak, a támadók új hitelszámlát nyithatnak, jogosulatlanul vásárolhatnak, vagy akár egészségügyi és kormányzati szolgáltatásokhoz is hozzáférhetnek az áldozat nevében.

A személyazonosság-lopás kezdeti lépései gyakran a phishing és a social engineering, mivel ezeket a technikákat arra használják, hogy összegyűjtsék az áldozat személyazonosságának megszemélyesítéséhez szükséges személyes adatokat.

A személyazonossággal való visszaélés megelőzése az éberség és a proaktív biztonsági intézkedések kombinációját igényli. A magánszemélyeknek erős, egyedi jelszavakat kell használniuk minden egyes fiókjukhoz, és amikor csak lehetséges, engedélyezniük kell a többfaktoros hitelesítést. A bankszámlakivonatok, hiteljelentések és a számlaforgalom rendszeres figyelemmel kísérése szintén segíthet a jogosulatlan tranzakciók vagy változások korai szakaszban történő felismerésében.

Scamming és scareware

A scamming (csalás) és a scareware a kiberbűnözők által alkalmazott rosszindulatú taktikák, amelyek célja az egyének megtévesztése és félelmeik kihasználása, ami gyakran pénzügyi veszteséghez vagy személyes adatok veszélyeztetéséhez vezet. Az ilyen típusú támadások inkább a manipulációra és a félelemre támaszkodnak, mint technikai hacking módszerekre, ami megnehezíti a felismerésüket és a kivédésüket.

A *scamming* a csalások széles skáláját jelenti, amelyek célja, hogy az egyéneket pénz, személyes adatok vagy érzékeny számlákhoz való hozzáférés átadására rávegyék. A csalók gyakran törvényes szervezeteknek, például bankoknak, kormányzati szerveknek vagy ismert vállalatoknak adják ki magukat, hogy elnyerjék az áldozat bizalmát. Az egyik leggyakoribb példa a “tech support scam”, amikor a csaló azzal az állítással lép kapcsolatba az áldozattal, hogy a számítógépét vírus fertőzte meg. A csaló ezután felajánlja, hogy díj ellenében orvosolja a problémát, vagy arra kéri az áldozatot, hogy töltsön le egy olyan szoftvert, amely távoli hozzáférést biztosít a csalónak az eszközhöz. Ha megvan a hozzáférés, ellophatnak érzékeny információkat, vagy fizetést követelhetnek olyan szolgáltatásokért, amelyekre soha nem volt szükség.

A *scareware* a malware egy speciális típusa, amely a félelemre építve manipulálja az áldozatokat,

hogy bizonyos lépéseket tegyenek. Általában felugró üzenetek vagy figyelmeztetések formájában jelenik meg a felhasználó számítógépén vagy okostelefonján, amelyek tévesen figyelmeztetnek arra, hogy az eszköz vírussal fertőzött, vagy, hogy az adatai veszélyben vannak. A scareware üzenet úgy tűnhet, hogy egy legitim vírusirtó cégtől vagy biztonsági szolgálattól származik, és arra ösztönzi a felhasználót, hogy töltsön le egy szoftvert vagy vásárolja meg egy termék "teljes verzióját" a nem létező probléma megoldása érdekében. A valóságban a javasolt szoftver letöltése a tényleges rosszindulatú szoftverek, kémprogramok vagy zsarolóprogramok telepítéséhez vezethet, ami tovább veszélyezteti a felhasználó eszközét és személyes adatait.

Az ilyen típusú támadások elleni védekezés érdekében fontos, hogy szkeptikusak maradjunk a kéretlen ajánlatokkal, figyelmeztetésekkel és fizetési vagy személyes adatok kérésével szemben.

Titoktartási megállapodások (NDA-k)

A *titoktartási megállapodások* (non-disclosure agreement — NDA) olyan jogi szerződések, amelyek a felek között megosztott bizalmas információkat védik. Ezeket általában üzleti környezetben használják, hogy megakadályozzák az érzékeny adatok, például üzleti titkok, üzleti tervek vagy védett technológia jogosulatlan nyilvánosságra hozatalát. Az NDA általában meghatározza a bizalmas információk körét, az érintett felek kötelezettségeit és a megállapodás megszegésének következményeit.

A titoktartási megállapodások döntő szerepet játszanak az információk bizalmas kezelésében, amikor harmadik felekkel — például vállalkozókkal, tanácsadókkal vagy potenciális üzleti partnerekkel — történik együttműködés. Az NDA aláírásával ezek a felek vállalják, hogy az üzleti kapcsolat során a rendelkezésükre bocsátott információkat nem hozzák nyilvánosságra, illetve nem élnek vissza velük. Ez a jogi védelem segít biztosítani, hogy az érzékeny adatok biztonságban maradjanak, és ne használják fel őket a vállalat kárára.

Fontos azonban felismerni, hogy az NDA-k nem bolondbiztosak. Bár jogi keretet biztosítanak az információk védelmére, nem akadályoznak meg minden lehetséges szivárgást vagy visszaélést. Az NDA betartásának biztosítása éberséget és rendszeres ellenőrzést, valamint erős belső titoktartási és adatbiztonsági kultúrát igényel.

Az információk osztályozása

Az NDA-k használata szorosan kapcsolódik az *információ osztályozásához* (information classification). Az alapos minősítési folyamat segít meghatározni, hogy mely információk elég kritikusak ahhoz, hogy NDA szerinti védelmet biztosítsanak. A szigorúan bizalmas információkat, például a védett üzleti stratégiákat vagy üzleti titkokat mindig szigorú NDA-kkal kell szabályozni a visszaélések vagy a véletlen nyilvánosságra kerülés megakadályozása érdekében.

Az információ osztályozása az adatok szisztematikus kategorizálása az érzékenységi szintjük és a jogosulatlan nyilvánosságra hozataluk lehetséges hatása alapján. Ez a folyamat segít a szervezeteknek azonosítani és megfelelő biztonsági ellenőrzések alkalmazásával védeni a legkritikusabb információs eszközeiket. Az általános minősítési szintek a következők: *publiks* (public), *belső használat* (internal), *bizalmas* (confidential) és *szigorúan bizalmas* (highly confidential).

A nyilvános információk olyan adatok, amelyek szabadon, a szervezetre vonatkozó kockázat nélkül megoszthatók, például marketinganyagok vagy sajtóközlemények. A belső információk a szervezeten belüli felhasználásra szolgálnak, de nyilvánosságra hozataluk nem jelent jelentős kockázatot. A bizalmas információk azonban kárt okozhatnak, ha nyilvánosságra kerülnek; ilyen információ például az alkalmazottak nyilvántartása, a pénzügyi kimutatások és az ügyfelek adatai. A szigorúan bizalmas információk a legérzékenyebbek, és nyilvánosságra hozataluk súlyos következményekkel járhat, ilyenek például az üzleti titkok vagy a kritikus üzleti stratégiák.

Az információk helyes osztályozása alapvető fontosságú a hatékony biztonsági intézkedések végrehajtásához. Például a szigorúan bizalmas információkat biztonságos, hozzáférés-ellenőrzött környezetben kell tárolni, és csak titkosított csatornákon keresztül szabad továbbítani. Az alkalmazottaknak képzést kell kapniuk arról, hogy hogyan kezeljék és védjék az adatokat azok minősítési szintje alapján, biztosítva, hogy az érzékeny információk véletlenül se kerüljenek nyilvánosságra.

A szervezeten belüli adatvédelem mellett az információosztályozás a jogi és szabályozási követelményeknek való megfelelés szempontjából is létfontosságú. Számos szabályozás bizonyos típusú adatok, például személyes információk vagy pénzügyi nyilvántartások esetében különleges védelmet ír elő. A megfelelő osztályozás segít a szervezeteknek megfelelni ezeknek a követelményeknek, és elkerülni a megfelelés elmulasztásáért járó esetleges büntetéseket.

Az e-mail alapú kommunikáció biztosítása

Az email *spam* a kéretlen, gyakran irreleváns vagy nem megfelelő üzeneteket jelenti, amelyeket nagyszámú címzettnek küldenek. Ezek az üzenetek jellemzően reklámokat, adathalászati kísérleteket vagy rosszindulatú tartalmakat, például malware szoftverekre mutató linkeket tartalmaznak. A spam nemcsak a postaládákat zsúfolja tele, hanem jelentős biztonsági kockázatot is jelent, mivel gyakran használják kibertámadások eszközeként.

A *spamszűrés* felismeri és blokkolja a nem kívánt vagy potenciálisan káros e-maileket, mielőtt azok eljutnának a címzett postaládájába. A spamszűrők különböző technikákat használnak a spamek azonosítására, beleértve az e-mail tartalmának elemzését, a feladó repputációjának ellenőrzését és a gépi tanulási algoritmusok használatát a spamekkel általában összefüggő minták felismerésére. Ezek a szűrők több szinten is működhetnek, beleértve az e-mail szervert, a

kliensszoftvert és a harmadik féltől származó szolgáltatásokat.

A *blacklist* és *whitelist filtering* egy másik módszer, ahol az ismert spamforrásokból vagy tartományokból érkező e-maileket reputációjuk alapján blokkoljuk, míg a megbízható küldemények átmennek a szűrőkön.

A spamszűrők kulcsfontosságúak, hogy megvédjék a felhasználókat az adathalászati kísérletektől, a malwarektől és más, e-mail alapú fenyegetésektől. Azáltal, hogy megakadályozzák, hogy a potenciálisan veszélyes üzenetek eljussanak a postaládába, csökkentik annak kockázatát, hogy a felhasználók rosszindulatú linkekre kattintsanak, fertőzött mellékleteket töltsenek le, vagy hogy social engineering támadások áldozatává váljanak.

A spamszűrők azonban nem tökéletesek. Néha előfordulhat, hogy legitim e-maileket tévesen spamnek minősítenek, ez a probléma az úgynevezett *fals pozitív* (false positive). Ezzel szemben egyes spam üzenetek elkerülhetik az észlelést, és eljuthatnak a postaládába, amit *fals negatívnak* (false negative) nevezünk. E problémák minimalizálása érdekében a felhasználók rendszeresen ellenőrizhetik a spam mappát, hogy vannak-e benne valós e-mailek, és ennek megfelelően módosíthatják a spamszűrő beállításait.

Az e-mail *mellékletek* (attachment) gyakori módja a dokumentumok, képek és egyéb fájlok megosztásának, de ha nem megfelelően kezelik őket, jelentős biztonsági kockázatot is jelentenek. A rosszindulatú mellékletek küldése a kiberbűnözők által gyakran használt módszer malwarek, zsarolóprogramok és más káros szoftverek terjesztésére.

Az egyik legfontosabb szabály az e-mail mellékletekkel kapcsolatban az óvatosság, különösen, ha az e-mail váratlan vagy ismeretlen feladótól érkezik. Még ha az e-mail látszólag ismerős forrásból érkezik is, a mellékletek megnyitása előtt feltétlenül ellenőrizni kell az üzenet legitimitását.

Mindig kerüljük a gyanús fájltípusokat tartalmazó mellékletek megnyitását! A rosszindulatú csatolmányokban használt gyakori fájlformátumok közé tartoznak az `.exe` (futtatható fájlok), `.vbs` (Visual Basic Script fájlok), `.js` (JavaScript fájlok) és `.bat` (batch fájlok). Ezek a fájltípusok potenciálisan veszélyes kódot futtathatnak a rendszerünkön.

Egy másik fontos gyakorlat a vírusirtó szoftver és az e-mail biztonsági eszközeinek frissítése. A modern vírusirtó programok alkalmasak arra, hogy átvizsgálják az e-mailek csatolmányait az ismert fenyegetések szempontjából, és ha rosszindulatú tevékenységet észlelnek, riasztanak.

Biztonságos információmegosztás

Az információk megosztása e-mailben, felhőalapú tárhelyeken és üzenetküldő szolgáltatásokon keresztül a személyes és szakmai kommunikáció rutinszerű részévé vált. Ezeknek a platformoknak a kényelme azonban biztonsági kockázatokkal is jár, különösen, ha érzékeny vagy

bizalmas adatokat kezelünk.

Ha *e-mailen* keresztül osztunk meg információkat, fontos, hogy az üzenetek tartalmának védelme érdekében használjunk titkosítást. A szabványos e-mail átvitel eredendően nem biztonságos, titkosítás nélkül illetéktelenek lehallgathatják és elolvashatják. A beépített titkosítást kínáló szolgáltatások, például a Gmail bizalmas üzemmódja, valamint az e-mail tartalmának titkosítására szolgáló, harmadik féltől származó eszközök, például a PGP (*Pretty Good Privacy*) használata segíthet megvédeni az érzékeny információkat a nyilvánosságra kerüléstől. Emellett kerüljük a bizalmas információk, például jelszavak vagy pénzügyi adatok megosztását közvetlenül az e-mailek szövegében. Ehelyett fontoljuk meg a biztonságos fájlmegosztási módszerek vagy titkosított mellékletek használatát.

A *felhőalapú tárhelyszolgáltatások*, például a Google Drive, a Dropbox vagy a Microsoft OneDrive népszerűek a dokumentumok és fájlok megosztására és közös használatára. Ha ezeket a szolgáltatásokat használjuk, gondoskodjunk arról, hogy a hozzáférési jogosultságok megfelelően legyenek beállítva a jogosulatlan hozzáférés megakadályozása érdekében.

Az *üzenetküldő szolgáltatásokat*, mint például a WhatsApp, a Signal és a Telegram, gyakran használják gyors kommunikációra és fájlmegosztásra. Számos ilyen platform kínál end-to-end titkosítást, ami biztosítja, hogy csak a feladó és a címzett tudja elolvasni az üzeneteket. Fontos azonban ellenőrizni, hogy a titkosítás engedélyezve van-e, mivel egyes szolgáltatások csak opcionális funkcióként teszik elérhetővé. A rendkívül érzékeny adatok esetében az üzenetküldő alkalmazások helyett célszerűbb lehet biztonságos e-mailt vagy titkosított felhőalapú tárhelyet használni.

Az érzékeny információk megosztása előtt mindig ellenőrizzük a címzettek identitását. A kiberbűnözők gyakran használnak social engineering taktikákat, hogy megbízható kapcsolatoknak adják ki magukat, és rávegyék az embereket bizalmas adatok megosztására.

A titkosított azonnali üzenetküldés a biztonságos és privát kommunikáció létfontosságú eszközévé vált mind személyes, mind szakmai környezetben. A hagyományos üzenetküldő szolgáltatásokkal ellentétben, amelyek lehet, hogy az üzeneteket egyszerű szövegként továbbítják, a titkosított üzenetküldés biztosítja, hogy a beszélgetések tartalma védve legyen a jogosulatlan hozzáféréstől, még akkor is, ha azt az átvitel során lehallgatják.

Az *end-to-end titkosítás* (E2EE) a biztonságos azonnali üzenetküldés sarokköve. Biztosítja, hogy csak a feladó és a címzett tudja elolvasni az üzenet tartalmát. Még a szolgáltató sem férhet hozzá az üzenetekhez, illetve nem tudja azokat visszafejteni, mivel a titkosítási kulcsokat csak a beszélgetésben részt vevő eszközökön tárolják.

Az E2EE mellett egyes üzenetküldő alkalmazások olyan funkciókat is kínálnak, mint az eltűnő üzenetek és biztonságos képernyő az adatvédelem fokozása érdekében. Az eltűnő üzenetek egy

meghatározott idő után automatikusan törlődnek, csökkentve annak kockázatát, hogy az érzékeny információk korlátlan ideig tárolódjanak a saját vagy a címzettünk készülékén.

Fontos továbbá, hogy folyamatosan frissítsük a titkosított üzenetküldő alkalmazásokat, hogy védekezzünk a biztonsági réseket és exploitokat veszélyeztető sebezhetőségek ellen. A fejlesztők rendszeresen adnak ki frissítéseket a biztonsági hibák kijavítására és a titkosítási protokollok javítására, így az alkalmazások naprakészen tartása elengedhetetlen a legmagasabb szintű védelem fenntartásához.

Végezetül, ne feledkezzünk meg a metaadatokról, amiket a titkosított üzenetküldő alkalmazások továbbra is gyűjthetnek, például arról, hogy mikor és kivel kommunikálunk. Míg egyes alkalmazások, például a Signal minimalizálják a metaadatgyűjtést, mások több információt tarthatnak meg. A legmagasabb szintű adatvédelem érdekében válasszunk olyan alkalmazásokat, amelyek átláthatóak az adatgyűjtési szabályzataikkal kapcsolatban, és kiemelten kezelik a felhasználók biztonságát.

A titkosított azonnali üzenetküldő szolgáltatások felelősségteljes használatával és azok biztonsági jellemzőinek megértésével garantálhatjuk, hogy magánbeszélgetéseink bizalmasak és biztonságosak maradjanak a lehallgatók és rosszindulatú szereplők előtt.

Gyakorló feladatok

1. Hogyan segítik a titoktartási megállapodások (NDA) az érzékeny információk védelmét üzleti környezetekben? Mik az NDA-k bizonyos korlátai?

2. Mi a kapcsolat az adathalászat, a social engineering és a személyazonosság-lopás között, és hogyan védekezhetnek az egyének ezekkel a fenyegetésekkel szemben?

3. Miért fontos az információk osztályozása az adatvédelem szempontjából, és melyek az általános osztályozási szintek?

Gondolkodtató feladatok

1. Vizsgáljunk meg egy közelmúltbeli nagy horderejű adatszivárgást vagy adatsértést, amely egy jól ismert szervezetet érint! Írjuk le, hogyan történt a szivárgás, milyen érzékeny információk kerültek nyilvánosságra, és milyen hatással volt a vállalatra és annak ügyfeleire! Fejtsük ki, hogy a szervezet milyen intézkedéseket vezetett be a biztonsági rés után a biztonság javítása és a jövőbeni incidensek megelőzése érdekében!

2. Vizsgáljuk meg a szervezetek által használt különböző információosztályozási modellek hatékonyságát, mint például az amerikai kormányzat osztályozási rendszere (pl. Bizalmas (Confidential), Titkos (Secret), Szigorúan Titkos (Top Secret)) vagy kereskedelmi modellek (pl. Nyilvános (Public), Belső Használat (Internal), Bizalmas (Confidential), Szigorúan Bizalmas (Highly Confidential))! Hasonlítsuk össze, hogy ezek a modellek hogyan segítik az adatbiztonság kezelését és a jogi előírásoknak való megfelelést! Írjuk le az egyes modellek előnyeit és lehetséges hátrányait különböző szervezeti kontextusokban!

Összefoglalás

Ez a lecke a digitális biztonság különböző aspektusait tárgyalja, kiemelve a bizalmas információk védelmének fontosságát és az olyan fenyegetések felismerését, mint az adathalászat (phishing) és a social engineering. Elmagyarázza, hogy az adatszivárgás és a lehallgatott kommunikáció hogyan vezethet pénzügyi veszteséghez, a jó hírnév sérüléséhez és jogi következményekhez, valamint kiemeli a titoktartási megállapodások (non-disclosure agreement — NDA) szerepét az érzékeny információk védelmében. Kitérünk a személyazonosság-lopásra is, részletezve, hogy a támadók hogyan használják fel az ellopott személyes adatokat az áldozatok megszemélyesítésére, valamint tárgyaljuk az átverések és a scareware-támadások során alkalmazott taktikákat, amelyek félelemmel és megtévesztéssel manipulálják az áldozatokat. Az információosztályozás fontosságát is hangsúlyozzák a megfelelő biztonsági intézkedések alkalmazása és a szabályozásoknak való megfelelés biztosítása során, bemutatva, hogy a szervezetek hogyan védhetik hatékonyan kritikus értékeiket.

 | |

Válaszok a gyakorló feladatokra

1. Hogyan segítik a titoktartási megállapodások (NDA) az érzékeny információk védelmét üzleti környezetekben? Mik az NDA-k bizonyos korlátai?

   Az NDA védi az érzékeny információkat, mivel jogilag kötelezi az érintett feleket arra, hogy a megosztott adatokat bizalmasan kezeljék, és ne hozzák nyilvánosságra, illetve ne éljenek vissza azokkal. Meghatározzák a bizalmas információk körét, a felek kötelezettségeit és a megállapodás megszegésének következményeit. Ez a jogi keret segít biztosítani, hogy az érzékeny adatokat, például az üzleti titkokat vagy üzleti terveket ne osszák meg illetéktelen személyekkel, illetve ne használják fel a vállalat érdekei ellen. Az NDA-knak azonban vannak korlátai, mivel nem tudják megakadályozni az információkhoz hozzáféréssel rendelkező személyek általi véletlen vagy szándékos jogsértéseket. A követelmények betartása éberséget, felügyeletet és erős belső adatbiztonsági kultúrát igényel.

2. Mi a kapcsolat az adathalászat, a social engineering és a személyazonosság-lopás között, és hogyan védekezhetnek az egyének ezekkel a fenyegetésekkel szemben?

   Az adathalászat és a social engineering olyan taktikák, amelyeket a támadók arra használnak, hogy manipulálják az egyéneket, hogy személyes adatokat fedjenek fel, amelyeket aztán személyazonosság-lopásra használhatnak. Az adathalászat jellemzően csalárd e-maileket vagy szöveges üzeneteket tartalmaz, amelyek legitim forrásból származónak tűnnek, és az áldozatokat érzékeny adatok, például felhasználónevek és jelszavak megadására csábítják. A social engineering taktikák szélesebb körét foglalja magában, mint például a megszemélyesítés vagy a színlelés, hogy rászedjék az egyéneket a biztonsági protokollok megsértésére. Saját védelmük érdekében a magánszemélyeknek óvatosnak kell lenniük a kéretlen információkérésekkel szemben, kerülniük kell a gyanús linkekre való kattintást, erős, egyedi jelszavakat kell használniuk, engedélyezniük kell a többfaktoros hitelesítést, és rendszeresen ellenőrizniük kell a fiókjaikat, hogy nincs-e gyanús tevékenység.

3. Miért fontos az információk osztályozása az adatvédelem szempontjából, és melyek az általános osztályozási szintek?

   Az információk osztályozása alapvető fontosságú az adatvédelem szempontjából, mivel segít a szervezeteknek azonosítani és alkalmazni a megfelelő biztonsági intézkedéseket a különböző típusú adatokra azok érzékenysége alapján. Az információk olyan szintekbe való besorolásával, mint a publikus, belső használat, bizalmas és szigorúan bizalmas, a szervezetek ellenőrizhetik a hozzáférést, és biztosíthatják az érzékeny adatok biztonságos kezelését. A szigorúan bizalmas információkat, például az üzleti titkokat vagy a kritikus üzleti stratégiákat biztonságos, hozzáférés-ellenőrzött környezetben kell tárolni, és titkosított csatornákon keresztül kell továbbítani. A megfelelő osztályozás segíti a szervezeteket abban is, hogy megfeleljenek a jogi

és szabályozási követelményeknek, csökkentve az adatsértések és a megfelelés elmulasztásának kockázatát.

Válaszok a gondolkodtató feladatokra

1. Vizsgáljunk meg egy közelmúltbeli nagy horderejű adatszivárgást vagy adatsértést, amely egy jól ismert szervezetet érint! Írjuk le, hogyan történt a szivárgás, milyen érzékeny információk kerültek nyilvánosságra, és milyen hatással volt a vállalatra és annak ügyfeleire! Fejtsük ki, hogy a szervezet milyen intézkedéseket vezetett be a biztonsági rés után a biztonság javítása és a jövőbeni incidensek megelőzése érdekében!

   Erre példa a Facebook 2018-as adatsértése, amikor mintegy 87 millió felhasználó személyes adatait osztották meg helytelenül a Cambridge Analytica politikai tanácsadó céggel. A jogsértés a laza adatmegosztási irányelvek miatt következett be, ahol egy harmadik fél által használt alkalmazás felhasználói adatokat gyűjtött, majd azokat hozzájárulás nélkül megosztotta. A nyilvánosságra került adatok között szerepeltek a felhasználók személyes adatai, kedvelései, sőt, még privát üzenetek is. A Facebookra gyakorolt hatás súlyos volt: jogi vizsgálatot, a részvények értékének jelentős csökkenését és a felhasználók bizalmának elvesztését eredményezte. Válaszul a Facebook szigorúbb adatmegosztási irányelveket vezetett be, javította adatvédelmi gyakorlatát, és átláthatóbbá tette a harmadik féltől származó alkalmazások felhasználói információkhoz való hozzáférésének módját.

2. Vizsgáljuk meg a szervezetek által használt különböző információosztályozási modellek hatékonyságát, mint például az amerikai kormányzat osztályozási rendszere (pl. Bizalmas (Confidential), Titkos (Secret), Szigorúan Titkos (Top Secret)) vagy kereskedelmi modellek (pl. Nyilvános (Public), Belső Használat (Internal), Bizalmas (Confidential), Szigorúan Bizalmas (Highly Confidential))! Hasonlítsuk össze, hogy ezek a modellek hogyan segítik az adatbiztonság kezelését és a jogi előírásoknak való megfelelést! Írjuk le az egyes modellek előnyeit és lehetséges hátrányait különböző szervezeti kontextusokban!

   Az Egyesült Államok kormányának minősítési rendszere a nemzetbiztonsági információk védelmét szolgálja azáltal, hogy az információkat bizalmas, titkos vagy szigorúan titkos kategóriákba sorolja aszerint, hogy milyen kárt okozhat a jogosulatlan nyilvánosságra hozataluk. Ez a modell rendkívül strukturált és hatékony az érzékeny kormányzati adatok kezelésében, de megvalósítása és fenntartása bonyolult lehet. A kereskedelmi modellek, mint például a publikus, belső használat, bizalmas és szigorúan bizalmas, rugalmasabbak és könnyebben alkalmazhatók a különböző iparágakban. Segítenek a vállalkozásoknak az érzékeny információk védelmében és az olyan szabályozásoknak való megfelelésben, mint a GDPR vagy a CCPA. Ha azonban nem megfelelően kezelik ezeket a modelleket, azok következetlenségekhez és a kritikus eszközök elégtelen védelméhez vezethetnek az adatkezelésben.

025.3 Adatvédelem

Hivatkozás az LPI célkitűzésre

Security Essentials version 1.0, Exam 020, Objective 025.3

Súlyozás

2

Kulcsfontosságú ismeretek

- A személyes adatok fontosságának megértése
- A személyes adatok rosszindulatú célokra történő felhasználásnak megértése
- Az információgyűjtés, a profilalkotás és a felhasználói nyomkövetés fogalmának megértése
- A profil adatvédelmi beállításainak kezelése a közösségi médiaplatformokon és online szolgáltatásokban
- A személyes adatok közzétételével járó kockázatok megértése
- A személyes adatokkal kapcsolatos jogok megértése (pl. GDPR)

A használt fájlok, kifejezések és segédprogramok részleges listája

- Stalking és cybermobbing
- HTTP-sütik, böngésző-ujjlenyomatok, felhasználói nyomkövetés
- Scripttblokkolók és reklámblokkolók a webböngészőkben
- Profilok az online szolgáltatásokban és a közösségi médiában
- Kapcsolatok és adatvédelmi beállítások a közösségi médiában

Lecke 1

Tanúsítvány:	Security Essentials
Verzió:	1.0
Témakör:	025 Identitás és magánélet
Fejezet:	025.3 Adatvédelem
Lecke:	1/1

Bevezetés

Az online szolgáltatások és közösségi médiaplatformok által megosztott hatalmas mennyiségű adat megkönnyíti a kiberbűnözők számára a sebezhetőségek kihasználását és az érzékeny információkhoz való hozzáférést. Sokan tudtukon kívül osztanak meg olyan személyes adatokat, amelyek felhasználhatók ellenük, például a tartózkodási helyüket, elérhetőségi adataikat vagy akár pénzügyi adataikat. Ez a kitettség súlyos következményekkel járhat, beleértve a személyazonosság-lopást, a pénzügyi veszteséget és a személyes és szakmai fiókokhoz való jogosulatlan hozzáférést.

A személyes adatok bizalmas jellegének megőrzése megköveteli, hogy proaktívan kezeljük, hogyan és hol osztják meg az adatainkat. Ez magában foglalja a közösségi média fiókok és más online szolgáltatások adatvédelmi beállításainak konfigurálását, hogy korlátozzuk a mások számára látható adatokat.

Ugyanilyen fontos, hogy tisztában legyünk azzal, hogyan gyűjtik, profilozzák és követik nyomon az információkat az interneten. Az olyan technikákat, mint a HTTP-sütik (cookie), a böngésző-ujjlenyomatok (fingerprint) és a felhasználói nyomkövetés, a webhelyek és a hirdetők gyakran használják a felhasználók részletes profiljának kialakítására. Ha felismerjük ezeket a

nyomkövetési módszereket, és tudjuk, hogyan csökkenthetjük őket — az adatvédelemre összpontosító böngészők használatával, a harmadik féltől származó sütik letiltásával vagy a nyomon követés elleni védelmi eszközök alkalmazásával --, akkor megőrizhetjük anonimitásunkat és megvédhetjük személyes adatainkat.

Ez a lecke végigvezet minket az adatvédelmi beállítások hatékony kezelésének alapvető lépésein, a személyes adatok kiszolgáltatottságával kapcsolatos kockázatok megértésén, valamint az online információgyűjtés és a felhasználói nyomon követés bonyolult folyamataiban való eligazodáson.

A személyes információk fontossága

A személyes információ magában foglal minden olyan adatot, amely felhasználható egy személy azonosítására vagy a róla való tájékozódásra. Ide tartoznak a nevek, címek, telefonszámok, e-mail címek, társadalombiztosítási számok, pénzügyi adatok, sőt még az online viselkedés, például a böngészési előzmények és az aktivitás a közösségi médiában is. Bár bizonyos személyes adatok megosztása szükséges az online szolgáltatások használatához vagy a mindennapi tevékenységekhez, a magánélet és a biztonság megőrzéséhez elengedhetetlen ezek jelentőségének és a visszaélések lehetséges következményeinek megértése.

A személyes adatok nemcsak az egyének, hanem a vállalkozások, a kormányok és a kiberbűnözők számára is értékesek. A vállalatok a személyes adatokat marketingcélokra, a hirdetések testre szabására és a felhasználói élmény javítására használják fel. Ezeket az adatokat azonban az egyén beleegyezése nélkül is összegyűjthetik, megoszthatják vagy eladhatják, ami adatvédelmi aggályokhoz vezet. A kormányok a személyes adatokat adminisztratív és biztonsági célokra használják, de visszaélhetnek velük megfigyelésre vagy a lakosság ellenőrzésére és manipulálására is. A kiberbűnözők viszont a személyes adatokat jövedelmező célpontnak tekintik csalás, személyazonosság-lopás és más rosszindulatú tevékenységek elkövetéséhez. Ez pénzügyi veszteségekhez, rossz hitelminősítésekhez, valamint a személyazonosság visszaszerzésének és az érintett felhasználói fiókok biztosításának hosszú és stresszes folyamatához vezethet. A pénzügyi károkon túlmenően a személyes adatok megfigyelésre (stalking), internetes zaklatásra (cyberbullying) és zaklatásra (harassment) is felhasználhatók, ami az egyéneket mind online, mind a magánéletükben veszélynek teszi ki.

Egy másik szempont az adatok megsértésével és kiszivárgásával kapcsolatos lehetséges kockázatok. Adatsérülés akkor következik be, ha biztonsági hiányosságok vagy kibertámadások miatt érzékeny információk kerülnek nyilvánosságra. Az ilyen incidensek személyes adatokhoz való jogosulatlan hozzáférést eredményezhetnek, ami személyazonosság-lopáshoz, pénzügyi csaláshoz és egyéb súlyos következményekhez vezethet. A szoftverek és rendszerek naprakészen tartása, az erős és egyedi jelszavak használata, valamint a többfaktoros hitelesítés lehetővé tétele olyan gyakorlatok, amelyek segíthetnek az adatvédelmi incidensek kockázatának csökkentésében.

A személyes adatok védelméhez elengedhetetlen annak megértése, hogy a különböző szervezetek hogyan gyűjtik, tárolják és használják azokat. Az online szolgáltatásokra való regisztrációkor az egyéneknek át kell nézniük az adatvédelmi irányelveket, és tudatában kell lenniük annak, hogy milyen adatok megosztásához járulnak hozzá.

A személyes adatok közzétételének kockázata

A személyes adatok közzétételével kapcsolatos egyik elsődleges kockázat a személyazonossággal való visszaélés. A kiberbűnözők olyan adatokat használhatnak fel, mint a nevünk, születési dátumunk vagy címünk, hogy megszemélyesítsenek minket, és így hozzáférjenek pénzügyi számláinkhoz, hiteleinkhez vagy akár a kormányzati szolgáltatásokhoz. Elegendő információ birtokában hitelkártyát vagy kölcsönt igényelhetnek, és csalárd módon vásárolhatnak a nevünkben, ami pénzügyi veszteséghez és sérült hitelpontszámhoz vezethet. A személyazonossággal való visszaélés következményei hosszú távúak lehetnek, valamint jelentős időt és erőfeszítést igényel a pénzügyi helyzet megoldása és helyreállítása.

A pénzügyi csalások mellett az online megosztott személyes adatok kiszolgáltatottá tehetnek minket az adathalász-támadásoknak is. Az adathalászok gyakran személyes adatokat használnak arra, hogy meggyőző e-maileket vagy üzeneteket írjanak, amelyek úgy tűnnek, mintha legitim forrásból, például a bankunktól, munkáltatónktól vagy kormányzati szervtől érkeztek volna. Ezeknek az üzeneteknek általában az a célja, hogy rávegyenek minket érzékenyebb adatok, például jelszavak, számlaszámok megadására, vagy rosszindulatú szoftverek letöltésére. Minél több információval rendelkeznek a támadók, annál könnyebb olyan meggyőző átverést létrehozni, amely komoly biztonsági résekhez vezethet.

A személyes adatokat online és a való életben is fel lehet használni megfigyelésre és zaklatásra. Ha megosztuk tartózkodási helyünket, utazási terveinket vagy akár napi rutinunkat, akkor kitehetjük magunkat a nem kívánt figyelemnek, vagy könnyű célponttá válhatunk a rosszindulatú szándékkal rendelkezők számára. Az internetes zaklatók felhasználhatják ezeket az információkat arra, hogy nyomon kövessék mozgásunkat, megfélemlítsenek minket, vagy álhíreket terjesszenek rólunk. Ez valós konfrontációvá fajulhat, és veszélybe sodorhatja a fizikai biztonságunkat. Még az olyan, látszólag ártalmatlan információk is, mint például a családtagjaink neve vagy az iskolák, ahová jártunk, felhasználhatók arra, hogy olyan profilt készítsenek rólunk, amelyet a megfigyelőink (a stalkerek) és zaklatók kihasználhatnak.

A rosszindulatú egyének a közösségi médiából származó információkat felhasználhatják a cyberbullying (vagy cybermobbing) során, ami súlyos hatással van áldozataik mentális és érzelmi egészségére. A cyberbullying ismételt és szándékos támadásokat jelent, például sértegetést, megalázást és fenyegetést, amelyeket digitális platformokon, például közösségi hálózatokon és üzenetküldő alkalmazásokon keresztül hajtanak végre, gyakran hamis profilokat használva az elkövető személyazonosságának elrejtése érdekében.

Vannak olyan, gyakran a darkweben található platformok, amelyek összegyűjtik az ellopott személyes adatokat, és eladják azokat a kiberbűnözőknek. Ezek az “adatbrókerként” vagy “underground piactérként” ismert platformok adatbetörésekből, adathalász-támadásokból és egyéb illegális tevékenységekből származó információkat gyűjtenek össze, és olyan kiterjedt adatbázisokat hoznak létre, amelyekben az e-mail címektől és jelszavaktól kezdve a társadalombiztosítási számokon és hitelkártyaadatokon át egészen az egészségügyi adatokig minden megtalálható. A kiberbűnözők megvásárolhatják ezeket az adatkészleteket, hogy személyazonosság-lopást, pénzügyi csalást vagy más rosszindulatú tevékenységeket kövessenek el.

Ráadásul, ha a személyes információkat egyszer már közzétették az interneten, nehéz eltávolítani őket vagy ellenőrizni a terjedésüket. Még ha törlünk is egy bejegyzést vagy fiókot, az adataink másolatai megmaradhatnak más weboldalakon, a keresőmotorok gyorsítótárában vagy valaki más eszközén.

E kockázatok csökkentése érdekében fontos, hogy mindent alaposan átgondoljunk, mielőtt személyes információkat tennénk közé online. Korlátozzuk a közösségi médiaplatformokon megosztott személyes adatok mennyiségét, és az adatvédelmi beállítások segítségével szabályozzuk, hogy ki láthatja a bejegyzéseinket és a profilunk adatait.

A személyes adatokkal kapcsolatos jogok — GDPR

A digitális platformok személyes és szakmai tevékenységekhez való egyre szélesebb körű használatával a személyes adatok védelme világszerte kritikus kérdéssé vált. Különböző törvények és rendeletek születtek annak érdekében, hogy az egyének nagyobb ellenőrzést gyakorolhassanak személyes adataik felett, és hogy a szervezetek felelősségteljesen kezeljék ezeket az adatokat. Az egyik legátfogóbb és legbefolyásosabb ilyen szabályozás az Európai Unió *általános adatvédelmi rendelete* (General Data Protection Regulation — GDPR), amely magas szintű előírásokat határoz meg az adatvédelem és az adatbiztonság tekintetében. A személyes adatokkal kapcsolatos, a GDPR-hez hasonló rendeletek szerinti jogainak megértése alapvető fontosságú a magánélet védelme és az adatok megfelelő kezelésének biztosítása szempontjából.

A 2018 májusában hatályba lépett GDPR célja az uniós polgárok és lakosok személyes adatainak védelme azáltal, hogy szabályozza, hogy a szervezetek hogyan gyűjtik, tárolják és dolgozzák fel ezeket az információkat. A rendelet minden olyan szervezetre vonatkozik, függetlenül annak székhelyétől, amely az EU-ban élő egyének személyes adatait kezeli. Ez azt jelenti, hogy még az EU-n kívüli székhelyű vállalatoknak is meg kell felelniük a GDPR-nak, ha uniós lakosok adatait kezelik.

A GDPR egyik alapvető joga a tájékoztatáshoz való jog. Ez azt jelenti, hogy az egyéneknek joguk van tudni, hogy milyen személyes adatokat gyűjtenek róluk, hogyan használják fel, kikkel osztják

meg, és mennyi ideig őrzik meg azokat. A szervezeteknek világos és átlátható tájékoztatást kell nyújtaniuk az adatfeldolgozási tevékenységeikről, jellemzően adatvédelmi irányelvek vagy tájékoztatók révén.

Egy másik kulcsfontosságú jog a *hozzáférési jog* (right of access), amely lehetővé teszi az egyének számára, hogy másolatot kérjenek a szervezet által tárolt személyes adataikról. Az emberek így megnézhetik, milyen adatokat tárolnak róluk, és meggyőződhetnek arról, hogy azok pontosak és a törvénynek megfelelően kerülnek feldolgozásra. A hozzáférésen kívül az egyéneknek joguk van a helyesbítéshez is, amely lehetővé teszi számukra, hogy kérjék a pontatlan vagy hiányos adatok helyesbítését.

A GDPR rendelkezik a *törléshez való jogról* (right to erasure) is, amelyet általában "az elfeledtetéshez való jogként" ismerünk. Ez lehetővé teszi az egyének számára, hogy bizonyos körülmények között kérjék személyes adataik törlését, például ha az adatokra már nincs szükség az adatgyűjtés céljának eléréséhez, vagy ha visszavonják hozzájárulásukat. Ez a jog azonban nem abszolút, és korlátozható, például ha az adatokra jogi kötelezettségek vagy közérdekű célok miatt van szükség.

Az *adatkezelés korlátozásához való jog* (right to restrict processing) lehetővé teszi az egyének számára, hogy korlátozzák adataik felhasználását. Ha például egy személy vitatja adatainak pontosságát, kérheti, hogy a felhasználást korlátozzák, amíg a probléma megoldódik. Hasonlóképpen, a *tiltakozáshoz való jog* (right to object) lehetővé teszi az egyének számára, hogy tiltakozzanak személyes adataik meghatározott célú, például közvetlen marketing vagy profilalkotás céljából történő feldolgozása ellen.

A GDPR egy másik jelentős aspektusa az *adatok hordozhatóságához való jog* (right to data portability). Ez a jog lehetővé teszi az egyének számára, hogy személyes adataikat strukturált, általánosan használt és géppel olvasható formátumban megkapják, és azokat egy másik szervezetnek továbbítsák. Ez különösen hasznos lehet a szolgáltatóváltás vagy a különböző platformokról származó adatok konszolidálása esetén.

E jogokon túlmenően a GDPR azt is előírja a szervezeteknek, hogy megfelelő biztonsági intézkedéseket hajtsanak végre a személyes adatok védelme érdekében, és az adatvédelmi incidenseket a felfedezéstől számított 72 órán belül jelenteniük kell az illetékes hatóságoknak és az érintett személyeknek. Ez magas szintű elszámoltathatóságot és reagálóképességet biztosít adatbiztonsági incidens esetén.

Bár a GDPR csak az Európai Unióra jellemző, hatása világszerte hasonló adatvédelmi szabályok elfogadásához vezetett. A *kaliforniai fogyasztói adatvédelmi törvény* (California Consumer Privacy Act — CCPA) például hasonló jogokat biztosít a kaliforniai lakosok számára, beleértve a jogot arra, hogy megtudják, milyen személyes adatokat gyűjtenek róluk, és hogy kérhessék azok törlését. Más

joghatóságok is követik a példát saját adatvédelmi törvényeikkel, ami az adatvédelmi jogok megerősítése felé mutató globális tendenciát tükrözi.

Az e rendeletek szerinti jogaink megértése alapvető fontosságú a személyes adataink feletti ellenőrzés fenntartásához. Ha úgy érezzük, hogy megsértették az adatainkhoz fűződő jogainkat, jogunk van panaszt tenni országunk illetékes adatvédelmi hatóságánál.

Információgyűjtés, profilalkotás és a felhasználók nyomon követése

Az információgyűjtést, a profilalkotást és a felhasználó nyomon követését a webhelyek, a hirdetők és néha rosszindulatú szervezetek használják a felhasználók online tevékenységeire vonatkozó adatok gyűjtésére és elemzésére. Ezek a technikák segítenek részletes profilok kialakításában, amelyek különböző célokra használhatók fel, például személyre szabott reklámozásra, a felhasználói élmény fokozására, vagy bizonyos esetekben a viselkedés manipulálására és a magánélet megsértésére.

A *HTTP sütik* (cookie) a felhasználói tevékenység nyomon követésének egyik legelterjedtebb eszközei. A sütik olyan kis szöveges fájlok, amelyeket a felhasználó által látogatott weboldalak tárolnak a felhasználó eszközén. Emlékezhetnek a bejelentkezési adatokra, nyomon követhetik a kosárban lévő tételeket, vagy tárolhatják a felhasználói beállításokat. Bár a sütik elengedhetetlenek bizonyos szolgáltatások lehetővé tételéhez, például a felhasználó nyelvi beállításainak vagy bejelentkezési státuszának megjegyzése, adatvédelmi aggályokat is felvetnek. A harmadik féltől származó sütiket, amelyeket nem a felhasználó által látogatott domainek állítanak be, a hirdetők gyakran arra használják, hogy a felhasználókat különböző weboldalakon keresztül nyomon kövessék, átfogó képet alkotva böngészési szokásaikról és preferenciáikról. Ezeket az adatokat aztán célzott hirdetések célba juttatására használhatják, vagy akár eladhatják más szervezeteknek további elemzés céljából.

A *böngésző ujjlenyomata* (browser fringerprinting) egy kifinomultabb nyomkövető technika, amely különböző adatpontokat gyűjt a felhasználó böngészőjéről és eszközkonfigurációjáról. Az olyan információk, mint a képernyő felbontása, a telepített betűtípusok, a böngésző bővítményei és az operációs rendszer adatai kombinálhatók, hogy minden egyes felhasználó számára egyedi azonosítót vagy “ujjlenyomatot” hozzanak létre. A sütikkel ellentétben, amelyek törölhetők vagy letilthatók, az ujjlenyomatokat nehezebb kijátszani, mivel nem támaszkodnak a felhasználó eszközén tárolt adatokra. Ez a módszer lehetővé teszi a nyomkövetők számára, hogy a felhasználókat különböző weboldalakon keresztül, kifejezett beleegyezés nélkül azonosítsák és kövessék, ami jelentős adatvédelmi aggályokat vet fel.

A *felhasználók nyomon követése* (user tracking) az online viselkedés nyomon követésének és

elemzésének számos módját foglalja magában. A sütiken és az ujjlenyomaton túl a felhasználói nyomkövetés olyan technikákat is magában foglalhat, mint a nyomkövető pixelek, amelyek apró, láthatatlan képek, weboldalakba vagy e-mailekbe ágyazva. Amikor a felhasználó betölt egy olyan oldalt vagy megnyit egy olyan e-mailt, amely nyomkövető pixelt tartalmaz, az olyan információkat küld vissza a nyomkövetőnek, mint például a felhasználó IP-címe, az eszköz típusa és a tartalom megtekintésének pontos időpontja. Ezek az adatok felhasználhatók a felhasználói aktivitás és a marketingkampányok konverzióinak nyomon követésére vagy további profilalkotáshoz szükséges adatok összeállítására.

Az ilyen nyomonkövetési módszerekkel összegyűjtött információk felhasználhatók az egyes felhasználók részletes profiljának létrehozására, beleértve az érdeklődési körüket, szokásaikat, sőt társadalmi és gazdasági helyzetüket is. Ezek a profilok értékesnek bizonyulnak a hirdetők számára, akik pontosan célzott hirdetéseket kívánnak megjeleníteni, de etikai és adatvédelmi kérdéseket is felvetnek. Például az ilyen részletes profilok felhasználhatók a felhasználói viselkedés befolyásolására, a tartalomhoz való hozzáférés korlátozására, vagy akár a vélt jellemzők alapján történő megkülönböztetésre.

Ezeknek a fogalmaknak a megértése alapvető fontosságú azon személyek számára, akik meg akarják védeni magánéletüket az interneten. A felhasználók olyan lépéseket tehetnek, mint például a sütik rendszeres törlése, az adatvédelemre összpontosító böngészők vagy a nyomkövetőket blokkoló bővítmények használata, valamint virtuális magánhálózatok (VPN) alkalmazása online tevékenységeik elrejtésére.

Összességében, bár az információgyűjtés, a profilalkotás és a felhasználó nyomon követése javíthatja az online élményeket és szolgáltatásokat, ugyanakkor jelentős kockázatot is jelent a személyes adatok védelmére nézve.

A profilok adatvédelmi beállítások kezelése

A közösségi médiaplatformokon és online szolgáltatásokban az adatvédelem fenntartása alapvető fontosságú a személyes adatok védelme érdekében a nem kívánt hozzáféréstől. A *profil adatvédelmi beállításainak* hatékony kezelése segít abban, hogy ellenőrizzük, ki láthatja személyes adatainkat, bejegyzéseinket és tevékenységeinket, csökkentve ezzel a rosszindulatú szereplők általi visszaélés kockázatát, vagy akár azt, hogy ismeretlenek lépjenek velünk nem kívánt kapcsolatba.

Jellemzően minden platform számos olyan beállítást kínál, amelyek lehetővé teszik a felhasználók számára, hogy meghatározzák, milyen információk legyenek láthatóak a nyilvánosság, a barátok vagy csak a kiválasztott kapcsolatok számára. A Facebookon például kiválaszthatjuk, hogy a bejegyzéseink csak a barátaink vagy akár egy egyéni listán szereplő személyek számára legyenek láthatóak, míg a LinkedIn-en szabályozhatjuk, hogy ki láthatja a kapcsolatainkat vagy a

profilfrissítéseinket. E beállítások rendszeres felülvizsgálata és frissítése létfontosságú, mivel a platformok gyakran frissítik adatvédelmi irányelveiket és beállításaikat, és néha a felhasználók egyértelmű értesítése nélkül alapértelmezetten nyilvánosabb beállításokra váltanak.

Profilok az online szolgáltatásokban és a közösségi médiában

Az online szolgáltatások és a közösségi média profiljai a felhasználók digitális reprezentációjaként működnek, és olyan személyes adatokat tartalmaznak, mint a név, fényképek, elérhetőségek és érdeklődési körök. Ezek a profilok felhasználhatók másokkal való kapcsolatteremtésre, tartalmak megosztására és különböző online tevékenységekben való részvételre. Ugyanakkor információforrássá is válhatnak a kiberbűnözők számára, akik személyazonosságot akarnak lopni vagy célzott támadásokat akarnak végrehajtani. A felhasználóknak figyelniük kell arra, hogy milyen adatokat osztanak meg profiljaikban, és figyelembe kell venniük, hogy milyen következményei lehetnek annak, ha ezek az információk rossz kezekbe kerülnek. Ha valaki például túl sok személyes adatot oszt meg, például a munkahelyéről vagy a napi rutinjáról, az kiszolgáltatottá teheti az adathalász-támadásoknak vagy akár valós fenyegetéseknek. Bölcs döntés, ha korlátozzuk a profilunkon látható személyes adatok mennyiségét, és gondoskodunk arról, hogy az olyan érzékeny információk, mint a lakcím vagy a telefonszám, titokban maradjanak.

A kapcsolatok és az adatvédelmi beállítások kezelése alapvető része annak, hogy biztosítsuk a közösségi média élményét. Az olyan platformok, mint a Facebook, az Instagram és a LinkedIn lehetővé teszik a felhasználók számára, hogy kapcsolataikat különböző csoportokba, például barátok, családtagok és ismerősök közé sorolják, és az egyes csoportok adatvédelmi beállításait testre szabják. Ez azt jelenti, hogy bizonyos posztokat megoszthatunk a közeli barátainkkal, miközben elrejthetjük azokat a szakmai kapcsolatok vagy a nagyközönség elől. Emellett sok platform lehetővé teszi, hogy letiltsuk vagy elnémítsuk azokat a kapcsolatokat, amelyek esetleg zaklatnak minket vagy spameket küldenek nekünk. Ha megválogatjuk, hogy kiket fogadunk el kapcsolatként, és rendszeresen felülvizsgáljuk adatvédelmi beállításainkat, megelőzhetjük a személyes adatainkhoz való illetéktelen hozzáférést, és biztonságosabb, élvezetesebb közösségi médiaélményt biztosíthatunk.

A *script-blokkolók* (script blocker) és a *hirdetésblokkolók* (ad blocker) olyan eszközök, amelyek segítenek az adataink védelmében és a böngészési élmény javításában azáltal, hogy megakadályozzák, hogy a böngésző nem kívánt tartalmakat töltsön be a webhelyekről. A scriptblokkolók, mint például a *NoScript* vagy az *uMatrix*, lehetővé teszik a felhasználók számára, hogy szabályozzák, mely scriptek futtatása engedélyezett az általuk látogatott webhelyeken. Ez megakadályozhatja a rosszindulatú scriptek végrehajtását, amelyek egyébként nyomon követhetnék a felhasználó tevékenységét, ellophatnák az adatait, vagy rosszindulatú szoftvereket juttathatnának a rendszerébe. A szükségtelen scriptek letiltásával a felhasználók növelhetik biztonságukat és csökkenthetik az oldalak betöltési idejét.

A hirdetésblokkolók, mint például az *AdBlock Plus* vagy az *uBlock Origin*, megakadályozzák a reklámok megjelenítését a weboldalakon. Bár a hirdetéseket elsősorban marketingcélokra használják, nyomon követés és adatgyűjtés forrásai is lehetnek. Sok hirdetés tartalmaz olyan nyomkövetőket, amelyek több webhelyen keresztül figyelik a felhasználók viselkedését, és részletes profilokat készítenek a böngészési szokásokról. Ezeknek a hirdetéseknek a blokkolása nemcsak a vizuális zavart csökkenti és felgyorsítja a böngészést, hanem a rólunk gyűjtött adatok mennyiségét is minimalizálja. A hirdetésblokkolók továbbá megakadályozhatják, hogy rosszindulatú hirdetéseknek (malvertising) legyünk kitéve, amelyek káros webhelyek meglátogatásához vagy rosszindulatú programok letöltéséhez vezethetnek.

A korábban említett scriptblokkolók és hirdetésblokkolók a Google Chrome, Firefox és Opera böngészőkhöz bővítményként elérhetők, és forráskódjuk a nyilvános GitHub repositoryjukban is megtalálható.

Gyakorló feladatok

1. Hogyan védheti meg a személyes adatainkat a jogosulatlan hozzáféréstől a közösségi médiaplatformok adatvédelmi beállításainak kezelése? Adjunk konkrét példákat azokra a beállításokra, amelyeket olyan platformokon használnánk, mint a Facebook vagy a LinkedIn, és fejtsük ki ezen beállítások fontosságát az adatvédelem fenntartásában!

2. Hogyan növelhetik az online adatvédelmet és biztonságot a scriptblokkolók és a hirdetésblokkolók? Fejtsük ki a két eszköztípus közötti különbséget, és mondjunk példákat arra, hogyan lehet hatékonyan használni őket az internetes böngészés során!

Gondolkodtató feladatok

1. Vizsgáljuk meg és hasonlítsuk össze az elérhető adatvédelmi beállításokat két különböző közösségi médiaplatformon! Határozzunk meg legalább három fő különbséget abban, hogy az egyes platformok hogyan teszik lehetővé a felhasználók számára személyes adataik kezelését és annak szabályozását, hogy ki láthatja a tartalmukat! Fejtsük ki, hogy ezek a különbségek hogyan befolyásolhatják a döntésünket arról, hogy milyen típusú személyes információkat osztunk meg az egyes platformokon!

Összefoglalás

A titoktartás fontosságának megértése alapvető fontosságú a személyes adatok jogosulatlan hozzáféréstől és visszaéléstől való védelméhez. Ez nemcsak azt jelenti, hogy éberen kell figyelni a személyes adatok megosztásának módjára, hanem azt is, hogy hatékonyan kell kezelni az adatvédelmi beállításokat a különböző online szolgáltatások és közösségi médiaplatformok esetében. Sokan digitális tevékenységeik során tudtukon kívül érzékeny információkat tesznek közzé, így kiszolgáltatottá válnak az olyan fenyegetéseknek, mint a személyazonosság-lopás, az adathalász-támadások és a social engineering. Az adatvédelmi beállítások kezelésének megtanulásával és a gyakori biztonsági fenyegetések felismerésével az egyének proaktív lépéseket tehetnek személyes adataik védelme és a digitális identitásuk feletti kontroll megőrzése érdekében.

Válaszok a gyakorló feladatokra

1. Hogyan védheti meg a személyes adatainkat a jogosulatlan hozzáféréstől a közösségi médiaplatformok adatvédelmi beállításainak kezelése? Adjunk konkrét példákat azokra a beállításokra, amelyeket olyan platformokon használnánk, mint a Facebook vagy a LinkedIn, és fejtsük ki ezen beállítások fontosságát az adatvédelem fenntartásában!

   Az adatvédelmi beállítások kezelésével szabályozhatjuk, hogy ki láthatja személyes adatainkat, bejegyzéseinket és tevékenységeinket. A Facebookon például korlátozhatjuk profilunk láthatóságát az “Ismerősök” számára, így megakadályozhatjuk, hogy idegenek lássák személyes adatainkat és bejegyzéseinket. Emellett az “Ismerőslisták” funkcióval csak a kiválasztott csoportokkal oszthatunk meg posztokat, például a “Közeli ismerősökkel” igen, míg a “Munkatársakkal” nem. A LinkedIn-en a profilunk beállításával korlátozhatjuk, hogy ki láthatja a kapcsolati listánkat, így megakadályozhatjuk, hogy a potenciális fejvadászok vagy versenytársak hozzáférjenek a hálózatunkhoz. Ezek a beállítások kulcsfontosságúak az adatvédelem fenntartásában, a nem kívánt kapcsolatfelvétel elkerülésében vagy az információinkkal való visszaélés kockázatának csökkentésében.

2. Hogyan növelhetik az online adatvédelmet és biztonságot a scriptblokkolók és a hirdetésblokkolók? Fejtsük ki a két eszköztípus közötti különbséget, és mondjunk példákat arra, hogyan lehet hatékonyan használni őket az internetes böngészés során!

   A scriptblokkolók, mint például a NoScript, megakadályozzák, hogy potenciálisan rosszindulatú scriptek fussanak a webhelyeken, lehetővé téve a felhasználók számára, hogy kiválasszák, mely scriptek legyenek engedélyezve. Ez segít megvédeni a jogosulatlan nyomon követéstől és a rosszindulatú kódok végrehajtásától. A scriptblokkoló például megakadályozhatja, hogy harmadik féltől származó nyomkövető scriptek töltődjenek be egy híroldalra, és ezáltal meggátolhatja a böngészési szokásaink nyomon követését.

   A hirdetésblokkolók, mint például az AdBlock Plus, blokkolják a gyakran nyomkövető elemeket tartalmazó hirdetéseket, és csökkenthetik a rosszindulatú hirdetéseknek (malvertising) való kitettség kockázatát.

   Míg a scriptblokkolók a scripteket ellenőrzik, a hirdetésblokkolók pedig a vizuális hirdetések blokkolására összpontosítanak, a két eszköz együttesen használható a biztonságosabb böngészési környezet megteremtéséhez az adatgyűjtés minimalizálásával és a potenciális biztonsági fenyegetések megelőzésével.

Válaszok a gondolkodtató feladatokra

1. Vizsgáljuk meg és hasonlítsuk össze az elérhető adatvédelmi beállításokat két különböző közösségi médiaplatformon! Határozzunk meg legalább három fő különbséget abban, hogy az egyes platformok hogyan teszik lehetővé a felhasználók számára személyes adataik kezelését és annak szabályozását, hogy ki láthatja a tartalmukat! Fejtsük ki, hogy ezek a különbségek hogyan befolyásolhatják a döntésünket arról, hogy milyen típusú személyes információkat osztunk meg az egyes platformokon!

   Ehhez a feladathoz mindkét platform specifikus adatvédelmi beállításainak felkutatására van szükség. A Facebook például részletesebb ellenőrzést kínál a posztok láthatósága felett az olyan lehetőségekkel, mint az “Ismerősök, kivéve…” vagy az “Egyéni” listák, míg az Instagram elsősorban a `"Publikus`" vagy “Privát” profilbeállításokat teszi lehetővé. Emellett a Facebook lehetőséget biztosít arra, hogy korlátozzuk, hogy ki jelölhet minket ismerősnek vagy ki vagy láthatja az ismerőseink listáját. Ez a funkció az Instagramon nem áll rendelkezésünkre. Ezek a különbségek befolyásolják a felhasználói információk feletti ellenőrzés szintjét, ami potenciálisan a Facebookot előnyösebb platformmá teheti az ellenőrzöttebb megosztáshoz, míg az Instagram egyszerűbb adatvédelmi keretei miatt nagyobb óvatosságot igényelhet a közzétett információkkal kapcsolatban.

Impresszum

PDF generálva: 2025-05-26

Az LPI Learning Materials a Linux Professional Institute (https://lpi.org) kezdeményezése. A tananyagok és a fordításaik a https://learning.lpi.org oldalon érhetők el.

Ezzel a kiadással és az egész projekttel kapcsolatos kérdéseket és megjegyzéseket az alábbi e-mail címre küldheti el: learning@lpi.org.