Számítógépes hardver 3
KIN/PS/IN/12

HÁLÓZATI BIZTONSÁG

13

előadás

Ing. Ondrej Takáč, PhD.
Informatika Tanszék
Gazdaságtudományi és Informatakai Kar
Selye János Egyetem

Tel.: +421 35 32 60 629
Email: takac.ondrej@gmail.com

piatok, 18. decembra 2020

A HÁLÓZATBA TÖRTÉNŐ BEHATOLÁS KOCKÁZATAI

- A behatolók hozzáférést szerezhetnek a hálózathoz a **szoftver** sebezhető pontjain keresztül, **hardver** elleni támadással vagy akár kevésbé fejlett módszerekkel is, mint például a felhasználó nevének és jelszavának kitalálása.
  - **Azokat a behatolókat, akik szoftver módosításával vagy a szoftver sebezhető pontjait kihasználva jutnak hálózati hozzáféréshez gyakran hekkereknek (hacker) nevezzük.**
- Ha egyszer a hekker hálózati hozzáféréshez jut, akkor a veszély négy típusa merülhet fel:
  - Információlopás
  - Azonosító ellopása
  - Adatvesztés illetve manipulálás
  - Szolgáltatás megszakítása

TÁMADÁSOK TÍPUSAI

- Információlopás
  - Behatolás információ megszerzése céljából. Az információ felhasználható, vagy értékesíthető különböző célokra.
- Azonosító ellopása
  - Személyes információ eltulajdonítása, valaki azonosságának átvétele céljából. Ezekkel az információkkal hitelt igényelhetnek, internetes vásárlásokat végezhetnek…
- Adatvesztés illetve manipulálás
  - Vírus küldése, mely módosítja, törli az adatokat, adatok megváltoztatása.
- Szolgáltatás megszakítása
  - A hivatalos felhasználók meggátolása abban, hogy hozzáférjenek a szolgáltatásokhoz, melyekre jogosultak.

BEHATOLÁSOK FORMÁI, TÁMADÁS MÓDSZEREK

A HÁLÓZATI BEHATOLÁS FORRÁSAI

- Külső veszélyek
  - A külső veszélyek a szervezeten kívül dolgozó személyekkel kapcsolatban merülnek fel. Ők nem rendelkeznek hozzáférési jogosultsággal a számítógép rendszerekhez vagy hálózathoz.
  - A külső támadók a hálózatba való bejutásukat főleg az Interneten, vezeték nélküli kapcsolatokon vagy a szerverekhez történő behívásos hozzáférésen keresztül hajtják végre.
- Belső veszélyek
  - A belső veszélyek akkor jelentkeznek, amikor valaki egy felhasználói fiókon keresztül hozzáférési jogosultsággal rendelkezik a hálózathoz, vagy fizikailag hozzáfér a hálózati eszközhöz.
  - A belső támadó ismeri a belső szabályokat és embereket. Gyakran azt is tudja, melyik információk értékesek és egyben sebezhetők és, hogy miként lehet ezeket elérni.

MEGTÉVESZTÉSI TECHNIKA (SOCIAL ENGINEERING)

- Az emberi hiszékenység kihasználása.
- A megtévesztési technika valaki vagy valami azon képességére utaló kifejezés, mellyel befolyásolja egy embercsoport viselkedést.
- Számítógép és hálózatbiztonsági szövegkörnyezetben a megtévesztési technika a technikák egy olyan csoportjára vonatkozik, mellyel ráveszik a belső felhasználókat arra, hogy adott tevékenységet végrehajtsanak vagy titkos információkat kiszolgáltassanak.
- A három legáltalánosabban használt megtévesztési technika (social engineering):
  - a hamis ürügy (pretext),
  - az adathalászat (phishing) és
  - a telefonos adathalászat (vishing).

HAMIS ÜRÜGY (PRETEXTING)

- A hamis ürügy (Pretexting) a megtévesztési technika egyik olyan formája, ahol egy előre megtervezett esetet (pretext) használnak fel az áldozat megtévesztésére azért, hogy információkat adjon vagy végrehajtson egy tevékenységet.
- Ez a támadó részéről gyakran előzetes tanulmányozást vagy kutatást követel meg.
  - Például ha a támadó ismeri a célszemély társadalombiztosítási számát, ezt az információt felhasználhatja arra, hogy elnyerje a célszemély bizalmát. Ekkor a célszemély nagyobb valószínűséggel ad meg további információkat.

HAMIS ÜRÜGY (PRETEXTING)

Szevasz, Amy vagyok az ügyféltámogatástól. Frissítenünk kell a számítógépeden található szoftvert a munkaidő után. Mi a felhasználói azonosítód (ID) és a jelszavad? A jelszót holnap megváltoztathatod, amikor bejelentkezel.

A Megtévesztés mestere
(Social engineer)

Rendben, a felhasználói azonosítóm (ID) és a jelszó ...

Gyanútlan alkalmazott
a Xyz
részvénytársaságnál.

ADATHALÁSZAT

- Adathalászat (Phishing)
  - Az adathalászat a megtévesztési technika olyan formája, ahol az adathalászok úgy tesznek mintha egy a szervezeten kívüli hivatalt képviselnének.
    - Tipikusan elektronikus levélen keresztül személyesen lépnek kapcsolatba a célszeméllyel (a 'hallal').
    - Az adathalász olyan hitelesítési információkat kérhet, mint a jelszó vagy a felhasználói név azért, hogy valami szörnyű következmények bekövetkezésétől óvjon meg.

- Telefonos adathalászat (Vishing/Phone Phishing)
  - A megtévesztési technika azon új formája, ahol az IP-n keresztüli hangtovábbítást (VoIP) használják, telefonos adathalászatként (vishing) ismert.
    - A telefonos adathalászatnál a gyanútlan felhasználóknak levelet küldenek, melyben utasítják őket, hogy hívják fel azt a számot, mely egy hivatalos telebank szolgáltatás számának néz ki. A hívást a tolvaj kapja meg.
    - A telefonon keresztül, hitelesítés céljából megadott bankszámlaszámot vagy jelszót így ellopják.

TÁMADÁS MÓDSZEREK

- Vírusok
  - A vírus egy program, mely lefut és más programok vagy fájlok módosításával terjed.
- Férgek
  - A féreg hasonló a vírushoz, de a vírustól eltérően nincs szüksége arra, hogy egy programhoz kapcsolódjon.
- Trójai lovak
  - A Trójai ló egy önmagát nem sokszorosító program, mely úgy készült, hogy hivatalos programként jelenjen meg, miközben valójában egy támadási eszköz.
- Nyers erő (Brute force)
  - A nyers erőt alkalmazó támadásnál egy gyors számítógép használatával kísérlik meg kitalálni a jelszavakat vagy visszafejteni egy titkosítási kódot.

TÁMADÁS MÓDSZEREK

- Szolgáltatás-megtagadás (Denial of Service, DoS)
  - A DoS támadások személyi számítógépek vagy számítógépek egy csoportja elleni agresszív támadások, melyeknek az a célja, hogy meggátolja a potenciális felhasználókat a szolgáltatások igénybe vételében. A gyakori DoS támadások:
    - SYN (szinkron) elárasztás - egy csomagáradat kerül elküldésre a kiszolgálóhoz kérve az ügyfél kapcsolódását. A csomagok érvénytelen forrás IP-címet tartalmaznak. A kiszolgálót teljesen lefoglalja az, hogy megpróbálja megválaszolni ezeket a hamis kéréseket és így nem képes válaszolni a valódiakra.
    - Halálos ping: egy olyan csomag kerül elküldésre az eszköznek, melynek mérete meghaladja az IP által megengedett méretet (65.535 bájt). Ez a fogadó rendszer összeomlását okozza.

TÁMADÁS MÓDSZEREK

- Nem minden támadás okoz károkat vagy akadályozza meg a hivatalos felhasználót abban, hogy hozzáférjen az erőforrásokhoz.
  - Bármely olyan program **kémprogram**, mely személyes információt gyűjt a számítógépről a hozzájárulásunk vagy tudomásunk nélkül.
  - A (**cookie**) a kémprogram egy formája, de nem mindig rossz-szándékú.
  - A **reklámprogram** (adware) a kémprogram egy olyan formája, melyet egy felhasználóról történő információgyűjtésre használnak azokra a webhelyekre alapozva, melyeket a felhasználó meglátogat.
  - Az **előugró** (pop-up) és **mögé nyíló** (pop-under) ablakok olyan újabb ablakok, melyek akkor jelennek meg, amikor meglátogatunk egy webhelyet.
  - A termékértékesítésnek ezen a széleskörű terjesztésen alapuló megközelítését az Interneten **levélszemétnek** (spam) hívják.

A BIZTONSÁGPOLITIKA

- A biztonsági kockázatok nem küszöbölhetők ki vagy nem védhetők ki teljes mértékben.
- A kockázat mértékének minimalizálása céljából fontos, hogy egyedül egy termék nem tehet egy szervezetet biztonságossá.
- Valódi hálózati biztonság a termékek és szolgáltatások kombinációját egyesítő átfogó biztonságpolitikából és a politikához való ragaszkodásra való elkötelezettségből származik.
- **A jelszavak feleljenek meg a minimumkövetelményeknek és rendszeresen módosításra kerüljenek**!

HÁLÓZATI BIZTONSÁG

- A hálózati biztonság megvalósításában használt alkalmazások és biztonsági eszközök:
  - Szoftver kiegészítések és frissítések
  - Vírusvédelem
  - Kémprogramok elleni védelem
  - Levélszemét szűrők
  - Előugró ablak blokkolók
  - Tűzfalak

HÁLÓZATI BIZTONSÁG

- Tűzfal
  - Egy biztonsági eszköz, mely a hálózatba befelé vagy onnan kifelé irányuló forgalmat ellenőrzi.
- Levélszemét szűrő
  - Egy végfelhasználói munkaállomáson vagy kiszolgálón telepített szoftver a nemkívánatos elektronikus levelek azonosítására és eltávolítására. A levélszemét-irtó szoftver azonosítja a levélszemetet, majd szeméttároló mappába (karanténba) helyezi vagy törli.
- Kiegészítések és frissítések
  - Egy OS vagy alkalmazás számára felhasznált szoftver egy ismert biztonsági hiányosság kiküszöbölésére vagy újabb feladatok ellátására. A hekker (hacker) leggyakrabban a szoftverek sebezhető pontjait használják ki.
    - A kiegészítés (patch) egy kis kódrészlet, amely egy meghatározott problémát orvosol.
    - A frissítés pedig új szolgáltatásokkal egészíti ki a teljes szoftvercsomagot amellett, hogy a meghatározott problémák javítását is elvégzi.

HÁLÓZATI BIZTONSÁG

- Kémprogram-írtó
  - Egy végfelhasználói munkaállomáson telepített szoftver a kémprogramok és reklámprogramok észlelésére és eltávolítására. A kémprogramirtó szoftver észleli és törli a kémprogram alkalmazásokat, valamint meggátolja a jövőbeni telepítésüket. Számos kémprogramirtó alkalmazás tartalmazza a sütik (cookie) és reklámprogramok (adware) észlelésének és törlésének lehetőségét is.
- Előugró ablak blokkoló
  - Egy végfelhasználói munkaállomáson telepített szoftver az előugró és mögé-nyíló hirdetési ablakok megjelenésének kiküszöbölésére. Számos webböngészőbe már beépítették az előugró ablak blokkoló szolgáltatást.
- Vírusirtó
  - Egy végfelhasználói munkaállomáson telepített szoftver a vírusok, férgek és Trójai lovak észlelésére és az állományokból illetve elektronikus levélből történő
  - eltávolítására. Néhány tulajdonság, mellyel a vírusirtó programok rendelkeznek:
    - Elektronikus levél ellenőrzése - átvizsgálja a bejövő és kimenő leveleket és azonosítja a gyanús mellékleteket.
    - Memóriarezidens dinamikus vizsgálat - ellenőrzi a végrehajtható fájlokat és dokumentumokat, amikor azokhoz hozzáférnek.
    - Ütemezett vizsgálat - a víruskeresést ütemezni lehet, hogy szabályos időközönként lefusson és ellenőrizze a kiválasztott meghajtókat vagy az egész számítógépet.
    - Automatikus frissítés - utánanéz és letölti az ismert vírusjellemzőket és mintákat. Ütemezni lehet, hogy a frissítéseket szabályos időközönként ellenőrizze le.

TŰZFALAK

TŰZFALAK

- személyi számítógépek és kiszolgálók védelmén kívül fontos a hálózatba érkező és onnan kimenő forgalom ellenőrzése is.
- A tűzfal az egyik leghatékonyabb olyan biztonsági eszköz, mely a belső hálózati felhasználók külső veszélyektől való megvédésére hasnálunk.
- A tűzfal két vagy több hálózat között helyezkedik el és ellenőrzi a közöttük zajló forgalmat, valamint segíti a jogosulatlan hozzáférés elleni védelmet.
  - **Csomagszűrés** - az IP vagy MAC-cím alapján akadályozza meg vagy engedélyezi a hozzáférést.
  - **Alkalmazás/Webhely** szűrés - Az alkalmazás alapján akadályozza meg vagy engedélyezi a hozzáférést. A webhelyek, egy meghatározott weblap URL címe vagy kulcsszavak alapján blokkolhatók.
  - **Állapot-alapú** csomagvizsgálat (Stateful Packet Inspection, SPI) - A bejövő csomagok csak a belső hálózat állomásairól kezdeményezett kérések válaszcsomagjai lehetnek. A nem kívánatos csomagokat külön engedély hiányában kiszűri. Az SPI felismerhet és kiszűrhet bizonyos típusú támadásokat is (pl.: DoS).

TŰZFALAK

- Ezen kívül a tűzfalak gyakran hálózati címfordítást (Network Address Translation, NAT) is végeznek.
- A NAT egy belső címet, vagy címek csoportját egy olyan külső, nyilvános címre fordítja, mely a hálózaton keresztül továbbítva lesz. Ez lehetővé teszi a belső címek külső felhasználók elől való elrejtését.
- A tűzfal termékek számos különböző formában készülnek:
  - Eszköz-alapú tűzfal - az eszköz-alapú tűzfal egy **biztonsági készülékként** ismert célhardverbe van beépítve. Nem rendelkezik perifériával és merevlemezzel.
  - Kiszolgáló-alapú tűzfal - a kiszolgáló-alapú tűzfal egy **tűzfalalkalmazás**, amely valamilyen hálózati operációs rendszer alatt fut (Network OS: UNIX, Windows, Novell). Kevésbé biztonságos az általános célú OS biztonsági hiányosságai miatt.
  - Integrált tűzfal - az integrált tűzfal egy meglevő eszköz (pl.: forgalomirányító) tűzfalszolgáltatással kiegészítve. Az integrált forgalomirányítók rendelkeznek alapvető tűzfal szolgáltatással (csomag, alkalmazás, webhely szűrés)
  - Személyes tűzfal - a személyes tűzfal a munkaállomáson helyezkedik el, nem LAN megvalósításra tervezték. Lehet az operációs rendszer beépített szolgáltatása, vagy származhat külső gyártótól is.

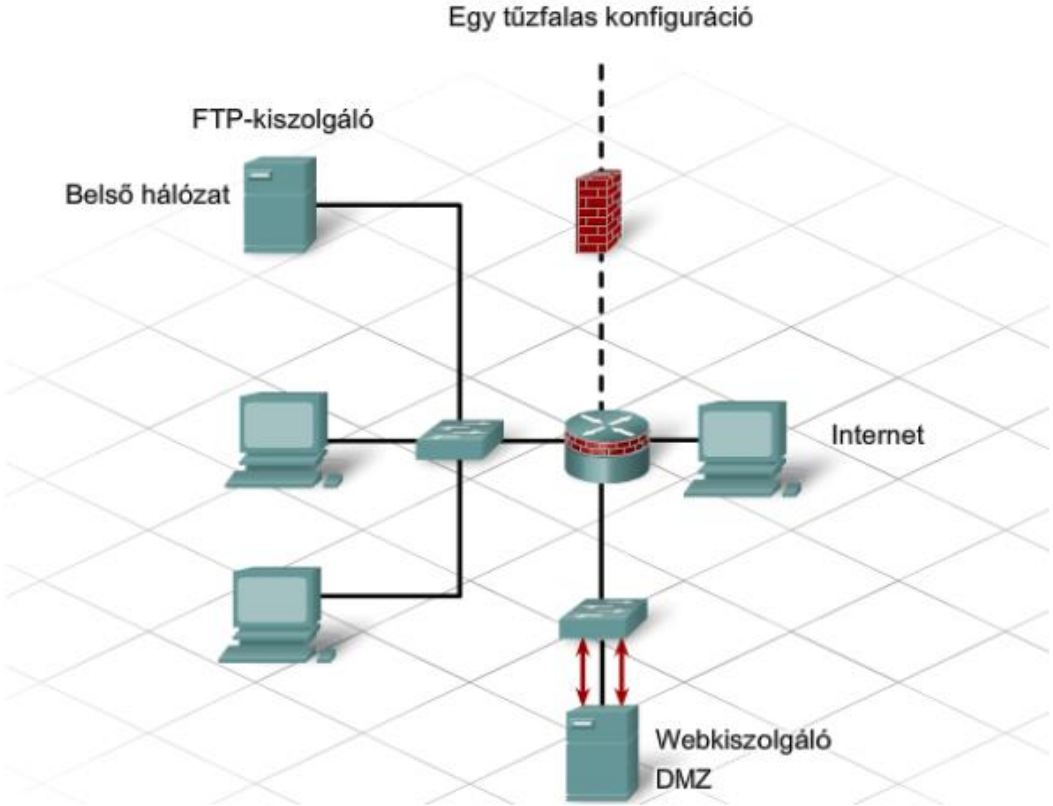
TŰZFALAK

- A tűzfalaknak, mint határkészüléknek, a belső hálózat (intranet) és az Internet közé helyezésével minden kifelé és befelé irányuló Internet forgalom megfigyelhető és ellenőrizhető.
- Ez egyértelmű védelmi vonalat létesít a belső és külső hálózat között. Mindemellett néhány külső ügyfélnek szüksége lehet a belső erőforrások használatára. Ennek biztosítására lehet kiépíteni a demilitarizált zónát (DMZ).
  - A demilitarizált zóna kifejezés a hadseregtől lett kölcsönözve, ahol a DMZ két haderő között kijelölt olyan terület, ahol tilos katonai tevékenység folytatása.
- A számítógépes hálózatok világában a DMZ a hálózat egy olyan területére vonatkozik, mely mind a belső, mind a külső felhasználók számára hozzáférhető.
  - Biztonságosabb, mint a külső hálózat, de nem olyan biztonságos, mint a belső hálózat.
  - A belső hálózatot, a DMZ-t és a külső hálózatot egy vagy több tűzfallal különítik el.
  - A nyilvános hozzáférésű webkiszolgálókat gyakran a DMZ-ben helyezik el. Ide kerülhetnek a webkiszolgálók, FTP kiszolgálók, SMTP kiszolgálók, DNS kiszolgálók.
  - A belső hálózatot, a DMZ-t és a külső hálózatot egy vagy több tűzfallal különítik el.

EGYTŰZFALAS KONFIGURÁCIÓ

- Az egyedüli tűzfal három területtel rendelkezik, egy-egy területtel a külső hálózat, a belső hálózat, és a DMZ számára. Minden külső hálózatból származó forgalom a tűzfalhoz kerül elküldésre.
- A tűzfallal szembeni elvárás az is, hogy ellenőrizze a forgalmat és határozza meg, hogy mely forgalmat kell a DMZ-be, melyet kell a belső hálózatba továbbítani és melyet kell végképp elutasítani.
- Az egytűzfalas konfiguráció a kisebb, kevésbé terhelt hálózatokhoz megfelelő. Mindemellett az egytűzfalas konfiguráció egyetlen meghibásodási ponttal rendelkezik és túlterhelhető.

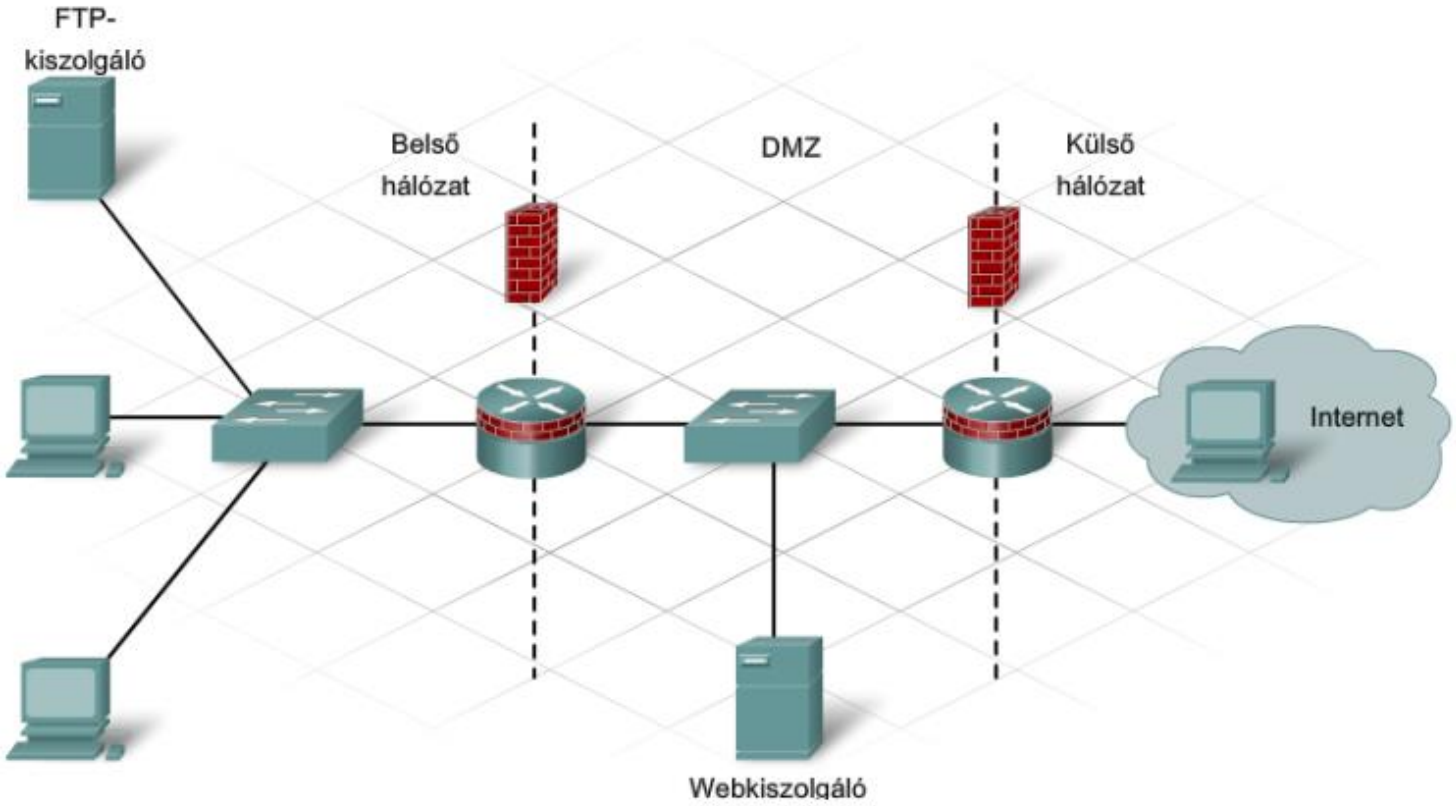
EGYTŰZFALAS KONFIGURÁCIÓ



KÉTTŰZFALAS KONFIGURÁCIÓ

- A két tűzfalas konfigurációnál egy belső és egy külső tűzfal található a kettőjük között elhelyezkedő DMZ-vel együtt.
  - A külső tűzfal kevésbé korlátozó és megengedi, hogy az Internet felhasználók hozzáférjenek a DMZ-ben levő szolgáltatásokhoz valamint megengedi, hogy bármely belső felhasználó által kért forgalom áthaladjon rajta.
  - A belső tűzfal jóval korlátozóbb és védi a belső hálózatot a jogosulatlan hozzáféréstől.
- A kéttűzfalas konfiguráció inkább az olyan nagyobb, összetettebb hálózatok számára alkalmas melyek jóval nagyobb forgalmat bonyolítanak le.

KÉTTŰZFALAS KONFIGURÁCIÓ



TŰZFALAK

- Sok otthoni eszköz, mint például egy integrált forgalomirányító, gyakran többfunkciós tűzfalszoftvert tartalmaz.
  - Az ilyen tűzfal jellemzően hálózati címfordítás (Network Address Translation, NAT), állapot alapú csomagvizsgálat (Stateful Packet Inspection, SPI), és IP, alkalmazás és webhely szűrő képességgel rendelkezik.
  - Ezen kívül támogatja a DMZ lehetőségét is.

PROXY

- ***Proxy**: Speciális tűzfal-típus, amely a közvetlen kommunikációt a külső és a védett hálózat között nem teszi lehetővé. E helyett a belső hálózatról érkező kéréseket feldolgozza, majd azokkal azonos értelmű kérést küld a külső szerver felé, az azokra érkező válaszokat pedig ismét a belső hálózat felé továbbítja. A proxy szerverek igen biztonságosak és általában egyszerűen konfigurálhatóak, azonban kizárólag olyan jellegű kommunikációra alkalmasak, aminek értelmezésére képesek. A proxy szerverek sok esetben tartalmi gyorsítótárat is magukban foglalnak, így bizonyos esetekben jelentős mértékben csökkenthetik a kifelé irányuló forgalmat.*

- ***Anonim proxy**: Az eredeti webező identitásának elrejtésére alkalmas proxy kiszolgáló. Az anonim proxy működésének lényege, hogy a webszerver és a böngésző közti kommunikációba harmadik félként beépül olyan módon, hogy valójában ő tölti le a kiszolgálóról a kliens által kért weblapokat, amiket persze továbbít annak részére. Mivel azonban így a kiszolgáló közvetlenül csakis a proxy szerverrel áll kapcsolatban, a tényleges böngésző identitása (IP-címe) a szerver elől rejtve maradhat*

VÉDEKEZÉS

A SEBEZHETŐSÉG ELEMZÉSE

- Az állomások és a hálózat biztonságának ellenőrzésére számos elemző eszköz áll rendelkezésre. Ezek a biztonságvizsgálóként ismert eszközök segítenek azoknak a területeknek az azonosításában, ahol támadás jelentkezhet, és iránymutatást adnak a teendő óvintézkedésekre.
- A sebezhetőség vizsgáló eszköz szolgáltatásai gyártótól függően változhatnak, közös szolgáltatásaik közé tartoznak:
  - A hálózaton rendelkezésre álló állomások számának megadása.
  - Az állomások által nyújtott szolgáltatások felsorolása.
  - Az állomás operációs rendszerének és verziószámának megadása.
  - A használt csomagszűrők és tűzfalak megadása.

MÓDSZEREK

- Számos módszer létezik a kockázatcsökkentés elősegítésére.
  - Határozzuk meg a biztonsági irányelveket.
  - Fizikailag védjük a kiszolgálókat és a hálózati berendezéseket.
  - Állítsuk be bejelentkezési és fájlhozzáférési engedélyeket.
  - Frissítsük az OS-t és az alkalmazásokat.
  - Változtassuk meg a megengedő alapbeállításokat.
  - Futtassuk le a vírusirtót és a kémprogram-irtót.
  - Frissítsük a vírusirtó szoftvert.
  - Kapcsoljuk be a böngésző biztonsági eszközeit - előugró ablakok (pop-up) blokkolása, adathalászat szűrő, beépülő modulok ellenőrzése.
  - Használjunk tűzfalat.

MÓDSZEREK

- A hálózat biztonságának irányába tett első lépés, hogy tisztában legyünk a forgalom haladásával a hálózaton keresztül, és hogy megismerjük a különböző veszélyforrásokat és a sebezhető pontokat.
- A biztonsági intézkedések megvalósítása után, egy valóban biztonságos hálózat megköveteli a folyamatos megfigyelést. A biztonsági eljárásokat és eszközöket folyamatosan felül kell vizsgálnunk, hogy lépést tudjunk tartani az egyre fejlődő fenyegetésekkel.

TÖRVÉNY

TÖRVÉNY

TÖRVÉNY

- Következő részben a Szlovákiai törvényrendszerer lesz foglalkozva. Ebből kifolyólag, csak szlovák nyelven fogjuk a törvény paragrafusait idézni!

- Zákon č. 300/2005 Z. z. Trestný zákon Slovenskej Republiky

§ 247 NEOPRÁVNENÝ PRÍSTUP DO POČÍTAČOVÉHO SYSTÉMU

- (1) Kto prekoná bezpečnostné opatrenie, a tým získa neoprávnený prístup do počítačového systému alebo jeho časti, **potrestá sa odňatím slobody až na dva roky.**
- (2) Odňatím slobody **na jeden rok až päť rokov** sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a spôsobí ním značnú škodu.
- (3) Odňatím slobody **na tri roky až osem rokov** sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
  - a) a spôsobí ním škodu veľkého rozsahu, alebo
  - b) ako člen nebezpečného zoskupenia.

§ 247a NEOPRÁVNENÝ ZÁSAH DO POČÍTAČOVÉHO SYSTÉMU

- (1) Kto obmedzí alebo preruší fungovanie počítačového systému alebo jeho časti
  - a) neoprávneným vkladaním, prenášaním, poškodením, vymazaním, zhoršením kvality, pozmenením, potlačením alebo zneprístupnením počítačových údajov, alebo
  - b) tým, že urobí neoprávnený zásah do technického alebo programového vybavenia počítača a získané informácie neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu, **potrestá sa odňatím slobody na šesť mesiacov až tri roky**.
- (2) Odňatím slobody **na tri roky až osem rokov** sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
  - a) a spôsobí ním značnú škodu,
  - b) a spôsobí ním vážnu poruchu v činnosti štátneho orgánu, orgánu územnej samosprávy, súdu alebo iného orgánu verejnej moci,
  - c) tak, že zneužije osobné údaje iného s cieľom získať dôveru tretej strany.
- (3) Odňatím slobody **na štyri roky až desať rokov** sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
  - a) a spôsobí ním škodu veľkého rozsahu,
  - b) a spôsobí ním vážnu poruchu v kritickej infraštruktúre, alebo
  - c) ako člen nebezpečného zoskupenia.

§ 247b NEOPRÁVNENÝ ZÁSAH DO POČÍTAČOVÉHO ÚDAJA

- (1) Kto úmyselne poškodí, vymaže, pozmení, potlačí alebo zneprístupní počítačové údaje alebo zhorší ich kvalitu v rámci počítačového systému alebo jeho časti, potrestá sa odňatím slobody **na šesť mesiacov až tri roky**.
- (2) Odňatím slobody na **tri roky až osem rokov** sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
  - a) a spôsobí ním značnú škodu,
  - b) a spôsobí ním vážnu poruchu v činnosti štátneho orgánu, orgánu územnej samosprávy, súdu alebo iného orgánu verejnej moci,
  - c) tak, že zneužije osobné údaje iného s cieľom získať dôveru tretej strany.
- (3) Odňatím slobody **na štyri roky až desať rokov** sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
  - a) a spôsobí ním škodu veľkého rozsahu,
  - b) a spôsobí ním vážnu poruchu v kritickej infraštruktúre, alebo
  - c) ako člen nebezpečného zoskupenia.

§ 247c NEOPRÁVNENÉ ZACHYTÁVANIE POČÍTAČOVÝCH ÚDAJOV

- (1) Kto neoprávnene zachytáva počítačové údaje prostredníctvom technických prostriedkov neverejných prenosov počítačových údajov do počítačového systému, z neho alebo v jeho rámci vrátane elektromagnetických emisií z počítačového systému, ktorý obsahuje takéto počítačové údaje, potrestá sa odňatím slobody **na šesť mesiacov až tri roky**.
- (2) Kto ako zamestnanec poskytovateľa elektronickej komunikačnej služby spácha čin uvedený v odseku 1 alebo inému úmyselne umožní spáchať taký čin, alebo pozmení alebo potlačí správu podanú prostredníctvom elektronickej komunikačnej služby, potrestá sa odňatím slobody **na jeden rok až päť rokov**.
- (3) Odňatím slobody **na tri roky až osem rokov** sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 alebo 2
  - a) z osobitného motívu,
  - b) závažnejším spôsobom konania, alebo
  - c) spôsobí ním značnú škodu.
- (4) Odňatím slobody **na štyri roky až desať rokov** sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 alebo 2
  - a) a spôsobí ním škodu veľkého rozsahu, alebo
  - b) ako člen nebezpečného zoskupenia.

§ 247d VÝROBA A DRŽBA PRÍSTUPOVÉHO ZARIADENIA, HESLA DO POČÍTAČOVÉHO SYSTÉMU ALEBO INÝCH ÚDAJOV

- (1) Kto v úmysle spáchať trestný čin neoprávneného prístupu do počítačového systému podľa § 247, neoprávneného zásahu do počítačového systému podľa § 247a, neoprávneného zásahu do počítačového údaja podľa § 247b alebo neoprávneného zachytávania počítačových údajov podľa § 247c vyrobí, dovezie, obstará, kúpi, predá, vymení, uvedie do obehu alebo akokoľvek sprístupní
  - a) zariadenie vrátane počítačového programu vytvorené na neoprávnený prístup do počítačového systému alebo jeho časti, alebo
  - b) počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do počítačového systému alebo jeho časti, potrestá sa odňatím slobody **až na dva roky**
- (2) Odňatím slobody **na šesť mesiacov až tri roky** sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a spôsobí ním značnú škodu.
- (3) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
  - a) a spôsobí ním škodu veľkého rozsahu, alebo
  - b) ako člen nebezpečného zoskupenia.

§ 189 VYDIERANIE

- (1) Kto iného násilím, hrozbou násilia alebo hrozbou inej ťažkej ujmy núti, aby niečo konal, opomenul alebo trpel, potrestá sa odňatím slobody **na dva roky až šesť rokov**.
- (2) Odňatím slobody **na štyri roky až desať rokov** sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
  - a) závažnejším spôsobom konania,
  - b) na chránenej osobe,
  - c) z osobitného motívu, alebo
  - d) a spôsobí ním väčšiu škodu.
- (3) Odňatím slobody **na desať rokov až dvadsať rokov** sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
  - a) a spôsobí ním ťažkú ujmu na zdraví alebo smrť, alebo
  - b) a spôsobí ním značnú škodu.
- (4) Odňatím slobody **na dvadsať rokov až dvadsaťpäť rokov alebo trestom odňatia slobody na doživotie** sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
  - a) a spôsobí ním ťažkú ujmu na zdraví viacerým osobám alebo smrť viacerých osôb,
  - b) a spôsobí ním škodu veľkého rozsahu, alebo
  - c) ako člen nebezpečného zoskupenia.

§ 201 SEXUÁLNE ZNEUŽÍVANIE

- § 201a
  - Kto prostredníctvom elektronickej komunikačnej služby navrhne dieťaťu mladšiemu ako pätnásť rokov osobné stretnutie v úmysle spáchať na ňom trestný čin sexuálneho zneužívania alebo trestný čin výroby detskej pornografie, pričom sám nie je dieťaťom, potrestá sa odňatím slobody **na šesť mesiacov až tri roky**.
- § 201b
  - Kto zneužije dieťa mladšie ako pätnásť rokov v úmysle vyvolania sexuálneho uspokojenia jeho účasťou na sexuálnych aktivitách alebo sexuálnom zneužití, hoci sa na nich takéto dieťa nemusí priamo zúčastňovať, alebo kto umožní také jeho zneužitie, **potrestá sa odňatím slobody až na dva roky**.

+ TÖBB AMI ÖSSZEFÜGHET

- § 221 – Podvod
- § 211 – Ohrozovanie mravnej výchovy mládeže
- § 230 – Nepovolená prevádzka lotérií a iných podobných hier
- § 283 – Porušovanie autorského práva
- § 296 – Založenie, zosnovanie a podporovanie zločineckej skupiny
- § 337 – Podnecovanie
- § 360 – Nebezpečné vyhrážanie
- § 369 – Rozširovanie detskej pornografie
- § 373 – Ohováranie
- § 422a – Výroba extrémistického materiálu
- § 424 – Podnecovanie k národnostnej, rasovej a etnickej nenávisti
- … iné

Idő a kérdésekre, diszkusszióra

Összefoglaló:

- Támadások
- Védelem
- Tűzfalak

https://www.kaspersky.com/blog/amazing-internet-maps/10441/

Selye János Egyetem
Informatika Tanszék
Gazdaságtudományi és
Informatakai Kar
Hradná 21.
945 01 Komárom

Számítógépes hardver 3
(Számítógépes hálózatok)
KIN/PS/IN/12
Kreditszám: 4
Tanulmány szintje: I.

13

előadás

KÖSZÖNÖM A MEGTISZTELŐ FIGYELMÜKET

Ing. Ondrej Takáč, PhD.
Informatika Tanszék
Gazdaságtudományi és Informatakai Kar
Selye János Egyetem
takac.ondrej@gmail.com
+421 35 32 60 629