ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel

Hálózatok Biztonsága

Frész Ferenc, Kálovics Tamás, Puha Gábor

Nemzeti Közszolgálati Egyetem

Budapest, 2014

Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

Tartalomjegyzék

1 Bevezetés

A számítógép hálózat egy határokkal rendelkező mérnöki alkotás szokott lenni, de manapság a legtöbb hálózati környezetnek nincs egyértelműen leírható határa. Ennek egyik oka, hogy a mai kommunikációs eszközök már teljes értékű számítógépek (okos telefonok, tábla PC-k, orvosi eszközök telemetrikus EKG, -vércukormérő, Leonardo műtőrobot). Ezek az eszközök már elhagyják a munkahelyi környezetet. Ma már virtuális irodai környezetben folyik a munka, akár útközben, akár otthonról vagy az ügyféltől. A tevékenység-kihelyezés (outsourcing) is megnöveli a hagyományos értelemben vett hálózatok határait.

A hálózatok minden esetben az elsődleges „immunrendszerét" adják a számítógépes rendszereknek. A vírusok, malware-ek nagyrészt a hálózatokon keresztül fertőznek. Így ha az első védelmi vonal – a hálózatok – jól működik, akkor a fertőzés megállítható. A hálózatok védelme ugyanilyen szereppel szolgál az információ-szivárgás –például: ipari kémkedés – esetén. Ha a hálózati forgalomelemzés kimutatja a visszaélést vagy a támadás előkészületeit, akkor ideális esetben rögtön megszakítható a visszaélés. Megfelelő logelemzési gyakorlattal és folyamatos monitorozással előre lehet jelezni a támadásokat. Ezért mindenképpen úgy kell tekinteni a hálózatokra, mint a védelem első vonalára.

Tökéletes védelem nem létezik, minden esetben a kockázat arányos védekezést kell megvalósítani. *Megjegyzés: tökéletes védelem végtelen mennyiségű erőforrással valósítható meg*. Azonban egy jól megtervezett, felépített és folyamatos monitorozással üzemeltetett hálózat jelentős **csillapítás**t gyakorol a rosszindulatú hálózati forgalom ellen.

A *Hálózat Biztonság* tananyag célja, hogy a **kormányzati informatikai biztonsági szakértő**knek egy magas szintű, átfogó képet adjon a hálózat biztonságáról, a hálózat ellen irányúló támadásokról és a védelmi teendőkről a magyar jogi környezetben. Konkrét megoldási javaslatok bemutatása nem célja az anyagnak, mivel annak implementálása az üzemeltető feladata. A bemutatásra kerülő támadás elhárítási teendők célja annak érzékeltetése, hogy napi tevékenység során az adminisztrátorok képesek eliminálni a leggyakoribb támadásokat.

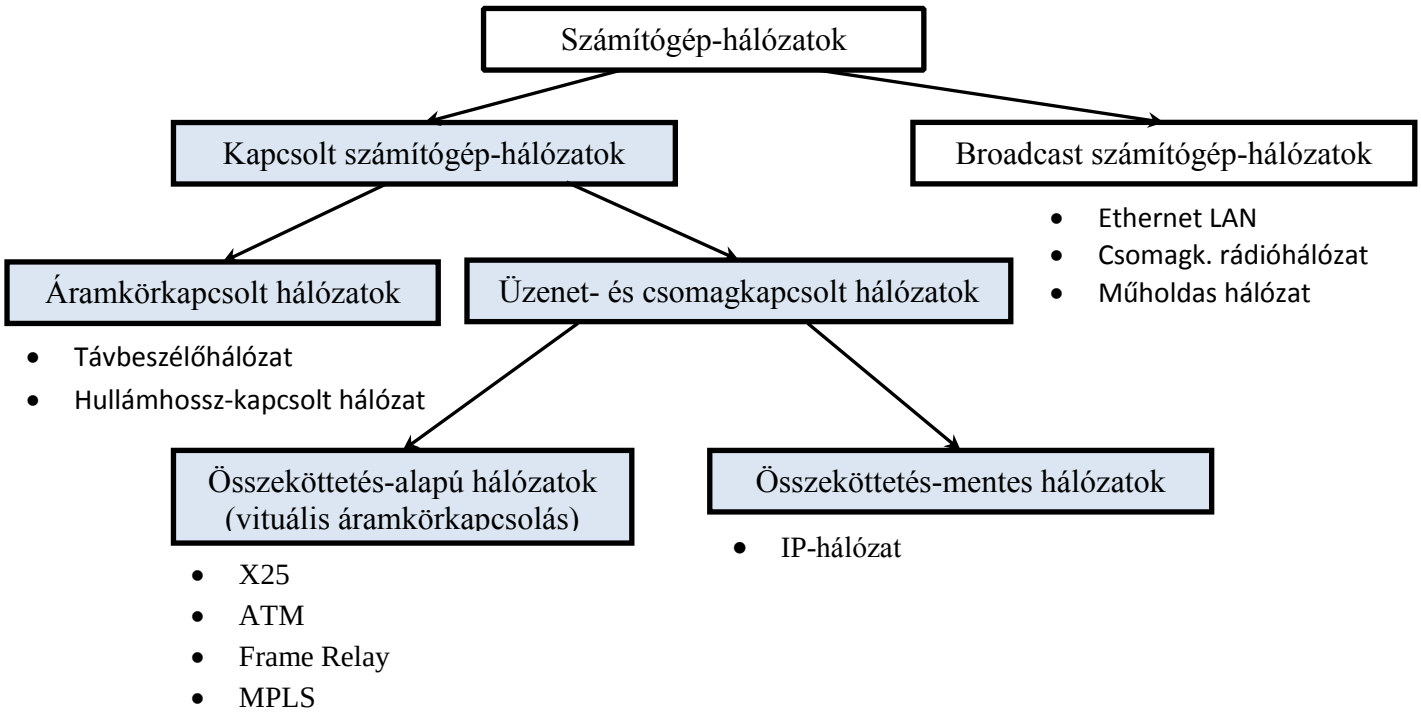
1.1 Informatikai és távközlő hálózatok

A mai információs társadalom elengedhetetlen kelléke a gyors információ-csere. A technika fejlődése során pont-pont kapcsolattól (távíró, telefon), pont-multipont kapcsolatokon keresztül (műsorszórás, rádió, tv) eljutottunk a multipont-multipont kommunikációhoz (konferenciahívás, közösségi hálózatok üzenőfalai, stb.). Az X generáció után már Y generációról, Web 2-ről (közösség alapú) és Web 3-ról (szemantikus Web) beszélünk.

A felhasználók információ-éhségét a távközlő hálózatok elégítik ki. A távközlő hálózatok különféle távközlési rendszerelemek összekapcsolásával, az átviteli és kapcsolási funkciók megvalósításával jönnek létre. A távközlő hálózatok egyidejűleg nagyszámú összeköttetést és különböző szolgáltatásokat képesek kiszolgálni. A kapcsolatok lehetnek egyirányúak és kétirányúak. A távközlő hálózat jellegét, méretét,

kapacitását, architektúráját a kiszolgált felhasználók száma, földrajzi eloszlása és a szolgáltatás minőségi igényei, forgalmi tulajdonságok határozzák meg.

Az igények óriási növekedése generálta a hálózati eszközök és technológiák gyors fejlődését. A kezdetekben célirányos hálózatok, mint távbeszélő-hálózat, adathálózat és műsorelosztó hálózat, mára egybeolvadtak. Például a valós idejű IP hálózatok; IP alapú telefon, adat és műsorszóró szolgáltatás is elérhető ugyanazon a médiumon. Az igények ma legmeghatározóbbja a mobilitás, a megszokott szolgáltatásokat földrajzi elhelyezkedéstől függetlenül, mozgás közben szeretnék elérni a felhasználók. Az informatikai és távközlő hálózatok, az összeköttetés megvalósítása alapján is megkülönböztethetőek, lásd következő ábra.



1. ábra Számítógép hálózatok kapcsolat és összekötetés szerinti osztályozása

1.2 Biztonság

A biztonság, mint fogalom, mindenkinek mást jelent. Így van ez az informatikai biztonság esetén is. A felhasználóknak legtöbbször a biztonság, a szolgáltatás meglétét, elérését jelenti (**rendelkezésre állás**), ugyanakkor a családi képek esetén a biztonság a digitális fotók „örök időkre" való elmentését is jelenti, változatlan minőségben (**sértetlenség**). A biztonság kompromittáló fotók esetén a tulajdonosnak a **bizalmasság**ot takarja, azaz illetéktelenek ne férhessenek hozzá.

Itt el is érkeztünk az információ-biztonság három fő alapelvéhez, a CIA-szabályhoz,(Confidentiality, Integrity, Availability) Bizalmasság, Integritás és Rendelkezésre-állás. E három alapelvből levezethető az információ-biztonság minden további esete.

Információ-biztonság tekintetében a fenti példában említett digitális fotók megőrzése jelenti az adatok veszteség nélküli megőrzését, azaz adatbiztonságot. Az erre épülő iparág az adatok (redundáns) mentésével és megőrzésével foglalkozik. Az adatmentés megvalósítására a kormányzatban is a kész megoldások vásárlása és implementálása a gyakorlat.

Ugyanakkor a biztonság egy rosszindulatú támadó számára azt jelenti, hogy tevékenysége nem kerül napvilágra – eltekintve a „megrendelőtől" – nem vonják törvényesen felelősségre tettéért. Természetesen a hálózat (rendszerek) üzemeltetőinek az ilyen biztonság nem érdeke, hanem ennek ellenkezője. Az üzemeltetők elsődleges feladata a támadások kialakulásának **megelőzés**e és másodsorban a támadások/incidensek **utólagos kezelése**. A támadások felderíthetőségének biztosítása és a támadó felelősségre vonásának feltétele a hálózati események **nyomon követhetőség**e. A nyomon követhetőséget a napló-, és log fájlok biztosítják. Ma már ismert, hogy adott nemzetek által felállított szervezetek is végeznek infokommunikációs **támadás**okat, egyfajta „megelőző" védelmi intézkedésként.

Az üzemeltetés során alkalmazott védelmek lehetnek védekező és támadó védelmi megoldások. Sok metodika foglalkozik offensive (támadás) alapú védelemmel, de jelen tananyagnak nem célja, és a magyar-, EU-s jogi szabályozás sem engedi a támadások végrehajtását. A defensive (védekező) védelem során is két alapesettel kell foglalkozni; a lehetséges támadási felületek megszüntetésével (**megelőzés**), és az esetlegesen bekövetkezett **incidensek kezelés**ével.

1.3 Hálózatok biztonsága

A hálózatok és a biztonság fogalmainak bevezetése során érzékelhető, hogy sokféle szempont szerint csoportosítható a hálózatok biztonsága. A kormányzati informatikai hálózatok esetén, ahogy a tananyag célja is, a **biztonságos üzemeltetés** és a **nemzeti adatvagyon védelme** a cél, az incidensek megelőzése és bekövetkezésük esetén a gyors érdembeli kezelése.

Az Internet kialakulása során a biztonság mindig utólagosan felmerült igény volt. Minden esetben feltételezték a jószándékú felhasználást a hálózat, a protokollok és az eszközök tervezői. Sok esetben utólag derült ki egy-egy protokollról, megoldásról, hogy sérülékeny biztonsági szempontból.

A jószándék feltételezése és a rohamosan fejlődő igények és megoldások kényszerítették ki a biztonsági hiányosságokat.

2 Hálózati alapismeretek

2.1 Technikai szabályozás

Hogyan és miért képesek működni a hálózatok? Természetesen adott szabály-, követelményrendszernek meg kell felelnie a hálózatnak és a hálózatot felépítő minden részegységeknek is. A világon több szervezet foglalkozik a hálózatok szabványosításával. Sok esetben a szabványban előírt

követelményeknek csak egy részhalmazát teljesítik a hálózati készülék. A legnagyobb hálózat szabványosító szervezetek az IEEE (Institute of Electrical and Electronics Engineers), IETF (Internet Engineering Task Force), ISO (International Standardization Organization), ANSI (American Standardization Organization), ITU (International Telecommunication Union), ETSI (Europian Telecommunication Standard Institute).

Az IETF munkacsoportokban dolgozik és RFC (Request for Comment) dokumentumokban rögzítik munkájukat. Az RFC-k nyilvánosan elérhetőek. Gyakran már a végleges verzió megszületése előtt az új termékek követelményrendszereként használják fel az RFC-ket.

Az IEEE is munkacsoportokban dolgozik, általában létező megoldások, termékek szabványosításával foglalkozik (de facto>> de jure). Természetesen a gyakorlat során felmerült problémák kiküszöbölésére újabb munkacsoportokban találják meg a szabványosított megoldások (pl.: Wifi WEP titkosítás) hiányosságainak kiküszöbölését.

2.2 Jogi szabályozás

A technikai szabályozáson túl foglalkozni kell a jogi szabályozással is. Itt két alapvető dolgot érdemes megemlíteni, az első milyen technikai szabályozásnak megfelelő készülék használata engedélyezett egy-egy nemzet területén, a második a technikai készülékek nem rendeltetésszerű használata esetén milyen jogorvoslatra, jogi szankcióra van lehetőség.

A távközlési eszközök használatának jogi szabályozásáért és a szabályok betartásáért Magyarországon elsősorban az NMHH (Nemzeti Média és Hírközlési hatóság) felel; például: engedélyköteles és szabad frekvenciasávok, adás teljesítmény, mobil-, internetszolgáltató esetén a forgalmi adatokra vonatkozó kötelező adatmegőrzések köre, időtartama; adott szolgáltatás esetén használandó titkosítási algoritmusok...

Jelenleg a ***2012. évi C. törvény a Büntető Törvénykönyvről* §422 (Tiltott adatszerzés), §423. (Információs rendszer vagy adat megsértése) és §424. (Információs rendszer védelmét biztosító technikai intézkedés kijátszása)** paragrafusai vonatkoznak az információs rendszert megtámadókra és az információs rendszerekkel visszaélőkre. Azaz §422-424/2012 évi C. tv. vonatkozik a hálózatokat megtámadókra és a hálózatokkal visszaélőkre is. *Figyelem:* ***a BTK 2012-ben megváltozott, a BTK300/C§*** *(Számítástechnikai rendszer és adatok elleni bûncselekmény) már* ***nem hatályos!***

Emellett meg kell említeni a **2013. évi L. törvényt** ***az állami és önkormányzati szervek elektronikus információ biztonságáról*** (továbbiakban: **Ibtv**). Az Ibtv szigorú előírásokat tartalmaz a kormányzat információs rendszereire, így a hálózatokra vonatkozóan is. Az Ibtv-ben előírt biztonsági intézkedéseket, technológiákat, ügyrendet felmenőleg kell implementálni a jelenleg is üzemelő rendszerekben. Erősen ajánlott az Ibtv és rendeleteinek tanulmányozása a kormányzati rendszereket üzemeltetők számára.

2.3 Protokollok

A hálózat által biztosított kommunikáció során adatcsere történik. Az adatcsere követelmény- és szabályrendszerét nevezzük protokolloknak. A protokollok írják le a végberendezések (pl.: telefon, fax, PC), a központok készülékei (pl.: telefon kapcsolóközpont) és az átviteli utak (1.-előfizetői hurok; 2.- központok közötti: trönk) szabályozását. A protokollok írják le a hálózati adatcserét, mely minden esetben két jól elkülönülő részből áll; statikus részből PDU (Protocol Data Unit = protokoll-adategység) ami az üzenetek szintaktikáját, szemantikáját írja le; és a dinakimus rész: adott üzenetek küldése/vétele esetén a teendőket és a kötelező teendőket írja le.

Ha végiggondolják, hogy milyen összetett feladat két végberendezés közötti kapcsolat felépítése (például IP alapú videotelefonhívás esetén) és a szolgáltatás biztosítása, akkor egyértelművé válik, hogy célszerű a protokollokat csoportosítani és rétegszerűen rendelni egymáshoz. Nagyon sok gyártó a kezdeti időkben a saját megoldásait használta: Appletalk, IBM token-ring, Novell Networks, Arcnet, Ethernet…A különböző gyártók operációs rendszerei és megoldásai között nehéz volt kapcsolatot létrehozni, például fájlokat átmásolni. Ezért szükségessé vált az interoperabilitási probléma megszüntetése. Az ISO OSI (Open System Interconnet – nyílt hálózatok összekapcsolása) 7 rétegű hálózati referencia modelljének célja a konformancia volt. Azonban az OSI csak ajánlás és a valóságban sehol nem implementálták teljes mértékben..

Az Internetet megalkotó ARPA (Advanced Research Projects Agency - Fejlett Kutatási Projektek Ügynöksége, később DARPA) hálózati modellje 4 rétegű. A valóságban is létezik, maga az Internet működésének leírása a **TCP/IP modell**, vagy más néven **Internet Protokoll Készlet**.

2.4 ISO OSI modell rétegei

Emlékeztetőül az alábbiakban átismételjük az egyes rétegek feladatait. Az OSI modell egy szabálygyűjtemény, amely leírja a protokoll készletet, hogyan történik az adatok kommunikációja és leírja a hálózati eszközöket, a hálózati eszközök működését is.

Alkalmazási réteg feladatai az felhasználó gépén az alkalmazások kiszolgálása. Az alkalmazások a hálózati szolgáltatásokat az alsóbb rétegeken keresztül érik el, így az alkalmazási réteg felel a kommunikációs partnerek meghatározásáért; az elérhető hálózati erőforrások meghatározásáért; a felhasználók közötti szinkronizációért; és a formátumok és biztonság egyeztetéséért. Az alkalmazási réteg ismert megvalósításai: HTTP, FTP, SMTP. Egy ismertebb példa a http szolgáltatás, általában a 80-as porton érhető el.

*A **port** (Szállítási réteg), mint címzési megoldás teszi lehetővé az egy IP címmel (Hálózati réteg) rendelkező számítógép több szolgáltatást is nyújtson. Három típusa van: jól ismert portok [0-1023]; regisztrált portok [1024-41951]; dinamikus (vagy privát) portok [49152-65535].*

Megjelenítési réteg felhasználói adatokat kezel, az adatok ábrázolásáért felel (szintaktikai ellenőrzés, adatábrázolás, operációs rendszerek miatti különbségek kezelése):adattitkosítás (kódolás-visszafejtés); adattömörítés (tömörítés-kibontás); fordítás kódlapok között (translation). Egy ismertebb példa az e-mailek Base64 kódolása-dekódolása.

Viszony réteg definíciója szerint a kapcsolat kezeléséért felel: kapcsolat iránya (duplex, fél-duplex, szimplex); kapcsolat felépítése-bontása; adatfolyamok szinkronizációja (az összetartozó adatfolyamok összehangolása). *Megjegyzés: ma már többnyire a szállítási rétegben valósítják meg a kapcsolatkezelési feladatokat.*

Szállítási réteg biztosítja a végpontok közötti megbízható kommunikációt. A hibamentes összeköttetést a hibás csomagok megismétlésével, a duplikált csomagok eldobásával, a csomag sorrendjének helyreállításával éri el.

Hálózati réteg feladata az egyedi kapcsolatok logikai összefűzése végpontok közötti csatornává; a csatornákra meghatározott QoS biztosítása több hálózaton keresztül is; logikai címzés: hálózati eszközök közötti kapcsolásokhoz; útvonalkeresés a hálózaton belül; forgalomirányítás és csomagjavítás.

A QoS (Quality of Service – szolgáltatás-minőség) a végpontok közötti átvitel tulajdonságainak biztosítása, mint a rendelkezésre állás, sávszélesség, késleletetés, késleltetés-ingadozás (jitter) és a csomagvesztés.

Adatkapcsolati réteg feladata: bitsorozatok kezelése, keretekbe foglalása; hibaellenőrzéshez szükséges adatok előállítása és lehetőség szerinti javítása; MAC címek kezelése a LAN (helyi hálózat) végpontjai közötti kommunikáció során. A LAN-ok közötti kommunikáció megvalósítása és a globális címzés a felsőbb rétegek feladata.

MAC (Message Access Control) hálózati interfész fizikai címét jelöli. Ethernet hálózat esetén a MAC 12 darab hexadecimális számból áll, amelyből az első 6 a gyártót azonosítja, a hátsó 6 pedig egyedi minden esetben.

Fizikai rétegben rögzítik a fizikai közeg (médium) specifikációját (feszültségszintek, hullámhosszak, kábeltulajdonságok, átviteli sebességek, csatlakozók, kábelek típusa…); bitek/bitcsoportok továbbítása a fizikai csatornán (vonali kódolás, moduláció); bitszinkron biztosítása.

2.5 OSI modell és az Internet Protokoll Készlet

Az OSI modell csak ajánlás, nem implementálták teljesen. A TCP/IP modell (más néven: Internet Protokoll Készlet) alapján működik az Internet. A két modell segít megérteni a hálózatok felépítését, működését. Az alábbi táblázat tartalmazza az OSI 7 rétegű és a TCP/IP 4 rétegű modelljének megfeleltetését. A protokollok kapcsán már említett PDU, azaz adategység rétegekhez rendelt specifikus nevét is tartalmazza a táblázat. Az adatkapcsolati rétegben **keret**, hálózati rétegben **csomag**, a szállítási rétegben **szegmens** és a felett maga az **adat** van.

1. táblázat: ISO OSI modell és a TCP/IP modell rétegei

OSI modell	TCP/IP modell	hálózati eszközök	címzés	PDU
Alkalmazás réteg	Alkalmazás réteg	Alkalmazás réteg Átjáró	munkamenet	Adat
Megjelenítési réteg				
Viszony réteg				
Szállítási réteg	Átviteli réteg (hoszt-hoszt)	4réteg-Kapcsoló	port	Szegmens
Hálózati réteg	Internet réteg	Útválasztó, 3réteg-Kapcsoló	IP cím	Csomag
Adatkapcsolati réteg	Hálózati hozzáférési réteg	Híd, Kapcsoló	MAC cím	Keret, Cella (ATM)
Fizikai réteg		Ismétlő, Hub		bit

2.6 Hálózati eszközök

Az OSI modell fizikai rétegét az **Ismétlő** (repeater) és Hub (több portos ismétlő) szolgálja ki. Feladata a jelerősítés, jelismétlés, nem rendelkezik semmilyen intelligenciával.

Az adatkapcsolati rétegben dolgozik a **Híd** (bridge) és a **Kapcsoló** (switch), ami valójában egy több portos Híd. A Híd különböző típusú hálózatok vagy hálózati szegmensek összekötésére alkalmas. A Híd képes a fizikai cím alapján (MAC) továbbítani a Kereteket a megfelelő portjára. Megjegyzés: itt a port a hálózati eszközön lévő aljzatot jelenti.

A hálózati rétegben dolgozik az **Útválasztó** és a **3. réteg-Kapcsoló** (layer 3 switch). Az Útválasztó a csomagokat ellenőrzi és a csomagban lévő IP cím alapján továbbítja a megfelelő irányba a csomagokat. A 3. réteg-Kapcsoló rendelkezik az Útválasztók és a Kapcsolók funkcióival. Ilyen eszköz az alkalmazás átjáró (application gateway).

A felsőbb rétegekben (OSI 5-7 rtg., Internet pk. Alkalmazási rtg.) lévő a feldolgozó eszközök az *adat* ellenőrzését, értelmezését végzik, természetesen az adat értelemzése során itt is előfordulhat címzés; email-cím, session-id; URL...

2.7 Hozzáférés Szabályozás

Hálózatok biztonságának első eszköze a hálózathoz történő **hozzáférés** korlátozása, **szabályozása** (access control)**.** A hozzáférés szabályozásnak két oka lehet; **anyagi** és **biztonsági**. Az anyagi ok esetén, csak azok a felhasználók érhetik el a hálózat szolgáltatásait, akik fizettek érte. A biztonsági okok azonosak az információ-biztonság kritériumaival: bizalmasság, sértetlenség, rendelkezésre állás.

A hozzáférés szabályozás (AAA) 3 dolgot valósít meg:

– Authentikáció (azonosítás), azaz ki léphet be

– Authorizáció (jogosultságkezelés), azaz mit csinálhat az authorizált/engedélyezett felhasználó

– Accountability (letagadhatatlanság), a felhasználó tevékenységének azonosítása/nyomon követése.

Az authentikáció háromféleképpen valósulhat meg: a felhasználó tud valamit (pl.: jelszó), a felhasználónak van valamije (pl.: token, authentikációs tanúsítvány) és a felhasználó valamilyen (pl.: retinaszkennelés, tenyér vénatérkép, ujjlenyomat, arcfelismerés).

Az authorizáció során dönti el a rendszer, hogy az azonosított felhasználónak mihez, milyen joga van. Például: Aladár felhasználó olvashatja a cég hálózati meghajtóját és nyomtathat az első emeleti nyomtatón és a vendég felhasználó csak a Guest-Wifi erőforrást használhatja. A jogosultságok karbantartása és nyomonkövetése a felhasználók számával exponenciálisan növekvő erőforrásokat igényel. Ezért alkalmazások és külön protokollok segítik ezt a munkát. Ma már minden több-felhasználós operációs rendszer rendelkezik felhasználó kezelővel és a hozzárendelt hozzáférési jogosultságokkal (access policy). Az útválasztókban ACL hozzáférési listákkal találkozunk, ahol definiálni lehet az engedélyezett forgalmat.

Accountability (letagadhatatlanság) a beléptetett (azonosított, authorizált) felhasználó tevékenységét követi nyomon. Ennek két célja van: egyrészt becsülni a szükséges erőforrásigényt, ezáltal optimalizálni az erőforrások felhasználását. Másrészt biztosítani a letagadhatatlanságot a naplózás által.

SSO(SingleSignOn - egyszeri belépés) több rendszer hozzáférési jogosultságának egy helyen történő, független megoldása. Ha egy felhasználó sikeresen belépett az egyik rendszerbe, akkor nem kell azonosítania magát a többi rendszerbe belépéskor. Ennek egyik megvalósítása az LDAP protokoll. Természetesen Webes technológiák esetén egy egyszerű süti (cookie) is megoldásul szolgálhat SSO-ra.

Az SSO biztonsági hiányosságai esetén a következmények halmozottak, mivel több rendszer hozzáférése kompromittálódik egyszerre. 2012 - Google ID, PayPal hozzáférések, a Facebook, a Farmville is érintett volt egy SSO sérülékenységben.

2.7.1 Hozzáférés szabályozás az OSI modell rétegeiben

1. A fizikai rétegben vezetékes hálózat esetén a kábel fizikai csatlakoztatása jelenti a hozzáférést. Vezeték nélküli kapcsolatok esetén (Wifi, Lifi, Micro, Lézeres átvitel) nem beszélhetünk a fizikai rétegben megvalósítható hozzáférés védelemről, mivel az elektromágneses sugárzás (fény és rádióhullám) a tér minden irányába terjed.

Egy különös esete a fizikai rétegben megvalósított hozzáférés szabályozás „hiányának” a **TEMPEST** általi passzív lehallgatás.

TEMPEST jelentése: Minden elektronikus eszköznek van elektromágneses kisugárzása. Megfelelően érzékeny vevővel ez a kisugárzás vehető és jelentése visszafejthető, értelmezhető jellé. Akár távoli monitorok képét is vissza lehet állítani. Ma már képesek WiFi eszközökkel megmondani a szomszád helyiségben lévő emberek pulzusát.

Ennek kivédésére kisugárzás védett eszközök használatát, vagy kisugárzás védett helységek használatát írja elő a nemzeti, NATO és EU szabályozás is minősített elektronikus rendszerek esetén.

Mit jelent a minősített adat [forrás: 2009. évi CLV. törvény a minősített adat védelméről]:

a) nemzeti minősített adat: a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést az e törvényben, valamint az e törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről - a megjelenési formájától függetlenül - a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére

hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt: károsítja), és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza;

b) b) külföldi minősített adat: az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza;

2. Az adatkapcsolati rétegben megvalósított hozzáférés szabályozás a fizikai cím (MAC) alapján történik. Mivel egy hálózati interfész kártya (NIC) fizikai címe drivertől függően megváltoztatható, így a MAC cím alapú hozzáférés szabályozás kijátszása egyszerű. Aktív hálózati megoldásokkal lehet védekezni a másolt, klónozott MAC ellen, melyek ujjlenyomat készítéssel és folyamatos monitorozással képesek kiszűrni a MAC elleni támadásokat.

3. A hálózati rétegben a hozzáférés szabályozás az IP cím alapján valósítható meg. Hálózati interfész IP címének beállítására alapvetően két megoldás lehetséges:a statikus és a dinamikus IP cím kiosztás. A tiltott, vagy illetéktelenül a hálózathoz csatlakozni kívánó eszközök kiszűrését port-security megadásával és aktív védelemmel – ujjlenyomat alapú azonosítással lehet megvalósítani.

4. A szállítási rétegben port alapján lehet hozzáférést szabályozni egy-egy hálózati interfész esetén. Természetesen egy rosszindulatú támadó eszköztárába tartozik a szolgáltatások felderítése (port-scan) és az elérhető szolgáltatásokhoz történő csatlakozás. Védelem szintjén a legfontosabb, hogy **a nem-használt szolgáltatásokat tiltsuk le**. Sok esetben az alapértelmezett telepítés (default install) operációs rendszer, alkalmazás, szerver, hypervisor esetén ez elérhető szolgáltatásokat eredményez. Gyakori megoldás **a nem publikus szolgáltatások esetén megváltoztatni az adott szolgáltatás portját.**

5-7 rétegek: A felsőbb rétegekben megvalósítható hozzáférés védelem függ a rétegben megvalósított technológiától. A TCP/IP modell alkalmazási rétegét tekintve, a hálózat korlátozásnak egy logikai módja van, a szolgáltatást megvalósító munkamenet azonosító (session ID) alapon lehet korlátozni a felhasználót, rosszindulatú támadót. Technológiától függően az egyre kifinomultabb támadások szinte minden 5.-7. rétegbeli protokoll gyengeségeit kihasználják. Nézzünk meg néhány gyakoribb protokollt és támadást:

5. A viszony rétegben valósul meg az SMB protokoll. Ez a protokoll a Windows rendszerek fájlmegosztását teszi lehetővé. Alapértelemezett telepítéskor az operációs rendszer elérhetővé teszi mások számára a Megosztott (Shared) könyvtárat. Gyakorlatlan felhasználó sok esetben megosztja a nyomtatóját, fotóit, zene állományait. Ha ide érzékeny fájlok kerülnek, akkor azok kompromittálódhatnak mások által, esetleg illegális tartalmakat másolhatnak kívülről ezekbe a megosztott könyvtárakba.

7. Az alkalmazási rétegben a hozzáférés kontroll megvalósításának bemutatására nézzük a rendszerüzemeltetők által gyakran használt SNMP protokollt. Az SNMP (Simple Network Management Protocol) a hálózati eszközök paramétereinek távoli lekérdezésére és beállítására szolgál. A rendszergazdák, hálózat üzemeltetők hatékony üzemeltetést megvalósító eszköze. Azonban az SNMP v1, v2a, v2b

authetikációja könnyen kijátszható, feltörhető, így egy rosszindulatú támadó rendszergazda jogokhoz juthat. Hatékony védelem az SNMP v2c és v3 verzió használata, megfelelő jelszó szabályzattal (feltéve hogy hálózatra kötött eszközeink támogatják ezen protokollokat).

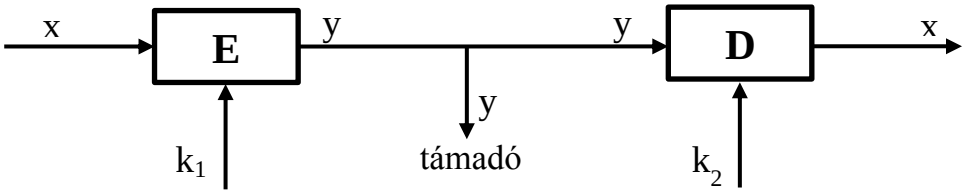
8. Nyolcadik rétegként meg kell említeni magát az embert, mint leggyengébb láncszemet. Leggyakrabban a felhasználó valamilyen felhasználónév/jelszó párossal és/vagy tokennel azonosítja magát. Azonosítás után pedig jogosultságainak megfelelő szerepkörben járhat el. Ha a felhasználó hanyag és a jelszavát a monitorra kiírva tárolja, akkor bárki, aki a géphez fizikailag hozzáfér, az eljárhat a nevében, megszemélyesítheti. Így hiába tett meg mindent a rendszerüzemeltető és a jól konfigurált hálózati eszköz, illetéktelenek mégis hozzáférhetnek a védett rendszerhez (hálózathoz, szerverhez, adatokhoz).

Megjegyzés: Egy gyakorlati példaként meg kell említenem a tárgyalókba lévő táblára felírt Wifi/egyéb hálózati hozzáférést biztosító felhasználó/jelszó párosokat. Az egyik legnagyobb magyar cég esetén, az irodaházon kívülről, az utcáról, távcsővel könnyen leolvasható volt a Wifi jelszó. Talán nem kell részletezni a biztonsági kockázatot – máris a belső hálózaton „találhatja" magát a támadó.

2.8 Kriptográfia alapfogalmak

Az alábbiakban csak a kriptográfia alapfogalmait tekintjük át, matematikai mélységek nélkül. Aki szeretné elsajátítani a téma elméleti, matematikai hátterét, azok olvassák *Buttyán Levente, Vajda István: „Kriptográfia és alkalmazásai" Typotex, Budapest, 2004* könyvét. Az említett könyvre támaszkodik jelen fejezet.

A **kriptológia** a titkos kommunikáció tudománya, amelynek két fő ága a **kriptográfia** és a **kriptoanalízis**. A kriptográfia az üzenetek titkosításával és hitelességével, a kriptoanalízis a titkok megfejtésével foglalkozó tudomány. Az információk védelmének az egyik alapja a kriptográfiai algoritmusok alkalmazása. Emellett fontos szerep jut a megfelelő **fizikai védelem**nek és **ügyviteli szabályozás**nak, azok **betartásá**nak. A kriptográfia az algoritmikus módszerek és protokollok alapja.



2. ábra A rejtjelzés modellje

A rejtjelzés célja a nem biztonságos kommunikációs csatornán továbbított üzenetek bizalmasságának, sértetlenségének biztosítása. Azaz, ha a támadó lehallgatja a csatornát, akkor sem lesz képes értelmezni, dekódolni az „elcsípett" üzenetet. Ha a támadó képes megváltoztatni az üzenet tartalmát, akkor azt a fogadó fél felismeri (és így a küldő fél is), a visszajátszott üzeneteket is felismerik. A hitelesség, letagadhatatlanság igénye is felmerül a biztonságos kommunikációhoz, erre is szolgál megoldással a

kriptográfia, például a digitális aláírással.Tekintsük át a rejtjelzés modelljét: **A** az ***x*** nyílt üzenetet szeretné elküldeni a nem biztonságos kommunikációs csatornán. Első lépésben az ***x*** üzenetre alkalmazza az $\mathbf{E_{(k)}(\ )}$ rejtjelző transzformációt (encryption, kódolás) és megkapja az ***y*** rejtett üzenetet,$\boldsymbol{y=E_{(k1)}(x)}$. A kódolás - $\mathbf{E_{(k)}(\ )}$ – transzformáció kölcsönösen egyértelmű adott ***k*** kulcs esetén. Az üzenet célba érkezésekor a kódoló transzformáció inverzét (decrypt, dekódolás) kell alkalmazni a nyílt szöveg visszanyeréséhez. $\boldsymbol{x = D_{(k2)}\ (y)}$.. Összefoglalva az **E** és **D** transzformációk ismeretében sem képes a támadó dekódolni az üzenetet a $\mathbf{k_2}$ kulcs ismerete nélkül.

Szimmetrikus kulcsú (hagyományos vagy titkos kulcsú) titkosításról beszélünk ha $\mathbf{k_1 = k_2}$. Ekkor a kulcsot valamilyen védett módon kell eljuttatni a kommunikáció résztvevőinek és hosszú távon is meg kell védeni a kulcsot, mivel későbbi kulcs kompromittálódás esetén a lehallgatott üzenetek később is visszafejthetőek.

Ha $\mathbf{k_1 \neq k_2}$, akkor aszimmetrikus kulcsú titkosításról beszélünk, ez esetben minden kommunikációs résztvevőnek kettő kulcsa van: egy $\mathbf{k^P}$ – nyilvános (public) kulcs és egy $\mathbf{k^S}$ titkos (secret) kulcs. A rejtjelzés modellje alapján úgy tudunk üzenetet küldeni **A**-ból **B**-nek, hogy ***x*** üzenetet **B** nyilvános kulcsával kódoljuk és azt csak a **B** által ismert **B** titkos kulcsával lehet dekódolni. $\boldsymbol{y = E(k^P_B)(x)}$ **és** $\boldsymbol{x = D(k^S_B)(y)}$. Természetesen a kriptoanalízis során adott protokollok és algoritmusok gyengeségeit, az algoritmus ismeretében könnyebb kihasználni. A nyilvános kulcsú titkosítás során megfelelő szabályozással kell eljárni a nyilvános kulcsok tárolásában és hozzáférhetőségének biztosításában. Azaz fontos, hogy megbízható forrásból jussunk hozzá adott kommunikációs partner nyilvános kulcsához. Például úgy is szabotálhatják a sikeres kommunikációt, hogy elhitetik a résztvevőkkel adott hamis nyilvános kulcsot igazinak.

A kriptográfiai módszerek elleni támadások az algoritmikus támadások, melyeket a kommunikációs csatornán hajt végre a támadó. Természetesen támadható nem algoritmikussan is a kriptográfia, ilyen a Social Engineering támadás. SocialEngineering során a támadó hozzáfér a titkos kulcsokhoz, úgy hogy a kulcs tulajdonosából „kibeszéli” – például attraktív hölgyek meggyőzőképességével bizalmas adatokat tudnak meg uriember áldozataiktól, vagy egészen a hónapokon át tartó előkészületekkel, az áldozat bizalmába férközve jutnak „használható” információhoz. Egy elgondolkodtató eredményekkel szolgáló felmérés során 2012-ben Angliában a járókelőket kérdezték jelszavaikról, 10EUR jutalomért 30% elmondott egy-egy általa használt otthoni/munkahelyi jelszót!

Kriptográfiai passzív támadáskor lehallgatják a rejtett szöveget. Akkor sikeres a támadás, ha sikerül visszafejteni a nyílt szöveget a rejtett szövegből. Ennek elégséges feltétele, ha a támadó megfejti a dekódoló kulcsot. Passzív támadások során az üzenetek kódolása ugyanazzal a kulccsal történik. A támadásokat három csoportba soroljuk, technikailag passzívak, mivel az átviteli csatornán egyébként is folyik a kommunikáció:

- **Rejtett szövegű támadás**. Ennél a módszernél a támadó csak a rejtett szöveghez fér hozzá és abból próbálja meg visszafejteni a dekódoló kulcsot, vagy kihasználni az adott protokoll hiányosságait a nyílt szöveg visszaállításához.

- **Ismert nyílt szövegű támadás**. Ekkor a támadó nyílt szöveg – rejtett szöveg párokat használ fel a támadáshoz.
- **Választott szövegű támadás**. Ennél a módszernél a támadó választja ki a nyílt szöveget és szintén nyílt szöveg – rejtett szöveg párokat használ a támadáshoz. A kommunikáció résztvevőit a támadónak rá kell vennie, hogy az általa választott nyílt szöveget küldje át.

Aktív támadásról akkor beszélünk, ha a kommunikációs csatornát manipulálni tudja a támadó: **üzenetet töröl, módosít** vagy **beszúr. Ez utóbbihoz tartozik a korábban lehallgatott üzenet visszajátszása is.**

A rejtjelzés a passzív támadások ellen véd. Az aktív támadások ellen a kriptográfiai protokollok védenek. Ez a korábban ismertetett protokollokhoz hasonlóan a kommunikáció előre meghatározott folyamatát szabja meg. Ezáltal észlelik az aktív támadásokat. Például az üzenetek szekvenciális védett sorszámával felismerik a visszajátszott üzeneteket.

A kriptográfiai fogalmak közül meg kell említeni a **gyakorlati titkosság**ot. Jelentése, hogy a támadó a lehetséges kulcsok ismeretében sem találja ki a sikeres támadáshoz szükséges kulcsot, mivel a kor mai számítási kapacitása mellett gazdaságtalanul sok időbe tellene.

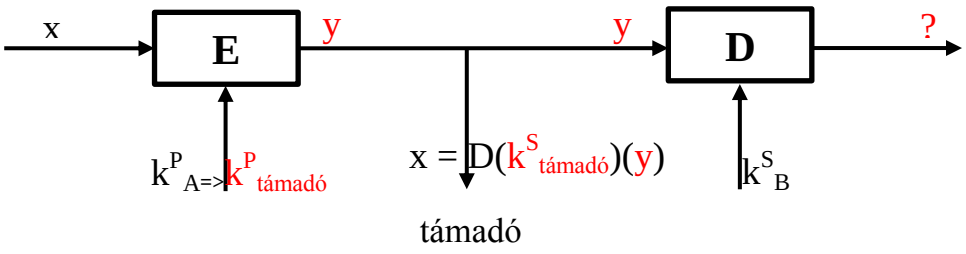
2.8.1 Kulcsmenedzsment

Fent már említésre került a kulcsok biztonságos megőrzésének fontossága, a későbbi kompromittálódás és visszafejtés miatt. Természetesen a titkosítás során használt kulcsokat cserélni kell, ennek több oka is van: ha túl sokáig használunk egy kulcsot, akkor megkönnyítjük a támadó dolgát; ha kompromittálódott a kulcs, akkor lecserélésével kiküszöbölhető újabb üzenetek kompromittálódása; ha nem tudjuk, hogy kompromittálódott a kulcs akkor is célszerű adott időközönként lecserélni. Ha **egy kulcsot lecserél**nek, akkor a továbbiakban **biztonságosan kell megőrizni, archiválni vagy biztonságosan kell megsemmisíteni**.

Nyilvános kulcsú titkosítás esetén a fentiek igazak a titkos kulcsra, de a nyilvános kulcs mindenki számára elérhető kell legyen, akivel kommunikálni szeretnénk. Miután a nyilvános kulcstárban (címtárban) bárki elhelyezheti saját nyilvános kulcsát, ezért fontos hiteles forrásból igazolni adott nyilvános kulcs kihez tartozik.

2.8.2 Nyilvános kulcsú titkosítás elleni támadások

Az egyik lehetséges támadási forma a nyilvános kulcsú titkosítás ellen, ha a címtárat támadják meg. A támadó „kicseréli”saját nyilvános kulcsára **B** résztvevő nyilvános kulcsát. Azaz a támadó elhiteti az **A** áldozattal, hogy saját nyilvános kulcsa a **B** kommunikációs partnere. Ekkor csak a támadó tudja értelmezni a saját titkos kulcsával az elküldött üzeneteket, a kommunikációs partner nem.



3. ábra Nyilvános kulcsú titkosítás címtár elleni támadása

Ez ellen a támadás ellen úgy lehet védekezni, hogy hitelesítik a küldőt. Ha tudjuk, hogy csak az **A** küldő rendelkezik saját titkos kulcsával, akkor az alábbiak szerint (RSA esetén) eljárva biztosíthatjuk, hogy **A**-hoz tartozó nyilvános kulcsot használja **B**-vel történő kommunikációban:

A kódolása: $y = E_{(k_B^P)}(E_{(k_A^S)}(x))$

B dekódolása: $x = D_{(k_A^P)}\left(D_{(k_B^S)}(y)\right) = D_{(k_A^P)}\left(D_{(k_B^S)}\left(E_{(k_B^P)}\left(E_{(k_A^S)}(x)\right)\right)\right) = D_{(k_A^P)}(E_{(k_A^S)}(x))$

A hitelességet úgy lehet biztosítani, hogy küldéskor felhasználják saját titkos kulcsukat is a rejtjelzéshez. Visszafejteni bárki képes mivel a nyilvános kulccsal dekódolható a titkos kulccsal rejtjelzett üzenet.

2.8.3 Nyilvános kulcsú infrastruktúra (PKI)

Ha olyan résztvevők szeretnének kommunikálni egymással, akik még nem rendelkeznek a másik résztvevő nyilvános kulcsával, akkor megoldást nyújthat a nyilvános kulcsú infrastruktúra. Előfordulhat, hogy a résztvevők nem is egy címtárban tárolják saját nyilvános kulcsaikat.

Egy nyilvános kulcs hitelességét a tanúsítvány igazolja (certificate). A tanúsítvány tartalmazza a személy/szervezet nevét, akihez a kulcs tartozik, a kiállító hitelesítés szolgáltató (Certificate Authority - CA) aláírását. A hitelesítés szolgáltatók fa struktúrába rendezettek és a falevelek / felhasználók, azok akik kommunikációra használják kulcsaikat (tanúsítványokat). *Megjegyzés: A valóságban több tanúsítványszolgáltató létezik, saját fa struktúrájával. ezen fák szigetszerűen és/vagy egymást viszont-tanúsítva összekapcsolódhatnak (erdő). A valóságban egy-egy tanúsítványszolgáltató felépítése sem teljes fa.* Egy felhasználó tanúsítványa ellenőrizhető a fa gyökerétől végighaladva a falevélig. Ezt az útvonalat hívják tanúsítvány láncnak. Több CA is létezik, azaz több tanúsítványfa van. A CA-k egymást keresztbe is tanúsítják. Az, hogy egy tanúsítványban megbízunk, azt jelenti, hogy megbízunk az ellenőrző programban (például: a Web böngészőnkben) és az adott CA-ban. *Megjegyzés: sokszor fordul elő, hogy olyan CA-tól vásárolunk tanúsítványt, akinek gyökértanúsítványa alapértelmezetten nincs benne az operációs rendszerünkben és/vagy böngészőnkben. Ilyenkor kézzel kell elvégeznie az felhasználónak a megbízható tanúsítvány hozzárendelését alkalmazásaihoz.* A nyilvános kulcsú infrastruktúra fogalmai között meg kell még említeni a visszavonási listákat. Ugyanis egy tanúsítvány nem örökéletű és kompromittálódhat is,

ilyenkor jelezni kell a CA felé, hogy visszavontuk a tanúsítványt. További érdekes kérdések merülnek fel jogi szempontból, mi tekinthető bizonyító erejűnek. Akit mélyebben érdekel a téma, annak javaslom: Dr. Berta István Zsolt, Nagy E-szignó könyvét, Microsec Kft. 2011 (innen letölthető: https://srv.e-szigno.hu/?lap=nagy_e-szigno_konyv).

2.8.4 *Lenyomatképző (hash) függvények*

A lenyomatképző függvények szerepe az integritás bizonyítása. A lenyomatképzés során egy bármilyen hosszúságú bitsorozathoz egy meghatározott hosszúságú bitsorozatot rendelünk. A leképezésnek *egyirányú*nak kell lennie, azaz a lenyomat könnyen számítható legyen, de adott lenyomathoz ne tudjanak érvényes üzenetet számítani. Másik fontosabb tulajdonsága a lenyomatképző függvéneknek az *ütközéssel szembeni ellenállás*. Ez azt jelenti hogy legyen nagyon nehéz olyan üzenetet találni, aminek ugyanaz a lenyomata. (A lenyomat egy sokkal kisebb halmaz mint a lehetséges üzenetek halamaza, mivel a lenyomat hossza rövidebb.)

Lenyomatok felhasználása a telepítő csomagok hitelességének ellenőrzésétől a digitális aláírásig sok helyen előfordul. Egy érdekes példa a hivatalos nyomozati munka során is SHA lenyomatot rögzítenek a digitális adatok vizsgálatának megkezdésekor, hogy utólag a jogi munka során bizonyítható legyen a bizonyíték sértetlensége (integritás), azaz eredetisége.

A leggyakrabban használt kriptográfiai lenyomatképző függvények: MD4, MD5, SHA-1, SHA-2 (SHA-256, SHA-384, SHA-512) és SHA-3. Az SHA-3 függvénycsoport, az Amerikai Szabványügyi Hivatal (NIST) 2012-es pályázatának nyertese a Keccak. Tanulva az MD4, MD5 és SHA-1 hibáiból, újabb és biztonságosabb lenyomatképző függvényeket kerestek. A Keccak-ot FIPS 202 szabványként definiálták. Hamarosan napi szinten fogjuk használni, hasonlóan a korábbi verziókhoz.

2.8.5 *Üzenet-hitelesítés*

Az üzenet-hitelesítés célja, hogy a fogadó fél számára garantált legyen a küldő fél kiléte és az üzenet tartalma változatlanul érkezzen meg hozzá (a letagadhatatlanság nem cél). Ezt úgy lehet elérni, hogy az üzenethez hitelesítő kódot (MAC – Message Authentication Code) is elküldi a feladó. A MAC egy ellenőrző összeg, amit az üzenetből és egy titkos kulcsból lehet kiszámítani, azaz az eredeti üzenetre jellemző. A MAC átküldésre kerül az eredeti üzenettel együtt, majd a fogadó oldalon a vevő is kiszámolja a MAC-t és összehasonlítja a fogadott értékkel. A küldő és fogadó fél egy közös titkos kulcsot használ, így a támadó a kulcs ismeretének hiányában nem tudja hamisítani a MAC-t.

2.8.6 *Digitális aláírás*

A digitális aláírás célja, hogy mindenki számára bizonyítsa az üzenet hitelességét és integritását. A jog által elismert digitális aláírást nevezik elektronikus aláírásnak, ez EU direktíva. Digitális aláírás

készítésekor nem a teljes dokumentumot szokták aláírni a saját kulccsal, mert túl az erőforrásigényes lehet. Ehelyett a dokumentum lenyomatát írják alá.

2.8.7 Virtuális magánhálózat (VPN)

Virtuális Magán Hálózat (VPN) célja az egymástól távol elhelyezkedő telephelyek biztonságos hálózati összekapcsolása. Szinte minden hálózati technológiáról elmondható, hogy kezdetben a biztonsággal nem foglalkoztak, hanem feltételezték a jó szándékú felhasználást. Így volt ez a VPN technológia esetén is. Két alapvető megoldást különböztetnek meg:

1. A **trusted VPN** megoldás esetén, kezdetben bérelt vonali majd később csomag-kapcsolt megoldásokkal biztosította a szolgáltató a közvetlen kapcsolatot. Ebben az esetben a szolgáltató képes érdemben lehallgatni, módosítani a forgalmat. Vagyis a felhasználó megbízik (trusted) a szolgáltatóban. Trusted VPN esetén a szolgáltató garantált paraméterekkel nyújt szolgáltatást – QoS. Természetesen a szolgáltatónak mindent meg kell tennie a támadások elkerülésére.

2. A másik megoldás a **secure VPN**, ahol a szolgáltatótól függetlenül, nyilvános adathálózaton valósítanak meg biztonságos kapcsolatot (ezt megteheti a szolgáltató is). Ekkor a kommunikációs csatorna lehallgatása esetén sem képes értelmezni a támadó a titkosított adatforgalmat.

A kettő keveréke a hibrid VPN mely biztonságos kapcsolatot nyújt garantált forgalmi feltételek mellett. Hálózatbiztonsági szempontból minket a secure VPN megoldás érdekel, továbbiakban VPN alatt ezt értjük és a secureVPN-ek néhány megvalósítását tekintjük át. A VPN megoldások, amennyiben nem biztonságosak, akkor biztonságossá tehetőek csatorna (tunneling) protokollok alkalmazásával. A csatorna protokollok alkalmazásával beágyazzák (encapsulate) a továbbítandó adatot (payload), amivel biztonságossá tehető a kommunikáció (, illetve inkompatibilis átviteli csatornák felett is lehetővé teszi a kommunikációt).

Biztonságos kommunikáció VPN megvalósításai a következők:

- A PPTP-t a PPP kapcsolatok IP feletti bővítésére használják.
- L2TP-t a PPP nem IP hálózat feletti bővítésére használják
- IPSec az IP alapú forgalom védelmére használják, gyakran átjáró –átjáró kapcsolatok között.
- SSL VPN-t adott alkalmazás rétegbeli forgalom védelmére használják.

Csatorna protokollok összefoglalása	
Point-to-Point Tunneling Protocol (PPTP)	kliens / szerver modellen működik
	kibővíti és védi a PPP kapcsolatokat
	az adatkapcsolati rétegben működik
	csak IP hálózatok felett továbbít
Layer 2 Tunneling Protocol (L2TP)	az L2F és a PPT keveréke
	kibővíti és védi a PPP kapcsolatokat
	az adatkapcsolati rétegben működik
	többféle hálózat felett továbbít, nem csak IP felett
	IPSec-kel együtt biztonságos

IPSec	Több VPN kapcsolatot tud kezelni egyszerre
	Biztonságos authentikálást és titkosítást ad
	Csak IP hálózatokat támogat
	LAN-LAN kommunikációra fokuszál és nem felhasználó-felhasználóra
	Hálózati rétegben működik, és az IP –n ad biztonságot
Secure Sockets Layer (SSL)	szállítási rétegben működik és főként Web-alapú forgalmat véd
	finom beállításokat enged a hozzáférés kontrollban
	könnyű telepítés, mióta az SSL-t beágyazták a böngészőkbe
	csak kisszámú protokollt támogat, ezért nem infrastruktúra szintű VPN megoldás

2. táblázat: Csatorna protokollok tulajdonságai

2.8.8 IPSec

Az Internet (IPv4) nem volt biztonságos. A megoldásáért – melyik rétegben célszerű megvalósítani a biztonságot– eltérő nézetek ütköztek, melyek közül a Szállítási rétegben megvalósuló megoldás – IPSec - nőtte ki magát. Az IPSec már alapértelmezett része az IPv6 protokollnak.

Az IPSec-t felépítő főbb protokollok:

- **AH (Authentication Header - Authentikációs Fejléc)** biztosítja az adat integritást, az adat származásának authentikálást és a visszajátszásos támadások elleni védelmet.
- **ESP (Encapsulating Security Payload)** biztosítja a bizalmasságot (titkosítás), az adat forrásának authentikálását és az adat integritást.
- **IKE (Internet Key Exchange) v2** feladata a kapcsolódási paraméterek egyeztetése, beleértve a kulcscserét is.

IPSec két üzemmódja:

Csatorna mód: a teljes eredeti csomag újból becsomagolódik és titkosításra kerül és új fejlécet kap. Ez lehetőséget ad arra, hogy az olyan eszközök, mint például az útválasztók IPSec proxy-ként funkcionáljanak, azaz a hosztok helyett ezek végezzék el a titkosítást és a dekódolást. A csatorna módban az IPSec-et alkalmazó gépek átjáróként funkcionálnak és akárhány, logikailag az átjáró mögött elhelyezkedő gép forgalmát képesek továbbítani a *csatornában*. A kliens gépeken semmilyen IPSec-hez kapcsolódó feldolgozást nem szükséges végezni, az egyetlen kritérium, hogy az útválasztó táblájukban szerepeljen a megfelelő IPSec átjáró címe. Ez a módszer nagyobb védettséget nyújt a forgalomelemzés ellen, mivel az eredeti fejlécek is rejtve maradnak, így a támadó nem tudja, hogy pontosan hova voltak címezve a csomagok, csak azt, hogy melyik két átjáró között mentek át.

Átviteli mód (transport mode): hoszt-hoszt kapcsolat épül fel, amelynek résztvevői kizárólag azok a gépek, amelyek a kapcsolat végpontjai. Gyakorlatilag a hoszt gépek saját maguk biztonsági átjárói (security gateway). Ebben a módban, csak az IP payload (csomag) kerül titkosításra, az eredeti IP fejlécek változatlanul maradnak. Ez a mód kevésbé ellenálló a forgalomelemzés jellegű támadásokkal szemben. Előnye, hogy csak néhány bájtot ad hozzá minden csomaghoz.

2.8.9 PPTP

Éveken át a de facto VPN szabvány volt a PPTP (Point-to-Point Tunneling Protocol). Népszerűsége a Windows-ba implementálásával tetőzött. Eredetileg a PPTP célja az volt, hogy IP hálózaton keresztül hozzon létre csatornát.A PPTP GRE-t (Generic Routing Encapsulation) és TCP-t használ a PPP csomagok becsomagolására és a PPP kapcsolatok IP feletti hálózatokon való bővítésére.

A PPTP nem támogat több kapcsolatot egy VPN csatornán, azaz csak rendszer-rendszer kapcsolatra használható és átjáró-átjáró kapcsolatra nem. Mivel a PPP sosem lesz ipari szabvány, ezért a különböző gyártók implementáció között vannak inkompatibilisek.

2.8.1 L2TP

Egy másik VPN megoldás a PPTP és a Cisco L2F (layer 2 Forwarding) protokoll tulajdonságait ötvöző L2TP (Layer 2 Tunneling Protocol). Az L2TP a PPP forgalmat csatornázza nem csak IP hálózatokon, hanem ATM, X25… Az L2TP célja hasonló, azaz a PPP forgalmat kézbesíteni a végpontnak olyan hálózaton, ami nem valósít meg PPP protokollt. Ahogy a PPTP, az L2TP sem látja el védelemmel a PPP forgalmat, de magába integrál protokollokat, amik biztosítják azt.

Az L2TP a PPP-től örökli az authentikációt és az IPSec-kel integrálja, hogy bizalmasságot, sértetlenséget és egy potenciálisan másik rétegbeli authentikációt biztosítson.

2.8.2 TransportLayerSecurity (TLS)

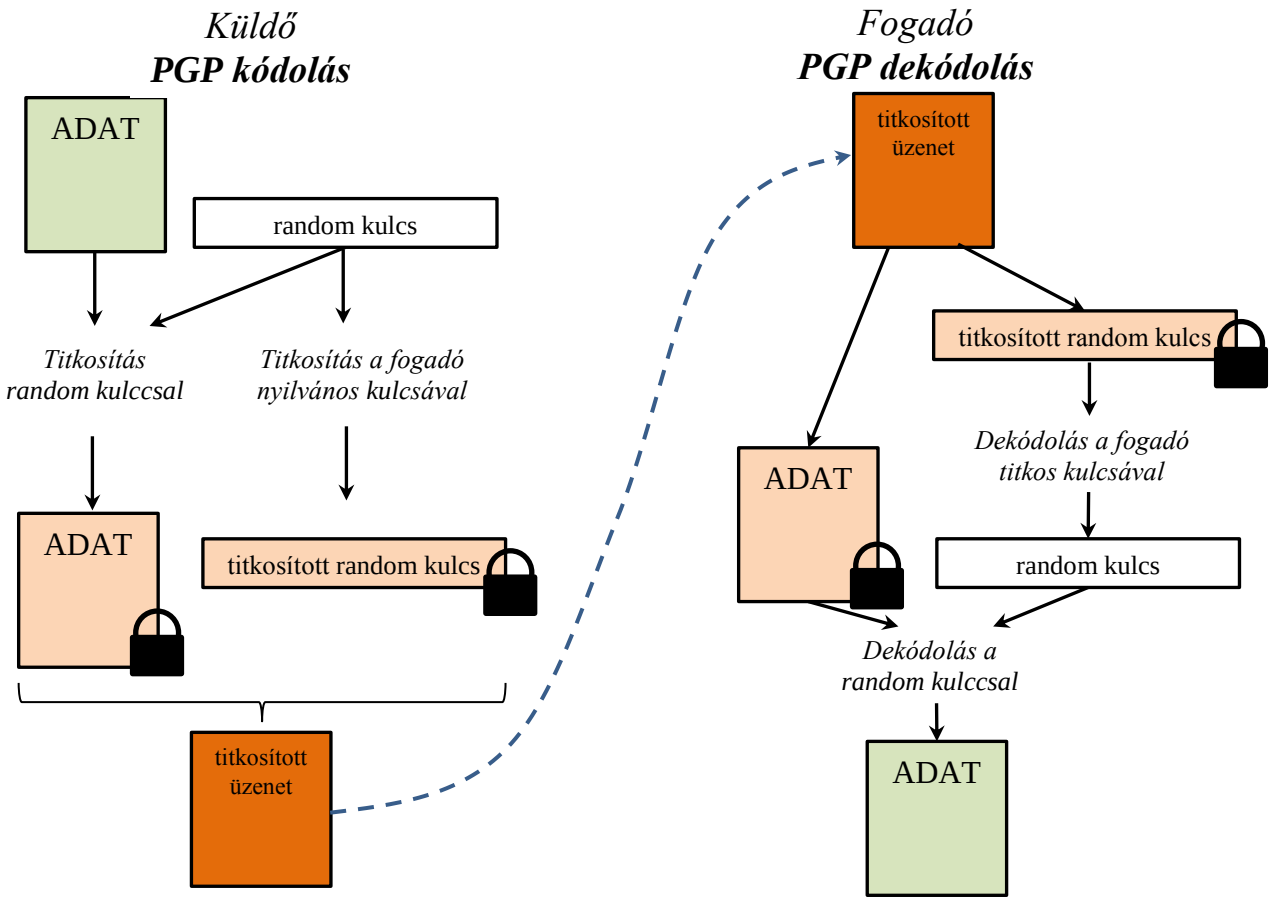
A TLS és elődje az SSL (Secure Socket Layer) a biztonságos Internetes kommunikációhoz tervezték. X.509 tanúsítványokat használ, vagyis aszimmetrikus titkosítást az authentikációhoz és a szimmetrikus kulcsok cseréjéhez. A biztonságos kommunikációhoz szimmetrikus kulccsal titkosítják a forgalmat, amely biztosítja az integritásvédelemt is. Az OSI modell 5. rétegében történik a kézfogás, majd a 6. rétegben a biztonságos kommunikáció. Legismertebb megvalósításai: https, ftps, imaps, pop3s és sip protokollok.

A leggyakoribb SSL VPN implementációk a következők:

- SSL portál VPN. Egy egyén használ egy szabványos SSL kapcsolatot egy Web oldalhozazért, hogy biztonságosan férjen hozzá több hálózati szolgáltatáshoz. A Web oldal elérését portálnak hívják, mert az egy helyen van, ami további erőforrásokhoz biztosít hozzáférést. A távoli felhasználó az SSL VPN átjárót a böngészőjén keresztül éri el, authentikáció után kap egy Web oldalt, ami portálként működik más szolgáltatásokhoz.
- SSL csatorna VPN-ek. Egy egyén több hálózati szolgáltatást ér el biztonságosan egy SSL csatornán keresztül a böngészőjét használva, beleértve alkalmazásokat és protokollokat, melyek nem Web-alapúak. Ez gyakran egyedi programozást igényel, hogy minden szolgáltatás a Weben keresztül legyen elérhető.

2.8.3 PGP

A PGP protokoll biztosítja az offline kommunikáció információ-biztonságát. Vagyis a fájlok, e-mailek, faxok, könyvtárak és akár teljes merevlemez bizalmasságát, hitelességét. A PGP az alábbi ábra alapján működik:



Tehát a titkosításhoz nyilvános kulcsú titkosítást használ a PGP. Fontos kiemelni, hogy a nyilvános kulcsok megbízhatóságát, megbízható forrásból történő beszerzését kiemelten kezeli. Azonban az adat titkosításához kevésbé számításigényes szimmetrikus titkosítást használja.

2.9 Védelmi eszközök

2.9.1 DMZ

A demilitarizált zóna (továbbiakban: DMZ) egy olyan hálózati szegmenst jelöl, ahol a nem-biztonságos felhasználóknak szolgáltatást nyújtó szerverek vannak. Ilyen szolgáltatás lehet az email, Web, proxy, fordított proxy szolgáltatás. Lényege, hogy a DMZ kompromittálódása esetén még nem férnek hozzá a belső hálózathoz közvetlenül, mivel azt aktív hálózati védelem választja el a DMZ-től.

2.9.2 Tűzfal

A tűzfal feladata a (hálózati) biztonsági házirend betartatása **hozzáférés szabályozással** a hálózati erőforrásokhoz. A tűzfalak is nagy fejlődésen mentek keresztül a mai verziók eléréséig. A kezdetekben két alapvető megközelítés volt a hálózati erőforrások hozzáférés szabályozására: a bastionhost és az csomagszűrő alapú útválasztó. A **bastionhost** megoldás lényege, hogy minden hálózati forgalom egy kitűntetett gépen megy keresztül, ami eldönti, hogy az adott kommunikáció engedélyezett vagy nem. A **csomagszűrő tűzfal** lényege, hogy hozzáférési listák (ACL) szerint, csomag paraméterek alapján, átenged adott forgalmat vagy nem. A tűzfalak következő típusait különböztetjük meg:

- Állapotmentes csomagszűrő tűzfal (stateless packet filtering)
- Állapotmegőrző tűzfal (stateful packet filtering)
- Proxy tűzfal
- Dinamikus csomagszűrő tűzfal (dynamic packet filtering)
- Kernel proxy

2.9.2.1 Állapotmentes csomagszűrő tűzfal

A csomagszűrés egy tűzfal technológia, amely a hálózati szintű protokoll fejlécek alapján hozzáférést biztosít. Az eszközön a konfigurált ACL-n keresztül történik a csomagok engedélyezése, illetve eldobása (tiltása) a megfelelő hálózatok irányába. Ez a technológia az **első generációs tűzfal** megvalósításának alapvető formája, az OSI alsó 3 rétegében végzi feladatát. A döntés a csomagban lévő információk alapján történik:

- forrás IP
- cél IP
- forrás port
- cél port
- protokoll típus
- forgalom iránya

A csomagszűrő eszközök **korlátozottan képesek a hálózati szintű támadások blokkolására** és **nem nyújtanak hatásos védelmet az exploit alapú támadásokkal szemben sem**, mivel a csomagok tartalmát az eszköz ebben az eseten nem vizsgálja, így az exploit tartalma eljuthat a célállomáshoz. A csomagszűrés gyengeségei:

- Az alkalmazás alapú támadásokat nem képes megszűrni
- A naplózási funkciók korlátozottak
- A komplexebb felhasználói authentikációt nem támogat
- A csomagszűrő tűzfalak nem képesek a hamisított (spoofed) címek detektálására

A csomagszűrés előnyei:

- Alkalmazás független
- Szabadon méretezhető
- Rendkívül gyors

2.9.2.2 Állapotmegőrző tűzfal

Az állapotmegőrző tűzfal (stateful firewall) nemcsak a csomagok fejlécét ellenőrzi, hanem a csomag tartalmát is és nyilvántartja a felépült kapcsolatokat. A kommunikáció ellenőrzéséhez az állapotmegőrző tűzfalak állapot táblákat (statetable) tartanak nyilván. A tábla tartalmazza, hogy az adott forrásnak van már érvényes kapcsolata.Az állapotmegőrző tűzfalak az OSI modell alsó 4 rétegében működnek. Ez második generációs tűzfal.

Megjegyzés: A TCP kapcsolatokban a megfelelő időpillanatban a csomagoknak tartalmazniuk kell a helyes SYN, SYN/ACK és ACK értékeket. Ezek az értékek a csomagokban a megfelelő helyen magasra állított bitek. Ha például egy állapotmegőrző tűzfal olyan csomagot kap, amelyben az összes bit magasra van állítva, akkor az egyértelmű DoS támadás, így eldobja a csomagot.

Az állapotmegőrző tűzfalak képesek a nem teljesen felépült kapcsolatból eredő csomagok szűrésére, valamint hatásos védelmet nyújtanak a „SYNC flood” támadásokkal szemben.

2.9.2.3 Proxy tűzfal

A **proxy tűzfal** megvizsgálja a csomagokat a kézbesítés előtt. Az eszköz fizikai elhelyezése a megbízható és a nem megbízható hálózatok között történik. A legfontosabb tulajdonsága, hogy a két eszköz között megszakítja a közvetlen kapcsolatot. A valóságban két kapcsolat épül fel, egy a kliens és a proxy között a másik a proxy és a szerver között. Működése során a klienstől kapott csomagokat saját nevében továbbítja. Csak olyan csomagokat képes továbbítani, aminek ismeri a protokollját és fel tudja dolgozni.

A **kapcsolat szintű proxy** egy speciális kapcsolatot hoz létre a két kommunikáló eszköz között és hálózati szinten monitorozza a kommunikációt. Nem képes a csomag tartalmának a vizsgálatára csupán a fejlécekből nyert információk alapján hozza meg a döntéseket.

Az **alkalmazás-szintű proxy** az alkalmazás rétegen keresztül ellenőrzi teljes mélységben a csomagokat és hozza meg a megfelelő döntést. Erre a legjobb példa a SOCKS kapcsolat-szintű proxy átjáró, amely biztosítja a titkosított csatornát két eszköz között. Ez a harmadik generációs tűzfal, amely már az OSI modell legfelső rétegében dolgozik.

Alkalmazás szintű tűzfalak speciális esetei acélorientált vizsgálatot megvalósító tűzfalak:

- **Web Application Firewall** – WEB protokollok elemzésével, alkalmazásszintű támadásait elemzi.
- **Database Access Management** – Adatbázis hozzáféréseket, adatbázis elleni támadásokat vizsgálja…

2.9.2.4 Dinamikus csomagszűrő tűzfal

Amikor a belső rendszernek kommunikálnia kell a hálózatán kívül eső entitással a rendszernek egy forrásportot kell választania, így a vevő rendszer tudja, hogyan válaszoljon helyesen. A 0-tól 1023-ig terjedő portokat „wellknown” portoknak nevezzük és a szerver oldali szolgáltatások számára foglaltak. A küldő rendszernek egy dinamikus 1023-nál magasabb portot kell választania, amikor megalakítja a kapcsolatot egy

másik entitással. A dinamikus csomagszűrő tűzfal létrehozza az ACL-t, engedélyezve ezzel a kommunikációt a belső rendszerrel a kijelölt porton keresztül. A dinamikus tűzfal előnye, hogy a beérkező teljes forgalmat szűri.

2.9.2.5 *Kernel Proxy tűzfal*

A **kernel proxy** az ötödik generációs tűzfal. Az eszköz technológiailag teljesen különbözik az előző eszközöktől, mivel méretezhető verem kerül kialakításra, ahol a csomag megfelelően vizsgálható vagy értékelhető. Amikor a csomag megérkezik a tűzfalhoz egy új virtuális hálózati verem kerül megvalósításra a csomagnak megfelelően. Például FTP csomaghoz az FTP proxy fog betöltődni a verembe. Ez azt jelenti, hogy az eszköz a csomag összes fejlécét (data link, network, transport, session layer, application layer) megvizsgálja a csomag információ tartamával együtt. Ha az eszköz úgy ítéli meg, hogy a csomag nem biztonságos, akkor eldobja. A kernel proxy tűzfalak rendkívül gyorsak, mivel a csomagok vizsgálata és feldolgozása a kernelben belül történik, nincs szükség a csomagok felsőbb rétegekbe történő juttatására.

Tűzfal típus	OSI réteg	Tulajdonság
Csomag szűrés	Hálózati réteg	ellenőrzi a forrás és cél címeket, portokat és a kért szolgáltatást. Az útválasztók ACL-eket használnak a hálózati forgalom monitorozására.
Állapotmegőrző	Hálózati réteg	A csomag állapotát és a környezetét is vizsgálja. Állapot táblában rögzíti minden egyes kommunikáció aktuális állapotát
Alkalmazás szintű	Alkalmazás réteg	Mélyen vizsgálja a csomagot és finom, testreszabott döntést hoz. Minden protokollhoz egy proxy szükséges.
Kapcsolat-szintű proxy	Viszony réteg	Csak a fejlécet ellenőrzi, többféle protokollt és szolgáltatást támogat, mint az alkalmazás-szintű proxy, de részletes döntést, mint az alkalmazás-szintű proxy
Kernel proxy	Alkalmazás réteg	Gyorsabb a kernel szintű feldolgozás miatt, minden egyes csomaghoz külön hálózati verem készül

3. táblázat: Tűzfal típusok

2.9.2.6 *Tűzfal architektúrák*

Tűzfal architektúrák tulajdonsága	
Dual-homed:	Egy számítógép elkülönített hálózati kártyákkal kapcsolódik minden egyes hálózathoz. Az eszköz megosztja a belső és a külső hálózatot. A számítógépeken a továbbító (forwarding) és az útválasztó (routing) funkciókat tiltani kell a hálózat szegregációjához.
Monitorozott munkaállomás (Screened host)	Az eszköz megszűri a forgalmat mielőtt a tűzfalba érkezne.
Monitorozott alhálózat (Screened subnet)	A külső router megszűri a forgalmat mielőtt a belépő a forgalom elérné az alhálózatot. A hálózati forgalom ezután egy belső útválasztóba azon keresztül a megfelelő alhálózatba kerül

4. táblázat: Tűzfal architektúrák

2.9.2.7 Tűzfalak biztonsága

A tűzfalak alapvető beállítása a nem engedélyezett csomagok tiltása. Ez azt jelenti, hogy ha nincs szabályrendszer felállítva egy csomaghoz, akkor a csomag továbbítása megtagadásra kerül. A masquerading és a spoofing egy népszerű támadási forma, amelyben a támadó módosítja a csomag fejlécét a belső hosztok címének megszerzéséért. A tűzfal szemszögéből vizsgálva: „ez a csomag az internet irányából érkezett, de belső címmel rendelkezik, tehát megtagadom a beléptetését". De ennek az ellenkezője is igaz azaz: „nem engedem annak a csomagnak a továbbítását az internet irányába, amely nem rendelkezik belső címmel". Például a belső címmel nem rendelkező csomagok „zombi" munkaállomásra utalnak, annak forgalmát tiltani kell. A tűzfalaknak újra kellene építeni a csomagokat mielőtt kiküldésre kerül, mert sok támadási formában a támadók a csomag teljes tartalmát megváltoztatják. A **több darabban érkező csomagok vizsgálata** esetén a tűzfalnak döntést kell hozni a csomagok tartalma alapján. Azonban a megfelelő döntéseket csak akkor lehet meghozni, ha a teljes és felépített csomag áll rendelkezésre. Ha a csomagokat részleteiben vizsgálja az eszköz, akkor lehetséges, hogy a kártékony kód vagy eljárás a célba érkezéskor összességében egy kártékony kód egésszé alakul, amely már képes aktivizálódni és a megfelelő hatást kifejteni. Azonban a teljes csomag felépítése a tűzfal számára időbe telik és hálózati késedelmet okozhat a hálózat sebességétől és a csomag nagyságától függően. Ezért fontos a vállalati környezetben a megfelelő policy kidolgozása.

2.9.3 Honeypot

A **honeypot** egy számítógép a monitorozott hálózati szegmensen vagy a DMZ-ben, célja a támadókat magához csalogatni, hogy ne a valódi, éles gépekkel foglalkozzanak. Az adminisztrátorok elérhetővé tehetnek néhány népszerű portot, mint könnyű támadási célpont a honeypot rendszeren. Bizonyos honeypotok szolgáltatásokat emulálnak, valójában szolgáltatás nem fut. A honeypotok megtévesztésig hasonlóak az adott cég éles rendszereihez.

Valójában **a honeypot-ok a támadások korai felismerésének eszközei.** Ugyanis normál felhasználó, még csak nem is tévedhet a honeypot rendszerre. Ha valamilyen aktivitás megjelenik a honeypoton, akkor az biztosan egy behatolótól származik. A honeypoton végzett tevékenységek rögzítésével, naplózásával és elemzésével hatékony védelmet lehet építeni az éles rendszerre. Több honeypot egyidejű használata a **honeynet.**

Nagy szervezetek adott típusú forgalom felismerésére, mérésére használják, amivel meghatározzák saját veszélyszintjüket. A rendszer hálózati forgalmi statisztikákat gyűjthet, amit központi elemzésre visszaküld. Amint megtámadják a rendszert, elkezd használható információt gyűjteni, ami által a hálózatüzemeltetők megérthetik, mi folyik a rendszerükben.

Tehát a honeypot nem része az éles produkciós rendszernek, nincs vele semmilyen kapcsolatban, így nem szolgálhat ugródeszkaként további támadásokhoz. *Megjegyzés: bizonyos megvalósítások, adatbázis honeypot éles, éleshez hasonló adatokkal dolgoznak a „hiteles" csapda érdekében.* Helytelen honeypot

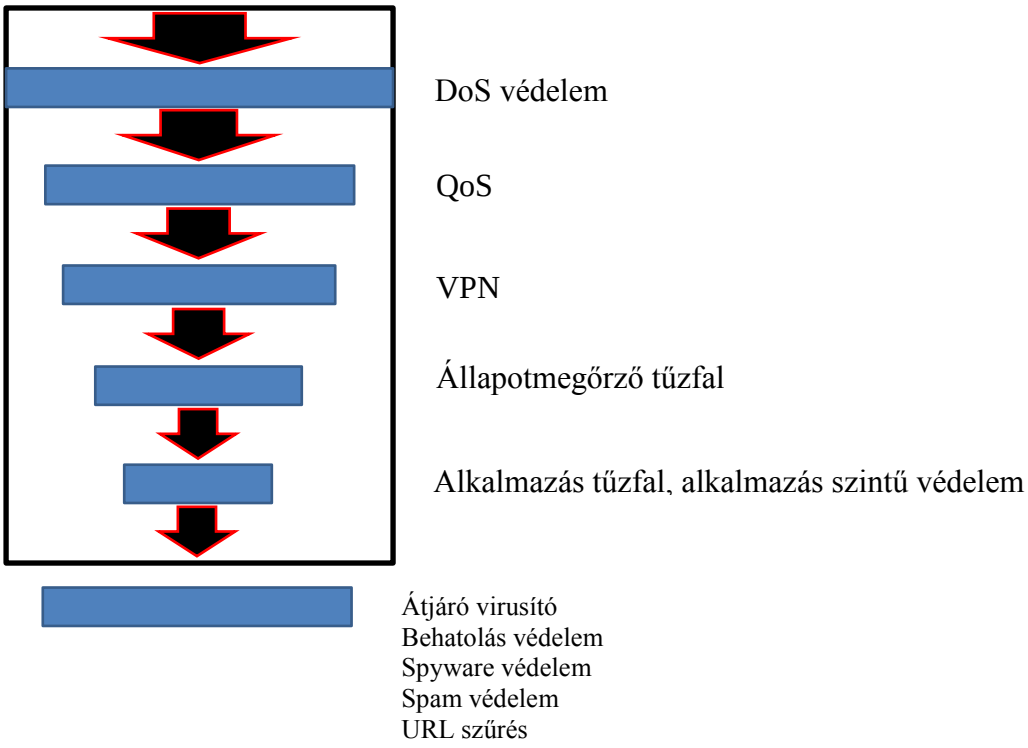
beállítás esetén segítheti a további támadásokat. Rendkívül fontos a honeypotok hálózati szeparációja az éles rendszerektől.

2.9.4 Tarpit

A **tarpit** egy olcsóbb és egyszerűbb megoldás a támadók ellen. A tarpit célja szintén a támadó figyelmének magára vonása. Azonban az „ígéretes" kihasználás során a tarpit válaszideje folyamatosan romlik. A kapcsolat a támadóval él, de a válaszok „time-out" üzenetet adhatnak. A legtöbb támadás a hálózat szkennelésével kezdődik, amit automaták hajtanak végre. Így a késleltetett válaszokkal sikeresen terelik el a figyelmet és a hálózat felderítést is ellehetetlenítik. A mai tűzfalak rendelkeznek tarpit funkcióval.

2.9.5 Egységes Fenyegetettség Menedzsment - UTM

Egyre nagyobb kihívás a biztonsági intézkedések hosszú listáját karbantartani, amire minden hálózat üzemeltetése esetén szükség van. Ez a lista ma biztosan tartalmazza a következőket; tűzfal, antimalware, Anti spam, IDS/IPS, tartalomszűrés, adatszivárgás védelem, VPN képességek, folyamatos monitorozás és jelentés. Az UTM készülékek, egy dobozba zárt megvalósítása a lista minden elemét megvalósítja. Az UTM célja az egyszerűség, modern telepítés és karbantartás, központosított felügyelet, és a hálózatbiztonság teljes körű, minden szempontból való megértésének képessége. Az ábra egy UTM eszköz forgalom feldolgozását mutatja be.



4. ábra: UTM séma

UTM eszközök implementációs problémái:

- SPF (Single Point of Failure – egy pontba koncentrált hibalehetőség) a forgalomra. Mindenképpen redundáns megvalósítást kell alkalmazni.
- SPC (Single Point of Compromise – egy pontba koncentrált kompromittálhatóság). Ha az UTM-et kompromittálták, akkor az UTM teljes egészét kompromittálhatják.
- Teljesítmény problémák - késleltetés és sávszélesség problémák előjöhetnek (szűk keresztmetszet) a számítási igény miatt.

2.9.6 IDS

IDS jelentése Behatolás Érzékelő Rendszer. A szakirodalom háromféle behatolás érzékelést különböztet meg, kezdve az alapoktól, a fizikai biztonságtól: fizikai-, hoszt- és hálózati behatolásérzékelés. A hálózati biztonság esetén mindhárommal kell foglalkozni, hiszen ha a „védett" hálózati eszközökhöz szabadon hozzáférnek fizikailag, akkor kikapcsolhatják, kicserélhetik, lehallgathatják a forgalmat és átkonfigurálhatják az eszközt.

A fizikai behatolás érzékelésről bővebben a megelőzés című fejezetben lesz szó, addig csak egy felsorolás:

- biztonsági őrök
- biztonság kamerák
- beléptető rendszer
- tűzfal
- zsilipelt beléptető rendszer (man trap)
- mozgás érzékelő

A **hoszt alapú behatolás érzékelés (HIDS)** foglalkozik a jogosulatlan, tiltott és rendellenes viselkedéssel adott eszközön. A HIDS működéséhez általában valamilyen alkalmazás telepítése szükséges a vizsgált rendszeren, amely riasztást ad az operációs rendszer és az alkalmazások anomáliája során. A HIDS passzív eszköz, csak információt gyűjt, logol, azonosít és figyelmeztet (fájl integritás ellenőrzés). Mivel ma már a hálózati eszközök is saját operációs rendszert futtatnak, ezért a HIDS-nek is van létjogosultsága hálózatbiztonság tekintetében.

Hálózatbiztonság szempontjából a **hálózat behatolás érzékelő rendszer (NIDS)** a legfontosabb. Kizárólag a hálózati forgalom anomáliáival foglalkozik: jogosulatlan, tiltott és rendellenes viselkedéssel. Működéséhez networktap (speciális céleszköz, a forgalom passzív kicsatoláshoz), span port (tükrözött port), vagy Hub (elosztó) eszköz szükséges, amivel kicsatolható a forgalom az elemzéshez. Titkosított forgalmat nem tud elemezni a NIDS, mivel nem tudja dekódolni (értelmezni) a csomagok tartalmát. Ilyen esetekben **a határvédelmi eszköznél terminálni kell a titkosított kapcsolatokat, majd vizsgálat után újra-titkosítani a továbbításhoz!**

A behatolás érzékelő rendszerek minták (szignatúra, ujjlenyomat) alapján és/vagy viselkedés alapján adnak riasztást.

2.9.7 IPS

A behatolás megelőző rendszerek (IPS) aktívan megszüntetik az IDS rendszerek által támadásnak vélt tevékenységet, például megszakítják a hálózati kapcsolatot. Az IPS rendszerek üzemeltetése megfelelő szakértelmet és folyamatos üzemeltetést kíván. Nagyon könnyen hatalmas károkat okozhat egy nem megfelelően beállított és/vagy üzemeltett IPS. Negatív példa lehet az egy forrásból érkező forgalom kitiltása NAT-olt forrás esetén, mivel az a NAT „mögött" lévő összes klienst érint, ha pedig az adott forráscím hamisított, akkor egy támadó célzottan tiltathat ki cégeket, szervezeteket. Ebben az esetben az okozott kár összetett jogi kérdéseket is felvet. (IDS/IPS rendszerekről bővebben: http://www.sans.org/security-resources/idfaq/communication.php)

2.10 Távoli hozzáférés

A távoli kapcsolatokra azért van szükség, mert sok esetben az üzemeltető fizikailag távol van, így nem tudja használni az üzemeltetett gép billentyűzetét. Másik eset, amikor a távoli felhasználónak szüksége van a céges erőforrásokra, például otthoni munkavégzéshez. A probléma kiküszöbölésére sok technológia született. Ma legtöbbször Internetes kapcsolaton keresztül csatlakoznak a távoli erőforrásokhoz, és valamilyen authentikáción keresztül férnek hozzá a központosított erőforrásokhoz. A „távmunka" előnyei közé tartozik az olcsóbb üzemeltetési költség, otthonról végezhető munka, használhatják a saját számítógépeiket, okos eszközeiket, az ügyfelek és partnerek naprakész információval dolgozhatnak. A távoli hozzáférést lehet megvalósítani

- Telefonhálózaton keresztül (betárcsázás)
- Dedikált (bérelt) vonalakon (trusted VPN)
- Interneten keresztül (VPN).

2.10.1 Betárcsázás

Mivel szinte minden háztartásban és irodában van működő telefon, ezért a betárcsázás minden esetben működhet. A csatlakozáshoz modemre van szükség, és a hagyományos telefonvonalon keresztül lehet kapcsolódni a hálózatra.

A telefonvonalak UTP réz vezetéket használnak átviteli közegként, analóg vivőjellel és tartománnyal rendelkeznek az adat küldéshez és fogadáshoz. A modem (modulátor-demodulátor) a kimenő digitális jelet illeszti analóg jelre, amit az analóg vivő továbbít. Az érkező oldalon a demodulátor alakítja vissza a jelet digitális jellé.

Amíg a munkaállomások önálló modemmel rendelkezhetnek az Internetre csatlakozáshoz, addig a cégek sok modem-poollal rendelkeznek a távoli hozzáférések kezeléséhez. Néhány esetben a szerverekre van telepítve a modem-pool.

2.10.2 Wardialing

Sok esetben nincs megfelelően kezelve a modemen keresztüli távoli kapcsolat, authentikáció nélkül lehet csatlakozni. Így a támadók war-dial módszerrel, próbálgatásos alapon felderítik a potenciális modem hívószámokat. Sikeres modemszám esetén már direkt kapcsolattal rendelkeznek a cég hálózatához. Általános szabály, hogy a távoli kapcsolatokat nem védik olyan jól, mint az egyéb hálózati csatlakozási pontokat.

Figyelem: A cégek munkaállomásain gyakran van modemes kapcsolat, amiről a hálózatüzemeltetők nem is tudnak. Akár az alkalmazott csatlakoztatta, vagy az üzemeltetés feledkezett meg róla. Ezért fontos, hogy a cég war-dial ellenőrzéseket végezzen a saját hívószámaira és legyen tisztában saját számaival.

- Mint a legtöbb kapcsolat a betárcsázás is PPP felett valósul meg, ami rendelkezik authentikációval. Az authentikációt engedélyezni kell a PPP kapcsolatra, de a felhasználó hálózatra csatlakozása előtt egy másik authetikációt kell megvalósítani. Erre alkalmas a TACACS+ és a RADIUS.

Néhány betárcsázásra jellemző biztonsági szempont:

- A távoli szervert úgy állítsák be, hogy az visszahívja a hívót, így ellenőrizve az engedélyezett forrást
- A modemet úgy kell beállítani, hogy csak adott számú kicsörgés után válaszoljon, gyengítve a war-dial sikerességét
- Nem használt modemeket tiltsák le
- Minden modemet központosítani kell helyileg és üzemeltetés szerint
- Kétfaktoros authentikációt kell használni, VPN-eket és személyes tűzfalat a távoli elérésekhez

3 Támadások

A technológiai robbanás okozza a támadások számának exponenciális növekedését és a támadások kifinomultságának javulását. A mai támadók gyakran a szervezett bűnözés résztvevői vagy egyes nemzetek által létrehozott szervezetek alkalmazottai. Ez azt jelenti, hogy a mai támadók jól képzettek, szervezettek és cél orientáltak. Különböző módon lopják el a forráskódokat, jelszavakat, üzleti titkokat. A szerzői jogvédett termékek lopásainak száma folyamatosan nő. A kiberháború közismert ténnyé vált 2010-ben a Stuxnet féreg „sikeres” küldetésének hírekbe kerülésével. A Stuxnet tönkretette az iráni urándúsító infrastruktúrát, így késleltetve (egyes becslések szerint kettő évvel) Irán nukleáris programját.

A támadásokat sokféle szempontból lehet csoportosítani: motiváltság, kifinomultság, károkozás mértéke, eszköz/protokoll ellen irányul, automata támadás, külső/belső támadó, stb...

3.1.1 Sérülékenység faktorok

A sérülékenység faktorok szerinti besorolással a sérülékenység-vizsgálati jegyzőkönyvekben biztosan fognak találkozni a biztonsági vezetők. Ha menedzsment szemlélettel közelítjük meg a biztonság elérését és fenntartását, akkor ki kell választanunk a menedzselésnek legmegfelelőbb csoportosítást. A megelőző védekezési forma esetén a lehetséges hiányosságok, biztonsági lyukak – azaz sérülékenységek –

osztályba sorolása vezet a könnyebb értelmezhetőséghez és ezáltal a gyorsabb javításokhoz, hibák kiküszöböléséhez.

A Tihanyi Norbert, Vargha Gergely, Biztonsági tesztelés a gyakorlatban (2014, NKE) tananyag 8 nagy kategoriába sorolja a sérülékenységeket:

- Információ-szivárgás
- Viharszerű lekérdezések
- Adathalászat
- Bemeneti adatellenőrzés
- Jelszó menedzsment
- Gyári beállítások
- Hozzáférés szabályozás
- Konfigurációs hiba

A sérülékenység faktorok szerinti besorolás értelme a platformfüggetlen és technológia-független csoportosítás. Ha adott faktor többször előfordul egy sérülékenység vizsgálat során, akkor célszerű a vizsgált szervezetet adott faktorra átfogóan megvizsgálni. Például, ha a rendszergazdák is gyenge jelszavakat használnak, akkor nagy valószínűséggel a felhasználóknál sincs kikényszerítve az erős jelszó használata.

3.1.2 Támadások sérülékenység vizsgálatok szerint

A Nemzeti Biztonsági Felügyelet sérülékenység vizsgálati módszertanát követve, amit a fent hivatkozott jegyzet bemutat, három fő csoportra osztja a vizsgálatokat:

- Külső sérülékenység-vizsgálat
- Belső sérülékenység-vizsgálat
- WiFi / 3G vizsgálat

Külső vizsgálat és külső támadó esetén ma a legnagyobb veszély a Web alkalmazások és Web szolgáltatások jelentik. A külső támadások több mint 80%-át a Webes támadások teszik ki. Ekkor az OSI modell alkalmazási rétegében működő protokollokon keresztül jutnak át a hálózati határvédelmen és máris a DMZ-ben (jól tervezett hálózat esetén) találja magát a támadó. Hiába korlátozzák a MAC, IP és port alapján a forgalmat, a támadó csak az engedélyezett szolgáltatást nyújtó Web szerverhez fordul kérésekkel. A támadás sikerességének több oka is lehet:

- a Web szerver nincs frissítve
- engedélyezett a fájlfeltöltés és kitakarható a Web-root
- rosszul beállított Web-alkalmazás jogosultságok
- ha indítható fordított proxy (reverse shell)
- social engineering + XSS sérülékenység…

Ha a támadó bejutott a DMZ-be, rosszabb esetben a belső hálózatra (ha a Web-szerver a belső hálózaton van), úgy tud továbbjutni a belső hálózaton a támadó, hogy a Web-szerveren adminisztrátori jogokat kell szereznie. Ehhez elég egy nem jól beállított Web-motor hozzáférés. Adminisztrátori jogokkal a Web-szerveren olyan jogokkal tud hozzáférni a LAN-hoz, mintha rendes felhasználó volna. Ekkor szkenneli

a Web-szerver hálózati szegmensét – megnézi, ki van mellette. Általában más szerverek is találhatóak a DMZ-ben. A támadó tovább szkenneli a Web-szerver operációs rendszerének alapértelmezett eszközeivel az adott hálózati szegmenst, vagy lehetséges fájlfeltöltés esetén célprogramokat alkalmaz.

Tehát egy szűk ponton keresztül bejutott a támadó a DMZ-be, belső hálózatra és ott szélességi támadást tud folytatni az egész belső hálózaton. Ehhez az OSI modell 2.-7. rétegeit használja: ARP, DHCP, ICMP, SMB, NFS, SIP...

Az ilyen támadások elleni védekezés egyik eszköze a célorient alkalmazás-tűzfal: Web-szerver esetén WAF. **A monitorozás, folyamatos logelemzés is kimutathat aktív támadást, sőt előre is jelezheti a támadásokat.** Célzott támadás esetén a támadó alaposan felméri a célpontját. Ezt az előkészületi fázist hálózati forgalomelemzéssel ki lehet mutatni, sajnos automatizálni a feladatot nehéz , a finomhangolás során és még utána is sok fals-pozitív riasztást jelezhet.

A külső támadások esetén az elérhető szolgáltatások felderítésével kezd a támadó; milyen porton, milyen protokollal van szolgáltatás. Emellett fingerprinting-vel kitalálja vagy kiolvassa a csomagok, szegmensek fejlécéből az adott szolgáltatást nyújtó szerver paramétereit; milyen Web-motor; milyen pluginokkal;… érhető el.

Belső vizsgálat a hálózat határvédelmén belül elvégzett vizsgálatok összességét jelenti. Egy szervezet több zónára is bonthatja hálózatát, melyek között további hálózati határvédelem van, ekkor érdemes mindegyik zónán belül elvégezni a vizsgálatokat. A vizsgálat ekkor az OSI modell 2. rétegétől felfelé próbálja kihasználni a biztonsági réseket, hiányosságokat.

Sok esetben a belülről indított támadások elégedetlen alkalmazottaktól erednek, ezt a legnehezebb kiszűrni főleg akkor, ha olyan adatok eltulajdonítását végzi, amihez rendszerint hozzáférhet. Másik gyakori forrás a malware-fertőzések által vezérelt gépek támadása. Továbbá kevésbé nyilvános, de egy néhányezer forintos eszközt felcsatlakoztatva a belső hálózatra, akár az utcáról, távolról is kivitelezhető a támadás.

Az idegen eszközök felcsatlakoztatása ellen port security beállításával lehet védekezni. Ez is érzékelteti, mennyire fontos nyilvántartani a hálózati infrastruktúra aktuális, érvényes felépítését. Nem csak rosszindulatú támadó csatlakoztathat idegen eszközt a vállalati infrastruktúrára. A mai telefonok beépített modemmel rendelkeznek, azt csatlakoztatva a céges gépre védelem nélkül kerül kicsövezésre a céges infrastruktúra!

A **WiFi és 3G vizsgálat** esetén a hagyományos (TCP/IP) hálózatok minden sérülékenységével találkozhat a támadó. Ehhez adódik hozzá a fizikai hozzáférés-szabályozás hiányából eredő minden probléma. A rádióhullámok szabadon lehallgathatóak, zavarhatóak. Engedélyköteles sávok zavarását a törvény bünteti. *Megjegyzés: Sok helyen tilos mobiltelefonok használata: színház, oktatóterem… Van ahol ezt jammerek segítségével kényszerítik ki, de nem árt tudni, hogy ez bűncselekmény. Talán nem véletlenül alkalmas bármely mobiltelefon ingyenes segélyhívásra.*

Visszatérve a vezeték nélküli hálózatok sérülékenységeire, a hozzáférés szabályozást az alkalmazás rétegben kell megoldani. WiFi esetén ez később részletesen bemutatásra kerül. Természetesen a WiFi

hálózati eszközök fizikai hozzáférés védelméről is gondoskodni kell. Ha egy támadó fizikailag hozzáfér egy AP-hez, akkor az AP és az elosztó rendszer (DS) között közbeékelődéses támadást hajthat végre.

Sajnos a mobiltelefon hálózat fizikai védelmére is igazak a fentiek, ha valaki fizikailag hozzáfér egy bázisállomáshoz, akkor közbeékelődéses támadást végrehajthat (kompromittálhatja a szolgáltatót teljes mértékben).

A 3G hálózatoknak a fentieken túl van még három további súlyos biztonsági hiányossága.

- Csak a mobil-készülék és a bázisállomás között titkosított a kommunikáció. Ez a titkosítás is gyenge: minden készülék képes az A0 – titkosítás nélküli kommunikációra, az A5 titkosítás pedig visszafejthető egyszerűbb eszközökkel is.
- A jelzések titkosítatlanul "utaznak" a rádióhullámokkal, így szabadon megfigyelhető ki van a közelben
- Az elosztó hálózat IP alapú és titkosítás nélküli. Ebből csak az következik, hogy aki bejutott a belső hálózatra az szinte "szabadon" garázdálkodhat (fizikai hozzáféréssel vagy szolgáltatáson keresztül)

A mobiltelefonhálózatoknak van még néhány közismert kritikus sérülékenysége, mint a SIM kártyák klónozhatósága, az ál-bázisállomásokkal történő adatlopások, roaming alapú lokáció lekérdezések.

3.1.3 Sérülékenységek típusai

Léteznek **jól ismert sérülékenységek**, melyekről részletes, nyilvános leírások szabadon hozzáférhetőek. A sérülékenység vizsgáló szoftverek kimutatják ezeket a hibákat. És általában létezik a jól-ismert sérülékenység kihasználásához PoC (Proof of Concept) program. Mivel széles körben ismert hiba ezért a gyártók rendelkeznek védelmi megoldással. De a támadók szabadon elérhető támadó eszközöket készítenek.

Léteznek a **kevésbé ismert sérülékenységek**, melyeket erre szakosodott, jó és rossz szándékú szakemberek kutatnak. Védekezni sokkal nehezebb ellenük, mivel nem ismert a hiba és nincs megoldás sem az automatikus felismeréséhez.

Egy speciális sérülékenység csoportot képviselnek a **zero-day** sérülékenységek. A zero-day sérülékenység, olyan biztonsági hibát jelent, amelyre még nem létezik hivatalos patch (javító csomag).

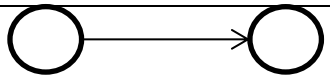
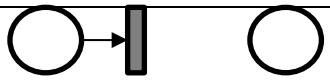
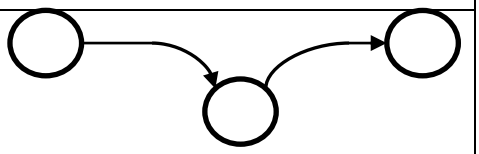
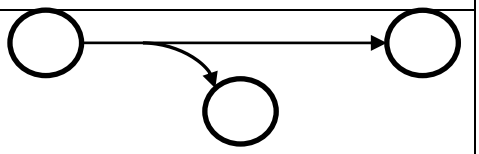
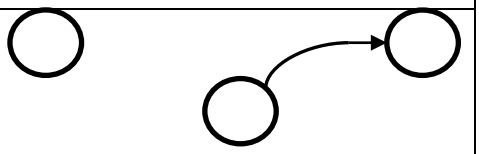
3.1.4 Támadási potenciál

Mekkora eséllyel támadhatnak sikeresen? A sikeres támadás mértékét a támadási potenciál mutatja meg, amely a CC (Common Criteria) szabvány szerint egy 5 tényezős szorzat. Az öt tényező mindegyikéhez egy-egy értéket rendel a CC és a végeredmény a szorzat:

sérülékenység kihasználásához szükséges idő (felkészülés)	0-1nap;1nap-1hét;1-2hét;2hét-1hónap;1-6hónap;6+hónap
szükséges szakértelem	laikus;profi; szakértő; több részterületi szakértő
a célpont ismerete (felépítés, működés)	nyilvános információk (Internetről elérhető); korlátozott információk (egy közösség ismeri); érzékeny információk (csak egy csapat ismeri); kritikus információk (csak néhány személy ismeri)
támadáshoz szükséges idő és szükséges próbálkozások száma (támadás)	korlátlan(támadás észrevétlen marad); egyszerű (0-1nap és max 10 próbálkozás szükséges); mérsékelt (0-1 hónap és legalább 100 próbálkozás); nincs (a rendelkezésre álló idő és/vagy szükséges próbálkozások száma nem elég a sikeres támadáshoz)
szükséges eszközök (szoftver, hardver)	szabványos eszközök (bárki által könnyen elérhető, beszerezhető); speciális eszközök (beszerezhető eszközök); egyedi eszközök (cél specifikus eszközök); több egyedi eszköz (több cél specifikus részeszköz).

3.1.5 Támadások csoportosítása

OSI modell	Internet Protokoll Készlet	ismertebb protokollok	gyakori támadási
*legfelső réteg az **emberi tényező***			*Social* engineering, *Adathalászat*
Alkalmazás réteg	Alkalmazás réteg	DNS, DHCP, HTTP, FTP, IMAP, IRC, LDAP, NTP, POP3, Radius, SSH, SMTP, SNMP, SCP,SFTP, HTTPS, Telnet, TFTP	DNS mérgezés, Adathalászat, befecskendezéses támadások, Spam/Scam
Megjelenítési réteg		SSL, TLS(kommunikáció)	SSL MItM, SSL DOS, SMB támadás
Viszony réteg		SMB, NFS, Socks SSL, TLS(kézfogás)	session eltérítés, L2TP támadás, SIP támadás
Szállítási réteg	Átviteli réteg (hoszt-hoszt)	TCP, UDP, DCCP, SCTP, RSVP	TCP támadások, Útválasztó támadások, SYN flood, Lehallgatás
Hálózati réteg	Internet réteg	IP (IPv4, IPv6), ICMP (ICMPv6), IGMP, IPSec, GGP, OSPF, RIP	Ping/ICMP Flood
Adatkapcsolati réteg	Hálózati hozzáférési réteg	PPP, PPTP, Token Ring, Wifi, Ethernet, ATM, X.25, ARP	ARP spoofing, MAC flooding, VLAN hopping, DHCP támadások, Hamisításos (spoofing) támadások, Lehallgatás
Fizikai réteg		RJ45, BNC	kábel elvágása, networktap, signaljammer

Kommunikáció elleni támadások		
Támadás típusa – példák	**Sérült alapelv**	**ábra**
Normális információ-áramlás		
Megszakítás • logikailag WIFI droppackets • fizikailag: jelelnyomás, kábelszakítás • Túlterhelés, eltérítés	Rendelkezésre állás	
Módosítás • MItM – ARP poison	Sértetlenség	
Lehallgatás • aktív: ARP poison; • passzív: TEMPEST, Network-tap	Bizalmasság (nyílt szöveg vagy dekódolás esetén)	
Hamisítás • beszúrás • visszajátszás	Bizalmasság/Sértetlenség	

Támadási eszközök

Általában a támadók célzott alkalmazásokat készítenek adott „feladat” elvégzésére. Az egyre fejlettebb és kifinomultabb támadások ellen összetett auditor és sérülékenységvizsgáló alkalmazásokat készítettek. Erre is igaz, hogy ami jó a védelemnek az „hasznos” a támadónak is, felhasználhatóak rossz célra is. Ezek már összetettebb vizsgálatok elvégzésére alkalmasak. Ezek az eszközök célzott támadásra, egy-egy ismert hiba kihasználására alkalmas célprogramok. A sérülékenység vizsgáló programok felsorolják adott rendszer exploit-tal kihasználható sérülékenységeit. Az **exploit**-okat elképzelhetjük cél-programnak is, de esetükben már nem feltétlenül protokoll hibák kihasználása történik. Sokszor puffer túlcsordulással juttatnak futtatható programrészeket adott memóriaterületre. Exploit-ok elleni védekezésnek két módja van: az eszközök és szoftverek folyamatos frissítése és a másik a megfelelő szoftverek és eszközök kiválasztása. Természetesen a támadás-védekezés ebben az esetben is egy „macska-egér” játék, ki tart éppen egy kicsivel a másik előtt.

3.2 Automata támadások, malware, vírus, trójai, botnet

Sok esetben már a támadások is programozott módon futnak. Például ha 2010-ben egy friss Windows XP-t frissítések nélkül az Internetre csatlakoztattak, akkor pár percen belül biztosan fertőzött lett.

Milyen támadó programokat különböztetünk meg. A gyűjtő nevük malware, ami kártékony programot jelent. A kártékony kódok csoportjai:

vírus, egy futtatható (nem futtatható esetben is a feldolgozáskor végrehajtják) állományba ágyazza be magát a cél számítógépen a felhasználó tudta nélkül. A vírus futtatáskor továbbterjed más futtatható állományokba.

féreg, önmagát képes továbbítani a hálózaton a cél számítógépre, vírussal ellentétben nem kell futtatni a fertőzött állományt, mert önálló fájl, nem kapcsolódik hordozóhoz.

trójai: egy olyan program, ami a felhasználó tudta nélkül települ fel a rendszerre, vagy felhasználói jóváhagyással, de könnyen félreérthető EULA-val (végfelhasználói szerződés), ez utóbbihoz tartoznak a spyware és addware programok.. A trójai működése során jelszavakat, hozzáféréseket szivárogtat ki, így biztosítva további támadásokat.

spyware: a felhasználói tevékenységek nyomon követésére és eltárolására készítik és személyes adatok gyűjtésére. Ilyen például a keylogger (billentyűzet leütés rögzítő). Kormányzat által „hivatalosan használt"spyware-ek elnevezése govware vagy policeware.

addware: hírdetés generáló program

ransomeware: olyan malware, amely megakadályozza a megfertőzött számítógéphez vagy annak egy részéhez történő hozzáférést. A ransomware eltávolításáért pénzt kér a készítője. Általában a fájlrendszer titkosításával érik el a céljuk. [CryptoLocker]*Védekezés: 1. jól tervezett hálózattal és hálózati megosztásokkal. 2. antivírus programokkal. 3. a forrás általában valamilyen fertőzött Weboldal vagy kéretlen email (spam), ezért ne engedjük szabadon használni a céges gépekről az Internetet és alkalmazzunk spam szűrőket.*

rootkit: egy rejtett program, célja adott folyamatok és programok elrejtése a magas szintű hozzáférések közben. Tehát behatolás közben rejti el a behatolás tényét. A rootkit telepítésének felismerése nehéz, akár hardware cserével is járhat.

hátsó ajtó (backdoor): a normál authentikációs folyamatok megkerülését jelenti egy rendszerhez, például távoli elérést biztosít, miközben rejtve marad a belépés. Ez lehet alapértelmezett jelszó, vagy titkosítatlan (clear text) protokollokon keresztül.

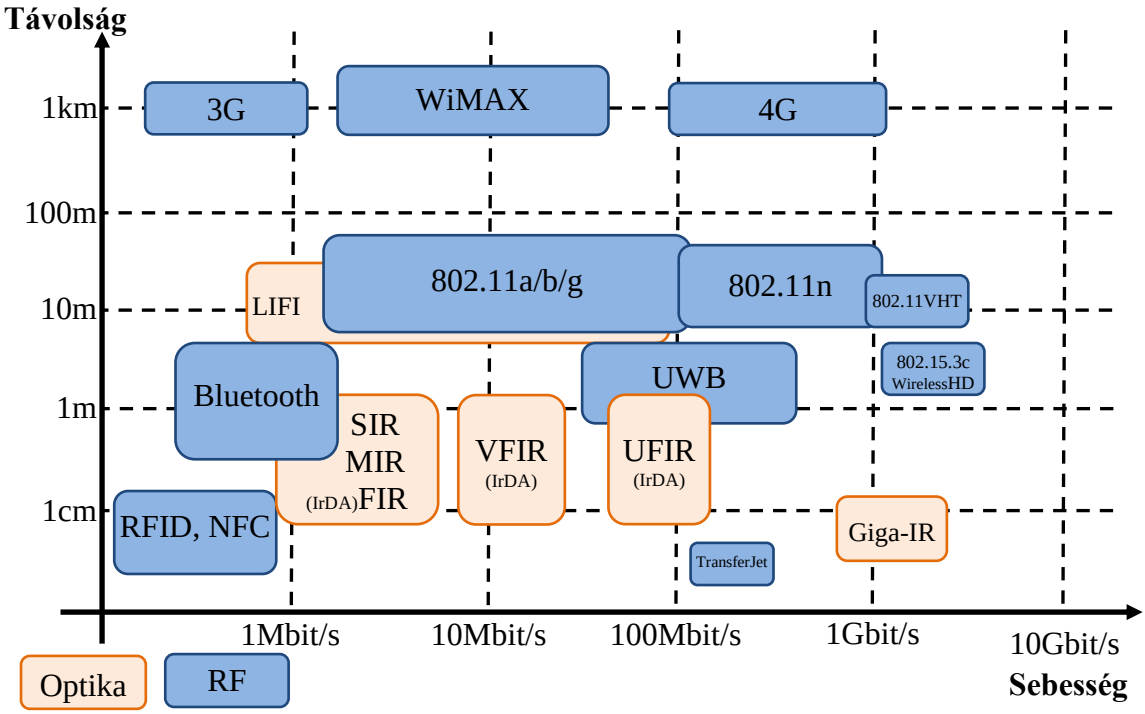
botnet: olyan Internetre kapcsolt (nem szükséges folyamatos kapcsolat) számítógépek halmaza, melyeken a fertőzés (malware) biztosít kapcsolatot a többi fertőzött géppel. Parancsokat a Command&Control szerverektől kap. Léteznek legális botnet hálózatok is, például az IRC.

Az illegális botnet (robot+network) célja a megfertőzött gépeken keresztül adott műveletek elvégzése; spam terjesztés; DDoS támadás; tovább fertőzés stb… A fertőzött gépet gyakran zombi gépnek hívják, mivel a tulajdonos tudta nélkül követ el műveleteket. Sokszor nem közvetlen parancsot kapnak a gépek adott tevékenység elvégzésére, hanem C&C (Command and Control) gépen keresztül jutnak parancshoz. Így megnehezítve az üzemeltetők számára a fertőzött gépek felkutatását.

3.3 *Vezeték nélküli hálózatok*

A vezeték nélküli hálózatok legnagyobb előnye a vezetékes hálózatokkal szemben a kapcsolódó kliensek nincsenek helyhez kötve, akár mobilak is lehetnek (mozoghatnak). Emellett új telephelyek létesítésénél nincs szükség kábelezésre, így versenyképes megoldás lehet, sokszor a biztonsági tényezők figyelmen kívül hagyásával.

Legnagyobb felhasználása a vezeték nélküli hálózatoknak az Internet megosztása a vezeték nélküli kliensek felé (Wifi hotspot) és a mobiltelefon hálózat. Ide tartoznak még a headset-ek (Bluetooth) a vezeték nélküli perifériák (egér, nyomtató, billentyűzet, monitor, stb.), műholdas távközlés, Wimax, IRDA, NFC (PayPass, RFID)...



5. ábra Vezeték nélküli szabványok hatótáv-sebesség összehasonlítása

A vezeték nélküli kommunikációs kapcsolatok mind valamilyen rádióhullámot használnak átviteli közegként, az infra és lézeres adatátvitel kivételével, ahol adott hullámhosszú fényt (többnyire infra tartomány) használnak.

A rádiós kommunikáció a rádióhullámok fizikai tulajdonságai miatt könnyen lehallgatható, mivel a rádióhullámok a tér minden irányába terjednek és az épületek szerkezetén is (részben) áthatolnak. A fény alapú - lézeres és infrás – kommunikáció esetén szükség van közvetlen rálátásra a kommunikációs végpontok között (FSO – Free Space Optics). *Megjegyzés: gyakori probléma forrása az épületek tetején létesített lézeres átvitel végpontjai közé kerülő idegen tárgy, például egy építkezési daru.*

A vezeték nélküli technológiák többféle szempont szerint csoportosíthatóak; a hálózat kiterjedtsége; használt spektrum; üzemmód; támadhatóság szerint…

3.3.1 Vezeték nélküli hálózati infrastruktúra

IBSS Independent Basic Service Set – Független alapszolgáltatás készlet. Ad-hoc hálózat, egymással közvetlenül kommunikáló 802.11 állomások (STA) csoportja. Szabványban nincs maximalizálva az állomások száma.

BSS Basic Service Set – Alap szolgáltatáskészlet. „Csillagpontos" hálózat, melynek közepén a hozzáférési pont (AP) van. Az AP-nek lehet egy WAN/uplink portja, amin keresztül a csatlakozhat vezetékes hálózathoz, Internethez.

ESS Extended Service Set – Kiterjesztett szolgáltatáskészlet. Amikor több AP összekapcsolódik az uplink porton keresztül, akkor az elosztó rendszer (DS) vezérli a BSS-ek egymás közötti kommunikációját. Így összekapcsolódó BSS-eket nevezik kiterjesztett hálózatnak (ESS). Legjobb példája a mobil távközlő hálózat. Mobiltelefon hálózatok esetén:

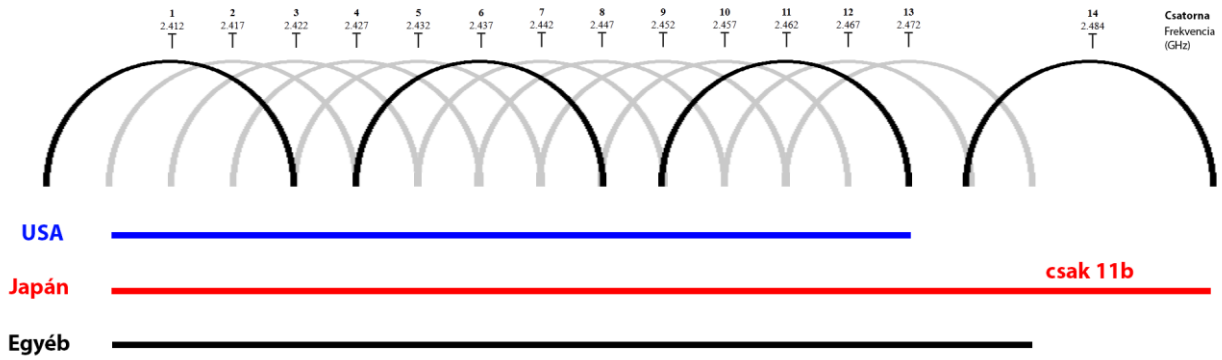
a kliens neve: MS – Mobil Station,

a hozzáférési pont neve: BSS – Base Station Subsystem

az elosztó rendszer neve: NMS - Network Management Subsystem.

3.3.2 WIFI

A WiFi az IEEE 802.11 WLAN szabványa. Az OSI modell fizikai és adatkapcsolati rétegének MAC alrétegét szabályozza a WLAN-okhoz. Több vezeték nélküli hálózati szabványt rögzít. A szabvány szerint rádióhullámokat és Infra fényt használ a fizikai rétegben (ISO OSI). A rádióhullámok a szabadon használható 2,4 GHz, 3,5 GHz és 5GHz-es tartományba esnek. Országonként eltérő a szabadon használható csatornasáv (lásd lenti táblázat).



6. ábra: WIFI 2.4GHz csatorna kiosztása a világon

A 3.5GHz és az 5GHz-es tartomány országonkénti szabad felhasználása, ennél sokkal eltérőbb képet mutat. Ezen tartományok Magyarországi szabályozásáért az NMHH felel (minden rádiós frekvencia kiosztásáért, ideértve a 2.4GHz-et is). A 3.5 (WIMAX) és az 5 GHz felosztása, azaz az

engedélyköteles/szabad sáv „folyamatosan” változik, ezért erősen ajánlott ellenőrizni az aktuális jogszabályi hátteret.

A fenti táblázatokból kiderül, hogy WiFi eszköz beszerzése során figyelmet kell fordítani a lokális szabályozásra.

A 802.11 szabvány meghatározza a legnagyobb kisugározható teljesítményt, így is segítve a WiFi eszközök kölcsönös zavarásának elkerülését. A rádióhullámok előnye a fénnyel (lézer és infra), hogy nem szükséges a két kommunikációs végpontnak közvetlenül „látnia” egymást (LOS - Line Of Sight, közvetlen rálátás), mivel a rádióhullámok a szilárd anyagokon áthatolnak, viszont jelerősségük jelentősen csökkenhet.

Ma már számtalan eszköz WiFi szabvány szerint kommunikál: okos telefonok, tábla PC-k, PC-k, notebook-ok, dokkoló állomások, fényképezők, stb…

A különböző WIFI szabványok jellemzőit az alábbi táblázat tartalmazza:

5. táblázat: WIFI (802.11) hálózati szabványok néhány jellemzője

802.11protokoll	Kibocsátás	Frekvencia (GHz)	Sávszélesség (MHz)	Átviteli sebesség (Mbit/s)	MIMO átvitelek	Moduláció	Hatótáv (m)	
							Beltéri	Kültéri
—	1997/VI.	2.4	20	1, 2	1	DSSS, FHSS	20	100
a	1999/IX.	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	35	120
		3.7					—	5,000
b	1999/IX.	2.4	20	1, 2, 5.5, 11	1	DSSS	35	140
g	2003/VI.	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS	38	140
n	2009/X.	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	4	OFDM	70	250
			40	15, 30, 45, 60, 90, 120, 135, 150			70	250
ac	2012/XII.	5	20	- 87.6	8			
			40	- 200				
			80	- 433.3				
			160	- 866.7				
ad	~2014/II.	2.4/5/60		- 6912 (6.75Gb/s)				

3.3.3 Vezeték nélküli biztonság

A vezeték nélküli hálózatok biztonságát is – az információ-biztonság három alap szabályát figyelembe véve **– bizalmasság, integritás és rendelkezésre állás szempontjából kell vizsgálni.** Mivel az átviteli közeg (fizikai réteg) hozzáférés szabályozását nem lehet befolyásolni, ezért foglalkozni kell két másik feladattal: a szolgáltatáshoz történő hozzáférés szabályozással és ehhez kapcsolódóan a felhasználók hitelesítésével (authentikáció).

A vezeték nélküli forgalmat bárki lehallgathatja. Ha titkosítatlan vagy könnyen-feltörhető titkosítással rendelkezik a kommunikáció, akkor értelmezni is tudja azt. Azaz a **bizalmasság** biztosításához titkosítani kell a forgalmat, olyan módon hogy mások ne tudják értelmezni a forgalmat. *Megjegyzés: Érdemes végiggondolni, hogy már az is információt hordoz - adott körülmények között kritikus információt - , hogy egy forrás rádiójeleket sugároz. Egy rosszindulatú támadó figyelmét felkeltheti a célpont körül*

található összes rádióforrás. Legjobb szemléltetés az idegen területen lezuhant katonai pilóta még a vészhívót is csak rövid időre kapcsolja be.

Minősített hálózatok esetén WiFi alkalmazása nem engedélyezett. Kritikus rendszerek esetén erősen nem ajánlott használata. Banki rendszerek esetén a **PCI-DSS Wireless Guidelines**, a banki rendszerekre kötelező ajánlásokat jól összefoglalja (további információ: https://www.pcisecuritystandards.org): változtassák meg az alapértelmezett beállításokat; fizikailag védjék meg az eszközöket; alkalmazzanak 802.11i védelmet; központilag logoljanak és monitorozzák folyamatosan a WIFI tevékenységet – jelentsék a támadásokat.

WiFi esetén szinte senki sem számol az adatok **integritásának** védelmével. Egy rosszindulatú támadó megváltoztathatja a forgalmazott csomagokat. Így teljesen megtéveszteti a kommunikációban résztvevőket. Ez ellen szintén megfelelően titkosított forgalmazással, authentikálással és a rogue (hálózathoz rosszindulatúan hozzáférő) végpontok kitiltásával lehet védekezni.

A harmadik biztonsági kritérium a **rendelkezésre állás**. A vezeték nélküli hálózatok átviteli közegének zavarását egy erősebb energiájú jellel el lehet nyomni. Egy másik támadási lehetőség a rendelkezésre állás ellen a WiFi kommunikációs kapcsolat kiépítésekor a támadó által „beszúrt" kézfogás elutasítása/resetelése – amit a 802.11 szabvány rögzít (deauth csomag). (A biztonságos vezeték nélküli kommunikációhoz szükség van a kliensek authentikálására. Az authentikációs folyamat egy „kézfogás", amit a támadó által „beszúrt elutasítás" megakadályozhat. Ez ellen folyamatos figyeléssel, a Rogue végpontok kitiltásával lehet védekezni – ehhez megfelelő tudású infrastruktúra szükséges.)

3.3.3.1 Zajgenerátoros jel elnyomás (jamming)

Az információ-biztonság három alapelve közül a rendelkezésre állást lehet legkönnyebben megtámadni. Erősebb rádió (fény) hullámú zajt kell szórni a vevő környezetébe és akkor a jelek hullámtermészetüknél fogva összeadódnak és a vevő képtelen lesz értelmezhető jelet venni.

A mobiltelefonos kommunikációban folyamatosan monitorozzák a zavaró rádióhullámokat és „támadás" esetén riasztást küldenek az üzemeltetőnek.

Misszió kritikus rendszereknél ez ellen úgy védekeznek, hogy több csatornán és/vagy folyamatos csatorna, frekvenciaugrásokkal küldik az adatot. Azaz kritikus rendszereknél – ahol felmerülhet a zajgenerátoros rosszindulatú támadás – folyamatosan több csatornán adnak és folyamatosan változtatják az érvényes csatornát = „ugrókód".

3.3.3.2 Élettani hatások

További biztonsági szempont kell, hogy legyen a rádiós sugárzás egészségre gyakorolt káros hatása.

…"Az emberben elnyelt RF teljesítmény a biológiai anyagok dielektromos állandójának frekvenciafüggése, valamint a testméret és a hullámhossz aránya miatt erősen függ az embert érő külső EM

tér frekvenciájától. Ezt a frekvenciafüggő elnyelést négy szakaszra szokták bontani: szubrezonáns tartomány 20 MHz alatt, rezonáns tartomány 20-300 MHz között, **inhomogén lokális elnyelődés tartománya 300 MHz-2 GHz**, felszíni elnyelődés 10 GHz felett. Az elnyelt energia eloszlása, különösen a 300 MHz-3 GHz frekvenciatartományban, a biológiai objektumon belül erősen inhomogén.”…

3.3.3.3 WEP gyengeségei

Továbbiakban átnézzük a WiFi protokollok néhány gyengeségét. 2001-ben publikálták a Berkley egyetemről a 802.11 WEP (Wired Equivalent Privacy) titkosítás hiányosságait. Majd Fluhrerm, Mantin és Shamir publikálta a WEP által használt RC4 algoritmus gyengeségeit. Ezután jelentette be Adam Stubblefield az AT&T-vel közösen az első sikeres WEP elleni támadást, mely során jogosulatlan hozzáférés szerezhető bármely WEP hálózathoz. (forrás: Buttyán Levente és Dóra László, WiFi biztonság – A jó, a rossz és a csúf, BMGE – HIT - CrySySLab.)

Ezért az IEEE felállított egy csapatot, akik a 802.11i szabványban további biztonsági megoldásokat implementáltak. A WiFi Alliance bejelentett egy köztes megoldást a WPA-t (WiFi Protected Access) 2003 közepén, majd a végleges 802.11i szabványt a WPA2-vel 2004 közepén.

3.3.3.4 WPS - WiFi Protected Setup

A 802.11 szabvány javasolja a könnyű kezelhetőséget és a biztonságot. 2006-ban a WiFi Alliance bemutatta a WPS protokollt, melynek célja a WiFi hálózathoz újonnan kapcsolódó végpontok gyorsabb regisztrálása (kapcsolódása). 2011-ben sikeres támadást mutattak be, mely során kevesebb, mint négy óra alatt adminisztrátori hozzáférést lehet szerezni bármely WPS engedélyezett WiFi routeren. Nem minden esetben segít a funkció tiltása, van olyan router, amin firmware frissítés után lehet kikapcsolni a funkciót. Másik probléma, hogy a gyártok alapértelmezetten engedélyezik a WPS funkciót. A WPS funkciót célszerű kikapcsolni. 2014-ben jelent meg, hogy egy svájci biztonsági cég másodpercek alatt töri fel a WPS jelszavakat passzív forgalom analízis után. A hiba forrása a WPS megvalósításához használ chipek álvéletlenszám generátorának gyengesége: minden újraindítás után ugyanazokat a „véletlen számokat” adja. Egy WPS kérés után, előre készülve, a második próbálkozás sikeres.

3.3.3.5 Rogue AP

Rogue Access Point (ejtsd: roug) fogalma egy olyan ál-AP-t takar, ami nem része az eredeti infrastruktúrának és a rosszindulatú támadó rá akarja venni a gyanútlan klienseket, hogy hozzájuk csatlakozzanak. Ekkor a megtévesztett kliensek forgalma a támadón keresztül áramlik, így sérülhet a bizalmasság, sértetlenség és rendelkezésre állás elve is.

3.3.3.6 Jogosulatlan hozzáférés

Gyakran fordul elő, hogy valaki ingyen szeretné használni az Internetet és megpróbál hozzáférést szerezni egy WiFi hálózathoz. Rosszabb esetben egy támadó azért akar hozzáférést szerezni a WiFi hálózathoz, hogy lehallgassa az ottani forgalmat, esetleg közbeékelődéses támadással beavatkozzon a kommunikációba.

Jogosulatlan hozzáférés ellen kikényszerített (kötelező) authentikálással lehet védekezni. WiFi hálózatok esetén a WEP alapú titkosítás és hozzáférés perceken belül törhető, így használatát kerülni kell. A WPA és WPA2 már erősebb authentikálást követel, így biztonságosabb kommunikációt szolgáltat. Szótár alapon azonban a WPA és WPA2 titkosítás is törhető, így nagyvállalati környezetben valamilyen authentikációs infrastruktúra használata erősen ajánlott – pl.: Radius.

3.3.4 Védelmi eszközök - WIDS

Az ál-AP támadások elleni védekezés a WIDS (Wireless Intrusion Detection System) – vezeték nélküli támadás érzékelő rendszerrel valósulhat meg. A WIDS eszköz folyamatosan monitorozza a csatornákat jogosulatlan/azonosítatlan AP után kutatva. A modern WIDS „eszközök” elérési pontjai háromféle üzemmódban is képesek működni; AP; spektrum analizátor és behatolás érzékelés. Azaz egy teljes vezeték nélküli infrastruktúrában az elosztó rendszer végpontjai 3 üzemmódban képesek működni. Értelemszerűen az AP üzemmódban szolgálja ki egy bázisállomás a klienseket. Szkenner üzemmódban figyeli a rogueAP-ket és spektrum analizátor üzemmódban vizsgálja a sáv telitettségét, így optimalizálhatja az AP-k teljesítményét. Az ál-AP-kre tévesen felcsatlakozni kívánó eszközöket védi a rossz helyre csatlakozástól deauth csomagokkal.

3.3.5 Hotspot – ingyenes, WiFi Internet elérés

Minden cég törekszik ügyfelei teljes körű kiszolgálására. Ide tartozik a vendég hotspot, ami megkönnyíti az ügyfelek és partnerek napi munkáját. Például ezen keresztül érhetik el a saját levelezésüket.

Ez két biztonsági problémát vet fel; az első: amikor a hotspot hozzáférést enged a cég védett hálózatához; a második, ha a hotspot használója titkosítatlanul fér hozzá bizalmas adatokhoz, akkor azok máris kompromittálódtak. **Azaz vendég hotspotot DMZ-be kell telepíteni és felhasználóként használatát kerülni kell, de legalábbis csak titkosított csatornán és/vagy nem bizalmas adatokat szabad elérni.**

3.3.6 Otthoni munkavégzés, kiküldetés

Hasonló problémával nézhet szembe az a cég, aki megengedi vállalati számítógép otthoni használatát, mivel már léteznek kifinomult támadások a vezeték nélküli hálózatba történő authentikációs adatok kicsalására, a vállalati környezeti AP-t szimulálva. Támadás során a vállalattól távol bekapcsolt (pl.: otthon), egyébként munkahelyi WiFi-t használó eszköz elkezdi keresni, majd kapcsolódni a „vállalati” AP-

hez. Ha a támadó a megfelelő SSID-vel szimulálja a vállalati AP-t, akkor rögzítheti a WiFi kézfogás kezdeti lépéseit. Ezután sikerrel próbálhatja meg visszafejteni a kulcsokat. Ha a visszafejtés sikerrel jár, akkor képes lesz belépni a vállalati WiFi-re és onnét folytatni a támadását tovább. Ez a támadás észrevétlen marad a vállalati infrastruktúra üzemeltetői számára. A rendszergazdáknak és biztonsági vezetőknek tisztában kell lennie ezekkel a technikákkal és védekezni kell ellenük.

3.3.7 Wardriving támadás

Ez a fajta támadás inkább nyers-erő (bruteforce) alapú. Célja a vezeték nélküli hálózatok felderítése, feltérképezése egy nagyobb területen. Például egy autóban ülve egy notebook folyamatosan szkenneli az elérhető vezeték nélküli hálózatokat és megpróbál azokhoz csatlakozni, akár feltörve azokat. A felderítés közben GPS alapon rögzítésre kerülnek az elérhető hálózatok, így a végeredmény egy térképen megjeleníthető adatbázis az elérhető / sikeresen feltört hálózatok listájával, térképen.

3.4 IP telefon (VoIP) biztonság

A VoIP TCP/IP integrációja számtalan biztonsági kihívást hozott magával, mert a rosszindulatú felhasználó TCP/IP tudását kihasználhatja ezen a relatív új platformon, próbálgatásos módszerrel kereshet gyenge pontokat az architektúrán és a VoIP rendszeren. Sajnos a szokásos hálózati biztonsági problémák itt is jelentkeztek, mint a jogosultatlan hozzáférés, a kommunikációs protokoll kihasználása, malware terjesztés. A lopott, „ingyenes” hívások nagy kísértésbe viszik a támadókat. Röviden a VoIP telefónia rendelkezik a hagyományos számítógép hálózatok minden hiányosságával. Sőt, a VoIP eszközök hasonlítanak a hagyományos számítógépekre – van operációs rendszerük, Internet protokollokon kommunikálnak, szolgáltatásokat nyújtanak és alkalmazásokkal rendelkeznek. A SIP alapú jelzések titkosítás authentikálás nélküliek. Egy támadó lehallgathatja a SIP szerver és kliens kommunikációját, így a belépési azonosítót, jelszót/PIN-t és telefonszámot. Ezáltal megszemélyesítheti a lehallgatott klienst és ingyen hívásokat intézhet. A szolgáltatási díjcsalás a legnagyobb fenyegetés a VoIP-re.

A támadók keverhetik az azonosságukat úgy, hogy a SIP vezérlő csomagokat átirányítják a hívótól egy álcázott végpontra és a hívó tudtán kívül azzal kommunikálnak. A VoIP eszközök is sérülékenyek DoS támadásra; ami a TCP hálózatokon a SYN elárasztás, az VoIP hálózatokon az RTP szerver hívás elárasztása. A támadók számítógépeket is beköthetnek, hogy az VoIP eszközként működjön.Ezek az eszközök DoS támadás kivitelezésére is alkalmasak. Ha a támadó képes elfogni egy hang csomagot, akkor a folyamatban lévő beszélgetést lehallgathatja. A támadók RTP csomagokat is elfoghatnak, ami a kommunikációs kapcsolat médiafolyamát tartalmazza, azért, hogy video és hang adatot szúrjanak be. Ezzel megzavarják a kommunikáció résztvevőit.

A támadók megszemélyesíthetik a szervert és parancsokat adhatnak ki, például BYE, CHECKSYNC és RESET a VoIP parancsokat a kliensek felé. A BYE parancs a kommunikációs kapcsolat lezárását

eredményezi, beszélgetés közben, a CHECKSYNC újraindíthatja a VoIP terminálokat, a RESET a szerver kapcsolat megszüntetését és ismételt kapcsolat létrehozását eredményezi, ami sok időbe telik.

Megjegyzés: Mostanában, a hagyományos email spam-ek egy új változata terjed a VoIP hálózatokon, Ismertebb nevén a SPIT (Spam over Internet Telephony). SPIT a VoIP hálózat sávszélességének csökkenését okozza és az áldozatok idejét rabolja feleslegesen. Ugyanis a SPIT olyan spam, amit nem lehet törölni és az áldozat kénytelen végighallgatni a teljes spam üzenetet minden telefonhasználat előtt. A SPIT felelős a túlterhelt üzenetrögzítő szerverekért.

A VoIP biztonsági fenyegetettségek elleni harc jól átgondolt infrastruktúra tervet igényel. A VoIP és számítógépes hálózatok egyre hasonlóbbá válásával, a biztonsági egyensúly úgy teremthető meg, hogy csak kikényszerített forgalmat engedélyez. Az engedélyezés (authorization) használatával korlátozható az illetéktelen és jogosulatlan eszközök száma a hálózaton. A White-List alapú engedélyezés a leghatékonyabb biztonsági szempontból. Ez sem teljesen üzembiztos, de a védelem első vonalának megfelel, hogy ál-eszközök ne csatlakozzanak a hálózatra és tiltott csomagokkal ne árasszák el a hálózatot. Fontos továbbá, hogy a két VoIP eszköz authentikálja egymás azonosságát. Az authentikáció alapulhat hardver tulajdonságokon, mint MAC cím vagy valamilyen „szoftver” kód, ami szerver oldalon rögzített.

A biztonságos kriptográfiai protokollok használata, például a TLS, biztosítja, hogy minden SIP csomag egy titkosított és biztonságos csatornán utazik. TLS alkalmazása biztosíthatja a csatornát mind a VoIP kliens és szerver számára a lehallgatás és csomagmanipulálás ellen.

3.4.1 VoIP biztonsági intézkedések

A rosszindulatú felhasználók elkaphatják a kimenő hívásokat, DoS támadást végezhetnek és lehallgathatják a bizalmas beszélgetéseket. A legtöbb ellenintézkedés hasonló az adat-orientált hálózatokon alkalmazott védelmi intézkedésekhez:

- Frissítsék a hálózati eszközöket beleértve a VoIP-ért felelőseket: hívás kezelő szerver, üzenetrögzítő szerver és az átjáró szerver.
- azonosítsák az ismeretlen vagy ál-telefonrendszer eszközöket, vezessenek be authentikációt, azért, hogy csak engedélyezett eszközök legyenek a hálózaton
- telepítsenek és üzemeltessenek állapotmegőrző tűzfalat, VPN-t az érzékeny hanghívásokhoz, behatolás érzékelő rendszert
- tiltsák a nem használt portokat és szolgáltatásokat minden eszközön
- üzemeltessenek valós-idejű monitorozást, ami felderíti a támadásokat, csatornákat és a kéretlen hívás mintákat az IDS/IPS-en keresztül
- alkalmazzanak tartalom ellenőrzést
- használjanak titkosítást, amikor nem-megbízható hálózaton halad át az adat (hang, fax, video)
- kétfaktoros authentikálást használjanak
- korlátozzák a média gateway-en keresztüli hívások számát
- zárják be a média kapcsolatokat a hívás után

3.5 Mobil telefon biztonság

A legtöbb vállalat integrálja a hordozható eszközök és mobil telefon technológiák használatát a biztonsági szabályzatukba vagy hosszú távú biztonsági programjukba. Ez addig rendben is volt, amíg a telefonok csak telefonálásra voltak alkalmasak, de ma a telefonok már mini számítógépek, amik Weboldalakat böngésznek, sokféle eszközhöz csatlakozhatnak, ezért új támadási felületet jelentenek.

Amióta a mobiltelefonok már mini számítógépek, a legtöbbjük sérülékeny, kockázatot hordoz magában ez a fejlődő technológia. A mobilokra különböző támadási vektorokkal hatolnak be, malware-rel fertőzöttek lehetnek, érzékeny adatokat lehet lopni azokról, DoS támadást lehet intézni ellenük. Ma már egyének és cégek is banki tranzakciókat hajtanak végre mobiltelefonokon. Gyorsan fejlődnek a mobiltelefonok, így a technológiailag új megoldások miatt számos sérülékeny ponttal rendelkeznek.

A legnagyobb akadály a mobil és hordozható eszközök biztonságának területén, hogy az emberek nem tekintik a munkaállomással azonos biztonsági kockázatúnak a mobilokat. Nem telepítenek antimalware alkalmazásokat és nem frissítik a programokat, operációs rendszert, folyamatosan újabb alkalmazásokat/app-okat telepítenek rájuk hihetetlen számú funkcionalitással bármilyen elérhető Internetes oldalról. A mobil eszközök biztonságának hiánya nem csak az eszközön lévő adatokat veszélyezteti, de a legtöbben munkaállomáshoz csatlakoztatják a mobiljukat és engedik szinkronizálni. Ez egy ugró pontot jelent a mobil eszközön keresztül a számítógép hálózatra, ami akár a céges hálózat közvetlen elérését jelenti!

Mivel a mobil eszközöknek nagyobb háttértáruk van és rengeteg alkalmazás széleskörű funkciókkal érhető el azokon, ezért a felhasználók gyakran tárolnak rajtuk táblázatokat, dokumentumokat, kisebb adatbázisokat és sok minden mást. Ez azt jelenti, hogy sok mindent tesznek ki adatszivárgási kockázatnak.

A mobilok másik gyakori biztonsági problémája, hogy a telefonnak authentikálnia kell magát a bázis állomáshoz a hívás megindítása előtt, de a bázisállomásnak nem kell authentikálnia magát a telefon felé. Így a támadók ál-bázisállomásokat üzemeltethetnek. Ha egy ál-bázisállomás olvassa egy hozzá kapcsolódó mobil adatait, akkor későbbiekben felhasználhatja az adott eszköz megszemélyesítésére azt igazi rendszeren.

A telefon klónozás néhány éve ismert és nem lehet megszüntetni. Arról van szó, hogy egy normál mobilt ellophatnak és újra programozzák valaki másnak a hozzáférési jogosultságaival. A szervezett bűnözés és drogkereskedők egyik bevett gyakorlata a telefon klónozás. Így próbálják félrevezetni a rendfenntartó szervek előtt kilétüket. De ma már személyazonosság bejelentése nélkül is lehet GSM (Global System Mobile) telefonkészüléket és a SIM (Subscriber Identity Module) kártyát vásárolni. A SIM kártya tárolja az authentikációs adatokat, telefonszámot, elmentett üzeneteket, stb. Mielőtt a GSM telefon hozzáférést nyerhetne a mobil hálózathoz, a SIM-nek a készülékben kell lenni. Megjegyzés: a sürgősségi hívásra SIM nélkül is alkalmas minden készülék, ezt a törvény szabályozza. A támadók magát a SIM kártyát klónozzák, így hajthatnak végre hívásokat adott SIM tulajdonosát megszemélyesítve, az áldozat számlájára. Fontos tudni, hogy a mobil telefonok rádióhullámokkal érik el a bázisállomást, ezután az adatok vezetékes hálózaton továbbítódnak a szolgáltató hálózatán. Így a távolság egy részét, amit az adatnak utaznia kell,

vezeték nélküli kapcsolaton teszi meg, majd a fennmaradó részt vezetékes hálózaton. A vezeték nélküli szakaszon van titkosítás. Amint eléri a vezetékes hálózatot már nincs titkosítva a forgalom. Azaz a mobil hálózaton történő forgalmazás esetén nincs alapértelmezett végpont-végpont közötti titkosítás.

A mobilhálózatok sem mentesülnek a támadók újabb és újabb próbálkozásaitól, visszaéléseitől. Ez ugyanaz a macska-egér játék, amit már ismerhettünk a hagyományos hálózatok világából. A legnagyobb probléma a mobil készülékek elleni támadásokban van, mivel a mobil eszközök (telefon, okos eszköz, tablet) nincsenek a vállalatok biztonsági programjában, üzemeltetésében és még csak nem is kezelik potenciális biztonsági veszélyforrásként. Az elkövetett támadások számával ez lassan megváltozik, az újabb vírusokkal melyek a mobil eszközök, okos telefonok és tabletek használatával terjednek tovább a vállalati hálózatra. Néhány példa a mobil készülékek használatából eredő néhány problémára:

- hamis bázisállomást lehet üzemeltetni
- Bizalmas adatok lophatóak el
- A beépített kamerákat távolról vezérelhetik
- Közvetlenül elérhetik az Internetet a vállalati tűzfal megkerülésével
- SMS spamek
- Kártékony kód tölthető le
- A titkosítás lehet gyenge és nem végpont-végpont közötti

Néhány mobil szolgáltató kínál nagyvállalati megoldásokat, amely lehetővé teszi a hálózati üzemeltetőknek, hogy profilokat készítsenek, amit minden telefonra távolról telepítenek (deploy). Mai napig a BlackBerry rendelkezik a legrobosztusabb ilyen nagyvállalati szolgáltatásával. *Megjegyzés: Oroszországból 2008 óta ki vannak tiltva a BlackBerry telefonok, hivatalosan a határon elkobozzák.* Ahogy a céges alkalmazottak több és több BlackBerry-t, iPhone-t, iPad-et, Android-ot igényelnek, egyre bonyolultabbá válik a mobil készülékek központi felügyelete. A következő rövid lista néhány nagyvállalati mobil-biztonsági szempontot tartalmaz:

- csak azoknak az (mobil) eszközöknek szabad hozzáférést engedélyezni a vállalati erőforrásokhoz, melyek központilag felügyeltek, és központilag üzemeltetettek.
- Távoli szabályokat kell az eszközökre tolni, a felhasználói profilokat titkosítani kell, a lokális módosítás lehetőségét kizárva
- Az adat titkosítást, a késleltetett lezárást, a képernyőzárt, az authentikációt és a távoli adattörlést engedélyezni kell
- A Bluetooth funkciót ki kell kapcsolni, csak engedélyezett alkalmazásokat szabad telepíteni, kamera használatának szabályozását ki kell kényszeríteni, a közösségi oldalak elérését tiltani kell (Facebook, twitter, iwiw)
- A végpont biztonságot (endpoint security) ki kell terjeszteni a mobil eszközökre is
- a 802.1x vezeték nélküli VoIP klienst kell telepíteni a mobil eszközökre

A biztonság bevezetése és karbantartása minden egyes készüléken nagyon nehéz feladat, így az „eszköz lezárás” és határvédelem megközelítése és a szűrés egy keverékét kell alkalmazni és monitorozni.

3.6 Emberi tényező

Az emberi tényező tekintetében tisztán kell látni, hogy **a leggyengébb láncszem szinte mindig az alkalmazottak biztonság-tudatossága**! Ezen folyamatos képzéssel és szinten tartással lehet javítani. Sajnos még a profik is idővel belefásulnak a biztonságtudatos viselkedésbe. A **folyamatos biztonságtudatossági képzésre** szükség van.

Milyen gyakori problémákkal találkozhatunk?

- monitorra ragasztott jelszavak
- hitelesítő kártyára írt jelszavak
- 7/24-ben a kártyaolvasóban lévő elzáratlan hitelesítő végpontok
- titkárnőnél felírt vezetői jelszavak
- nyílt emailben továbbított jelszó, jelszó listák, tanúsítványok, minősített információk!
- telefonban elmondott személyes jelszavak
- tail-gating

Csak a vezetői támogatással és viselkedéssel lehet változtatni a hozzáálláson.

4 Megelőzés

Kétféle szemlélettel közelíthetjük meg, hogy hogyan kell felelősségteljesen végezni a munkát:

- Tisztán, csak a jogszabályoknak történő megfelelés.
- A professzionális mérnöki megközelítés a jogi megfelelést betartva.

Szerencsére a jelenlegi jogi szabályozás (2014) nagyon jól leírja (magas szinten) és megköveteli a mérnöki szakmai munkát. A 2013. évi L. törvény (továbbiakban Ibtv.) 77/2013. (XII.19.) NFM rendelete kötelezően teljesítendő feltételek ír elő az információ-biztonságot lefedve. **Kötelező olvasmány!** A törvény célja, hogy minden kormányzati rendszerre előírja az információbiztonsági szempontból teljesítendő minimum követelményeket. 5 szintre soroltatja bizalmasság, sértetlenség és rendelkezésre állás alapján a rendszereket. Minden szinthez előírja a teljesítendő kritériumokat. „Természetesen” hagy kiskapukat, viszont az Ibtv-től való eltérés csak alapos szakmai indokkal történhet. Már meglévő rendszereknél folyamatosan 2 évente kell legalább egy szintet javulni, amíg adott rendszer eléri az előírt besorolást. Új rendszerek esetén kötelezően kell teljesíteni a törvény (határozat) előírásait.

Térjünk vissza a mérnöki munkához. Bármilyen mérnöki alkotás elkészítése 3 (4) lépcsőből áll:

- **jelenlegi állapot felmérése** **- hol vagyunk**
- **elérni kívánt cél felmérése** **- hova megyünk**
- **célhoz történő eljutás megtervezése** **- merre kell menni**
- (megvalósítás - utazás)

Sajnos a profitorientált cégek esetén is előfordul hiányos mérnöki munka, viszont a kormányzatban „szinte” gyakorlat. Képzeljük el a fenti analógiával megfogalmazva: tudjuk, hogy Budapesten tartózkodunk, majd elindulunk síelni (mert ez a célunk), félúton kiderül, hogy minden pályát lezártak lavina veszély miatt. Így már csak egy megoldás maradt, elrepülni Dubai-ba a fedett pályára síelni (már csak erről a lehetőségről tudunk – és ez garantáltan működik). A példa a mérnöki tervezés fontosságát emeli ki, költség hatékony, kockázatarányos megoldást csak gyakorlott szakemberek képesek produkálni, megoldást „bárki”. A költséghatékonyságot pedig vizsgálni kell közép/hosszú távon is, gyakran elfelejtik az üzemeltetési költségeket.

Az informatikus munkája nem elég a sikeres felméréshez és célmeghatározáshoz, mivel az informatika minden esetben valamilyen más szakmát szolgál ki. Így a kiszolgált „ügyfél”-nek képesnek és hajlandónak kell lennie, hogy meghatározza mit vár az új (javítás esetén a jelenlegi) rendszertől. Mivel az információ-biztonsági törvény miatt minden szervezetnek felül kell vizsgálni az általa üzemeltett rendszereket, ott meg kell tudnia határozni milyen adatokat kezel az adott rendszer, azok mennyire bizalmasak, stb. Sok esetben csak az alkalmazás gazda aktív közreműködésével tudják elvégezni besorolást az Ibtv szerint.

Az első lépés bármilyen mérnöki munka esetén a „hol vagyunk” tisztázása. Mérjük fel a jelenlegi állapotot és kövessük nyomon a változásokat. Erre rendkívül nagy szükség lehet egy incidens kezelésekor is. Rossz példaként kell említeni, hogy sérülékenység-vizsgálatok során rendszeresen kerülnek elő **elfelejtett, nem-használt rendszerek**, ami lehet adminisztrációs hiba következménye is, de legtöbbször nem marad pénz adott rendszerek nyugdíjazására és/vagy alulmotiváltak az üzemeltetők. Természetesen az „elfelejtett” rendszerek a DMZ-ben vannak, nem tartják karban azokat, ezért sérülékennyé válnak és a támadók rendszeresen visszaélnek ezzel. Az „elfelejtett” rendszerek legegyszerűbb eliminálása a hálózati hozzáférésük megszüntetése – akkor legalább a hálózatra nem jelentenek további veszélyt.

Ha már van nyilvántartás az aktuális rendszerekről, akkor ez az információ bizalmas, legalább a nyilvántartott rendszer szintjének megfelelően. Ezért ezeket a nyilvántartásokat kiemelten kell védeni. Rossz példa: a központi monitorozó rendszer könnyű hozzáférhetősége esetén, a támadó átlátja a teljes rendszert és rossz esetben adminisztrátori jogosultsággal teszi ezt. Tehát az üzemeltetői hálózatot szeparáltan kell megvalósítani, lehetőség szerint legyen teljesen független (mint egy zárt láncú kamerarendszer). Üzemeltetés által leggyakrabban használt protokoll az SNMP, ennek v1 v2a és v2b verziója sérülékeny. Ha az eszközök támogatják v2c vagy v3 verziót kell használni.

Az Ibtv kockázatelemzés alapú rendszertervezést, rendszerüzemeltetést határoz meg, a ma használt informatikai szabványoknak megfelelően. A biztonság nem egy abszolút dolog (létezik tökéletes biztonság de elérni csak végtelen mennyiségű pénzzel lehet). **A biztonságnak mindig kockázat arányosnak kell lennie**. A mérnök meg tudja határozni az informatikai rendszer kockázatait, azokra jó ajánlást ad a törvény. Viszont az üzleti kockázatokat az alkalmazás gazdának kell meghatároznia, például mekkora kár keletkezik, ha 1 órára/napra/hétre kiesik az ország összes okmányirodája?

A következőkben tömör kivonatként megemlítjük az Ibtv-ben is előírt legszigorúbb rendszerekre vonatkozó követelményeket. Az Ibtv-ben teljes IT infrastruktúrára vonatkozó intézkedéseket fogalmaznak meg. A hálózatok biztonsága tekintetében, minden biztonsági intézkedést foganatosítani kell, hiszen a mai hálózati eszközök, saját operációs rendszerrel rendelkeznek és alkalmazásokat futtatnak.

Adminisztratív védelem

- Szervezeti szintű alapfeladatok
- Kockázatelemzés
- Tervezés
- Rendszer és szolgáltatás beszerzés
- Biztonsági elemzés
- Emberi tényezőket figyelembe vevő - személy - biztonság
- Tudatosság és képzés

Fizikai Védelem

- Fizikai és környezeti védelem

Logikai védelem

- Konfigurációkezelés
- Üzletmenet (ügymenet) folytonosság tervezése
- Karbantartás
- Adathordozók védelme
- Azonosítás és hitelesítés
- Hozzáférés ellenőrzése
- Rendszer- és információ-sértetlenség
- Naplózás és elszámoltathatóság
- Rendszer- és kommunikációvédelem
- Reagálás a biztonsági eseményekre

Maga az Ibtv rendelete is felsorolás jelleggel foglalkozik a kezelendő „problémákkal”, több szakterületet foglal össze, ezért egyes szakágak professzionális tudására van szükség.

4.1 Üzemeltetői hálózat

Minél nagyobb egy rendszer, annál erőforrásigényesebb a fenntartása. A hatékonyság növelését újabb technológiák, protokollok bevezetésével oldották meg. Például az otthoni router beállítását közvetlen csatlakozással lehet kezelni, míg egy nagyvállalati rendszer párszáz aktív hálózati elemét már nem lehet lokális hozzáféréssel menedzselni. Egy kritikus határt átlépve a költséghatékony üzemeltetéshez ki kell építeni egy üzemeltetői hálózatot, ami dedikált és csak erre a célra használható. Ma már szinte minden eszköz alapértelmezetten támogat olyan protokollokat, melyekkel az eszközök távolról menedzselhetőek. A feljebb említett SNMP protokoll is ezt a célt szolgálja. Az üzemeltetői hálózat alkalmas lehet az eszközök és tevékenységek naplózásának továbbítására, távoli elemzésére.

De ami jó az üzemeltetőknek az jó a támadónak is. Sok támadást gyorsított fel és/vagy tett lehetővé a védtelen „üzemeltetői” hálózat. Például SNMP v1 verzió esetén a community stringekkel kiolvassa a támadó az adott eszközök állapotát. Vagy lehallgatja a belső hálózati forgalmat és a nyílt jelszóval adminisztrátori jogosultságokkal képes „távmenedzselni” minden hálózati eszközt. Összefoglalva a központosított menedzsment megoldások erőforrás-hatékony megoldást nyújtanak, viszont SPoF (Single Point of Failure) egypontos hibalehetőséget nyújtanak. A menedzsment hálózatot legalább annyira meg kell védeni, mint az általa karbantartott rendszerek biztonsága – több rendszer esetén a kumulált biztonsági szint magasabb is lehet.

4.2 Naplózás, logelemzés

Az Ibtv tételesen leírja adott besorolású rendszerekre vonatkozó előírásokat. 5-ös osztályzatnál két fizikailag elkülönülő helyre kell rögzíteni a napló fájlokat. Miért van szükség naplózásra? Utólagos elemzéshez, hibák, támadások felderítéséhez. Azért kell legalább fizikailag két eltérő helyre menteni, mert egy képzett támadó el tudja „tüntetni” a támadásának nyomait. Ha letörli az egyetlen naplóállományt, akkor az utólagos elemzéssel sem lehet kideríteni mi történt.

4.3 Audit, sérülékenység-vizsgálat

Sokféle biztonsági tesztelési módszertan létezik az IT rendszerek ellenőrzésére. A legelterjedtebb az angolszász audit és a sérülékenység vizsgálat. Az audit, mint a PCI-DSS banki szabvány – ellenőrző lista alapú módszertan. Míg a sérülékenység vizsgálatok esetén valóságos támadások módszerét követik különböző mélységben. Mindegyik vizsgálat eredménye egy jegyzőkönyv, amit a megrendelő szervezet megkap. Ebben rövid, közép és hosszú távú javaslatokat tesznek a létező biztonsági hiányosságok kiküszöbölésére.

A rendszeres időközönként elvégzett vizsgálatok jó visszacsatolást adnak a megvalósított hibajavításokról, újabb hiányosságokról. A nemzetközi szabványok is előírják a rendszeresen végzett vizsgálatokat: ISO27002, Cobit, Fisma PCI-DSS.

Léteznek metodikák az alkalmazottak, üzemeltetők és folyamatok tesztelésére. Ezekkel foglalkozik az etikus hackelés.

5 Incidenskezelés

Mit kell tenni ha, kiderül, hogy megtörtént a baj? Természetesen valahogyan észlelni kell a problémát. A hálózati aktív eszközök közül az IDS és IPS képes riasztást jelezni. Az IPS-nél szabály alapon lehet meghatározni az automatikus beavatkozást. Hogy értelmes és hatékony reakciókat definiáljunk az IPS-ben, ahhoz üzemeltetni kell és folyamatosan visszacsatolni az újabb és kifinomultabb szabályokat. Felhívjuk

a figyelmet, hogy az üzemeltetés hiánya sérülékeny rendszerekhez vezet. **A sérülékeny rendszer által okozott károkért pedig a biztonsági vezető és az üzemeltető felel!** Nem minden környezetben célszerű önálló IPS megoldást alkalmazni, mert azt üzemeltetni is szükséges.

Az incidens kezelés nem szorítkozhat csupán a hibás viselkedés elhárítására. Ha informatikai biztonság szempontjából érett szervezetről beszélünk, akkor az rendelkezik incidens menedzsment rendszerrel. Adott esetben a hálózati incidens jelentése az incidenskezelő központba, szervezeti és nemzeti szinten is, további összefüggésekre világíthat rá, például egy átfogó, célzott támadás van előkészületben, folyamatban. A központban összefutó bejelentések elemzésével további jövőbeni lehetséges áldozatok védhetők meg. Az együttműködés nagyon fontos az incidensek kezelésénél.

Nemzeti szintű incidenskezelő központ feladatát a GOV CERT látja el a **233/2013. (VI. 30.) Korm. rendelet szerint (**lásd: http://www.cert-hungary.hu/node/23). Bejelentést bárki tehet. Az Ibtv hatálya alá eső szervezeteknek bejelentési kötelezettségük van. Tehát bármilyen, külső és/vagy belső érintettségű incidenst be kell jelenteni a GOV CERT-nek. Ha további intézkedésre van szükség, akkor a GOV CERT feladata továbbítani, leosztani, megoldani a feladatokat.

Sajnos a gyakorlati tapasztalatok azt mutatják, hogy sok támadást nem ismernek fel és ezért nem is kezelnek. Rosszabb esetben felismerik, de nem kezelik. Ennek több oka is lehet a felelőtlenségtől a bizalom hiányáig – ha kiderül, kirúgnak. **Törvényi kötelezettség bejelenteni az incidenseket a GOV CERT-nek!**

Ha támadás történt, akkor a kiértékeléshez nagy segítséget nyújthat az alábbi kérdőív (forrás: LarisaApril Long, Profiling Hackers, SANS Institute, 2012):

<table>
<tr><td>Célpont</td><td>ki? mikor?</td><td>Egyén</td><td>Cég</td><td>Kormányzat</td><td>Csoport</td></tr>
<tr><td colspan="2"></td><td colspan="4">Miért ez a célpont és nem másik hasonló?
Az áldozat volt az egyetlen megtámadott?
Kit támadtak még meg?</td></tr>
<tr><td colspan="2">Hacker</td><td>Egyén</td><td colspan="2">Csoport</td><td>Kormányzat</td></tr>
<tr><td colspan="2"></td><td colspan="4">Van Weboldaluk?
Vannak korábbi akciói?
Elkészíthető a támadó időbeli tevékenységének/fejlődésének története?</td></tr>
<tr><td colspan="2">motiváció</td><td colspan="4">Miért tették?
Megtévesztő és anyagi haszonszerzésből vagy hacktivizmusból cselekedték?</td></tr>
<tr><td colspan="2">Módszer</td><td colspan="4">Van valamilyen jellemzőjük/aláírásuk?
Milyen eszközöket és technikákat használtak?
A tudásuknak megfelelően, létezik olyan eszköz, technika, amit használhattak volna, de nem tették?
Szükségük volt alapos, átfogó kutatásra és felderítésre a támadáshoz?</td></tr>
<tr><td colspan="2">Kiváltó ok</td><td colspan="4">Volt valamilyen előzménye a támadásnak? Letartóztatás? Új törvény? Fenyegetés?</td></tr>
<tr><td colspan="2">Akadályok</td><td colspan="4">Milyen biztonsági intézkedéseket, megoldásokat kellett kijátszaniuk?
Átjutottak a tűzfalakon, IDS-en, útválasztókon, erős jelszavakon?
Sikeres volt a támadás?</td></tr>
<tr><td colspan="2">Jövő</td><td colspan="4">A jelenlegi tudás ismeretében, tekintve a célpontot és a támadót, folytatja a támadást a támadó?</td></tr>
</table>

5.1 Üzletmenet folytonossági terv (BCP)

Miért van szükség a folyamatos üzletmenetre? Felmérések alapján az az informatikai cég amely 1 hét „kényszerszünetet” tartott azok 50%-a és amelyek legalább kettő hét „kényszerszünetet” tartottak azok 80%-a csődbe ment 1 éven belül. Persze mondhatja valaki, hogy az állami szervezetek monopol helyzete miatt nem érdemes foglalkozni üzletmenet fenntartásával. Az is igaz, hogy a BCP terv nem hiányzik senkinek és különben is sok erőforrásba kerül megalkotása, tesztelése, amíg nem történik incidens. Az Ibtv adott besorolású rendszerekre kötelezően előírja BCP és DRP tervek elkészítését, tesztelését és karbantartását.

A mai rendszerek legtöbbje kommunikáció központú, például; Web-alkalmazás -szolgáltatás dedikált szervereken vagy nyilvános felhőben. Ezért a hálózati szolgáltatás folyamatos üzemének biztosítása az egész rendszerre nézve kritikus.

Amennyire kritikus a hálózati infrastruktúra az informatikai rendszerekre nézve, annyival könyebb BCP tervet készíteni, mivel A BIA (üzleti hatás analízis) alapján be kell kérni az alkalmazás-gazdáktól a szükséges szolgáltatási szint (SLA) paramétereket:

- adat sebesség, átvitel
- tartalék kommunikációs csatorna
- karbantartási ablak
- QoS
- késletetés, késleltetés ingadozás
- szolgáltatás kiesési idő

A BCP terv nem minden esetben informatika függő, például a reptéri beléptetéskor, ha elérhetetlenné válik a számítógépes nyilvántartás, akkor az előre nyomtatott listákkal tudják folytatni a beszállítást.

5.2 Katasztrófa terv (DRP)

Fel kell készülni természeti katasztrófák – villám, árvíz, erős havazás… - esetén is folytatódhasson az ügymenet. Hálózatbiztonsági szempontból ez többnyire kimeríti a redundáns és tartalék kommunikációs vonalak üzemeltetését, gyors elérését. Mielőtt bárki azt hinné, hogy erre sosem kerül sor: 2013-ban árvíz veszély miatt leállították a Kossuth tér kormányzati infrastruktúráit.

Kritikus hálózati szolgáltatások esetén gyakran előre felkonfigurált tartalék eszközökkel rendelkezik a hálózat üzemeltető.

A katasztrófa terv elkészítése során ki kell dolgozni, a katasztrófa-helyzet megszünése utáni, normál üzemre történő visszaállást.

5.3 IT Forensics

A forensics nyomozati munkát jelöl, megtörtént események kiderítését – „mi történt?”. Az események rekonstruálására akkor is szükség van, ha a hibát már elhárították. Egyrészt azért, hogy a

jövőben ne fordulhasson elő hasonló esemény, másrészt azért, hogy szándékos károkozás esetén felelősségre vonják az elkövetőt.

Az IT forensics során szintén a bizonyítékok elemzésével foglalkoznak, itt a bizonyítékok a naplózást, az érintett gépek lementett állapotának elemzését jelentik. Az IT forensics nagyon kis százalékban tud konkrét támadást/ támadót kimutatni, mivel a gyakorlatban kevés és nem megfelelő minőségű log áll rendelkezésre; a támadást túl későn észlelik és a nyomok teljesen „eltűntek"; a támadó sikeresen letörölte a támadás nyomait. Sokszor nem tudja az adott üzemeltető kit kell keresni, mit kell tenni. A tervezés itt is segít: ha szabályzat részletezi az üzemeltető feladatait és/vagy az üzemeltető megfelelő oktatáson esett át akkor tud helyesen eljárni.

Ökölszabályként: az érintett gép merevlemezéről hiteles másolatot kell készíteni. Adott géptől és környezettől függően kell eldönteni, hogy másolat elkészítéséhez le lehet/kell állítani a gépet. A naplózás megfelelő mélységéről gondoskodni kell. Egy érzékenyre állított tűzfal nagyságrenddel több logot termel, mint amekkora forgalmazás folyik. Az Ibtv ajánlása szerint legalább a forrás és cél IP/port és időpont kerüljön naplózásra, lehetőség szerint az igénybe vett protokollal.

Egy negatív példa: NAT-olt hálózatok esetén csak a kimenő cím látszik a külső szolgáltatónál lévő naplózásban. Ha nincs naplózva a NAT mögül kimenő forgalom, akkor nem lehet azonosítani a támadót (fertőzött gépet). Ez a mai modern malware-ek, botnet-ek esetén kritikus, mivel tényked̈esüket felfüggesztik és utólag nem lehet megtalálni a fertőzés forrását, így nem lehet megszűntetni támadásukat.

6 Kormányzati célú speciális hálózatok

346/2010. (XII. 28.) Kormányrendelet, a kormányzati célú hálózatokról: „A kormány, egységes rendeletben szabályozta a kormányzati célú elektronikus hírközlést, az elektronikus hírközlési tevékenységet, a hálózatokon a szolgáltatás nyújtásának és igénybevételének a feltételeit."

6.1 Nemzeti Távközlési Gerinchálózat (NTG)

Az NTG (elődje az EKG - Egységes Komrányzati Gerinchálózat) a kormányzat számára kialakított zárt, gerinchálózat, amely a kormányzat különböző helyszíneit köti össze, többnyire üvegszálon keresztül, gyűrű topológiával. A zárt jelző azonban nem igaz, mivel a kormányzat által nyújtott szolgáltatások egy része az interneten keresztül érhető el – lásd ügyfélkapu – minek következtében az Internet „be van csövezve" az NTG-re. Természetesen DMZ, tűzfal és egyéb védelmeken keresztül érhető el az Internet az NTG-ről. Az NTG-re csatlakozó ügyfelek különböző szolgáltatásokat használhatnak:

- Vezetékes hangszolgáltatások, VOIP technológiával
- Adatkommunikációs szolgáltatások (a felhordó hálózat hozzáférés-típusai: szimmetrikus elérés; aszimmetrikus elérés; IP SEC VPN elérés; mobil elérés)

- Internet-hozzáférés szolgáltatások (dedikált sávszélességű, központilag menedzselt, védett internetelérést biztosítunk saját VPN központjukban, menedzselt tűzfal rendszeren keresztül)

AZ EKG-ról (forrás: http://www.ekk.gov.hu/hu/emo/ekg/ekg):

„Az Elektronikus Kormányzati Gerinchálózat (EKG) egy olyan informatikai hálózat, amelynek feladata, hogy a kormányzati és közigazgatási adatbázisokat, hálózatokat és informatikai rendszereket összekapcsolja a vonatkozó kormány rendeletben meghatározott kormányzati körnek, - valamint a különböző kormányzati szolgáltatások elérhetőségét biztosítsa a civil szféra számára.

...

Az EKG célja:

1. Nagy sebességű, ***nagy üzembiztosságú és magas biztonsági követelményeknek megfelelő****, egységes architektúrájú hálózati infrastruktúra biztosítása a civil szféra számára az állami intézmények által nyújtott szolgáltatások eléréséhez (Front-Office feladatok);*

2. Az ***új infrastruktúrára épülő szolgáltatások*** *és egyes eddig elszigetelt (pl. ágazati) hálózatok elérhetővé tétele a jogosult felhasználók számára (Back-Office feladatok) ;*

...

4. ***Kormányzati szintű, több felhasználó által használt alkalmazások*** *hatékony működtetése;*

...

6. A kétirányú kormányzati ***kapcsolatok biztosítása a brüsszeli adminisztráció*** *rendszereihez (csak az EKG-n keresztül lehetséges !!!)*

7. A minisztériumok és a központi intézmények részére biztosítson ***védett, - security, - szolgáltatások*** *nyújtását és elérését.”*

6.2 Egységes Digitális Rádiórendszer (EDR)

Az EDR védett kommunikációt megvalósító kormányzati célú „vészhelyzeti mobilhálózat”. Legismertebb felhasználói a rendvédelmi szervek, a mentőszolgálat és a katasztrófavédelem. A korábbi URH rádiós rendszer lehallgatható volt, míg az EDR-ben megvalósított kommunikáció titkosított. A felhasználók egy erre a célra átalakított mobiltelefont használnak. Működése egy walki-talkie-hoz hasonló, adatküldéskor (beszéd megkezdésekor) meg kell nyomni egy gombot és a kiválasztott csatorna (csoport) minden tagja hallja a kommunikációt. Lehetőség van adott készülék direkt hívására. 24 órás ügyeletben érhető el a diszpécser, aki bármilyen üzemeltetési kérdésben segít. Az EDR rádiók jellemzője még, hogy pontos helymeghatározással rendelkeznek, így a vészhívó gombbal a rendvédelmi szervek azonnal a segítséget kérő készülékhez, tulajdonosához vonulnak. Vészhívás esetén a segítségnyújtásig állandó adásban marad az adott készülék.

Megjegyzés: a nemzetközi terminológiában az EDR rendszer megfelelője a TETRA (Terrestrial Trunked Radio).

7 Felhasznált irodalom

Buttyán Levente, Vajda István: Kriptográfia és alkalmazásai, Typotex, Budapest, 2004

Buttyán Levente, Dóra László: Wifi biztonság – A jó, a rossz és a csúf, Crysys LAb., Budapest, n.a.

Dr. Berta István Zsolt: Nagy e-szignó könyv, Microsec Kft., n.a., 2011

Andrew S. Tanenbaum, David J. Wetherall: Computer Networks 5th ed. Pearson. n.a., 2011

Shon Harris: CISSP Eexam Guide, McGrawHill, New York, 2013

ISACA: CISM Review Manual, ISACA, USA, 2013

Larisa April Long: Profiling Hackers, SANS Institute, n.a., 2012

Nokia: Nokia Systra Training Document, Nokia Networks Oy. na., 1985

Todd Lammle: CCNA Routing and Switching Study Guide, Sybex, Indianapolis, Indiana, 2013