Debreceni Egyetem

Informatika Kar

Egységesített kommunikációs rendszerek az IT biztonság tükrében

Témavezetők:

Dr. Almási Béla

Egyetemi docens

Segyik István

Rendszermérnök

Cisco Systems Magyarország Kft.

Készítette:

Király László

Mérnök informatikus BSc

Debrecen

2009

Tartalomjegyzék

Bevezetés

Napjaink nélkülözhetetlen részét képezik a különböző telekommunikációs és hálózati rendszerek. Bizonyos rendszerekkel kifejezetten az üzleti életben találkozhatunk, míg mások mindennapi életünk szerves részévé váltak. Dolgozatom egyik célja, hogy bemutassam melyek a ma használt legnépszerűbb kommunikációs technológiák, és hogyan olvadnak össze ezek egyetlen integrált rendszerré a vállalati környezetekben.

A kommunikációs és hálózati rendszerek használhatóságán túl, nagyon nagy szerepet kap a megbízhatóság és a védelem, egyre több kérdés és igény merül fel azok biztonságával kapcsolatban. Fontosnak tartok néhány olyan információvédelmi és hálózatbiztonsági témakört, amelyek elengedhetetlenek egy mai, modern, biztonságos vállalati rendszer tervezéséhez és üzemeltetéséhez. Az általános IT biztonsági témakörökön túlmenően részletesebben ismertetek biztonsági technológiákat és ajánlásokat, majd az egységesített kommunikációs rendszerek aktuális hálózatbiztonsági problémáinak vizsgálatára is sor kerül.

A dolgozat utolsó részében a tárgyalt ismeretanyaghoz kötődő gyakorlati feladat dokumentációja található, mely egy cég rendszerén elvégzett biztonsági felmérés menetét tartalmazza. A felmérést követő kiértékelés mellett javaslatokat tettem a biztonsági szint növelése érdekében, figyelembe véve a kockázatok mértékét.

A dolgozat egészére jellemző, hogy számos szabványos és Cisco specifikus hálózati ismeretre, ajánlásra és megoldásra támaszkodik. A megértéshez ezért bizonyos szinten tisztában kell lennie az olvasónak a hálózati alapfogalmakkal.

Diplomadolgozatom megírása során saját ismereteim és tapasztalataim felhasználása mellett, nagyon sokat kaptam külső témavezetőmtől, Segyik Istvántól, akinek ezúton is nagyon szeretném megköszönni szakmai segítségnyújtását, átadott tapasztalatait és türelmét.

Témaválasztás indoklása

Témaválasztásom fő indoka, hogy tanulmányaim, szakmai versenyek, szakmai szövegek fordítása kapcsán egyre közelebb kerültem a számítógépes hálózatokhoz és az alapismeretek megszerzésén túl fontosnak tartom, hogy bizonyos területeken mélyebb tudást, specializációt szerezzek. A dolgozatomban tárgyalt témakörök (egységesített kommunikáció, hálózatbiztonság) potenciális fejlődési irányt jelentenek számomra az IT szakmában. Gyakornokként egy hazai rendszerintegrációs vállalatnál a gyakorlati oldalról is szemügyre vehettem néhány tárgyalt technológiát és tanulhattam tapasztalt kollégáimtól.

A szakmában szerzett eddigi tapasztalataim alapján úgy látom, hogy ez az iparág rendkívül gyorsan fejlődik, napról-napra új dolgok születnek, melyek olyan kihívások elé állítják az embert, ami folyamatos tanulásra, fejlődésre késztet.

1. Az egységesített kommunikációs rendszerek bemutatása

A technológiák fejlődésével és elterjedésével a vállalati és lakossági területeken többféle kommunikációs forma jelent meg. Ezek alapvetően hang és adat alapú távközlési rendszerek. A vállalatok felismerték azt, hogy gazdaságosabb csupán egyetlen hálózatot fenntartani mind az adat, mind a hangszolgáltatások számára. Az integrált rendszerek amellett, hogy gazdaságosabbak, a kommunikációs formák összefogásával lehetővé teszik a felek közötti hatékonyabb együttműködést.

Az egységesített kommunikációs (Unified Communications, UC) rendszerek összefogják a valós idejű kommunikációs szolgáltatásokat, mint például az azonnali üzenetküldés (instant messaging, IM), IP-telefónia (VoIP), videokonferencia, hívás és hangvezérlés, valamint az olyan nem valós idejű rendszereket, mint az e-mail, integrált hangposta, fax és sms szolgáltatások. Az utóbbi nem valós idejű (aszinkron) rendszereket korábban az Egységesített Üzenetváltás (Unified Messaging, UM) névvel illetett rendszerekben próbálták összefogni, azonban ezek a megvalósítások kevésbé terjedtek el. Ezzel szemben a modern UC rendszereket egyre nagyobb arányban használják a kis-, közép- és nagyvállalatok is, bízva az új rendszer nyújtotta előnyökben. (Gregory [2008])

1.1 Élet az egységesített kommunikáció nélkül

A mai dolgozó emberek kezében számos kommunikációs lehetőség van. Ilyenek az irodai telefon, hangposta, fax, e-mail, az azonnali üzenetküldés (IM) különböző formái, valamint ma már elterjedőben vannak a webes kollaborációs megoldások és videokonferenciák. Azonban ezek a technológiák összefogás nélkül csak részben elégítik ki a szükségleteket, minden problémára nem jelentenek megoldást.

A mobiltelefonok és PDA-k, valamint a laptopok által biztosított mobilitásnak köszönhetően a vállalati dolgozók az irodán kívül, út közben is dolgozhatnak. A mobilitás új kihívásokat jelent, hiszen nem csak a vállalati hang és adathálózat kiterjesztéséről van szó az interneten keresztül, hanem meg kell oldani, hogy a vállalati kommunikációs lehetőségek a legnagyobb mértékben és minőségben elérhetők maradjanak a mobil dolgozók számára. (Gregory [2008])

A következő kérdések és problémák merülnek fel, ha sokféle, egymástól független technológiát használunk:

- A kommunikációs csatornák nem tudnak egymásról.
- A különálló hálózatok fenntartása költséges, probléma esetén a hibaelhárítás időigényes.
- Egymás elérhetőségeiről nincs egységes adatbázis, ezért nem mindenki rendelkezik a megfelelő kapcsolati információkkal.
- A nyilvános rendszerek jelentette biztonsági kockázat (nyomon-követhetőség, dokumentáltság, naplózás, és biztonság hiánya).

Hátrányokkal is rendelkeznek a konvergált hálózati rendszerek: ha nem elég robosztus és biztonságos egy integrált kommunikációs rendszer, akkor egyetlen meghibásodás, támadás vagy katasztrófa is megbéníthatja a vállalati kommunikációt. Míg az egymástól független rendszerek, például a hagyományos PSTN[1] telefonos és az elektronikus levelezést véve, ha az egyik felmondja a szolgálatot, a másikon keresztül továbbra is kapcsolatban maradhatunk a külvilággal. Gondoskodni kell a megfelelő védelemről, redundanciáról és tartalék (backup) kommunikációs vonalakról, hogy érvényesüljenek a technológia nyújtotta előnyök, az esetleges hátrányok nélkül.

1.2 Az érintett technológiákról

Az UC rendszerek működése szoros összefüggésben áll az IP telefóniás, VoIP rendszerekkel. Gyakorlatilag azok funkcionális kibővítésének, továbbfejlesztésének tekinthetők.

[1] Public switched telephone network: a világ nyílvános áramkörkapcsolt telefonos hálózata

1.2.1 A VoIP

A VoIP (Voice over IP) és az IP telefónia összefüggő, gyakran egymással felcserélt kifejezések. Mindkét fogalom mögött az a megvalósítási forma értendő, hogy egyetlen, közös hálózati infrastruktúra segítségével (hang, adat, multimédia), IP csomagok segítségével kerül megvalósításra a kommunikáció (konvergált hálózatok).

A VoIP a korábbi vonalkapcsolt megoldások helyett a csomagkapcsolt hangátvitelt hivatott megvalósítani. Az ok, amiért leváltásra szorulnak a régi technológiák, a csomagkapcsolt megoldások olcsóságában, megnövekedett teljesítményében, rugalmasságában, bővült funkcionalitásban és a nagy gyártók által „kitalált" egyéb előnyökben keresendő.

Maga a VoIP kifejezés hang átvitelét jelenti az IP protokoll használatával. A név tükrözi, hogy a technológia IP csomagok segítségével továbbítja a hangrészleteket, melyeket ténylegesen szállító (UDP, RTP, SRTP) és jelző protokollok (SIP, H.323, SCCP) segítségével juttatja el a másik félhez, és az ott lévő VoIP kliens (hardveres vagy szoftveres megoldás) segítségével az emberi fül számára is hallható hangként szólalnak meg.

A hanginformációk az analóg-digitális átalakítás után egy megfelelő hang kodek (ITU G.711, G.729) segítségével beágyazható formába kerülnek. A kodek felel azért, hogy a minőségi követelményeket figyelembe véve, szállítható méretűre lehessen csökkenteni a hangrészleteket. Egy-egy csomag általában 20 ms időnyi hangot hordoz. A beágyazás egy úgynevezett valós idejű szállítási (RTP, Real Time Transport Protocol) protokoll használatával történik. Ez UDP protokoll segítségével kerül beágyazásra az IP csomagba. Az RTP protokoll felel a csomagok sorba rendezéséért és a hibakezelésért. Hasonló feladatokat lát el, mint a TCP protokoll, ám az robosztussága miatt jelentős többletterhelést (és késleltetést) okozna, ezért nem megfelelő a valós idejű audio és/vagy video kommunikációra.

A jelzési protokollok végzik a hívás felépítési, kezelési és lebontási feladatokat. Léteznek szabványos protokollok (H.323, SIP, MGCP) és gyártó specifikus megoldások (SCCP, IAX2[2]). Napjainkban a SIP protokoll számít népszerűnek egyszerűsége miatt, korábban a H.323 (ami több protokoll esernyőprotokollja) volt az elterjedt.

[2] Az Asterix PBX rendszerek natív protokollja, mely jelzési és médiahordozási feladatokat lát el.

Egy VoIP rendszer összetevői a következők:

- Végponti eszközök: hardveres IP vagy szoftveres (softphone) megoldások, melyeken keresztül kommunikálnak egymással a felhasználók.
- Átjárók: többnyire olyan forgalomirányítók, melyek átjárást valósítanak meg a PSTN (ISDN, analóg), a mobil és az IP hálózatok között.
- Hálózati infrastruktúra eszközök: hangfeldolgozásra optimalizált forgalomirányítók, és olyan PoE (Power over Ethernet) kapcsolók, melyek az adatok hordozására használt UTP kábelen tápellátást biztosítanak az IP-telefonoknak vagy a vezeték nélküli hozzáférési pontoknak.
- Hívásvezérlő központ: hívásirányítási, híváskezelési és címfordítási feladataik vannak. (A hagyományos telefonos rendszerek alközpontjaihoz hasonlóak.)
- Egyéb alkalmazás kiszolgálók: hangposta, konferenciahívás vezérlő, interaktív ügyfélszolgálati központ, segélyhívó szolgáltatás.

Nagyon fontos követelménye a VoIP hívásoknak a megfelelő sávszélesség és időzítés biztosítása. Ehhez már a kisebb hálózatok esetén is alkalmazni kell QoS (Quality of Service, Szolgáltatás minősége) technikákat. A QoS segítségével nagyobb prioritással kezelhetőek a VoIP csomagok, így azok a többi csomagnál előbb kerülhetnek továbbításra. Tipikusan 100 ms (az ITU-T G.114 szerint 150 ms) a maximálisan megengedett késleltetés VoIP esetén, egy irányban és a csomagveszteség 1% esetén már jelentősnek mondható. Akkor a leghatékonyabb egy hálózatban a QoS funkciója, ha az IP csomagok minél hamarabb osztályozásra és megjelölésre kerülnek fontosságuk vagy típusuk alapján. A jelölés megtörténhet már adatkapcsolati szinten (CoS, Class of Service) a 802.1p specifikáció alapján, de elvégezhető a harmadik rétegben is az IPv4 csomagfejrész ToS (Type of Service, Szolgáltatás típusa) mezőjének segítségével. (Ranjbar [2007] 1. fejezet)

1.2.2 E-mail

Az elektronikus levél 1966-os első megjelenése óta (mainframek kora) egyre népszerűbbé vált, mára a hagyományos postai kézbesítést kiszorítva a leggyakoribb üzenetküldési forma az élet minden területén. Az üzenetek küldését és fogadását meghatározott protokollok végzik: a küldésért az SMTP (Simple Mail Transfer Protocol) felel, a fogadást kezelheti például a POP3

(Post Office Protocol version 3**)** vagy az IMAP (Internet Message Access Protocol) protokoll.[3] Vállalati környezetekben gyakran találkozhatunk olyan gyártói megoldásokkal, mint a Microsoft Exchange vagy a Lotus Notes (ezek gyakran gyártói protokollokat használnak). Az egységesített kommunikációs rendszerek képesek arra, hogy minden beérkezett üzenetet, legyen az hangposta üzenet, fax egyetlen levelező postafiókba továbbítsanak, így biztosítva, hogy egy helyről lehessen értesülni és válaszolni azokra.

1.2.3 Azonnali üzenetküldés

Az UC rendszerek egyik szolgáltatása az azonnal üzenetküldési lehetőség (IM). Az interneten felnőtt új generáció egyik kedvenc kommunikációs formája. Hatékonyan használható az üzleti párbeszédek során is. A párbeszéd szöveges alapú, és azonnali, valós idejű üzenetváltást biztosít. A különböző felhasználók egy központi kiszolgálóra jelentkeznek be és azon keresztül szereznek tudomást partnereik állapotáról. Egyes rendszerek a bejelentkezés után peer-to-peer alapon működnek, tehát az egyes felhasználók között közvetlen kommunikációs kapcsolat jön létre, nem terhelve a központi kiszolgálót. A szöveges üzenetek mellett lehetőség van állományok és multimédiás tartalmak megosztására is. Az UC rendszereknél központilag tárolt adatbázisban, egyetlen azonosítóval (pl. AD tartománynév vagy e-mail cím) hivatkozhatunk a felhasználókra.[4]

1.2.4 Fax

Dokumentumok másolatának átvitelére használható telekommunikációs technológia. Napjainkra a dedikált fax készülékek még sok helyen használatban vannak (részben hitelességi okok, részben szokások miatt). Léteznek fax kiszolgálók, melyek képesek a vállalatnak küldött fax üzeneteket digitális formában a felhasználó e-mail postafiókjába továbbítani, de analóg konverterek segítségével is IP-képessé tehetők a fax készülékek.[5]

---

[3] http://www.multicians.org/thvv/mail-history.html

[4] http://en.wikipedia.org/wiki/Instant_messaging

[5] http://en.wikipedia.org/wiki/Fax

1.2.5 Mobiltelefonok

Az UC rendszerek képesek integrálni a meglévő vállalati mobil kommunikációt, így a mobil munkaerő a munkahelyétől távol is kihasználhatja a technológia előnyeit. A telefonra telepített megfelelő kliens és csomagkapcsolt vagy Wi-Fi elérés segítségével használhatjuk a vállalati IM, e-mail, VoIP és video kommunikációs lehetőségeket. Ami fontos, hogy ugyanazon telefonszám vagy felhasználói azonosító segítségével hivatkozhatnak ránk, bárhol is vagyunk. Jelenleg még csak a fejlettebb operációs rendszerrel rendelkező mobilkészülékek UC-képesek (Nokia E-sorozat).

1.2.6 Videokonferencia

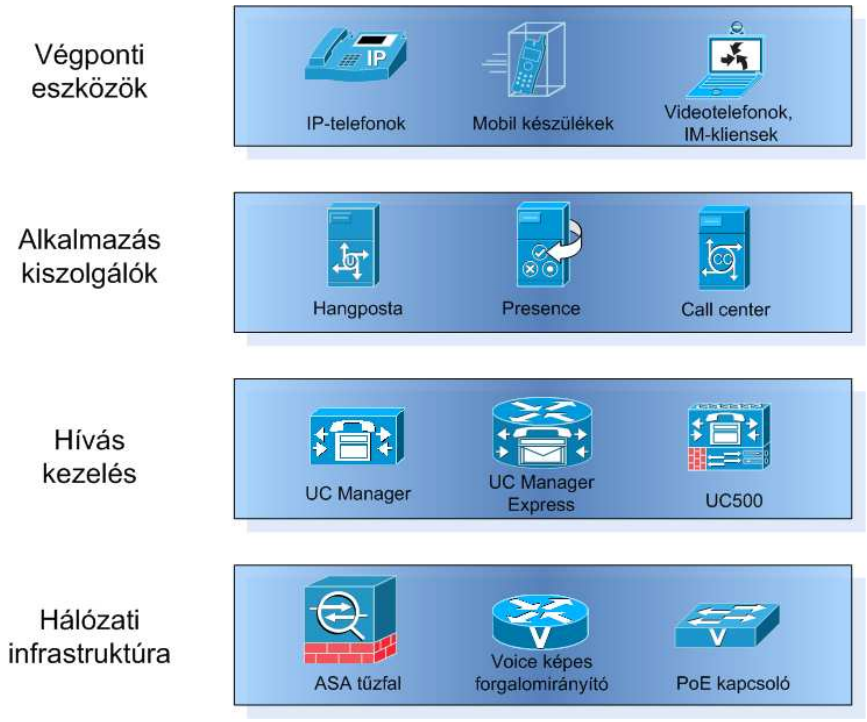
Hatékony és takarékos megoldása az egymással való kapcsolattartásnak. Több fél is részt vehet a valós idejű képet és hangot biztosító kommunikációban. A vállalati munka során a csoportmunka és a megbeszélések népszerű eszköze. Az UC rendszerek is rendelkeznek videokonferencia funkciókkal, így egyetlen rendszerből kezdeményezhető a video hívás is.

1.2.7 Webes kollaboráció

Egyidejűleg több felhasználó számára biztosít együttműködési lehetőségeket úgy, mint az alkalmazások és dokumentumok megosztása, vagy a video és hang kommunikáció. Az együttműködés bármilyen környezetben lehetségessé válik, ahol van internet kapcsolat és egy böngésző. Az UC alkalmazásokból is lehetőség van valós időben megosztani a számítógép képernyőjét vagy átadni az irányítást.

1.3 Cisco Unified Communications

A következőkben egy valós UC rendszerről, a Cisco egységesített kommunikációs megoldásáról lesz szó. A Cisco Unified Communications termékei elterjedésük és funkciógazdagságuk miatt jó hivatkozási alapul szolgálnak a technológia bemutatásához. A rendszer modellje többrétegű, akár az OSI-modell. A rétegek közötti átjárhatóságot többféle szabványos és gyártó specifikus protokoll oldja meg. A szabványos technológiák lehetővé teszik, hogy az egyes rétegekben teljesen más gyártók termékeit használjuk. Az 1. ábrán a bemutatásra kerülő rendszer modellje látható. (Cioara – Cavanaugh – Krake [2009] 2. fejezete alapján)



1. ábra: A Cisco egységesített kommunikációs modellje

1.3.1 Hálózati infrastruktúra

A kommunikációs rendszer hálózati infrastruktúrájának fő építőkövei közé tartoznak, a klasszikusnak számító forgalomirányítók és kapcsolók mellett, az analóg telefonokat támogató és a hagyományos analóg/digitális telefonos hálózatokkal való kommunikációt megvalósító átjárók, valamint a tápfeszültséget szolgáltató PoE kapcsolók. Az eszközök voice-enabled (hang-feldolgozásra képes) megnevezése azt jelenti, hogy rendelkeznek a valós idejű hang és videojelek feldolgozásához szükséges teljesítménnyel. Ezeket a funkciókat a digitális jelfeldolgozó processzorokkal (dsp) ellátott bővítőkártyák és modulok külön beszerelésével is el lehet érni. Az infrastruktúra támogatja a meglévő vállalati alközponti telefonos rendszerek és többletszolgáltatások (hangposta) megtartását, ami lehetővé teszi a fokozatos bevezetést.

Az infrastruktúra részét képezik az eszközöknek IP-cím információkat biztosító DHCP-kiszolgálók, valamint a konfigurációs és eszköz firmware állományokat tároló TFTP-kiszolgálók.

1.3.2 Híváskezelés

A Cisco UC megoldásának központi híváskezelő és feldolgozó szoftvere a Unified Communications Manager (régi, megszokott nevén Cisco Callmanager, CCM), ami jelenleg (2009. szeptember) a 7.1-es verziónál jár. A rendszer fizikailag egy kiszolgáló számítógépen fut (például IBM, HP vagy Cisco MCS[6] szerveren) és létezik Windows és Linux rendszer felett megvalósított változata is. Skálázhatósága miatt, a maximálisan kiszolgálható felhasználók száma 30 000 felett is lehet (klaszterek esetén 60 000+).

Kisebb szervezetek esetén a hívások feldolgozását a Callmanager mellett végezhetik például a Smart Business Communications System névre keresztelt család Cisco Unified Communications 500-as sorozatú eszközei is. Korlátozott funkciókra egy Cisco ISR (integrált szolgáltatáskészletű) forgalomirányító is megfelel, a rá töltött Unified Communication Manager Express szoftverrel (IOS telephony service). Ezek az eszközök használhatóak a Callmanager kiszolgálóval párhuzamosan is, ekkor elláthatnak tartalék szerepet (SRST, Survivable Remote Site Telephony) egy esetleges WAN kapcsolati leállást esetén.

[6] http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_models_home.html

1.3.3 Többletszolgáltatások

Az alkalmazás kiszolgálókon többletszolgáltatásokat biztosító rendszerek futhatnak (például: hangposta (Unity), automatikus hívásközpont (IVR) vagy a segélyhívások kezeléséhez szükséges helymeghatározó kiszolgáló, stb.).

Egyik fontos UC szolgáltatás a Presence. A szó arra utal, hogy a rendszer visszajelzést ad a felhasználók állapotáról és azok kommunikációs lehetőségeiről. Ez a funkció már jól ismert az internetes azonnali üzenetküldő programoknál (nincs a gépnél, elfoglalt, szabad), kiegészülve azzal, hogy felsorolja, milyen módon érhetjük el partnerünket: például hang, szöveges, video vagy webes kollaborációs formában.

1.3.4 Végponti eszközök

Számos kommunikációs végponti eszköz használható a rendszerben. Közös jellemzőjük, hogy Ethernet felületen vagy vezeték nélkül kapcsolódva, az IP hálózaton keresztül kommunikálnak egymással és egy szabványos, vagy gyártó specifikus jelzés protokoll segítségével végzik a hívások kezelését.

Teljes körű szoftveres kommunikációs felületet biztosítanak a Cisco IP Communicator[7] és a Cisco Unified Personal Communicator[8] alkalmazások. Az előbbi kinézetre teljesen hasonlít egy valódi IP telefonra és biztosít minden azon elérhető funkciót, utóbbi más publikus IM alkalmazásokhoz hasonlóan, (pl. Skype) egy ablakból biztosítja a hang, video és szöveges kommunikáció kezelését.

A hardveres IP telefonok vezetékes és vezeték nélküli változatai nagy számban elérhetőek. A vezetékes IP telefonok tulajdonságai között szerepel, hogy a tápfeszültséget képesek az adattovábbításra használt kábelből nyerni, ha egy PoE (Power over Ethernet) képes kapcsolóhoz csatlakoznak. Másik érdekesség, hogy a telefonok tulajdonképpen önmagukban is egy 3 porttal rendelkező kapcsolónak felelnek meg. Az egyik porton kapcsolódnak trönkvonal kialakításával az IP hálózat kapcsolójához, a második porton maga a készülék kapcsolódik a hálózathoz, a harmadik port pedig a telefonra fűzhető számítógép csatlakoztatására szolgál.

---

[7] http://www.cisco.com/en/US/products/sw/voicesw/ps5475/index.html

[8] http://www.cisco.com/en/US/products/ps6844/index.html

Így egyetlen kábelen csatlakozik a telefon és a számítógép, ami jelentős költségmegtakarítást eredményez a fizikai kábelezési igényeknél.

A régi analóg telefonok használatát is támogatja a Cisco UC rendszere. Az Analog Telephone Adaptor (ATA) névre keresztelt eszközök segítségével az IP hálózatra köthetők analóg telefonok és faxok. A VG224 és VG248[9] analóg telefonos átjárók használatával 24 vagy 48 analóg készülék használatára is van lehetőség (kisebb költségvetésű, IP funkciókat nem igénylő területeken használják).

A Cisco videós termékei között megtalálhatóak egyszerűen használható szoftveres változatok (Cisco Unified Video Advantage) - melyek a meglévő hardveres vagy szoftveres IP telefonunk funkciókészletét bővítik ki a video telefonálás lehetőségével - valamint a Tandberg eszközeihez hasonló hardveres video IP telefonok (Cisco IP Video Phone 7985G[10]) is.

A végponti eszközök körébe tartoznak a vállalati kommunikációt megkönnyítő videokonferenciás megoldások. Számos gyártó forgalmaz videokonferenciás termékeket: Tandberg (amely jelenleg már Cisco tulajdonban van), Sony, Polycom, Microsoft Netmeeting; melyek között a szabványos protokollok (H.323, SIP) teremtik meg a kompatibilitást. (Ugyanakkor a Cisco termékei a gyártó saját SCCP (Skinny) jelzés protokollját alkalmazzák elsődlegesen.) A három vagy annál több helyszínes virtuális találkozók lebonyolításához, a felek közötti szükség van úgynevezett Multipoint Control Unit (MCU) berendezésekre, ilyen például a Cisco Unified 3540 MCU[11]. Feladata a különböző résztvevők video és audio jelének szinkronizálása és a hívások vezérlése. A résztvevők által látott kép és hang lehet dinamikusan változó, az aktuálisan beszélő felet mutatva, vagy lehet folyamatosan megjelenített, az aktuálisan beszélő partner mellett, a képernyő szélén kis négyzetekben minden résztvevőt megjelenítve. A megjelenített kép minősége mára már eléri a HD 1080p minőséget (ez megfelelő berendezést és sávszélességet igényel).

Léteznek vezeték nélkül csatlakozó (Wi-Fi) képes IP telefonok is, melyek a vállalaton belül minden vezeték nélküli hálózati lefedettséggel rendelkező területen használhatóak, akár egy mobiltelefon. Kiterjeszthetők az UC előnyei a fejlett operációs rendszerrel rendelkező

[9] http://www.cisco.com/en/US/products/hw/gatecont/ps2250/index.html

[10] http://www.cisco.com/en/US/products/hw/phones/ps379/prod_models_home.html

[11] http://www.cisco.com/en/US/products/hw/video/ps1870/tsd_products_support_series_home.html

mobiltelefonokra, más néven okostelefonokra is. Az ezekre telepített segédprogram lehetővé teszi, hogy bárhol elérhetőek maradjanak a vállalati kommunikációs formák.

A későbbi fejezetek megértéséhez hasznos tudni az IP telefonok indulási folyamatát, mely az alábbiakban olvasható:

1. Az IP-telefont csatlakoztathatjuk a hálózathoz. A tápfeszültséget felveheti a hálózati kábelről (PoE) vagy hálózati adapteren keresztül is.
2. A telefon betölti a memóriájában lévő firmware-t (image fájl).
3. A kapcsoló CDP-n keresztül megadja a telefon hang VLAN azonosítóját.
4. A telefon DHCP kérést küld a hálózatra.
5. A DHCP kiszolgáló válaszol a kérésre, IP-cím információkkal, és a DHCP Option 150 paraméter segítségével a TFTP kiszolgáló IP-címét is elküldi a készüléknek,
6. A telefon felveszi a kapcsolatot a TFTP-kiszolgálóval és letölti a konfigurációs állományát.
7. Végül a telefon kapcsolatba lép a konfigurációs állományban lévő legelső Callmanager kiszolgálóval.

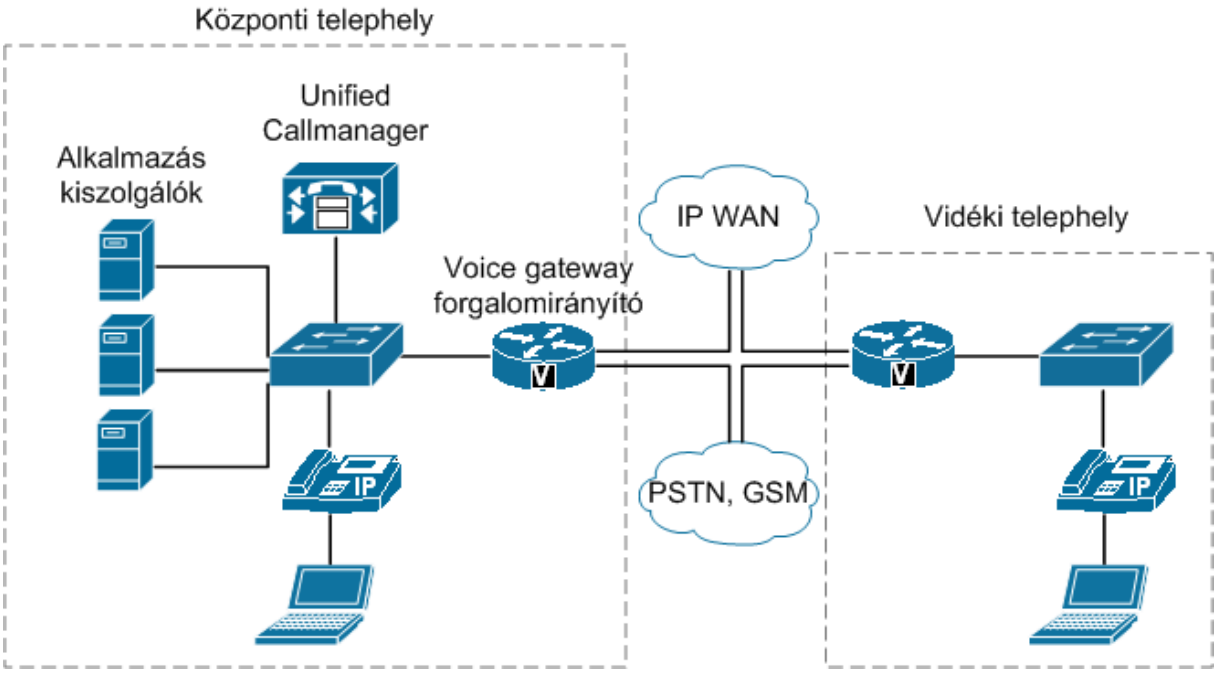
1.3.5 QoS

A hang alapú kommunikáció által támasztott késleltetési, sávszélességi és csomagveszteségi követelményeknek való megfelelésért, a Cisco UC megoldásai tartalmaznak QoS funkciókat. Többek között a forgalomosztályozás (traffic classification), sorkezelés (queuing), forgalomszabályozás (traffic shaping), a tömörített RTP protokoll (cRTP) használata és a TCP fejrészek tömörítése tartozik a QoS funkciók körébe. A QoS feladatok többségét az IP hálózati infrastruktúra kapcsolói és forgalomirányítói végzik.

1.3.6 Kiépítési változatok

A Cisco UC többféle kiépítési változatban működhet. Az egyetlen telephellyel rendelkező szervezetek mellett rugalmasan használható a több helyszínnel rendelkező vállalatok esetén. A kiépíthető centralizált változatban, ekkor a fő telephely ad helyet a híváskezelésért felelős Callmanager központnak, amellyel a másodlagos telephelyek UC eszközei egy WAN

kapcsolaton keresztül kommunikálnak. Ennek előnye a centralizáltság, ami jóval kevesebb eszközt igényel a másodlagos telephelyeken, ezáltal kevesebb helyre, energiára és pénzre van szükség. A rendszer használható elosztott hívás feldolgozási módban is, ekkor minden telephely rendelkezik a saját központjával. Lehetőség van a központok között klaszterek létrehozására, ami redundanciát és terheléselosztást biztosít.



2. ábra: Egyszerű UC topológia

A vállalatok számára rendkívül fontos a költséghatékonyság és a befektetés mihamarabbi megtérülése (ROI, Return On Investment), ezért ez a rendszer fokozatosan bevezethető és alapjaiban a meglévő IP hálózati infrastruktúrára támaszkodik. A 2. ábrán a rendszer egy egyszerű összeállítása látható. (Pintér Z. [2008])

2. Információbiztonság, hálózatbiztonság

Az elektronikus kommunikáció előnyei mellett számos új, adataink és szolgáltatásaink ellen irányuló veszéllyel kell szembenéznünk. A kockázatok csökkentésével az információ biztonság több részterülete is foglalkozik. Ezek közül részletesebben az IT biztonság legfontosabb tervezési elveit és a hálózati biztonság tipikus témaköreit szeretném tárgyalni, melyek jó alapot adnak a biztonságos adat és az IP-telefóniás hálózatok kialakításához és üzemeltetéséhez.

2.1 Az IT biztonság alapelvei

Az itt tárgyalt alapelvekről részletesen az ISC^2 CISSP tananyagban lehet olvasni.

2.1.1 Okok és veszélyek

Valós oka van annak, hogy miért beszélnek ilyen sokat az információ biztonságáról. A kommunikációs rendszereinket számos okból érhetik támadások (Thomas [2005]):

- Ellenségeket szereztünk egy vállalati alkalmazott, üzleti vetélytárs, családtag személyében.
- Anyagi helyzetünkre fény derült (tranzakciós csalások, zsarolások gyakori áldozatai).
- Politikai érdekeket sértő tevékenységet végzünk.
- Rendszerünk kihívást jelent a támadók számára (ez adta kezdetben a motivációt a 70-es, 80-as évek „ártatlan” hackereinek).

A veszélyek két típusra bonthatóak: külső és belső veszélyek. A felmérések szerint a támadások 60-80%-a belülről érkezik (Computer Security Institute, Kalifornia), védekezni nehezebb ellenük, mint a külső támadásokkal szemben. (Watkins – Wallace [2008])

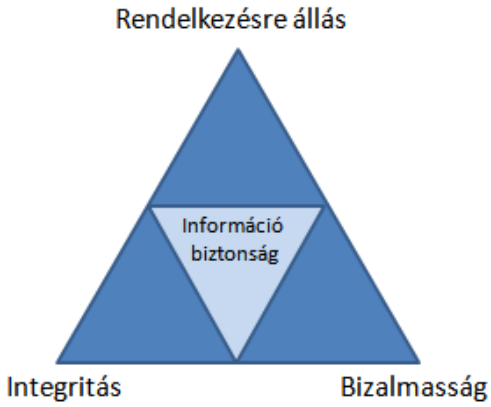
A vállalatokat és magánszemélyeket ért támadások néhány jellemző következménye:

- Adatokkal való visszaélés, zsarolás, ipari kémkedés
- Távközlési kapacitás lopása

- A termelés kiesése, csökkenése, anyagi kár
- Az ügyfelek bizalmának elvesztése, kártérítési kötelezettség
- A vállalat fennmaradása kérdésessé válik

2.1.2 Információbiztonsági fogalomhármas

Az információbiztonság célja és lényege a következő három fogalom alapján körvonalazódik (ISC^2 CISSP [2008]):



3. ábra: A három alappillér

Rendelkezésre állás (availability): a koncepció szerint adataink és rendszereink elérhetőségét biztosítanunk kell, mert bármikor szükségünk lehet rá. A rendelkezésre állást veszélyeztető tényezők például az emberi hibák, szoftveres hibák, fizikai meghibásodások, képzetlen munkaerő, kártékony programkódok vagy bármely olyan veszély, amely rendszerünket használhatatlanná vagy megbízhatatlanná teheti.

Bizalmasság (confidentiality): ez az információk titkosságát és diszkrécióját jelenti. Ez a védelem kiterjedhet üzleti, pénzügyi és személyes információkra. Egyre több előírást és törvényt hoznak e területen.

Integritás (integrity): amely az információ pontosságát és érintetlenségét hivatott biztosítani. Törekszik az adatok helyes feldolgozására, és megelőzi a szándékos vagy véletlen módosításokat. Ez a koncepció az adatok érzékenységével van összefüggésben

2.1.3 Az adatok osztályozása

Az információk és az adatok bármilyen formában is értékes üzleti tulajdont képeznek. Mint bármilyen más védendő tárgy esetén, az információ védelmének mértékét meghatározza annak értéke. Minden információt egyenlő súlyúnak és értékűnek tekinteni se nem hasznos, se nem kívánatos. Ezért van szükség az adatok osztályokba sorolására.

A szakirodalom kétféle alapvető osztályozást tart nyílván: létezik: a kormányzati/katonai és a kereskedelmi/szervezeti osztályozás. Az előbbi 5 osztályt különböztet meg: nem besorolt adatok; érzékeny, de nem besorolt adatok; bizalmas adatok; titkos adatok; szigorúan titkos adatok. A kereskedelmi osztályozás 4 eltérő típust határoz meg: nyilvános; érzékeny; privát; bizalmas. (Watkins – Wallace [2008])

A kereskedelmi adatok osztályozásba kerülnek azok az adatok és információk, melyeknek pénzügyi értékük van. Azonban nincs egyértelmű válasz arra, hogyan határozható meg az adatok értéke. Vizsgálni kell az adat aktuális piaci értékét (például amit a konkurencia megadna érte), az adatok újbóli előállítási költségét és azok elvesztéséből eredő károk mértékét (bizalomvesztés, forgalomkiesés).

2.1.4 A kockázatkezelés szerepe

Mit, miért és mitől kell megvédenünk? Ilyen és ehhez hasonló kérdésekre keresi a választ a kockázatkezelés. A megelőzés általában olcsóbb, mint a kezelés, ám csak a feltárt kockázatok ellen lehet megfelelően védekezni. A kockázatkezelés összetett feladat, azonban az ebbe fektetett munkának köszönhetően a szervezetek felkészültebben, költséghatékonyabban és gyorsabban védekezhetnek a veszélyekkel szemben.

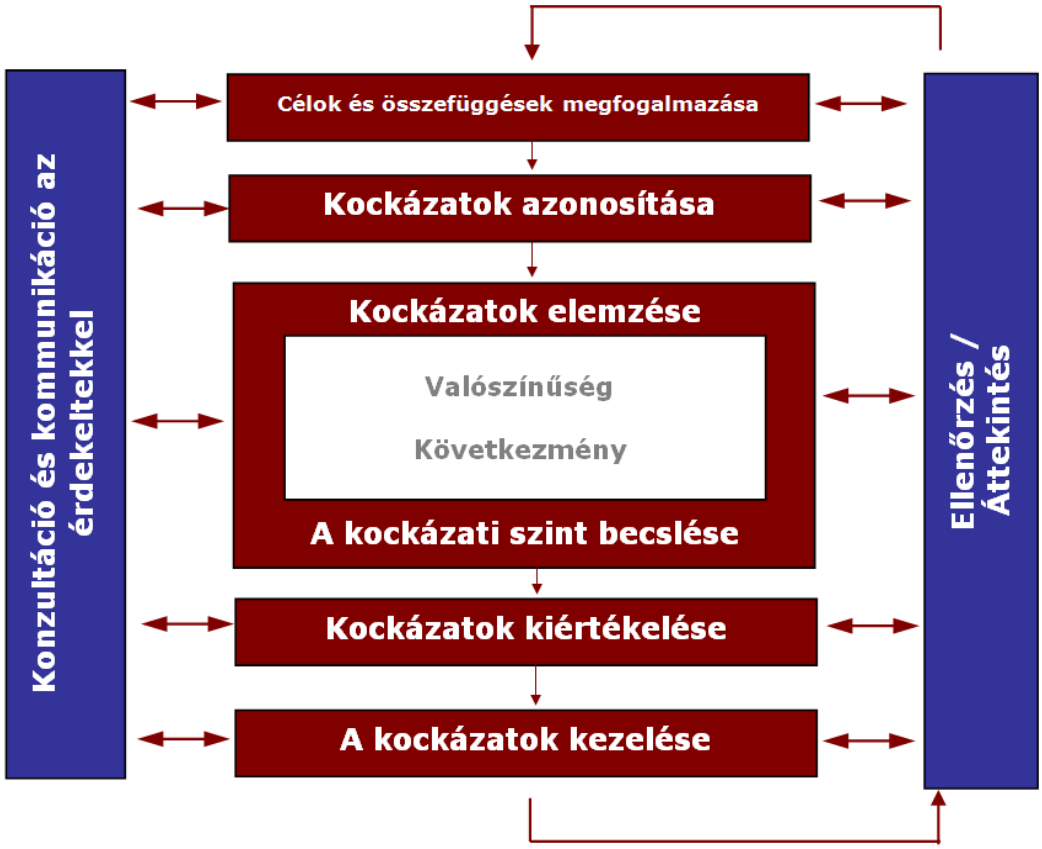
A kockázat magában foglalja a veszély, a sebezhetőség és a vagyon fogalmakat. Veszélynek tekintünk minden olyan emberi vagy természetes eshetőséget, melynek nemkívánatos hatása lehet a vállalati tulajdonra. Sebezhetőségnek nevezzük a védelem gyengeségét vagy hiányát, mely a veszélyek bekövetkezésének valószínűségét és hatásuk súlyosságát növeli. A tulajdon pedig minden olyan erőforrás, folyamat vagy termék, mely valamilyen értéket képvisel a szervezet számára. A veszély és a sebezhetőség kettőse adja a

kockázatot. (ISC[2] CISSP [2008]) Az AS/NZS 4360:2004 szabvány szerint a kockázat valami bekövetkezésének a valószínűsége, amely jó vagy rossz hatással van saját tulajdonunkra.[12]

A kockázatkezelés folyamata

A kockázatkezelés folyamatának bemutatásához külön szeretném kiemelni az AS/NZS 4360 (Australian Standard/New Zealand Standard 4360 vagy ANZ 4360) szabványt, mely egyszerűen és sok területen használható, általános kockázatkezelési vázat ad. A szabvány 2004-es változata tömören és tisztán (26 oldalban) fogalmazza meg a kockázatok azonosításához, kiértékeléséhez, kezeléséhez, felügyeletéhez és a szükséges eljárásokat és definíciókat.) Bár a szabvány használata licencköteles, sok ismertető található az interneten.

A kockázatkezelés munkafolyamatait szeretném szemléltetni (4. ábra) és röviden leírni az alábbiakban.



4. ábra: A kockázatkezelés folyamata az AS/NZS 4360 szerint

[12] http://www.ucop.edu/riskmgt/erm/documents/asnzs4360_2004_tut_notes.pdf

A kockázatkezelési folyamatokkal párhuzamosan, állandó kommunikációra van szükség a kiértékelendő szervezet menedzsmentjével. Közös munkával meg kell fogalmazni az elemzés céljait és stratégiai elveit és az elemzésre szánt tulajdont és területeket.

A kockázat azonosítás során azonosítják a veszélyeket, sebezhetőségeket és a védendő tulajdont.

A kockázat elemzés egy összetett munkafolyamat. Azonosítani kell a meglévő kontrollok hatékonyságát és az azok által nyújtott védelmi szintet a felismert kockázatokkal szemben. Minősítő (kvalitatív) vagy számszerűsítő (kvantitatív) módszerekkel kategorizálni kell a veszélyeket.

A kiértékelés során el kell dönteni, hogy egy adott kockázat elfogadható vagy sem. Az elfogadhatónak ítélt kockázatokat felügyelni kell, és időnként újra meg kell vizsgálni.

Az elfogadhatatlan szintet elérő kockázatokat kezelni kell. A kezelés lehet a tevékenység megszüntetésével elért elkerülés, a kockázat bekövetkezési valószínűségének vagy a következmények súlyosságának csökkentése, illetve a következmények áthárítása külső félre (például biztosítási szerződésekkel).

A munka végén szükség van arra, hogy értékeljék a kockázatkezelés hatékonyságát és visszajelzést adjanak a folyamatok során tapasztaltakról.

Szakdolgozatom utolsó fejezetében, a hálózati rendszer elemzése során feltárt biztonsági kockázatokat, az AS/NZS 4360 szabványban leírt osztályozás alapján, kvalitatív módszerrel fogom értékelni. A kvalitatív módszer szubjektív szemszögből tekint a kockázatokra. Egy-egy kockázat súlyosságának megítéléséhez figyelembe kell venni a szakértői véleményeket, gyártói ajánlásokat, szakirodalmakat és saját tapasztalatokat. A besoroláshoz a következő valószínűség-következmény mátrix nyújt segítséget (1. táblázat).

	Következmény				
Valószínűség	1 (jelentéktelen)	2 (kicsi)	3 (mérsékelt)	4 (jelentős)	5 (katasztrofális)
A (majdnem biztos)	H	H	E	E	E
B (valószínű)	M	H	H	E	E
C (lehetséges)	L	M	H	E	E
D (valószínűtlen)	L	L	M	H	E
E (ritka)	L	L	M	H	H

E	Extrém kockázat: Azonnali beavatkozás szükséges az elhárításhoz, vagy kerülni kell a tevékenység folytatását
H	Magas (high) kockázat: Beavatkozásra van szükség a kockázat ellensúlyozására
M	Mérsékelt (moderate) kockázat: Beavatkozásra van szükség a kockázat ellenőrzéséhez, nyomon követéséhez
L	Alacsony (low) kockázat: Előfordulása általánosan elfogadott

1. táblázat: Az ANZ 4360 szabvány kvalitatív kockázat besorolási mátrixa

A táblázat segítségével osztályozhatóak a felismert kockázatok, és sorba rendezhetőek fontosságuk alapján. A kockázatok besorolása után meg kell határozni azok kezelésének (treatment) mikéntjét. A kockázat kezelési módok közé tartozik a kockázat elfogadása, a kockázatot eredményező tevékenység megszüntetése, a kockázat átadása harmadik fél részére (pl. biztosítással), a bekövetkezés valószínűségének vagy a következmény súlyosságának csökkentése. A szabvány külön tárgyalja a kockázatok felügyeletét és áttekintését, a konzultációk fontosságát, a dokumentációk készítését, valamint a kockázatok forrásait és hatásait.

2.1.5 A költségek és a védelem

Az ügyfelek részéről a védelmi megoldások kiválasztásának egyik legfontosabb kritériuma a költséghatékonyság, melyet a ráfordítás-nyereség analízis útján próbálnak meghatározni. Ezt a következő egyszerű példa szemlélteti:

Egy elektronikus kereskedelemmel foglalkozó cég az interneten ad el termékeket. (A vizsgált időtartam 1 év). A cég éves szinten 400 ezer dollár bevételre tesz szert (ebből 360 ezer

az éves bevétel, 40 ezer dollár pedig az ügyfelekről tárolt adatok piaci értéke). A vizsgált kockázat az, hogy a cég kiszolgálóit feltörik és ellopják az adatokat. Az elemzők szerint évente kétszer fordulhat elő egy ilyen támadás, és a bekövetkezés után körülbelül 5 hétre van szüksége az adatok helyreállításához és a szolgáltatások újraindításához (5 hét / 52 hét ≈ 10%). Ezekből az adatokból kiszámolható az éves várható veszteség költsége (ALE[13]), amit áttételesen úgyis lefordíthatunk, hogy mekkora legyen a védelemre fordítható maximális költség.

$$ALE = 400 \text{ ezer} * 0{,}1 * 2 = 80 \text{ ezer dollár}$$

A kapott értéket össze kell vetni a kockázat ellensúlyozására használható védelmi megoldás beszerzési és telepítési költségeivel. Példánkban egy összesen 40 ezer dollárba kerülő hálózati IPS berendezés beiktatásával 80 %-ban kivédhetőek az említett támadások, tehát megéri befektetést. Ez a példa persze csak a szemléltetést szolgálta, de az eljárás egy valós helyzetben, valós értékek mellett döntéstámogató szereppel rendelkezik. (Segyik [2007]: Security Management I. előadás)

2.1.6 Biztonsági házirendek

A hálózatok biztonságának fenntartásához az első lépés a megfelelő biztonsági politika kialakítása. A biztonsági politika szabályok és útmutatások gyűjteménye. Ezek lehetnek szabványok, irányelvek, eljárások. (Thomas [2005] alapján)

Egy jó házirendben a vállalat minden alkalmazottjára vonatkozik a szabályok valamelyike, így például az általános felhasználók, a vezetőség, a könyvelés és a biztonsági csoport is megismerheti és megértheti, mit, miért és hogyan kell végezni az adott munkakörben a biztonság fenntartásáért.

A házirendnek tartalmaznia kell a támadásokat követően végzendő beavatkozási lépéseket. A támadásokra való reagálás leghatékonyabb módja, ha rögzítve van egy beavatkozó csoport (például rendszergazdák és szakértők), akik már a támadás előtt fel vannak készítve a válaszlépésekre és nem a támadás utáni feszült helyzetben próbálják megérteni azokat.

[13] ALE = Annual Loss Expectancy

Számos szabályzatról olvashatunk a www.sans.org/resources/policies webhelyén, melyet a SANS Institute[14] biztosít a nyilvánosság számára. Ezek közül néhány példa: vírusvédelem, jelszavak, virtuális magánhálózat, vezeték nélküli kommunikáció.

Törekedni kell a jó biztonsági házirend összeállítására és alkalmazására, ennek eléréséhez érdemes követni az alábbi ajánlásokat:

- a szabályokat tisztán, érthetően és tömören kell megfogalmazni
- a szabályzat legyen könnyen hozzáférhető és naprakész
- a vezetők mutassanak példát az alkalmazottaknak a szabályok betartásával
- járjon következményekkel, ha nem tartják be a biztonsági rendet
- a szabályok illeszkedjenek az üzleti folyamatokhoz, tehát ne legyenek túl bonyolultak

2.2 Tervezési alapelvek

2.2.1 Mélységi védelem

A mélységi védelem (defense in depth) egy információbiztonsági stratégiai elv, mely a többrétegű védelmen alapul.

Alappilérei:

- Biztonságmenedzsment alapelvek: ezek közé tartoznak például az adatok osztályozási szabályai, a biztonsági szabályzatok és eljárások, és a biztonsági törekvéseket tudatosító továbbképzések
- Biztonsági technológiák: tűzfalak, IPS/IDS rendszerek, végpont védelmi megoldások, biztonsági protokollok

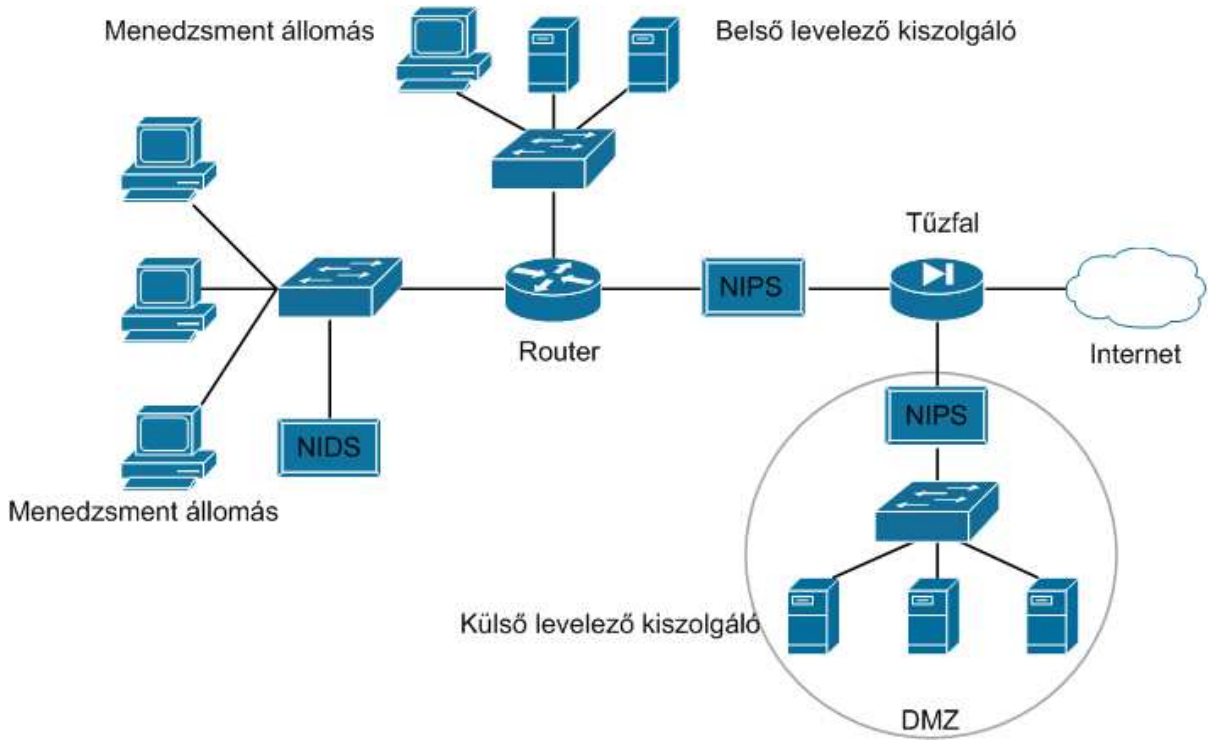
Ez a védelmi stratégia azt próbálja meg elérni, hogy a rendszerünk védelme ne csak egyetlen pillérre épüljön, mert az akaratlanul is kárhozatra van ítélve.

[14] Elsősorban IT biztonsági oktatással és minősítéssel foglalkozó szervezet.

A mélységi védelem elve eredetileg egy katonai stratégia volt, melynek célja a késleltetés, nem pedig a totális védelem. A hálózatok esetén sem biztos, hogy teljességgel kivédhetők a támadások, viszont időt nyerhetünk vele, így észlelhetjük és reagálhatunk egy támadásra.

A mélységi védelem mellett törekednünk kell az egyedi hibapontok (Single Point of Failure, SPOF) kiküszöbölésére. A hálózat egy pontját akkor nevezzük egyedi hibapontnak, ha annak meghibásodása az egész rendszer leállását okozhatja. Számos technológia létezik ennek kikerülésére: megbízható rendszertervezés (reliable system design), magas rendelkezésre állás (high-availability), klaszterek, tükrözés (RAID mirroring), failover rendszerek. A rendszerek rendelkezésre állását egy évre levetítve, százalékos formában, általában 9-es számokkal jelölik. Az úgynevezett „ötkilences” (99,999%) rendelkezésre állás például azt jelenti, hogy egy évben maximum 5 perc 16 másodperc leállás engedhető meg.

Az 5. ábra jól példázza a mélységi védelmi stratégia elveit.



5. ábra: Többszintű védelmi rendszer

Látható a topológiában egy külső és egy belső levelező kiszolgáló. A külső levelező kiszolgáló továbbítóként funkcionál a belső számára, így a támadónak mindkét kiszolgálót meg kell tudnia támadni a belső céges levelezés veszélyeztetéséhez. A több helyen implementált hálózati behatolás érzékelő (NIDS) és hálózati behatolás gátló (NIPS) eszközök egymást

kiegészítve jelzik a támadásokat. Az internet felé vezető kijáratot pedig a peremvédelmi tűzfal védelmezi.

Ezek mellett gondoskodni kell a megfelelő számú és biztonságú menedzsment állomásról, melyekről elvégezhető a hálózati eszközök beállítása és felügyelete. Ezek biztonsága azért kiemelkedően fontos, mert egy rájuk mért sikeres támadás után kikerülhetők a biztonsági rendszerek. (Watkins – Wallace [2008])

2.2.2 Komplexitás és egyszerűség

Az egyik legnehezebb tervezési feladat a bonyolultság és az egyszerűség közötti optimális út megtalálása. A túl bonyolult rendszerek természetüknél fogva megnehezítik a hálózati rendszergazdák és a felhasználók munkáját, ám a túl egyszerű megoldásokkal sem érdemes megkönnyíteni a támadók dolgát.

2.2.3 A jogosultságok minimalizálása

A hálózat védelem kialakításához egy jó megközelítés, ha az egyes felhasználókhoz a rájuk bízott feladatok ellátásához szükséges legkevesebb jogosultságot adjuk ki. Ez azt feltételezi, hogy alapból a „tilts meg mindent” szabály érvényes mindenkire és csak a legszükségesebb dolgokat engedélyezzük külön-külön. Ezt a szakma a legkisebb jogosultságok elvének nevezi (Policy of Least Privilege). A felhasználónkénti jogok meghatározása az üzemeltetés vagy a rendszergazda feladata. Azonban megvannak a maga hátrányai is ennek a megközelítésnek: sok adminisztrációs munkát jelenthet akkor, ha vannak olyan felhasználók, akik csak ritkán használnak bizonyos szolgáltatásokat. Ezért meg kell találni azt a maximális biztonsági szintet, mely lehetővé teszi a hatékony munkát, mind az üzemeltetés, mind a felhasználók részéről. (Thomas [2005])

2.2.4 Felhasználói tudatosság

A legjobban megírt biztonsági házirend és a legjobb védelmi mechanizmusok sem érnek semmit sem, ha a rendszer felhasználói nem értik meg a biztonsági alapelveket és azok célját. Tudatossá kell tenni a felhasználókat a megfelelő oktatások és továbbképzések segítségével. Az ilyen képzéseknek többes célja van, egyrészt meg kell ismertetni a felhasználókkal a biztonsági

veszélyeket, másrészt az ezek kivédésére használható legújabb biztonsági technológiák használatát. (Thomas [2005])

2.2.5 Nyomkövetés

A biztonságos hálózat egyik fontos összetevője - a tényleges biztonsági eszközök mellett - a nyomkövetés és a megfigyelés lehetősége. A folyamatos nyomkövetés bizonyítékot ad arról, hogy a rendszer tényleg biztonságosan működik, sikeresen hárítja el a támadásokat. Manapság ezt a feladatot főként a behatolás jelző rendszerek látják el. Tanácsos azonban az összes hálózati eszköz állapotüzenetit egyetlen központi helyre gyűjteni. Ez elősegíti a támadások kiértékelését. (Watkins – Wallace [2008])

2.3 Támadások, fenyegetések

Az élet szinte minden területe valamilyen szinten kapcsolatban van a világhálóval. A jó szándékú internetes felhasználók által kialakított virtuális világ mellett párhuzamosan létezik a sötét oldal is. A hálózatok többsége ma már csatlakozik az internethez, ezáltal bárhonnan, bármikor elérhetővé válik, jobbára csak a jogosult felhasználók számára. A probléma a jogosulatlan hozzáférésekkel és a károkozással van. Az ellenséges szándékú egyének vagy csoportok adatainkat próbálják megszerezni, szolgáltatásokat, vállalatokat bénítanak és zsarolnak meg, vírusokat, kémprogramokat és más kártékony szoftvereket írnak. Kik ők és mitől kell félnünk? Ezekkel a kérdésekkel foglalkozik ez az alfejezet.

2.3.1 Kiktől kell félnünk és miért?

A korai hackerek (1970-es, 80-as évek) olyan tehetséges, a számítástechnika és a kommunikációs rendszerek iránt érdeklődő „zsenik” voltak, akik szerették volna jobban megismerni a rendszerek működését. Felfedeztek több kiskaput a telekommunikációs cégek rendszereiben és a hálózati operációs rendszerekben, és ártatlan szándékuk ellenére károkat okoztak bennük. A hagyományos bűnözés meglátta a lehetőségeket az új virtuális világban és egyre több befolyásra tettek szert. Ez változtatta át a korai hackereket a ma ismert veszélyes

bűnözőkké. (Ezt az időszakot az „ártatlanság korának” nevezi Az Internet sötét oldala c. könyv.)

A szóban forgó számítógépes bűnözőket nevezhetnénk egyszerűen hackereknek, ez a kifejezés azonban nem pontos. Nem minden hackernek vannak támadó szándékai. A 2. táblázat felsorolja korunk különböző „hackereit”.

Támadók típusai	Leírás
Fehér kalapos hacker (white hat)	Rendelkeznek a betöréshez és a károkozáshoz szükséges tudással, azonban adottságaikat jó célokra, például biztonsági rések feltárására használják.
Fekete kalapos hacker (black hat)	Etikátlan, törvénytelen szándékkal tevékenykedő támadók, gyakran crackereknek nevezik őket, a rendszerek feltörése miatt.
Szürke kalapos hacker (grey hat)	Mindkét fentebbi csoportba beleillő egyének, akik esetenként etikátlanul cselekednek, máskor pedig segítséget nyújtanak, mint hálózatbiztonsági szakértők.
Vonal tolvaj (phreaker)	Az 1970-es évek telefonos rendszereinek hackerei voltak. Főként az ingyenes távolsági hívások kötődnek hozzájuk.
Scriptkölyök (script kiddy)	Az igazi hackereknél kevesebb tudással rendelkező felhasználók, akik tetteik következményeivel sokszor nincsenek tisztában. Mások által készített programokat töltenek le és azokkal hajtják végre támadásaikat. (Az igazi hackerek lenézik, az internet söpredékének nevezik őket.)

2. táblázat: Korunk hackerei

A különböző szakirodalmak a fentiek mellett szólnak még olyan hackerekről, mint például a politikai célokkal rendelkező "hacktivisták" (hacktivist), vagy az úgynevezett akadémikus hackerekről, akik elismerésvágyból szándékosan felfedik személyiségüket és elsősorban nyílt forráskódú rendszerekkel foglalkoznak. (Watkins – Wallace [2008])

2.3.2 Támadási kategóriák

A hálózati rendszergazdáknak és biztonsági szakembereknek számos támadási formával és módszerrel kell szembenézniük napjainkban. A támadások kivitelezésük módja szerint az alábbi néhány csoportba sorolhatóak. (Watkins – Wallace [2008])

- **Passzív**: passzívnak nevezünk egy támadást, amikor a támadó közvetlenül, aktívan nem küld kártékony kódokat, vagy forgalmat a hálózatra. A passzív támadások nehezen észlelhetőek. Tipikus példája, ha a hálózat csomagjainak elfogása után a támadó megpróbálja feltörni a kódolt tartalmat.
- **Aktív**: az előzővel ellentétben a támadó aktívan küld adatokat a hálózatra, melyek általában észlelhetőek.
- **Közeli** (close-in): nevükből adódóan ezek a támadások fizikailag kis távolságból érkeznek. Például ha egy támadó fizikailag hozzáfér egy forgalomirányítóhoz és így ki tudja kerülni a hozzáférésükhöz szükséges jelszavas védelmet.
- **Belsős** (insider): különösen gyakori támadások ezek, amikor a jogosult hálózati felhasználók kihasználva hozzáférésüket és a rendszerről megszerzett tudást, kártékony célokra használják a hálózatot.
- **Elosztott** (distributed): elterjed támadási módszer, melyeket a szoftverekben megbújó hátsó ajtók (backdoor) segítségével alkalmaznak a támadók. Az internetről letöltött szoftvert gyanútlanul telepítik számítógépükre a felhasználók. A támadók a szoftverbe épített kiskapukon keresztül később hozzáférhetnek az áldozatok adataihoz, elosztott támadásokhoz használhatják őket (DDoS, spam) vagy használhatatlanná tehetik a számítógépet.

2.3.3 Gyakori támadások

A gyakori hálózati támadásokat próbáltam a szerint kategorizálni, hogy az információbiztonsági fogalomhármas (bizalmasság, rendelkezésre állás, integritás) mely tényezője ellen irányulnak. Természetesen a támadások jó részével nem csak egyetlen terület vehető célba, valamint az itt tárgyalt támadási technikák mellett számos más módszer létezik. (Watkins – Wallace [2008], Thomas [2005] és saját gyűjtés alapján)

Az adatok bizalmassága ellen történő támadások

A bizalmassági támadások célja, hogy hozzáférjenek a titkosnak számító adatokhoz (felhasználói nevek, jelszavak, bankkártya számok, e-mail üzenetek). Mivel a támadó általában másolatot készít a titkosított tartalmú adatokról, ezért gyakran nem észlelhetőek közvetlenül ezek a támadások.

- **Csomag-elfogás**: passzív támadás, mely a hálózati forgalom összegyűjtését jelenti. A hálózati kártya ún. promiscuous (kevert) módba állításával a számítógép által látott minden csomagról másolat készíthető megfelelő segédprogram (pl. Wireshark) segítségével.
- **Port letapogatás:** egy vagy több IP-címre és különböző portokra küldenek csomagokat, azzal a céllal, hogy az esetleges válaszokból (TCP FIN, RST, SYN) kiderítsék az állomáson futó szolgáltatásokat és a nyitott portokat.
- **Ping letapogatás**: az előzőhöz hasonló letapogatási módszer, azzal a különbséggel, hogy általában egy teljes hálózati tartományban keres aktívan működő, visszhang válasszal (echo reply) válaszoló állomásokat.
- **Elektromágneses interferencia elfogás**: mivel az adatok többnyire árnyékolatlan csavart érpáron keresztül továbbítódik, a támadók képesek a vezeték által sugárzott elektromágneses interferencia elfogására és feldolgozására, amiből adatokat fejthetnek vissza.
- **Vezeték letapogatás (wiretapping)**: a régi telefonos rendszerekre jellemző, amikor a támadó fizikailag hozzáfér egy vezetékhez és párhuzamosan rácsatlakozva arra lehallgathatja a hívásokat. Egy másik hasonló veszély, amikor hozzáfér a támadó egy hub-hoz és arra rácsatlakozva minden hálózati forgalmat lemásolhat.
- **Adatküldés nyílt vagy rejtett csatornán**: a támadók bizalmas adatokat küldhetnek át a hálózaton keresztül olyan nyilvános protokollokat felhasználva csatornaként, mint a HTTP.
- **Szteganográfia**: közkedvelt megoldás, általában egy digitális kép pixeleiben, vagy szöveges dokumentum meta adataiban van beleágyazva az információ. Az adatokat csak a küldő és a fogadó képes visszafejteni a megfelelő kriptográfiai módszer kulcsaival.
- **Szociális manipuláció (social engineering)**: gyakran alkalmazott technika, az emberek jóindulatán és segítőkészségén (és tudatlanságán) alapszik, mely során a támadó magát hiteles személynek kiadva megszerez bizalmas információkat, akár személyesen vagy telefonon keresztül.

- **Kukabúvárkodás (dumpster diving)**: számos információt megtudhatunk valakiről, ha átvizsgáljuk az általa termelt hulladékot. Ezt tudják a támadók is, ezért fontos a papír alapú dokumentumok megfelelő megsemmisítése.

Adatintegritás elleni támadások

Ezek a támadások az adatok módosítására irányulnak.

- **Man-in-the-middle**: mely során a normális esetben két fél között lezajló kommunikáció közé beszáll harmadiknak (módosít, majd továbbít) a támadó. Megvalósítása például, amikor a támadó eltéríti a folyamatban lévő TCP kommunikációt, úgy hogy a felhasználó helyett fejezi be a háromfázisú TCP kézfogási folyamatot.
- **Jelszótámadások**: klasszikus támadási módszerek, a felhasználók jelszavainak megszerzésére törekednek, melyeket felhasználva hozzájuthatnak bizalmas adatokhoz. Több változata ismert: szótár alapú támadás, nyers erő (brute force támadás, trójai falovas vagy keylogger módszerek, csomag elfogás).

Rendelkezésre állás elleni támadások

A támadók megpróbálhatják korlátozni vagy megakadályozni egy rendszerhez való hozzáférést vagy annak használhatóságát. Általában a rendszert alkotó processzor és memória kapacitás kimerítésével érik el ezt, megakadályozva a jogosult felhasználók kiszolgálását. Ezeket a támadási formákat gyűjtőnéven nevezhetjük szolgáltatás megtagadás (DoS) támadásoknak. Leálláshoz vagy hibás működéshez vezetnek az alkalmazások hibáiból eredő (exploit) támadások is, például a puffer túlcsordulás (buffer overflow) gyakran okoz fagyást vagy újraindulást. A DoS támadásokat követően gyakran megzsarolják az áldozatot azzal, hogy anyagiak fejében megszüntetik a bénító támadást. Közkedvelt ez a módszert olyan vállalatok ellen, melyek szolgáltatásaikat az interneten keresztül nyújtják (például egy webes áruház), mert azok bevételeiket gyakorlatilag teljesen az interneten segítségével szerzik, így nagy valószínséggel sikeresen megzsarolhatóak. A rendelkezésre állás ellen irányulhatnak az energiaellátást befolyásoló, áramszünetet vagy túlfeszültséget előidéző támadások is, de ez már a fizikai biztonság témaköreibe tartozik.

- **TCP SYN elárasztás**: a TCP protokoll háromfázisú kézfogásának „gyengeségét” használja ki, mely során a támadó sok SYN (szinkronizáló) csomagot küld a kiszolgálónak, melyre soha nem küld majd választ ACK (nyugta) csomag formájában. A kiszolgáló ideiglenesen megtartja a félig felépült TCP kapcsolatokat, viszont a kapcsolatok véges száma miatt a jogosult felhasználók képtelenek lesznek használni a rendszert. A „Land” támadás egy változata a SYN elárasztásnak. Ekkor IP spoofing (IP hamisítás) segítségével a TCP SYN üzenet forrás és cél IP-címe egyaránt a célszámítógép, ezáltal önmagával hoz létre TCP kapcsolatot, ami az üresjárati időzítő lejártáig fennmarad.
- **UDP elárasztás**: hasonló az előzőhöz, de ennél nagymennyiségű UDP csomagot küldenek egy rendszernek (például DNS kiszolgálónak), hogy ellehetetlenítsék a valódi kapcsolatok kialakítását.
- **ICMP elárasztás**: ez a támadás az ICMP protokoll által használt echo-request csomagokat küldi el a célszámítógépnek, mely próbál válaszolni a kérésekre. Érdekes változata a Smurf (törpike) támadás, amikor a támadó módosítja az ICMP echo request csomag tartalmát. Forráscímként az áldozat számítógépének címét adja meg, célként pedig a célhálózat broadcast (szórásos) címét. Ebben az esetben a támadó kiléte rejtve marad, a tényleges támadást a hálózaton található többi számítógép végzi el.
- **Ping of death (halálra pingetés)**: az ICMP támadások olyan formája, amikor a protokoll által maximalizált csomagméretnél nagyobb méretűt küldenek a célszámítógépnek, ami fogadva a csomagot nem tudja értelmezni azt és puffer túlcsordulással lefagyhat.
- **„Teardrop” támadás**: ez a támadás a tördelt IP csomagok összeállításának gyengeségét használja ki. Az IP-fejléc eltolásért (fragment offset) felelős mezője tartalmazza azt az értéket, ami megmondja, hogy az eredeti IP csomag méretéhez képpest bájtban eltolva hol helyezkedik el a töredék IP csomag. Ha modosításra kerül ez az érték, az összeállításkor a részcsomagok között átfedés alakulhat ki, ami a teljes csomagot összeállító gép összeomlását okozhatja.

2.4 Biztonsági technológiák

Az előzőleg tárgyalt tervezési alapelvek, elsősorban a mélységi védelem megvalósításához, és az említett támadási formák kivédéséhez szükséges technológiák rövid áttekintését taglalja jelen alfejezet. A teljesség igénye nélkül a legfontosabb módszerekről, technológiákról és eszközökről lesz szó.

2.4.1 Biztonságos menedzsment és a hálózati eszközök védelme

A hálózatmenedzsment és jelentés készítő alkalmazások a hálózati rendszergazdák munkáját segítik a rendszerek felügyeletében és konfigurálásában. Ezek az alkalmazások is hálózaton keresztül kapcsolódnak a hálózati eszközökhöz, ezért gondoskodni kell a menedzsment-információkat, konfigurációkat és naplóüzeneteket tartalmazó hálózati forgalom védelméről.

A menedzsment forgalom hálózata

Alapvetően kétféle megközelítés létezik arra, hogy milyen útvonalon jut el a menedzsment forgalom a menedzselt eszköz és a menedzsment állomás között. Az egyszerűbb módszer, amikor a hagyományos hálózatot használjuk a menedzsment adatok továbbítására. A másik, költségesebb és külön tervezést igénylő megoldás az ún. out of band (OOB, sávon kívüli) menedzsment. Ez a megoldás a hagyományos hálózattól elszeparált, külön hálózatot használ a felügyeleti és konfigurációs adatok forgalmazásához.

SSH, telnet

A hálózati eszközök távoli elérésének legelterjedtebb módja a telnet kapcsolat. A telnet az egyik legrégebbi alkalmazás rétegbeli hálózati protokoll. A korai terminálrendszerekbe való belépésre szolgált. Azonban a telnet ma már nem tekinthető biztonságos módszernek, mivel minden adatot kódolatlan (clear text, nyílt szöveges) formában küld át a hálózaton. Helyette az SSH (Secure Shell, biztonságos távelérés) protokoll használata az ajánlott.

Az SSH biztonságos csatornát épít ki a két állomás között, és titkosítja a forgalmazott adatokat. A nyilvános kulcsú infrastruktúrát használja: az SSH-1-es változata az RSA-t, míg az SSH-2 a DSA kétkulcsú hitelesítést. Számos titkosítási eljárást kezel az SSH verziótól függően: DES, 3DES, IDEA, Blowfish.

Naplóüzenetek

A hálózati eszközök állapotüzeneteket generálnak (konfigurációtól függően), ha valamilyen esemény történik a rendszer állapotában. Ezeket az üzeneteket naplóüzeneteknek nevezzük és számos célra használhatóak: támadások, visszaélések lekövetésére, hibaelhárításra stb. Az eszközök korlátozott méretig képesek tárolni ezeket az üzeneteket saját memóriájukban. Azonban egy nagyobb hálózatban, ahol több tíz vagy száz forgalomirányító, kapcsoló és tűzfal van, körülményes a naplóüzenetek begyűjtése és azok elemzése.

Az állapotüzenetek központi tárolására több módszer is létezik. Egyik az SNMP protokoll használata, a másik a Cisco eszközök által alapértelmezetten használt Syslog szabvány. (E mellett a Cisco biztonsági eszközök támogatják a gyártó SDEE alapú jelzési módját is.) A Syslog kiszolgáló fogadja és tárolja a Syslog kliensek által küldött naplóüzeneteket.

A naplóüzenetek hatékony elemzésének másik követelménye az időszinkronizáció a hálózati eszközök között. Ha minden eszköz egységes időbeállítást használ, akkor valósítható meg a különböző eszközök naplóüzenetei közötti esemény-korrelációs elemzés (az események bekövetkezési sorrendje). Ehhez egy NTP kiszolgálóra van szükség a hálózatban. Az NTP (Network Time Protocol) protokoll 3-as verziója támogatja a kriptográfiai hitelesítést.

Manapság egyre elterjedtebb a naplóüzenetek automatikus feldolgozása, korrelált elemzése és automatikus incidens riasztások generálása. Ilyen feladatokra képes a Cisco MARS[15] (Monitoring, Analysis and Response System) rendszere.

SNMP

Az SNMP (Simple Network Management Protocol) első változata még 1988-ban jelent meg, azóta elkészültek az SMNPv2, SNMPv2c és SNMPv3 változatok, és az SNMP de facto szabvánnyá vált a hálózatmenedzsment protokollok között.

A protokoll három különböző rendszerkomponenst különböztet meg: a kiszolgálón futó SNMP menedzsert, a menedzselt eszközön található SNMP ügynököt és az azon futó, menedzsment információs adatbázist (MIB).

Biztonsági szempontból az SNMPv1 és az SNMPv2c community string-et (gyakorlatilag egy jelszó) használt hitelesítési módszerként. Ezektől jóval fejlettebb és biztonságosabb az

[15] http://www.cisco.com/en/US/products/ps6241/index.html

SNMPv3 által használt háromszintű biztonság: a noAuthNoPriv community string alapú, hitelesítést és titkosítást nem biztosít; az authNoPriv SHA vagy MD5 alapú HMAC hitelesítést használ, de titkosítást ez sem; és az authPriv, amely SHA vagy MD5 alapú hitelesítést és CBC-DES alapú 56-bites titkosítást nyújt. Ha a hálózati eszközök támogatják, napjainkban az SNMPv3 használata ajánlott. (Watkins – Wallace [2008])

AAA

A kifejezés az Authentication (hitelesítés), Authorization (feljogosítás) és Accounting (naplózás) angol szavak rövidítése. Ezeket az egymástól független szolgáltatásokat nevezzük együttesen AAA-nek.

A hitelesítés biztosítja, hogy a hálózati felhasználó valóban az, akinek mondja magát. Azt, hogy ki csatlakozhat egy adott eszközhöz, a rendszergazda által megalkotott felhasználói név és jelszó határozza meg. Nem megfelelő az olyan hozzáférés, amely csak egy jelszó megadását igényli.

A feljogosítás folyamata a hitelesítés befejezése után zajlik le. Feladata a hozzáférés szabályozás. Minden felhasználó számára megszabható, hogy melyek az általa végrehajtható jogos műveletek, milyen protokollokat használhat, mely erőforrásokhoz férhet hozzá.

A naplózás teszi lehetővé a menedzsment számára felhasználók ki- és bejelentkezésének, az általuk végzett műveletek és használt szolgáltatások, erőforrások nyomon követését. A naplózás használható felülvizsgálati vagy egy szolgáltató esetében számlakészítési célokra is.

Az AAA szemlélete alapvetően szerver/kliens alapú. A klienseket az AAA használatára konfigurált eszközök adják. A kiszolgálók pedig központilag felelősek hozzáférés szabályozásáért. Számos protokoll létezik ezen feladatok megvalósítására. A legismertebb protokollok a RADIUS, Diameter, illetve a Cisco TACACS és TACACS+ protokolljai. Egy központi kiszolgálón fut az aktuálisan használt AAA alkalmazás. A konfigurált AAA kliens a bejelentkezési adatokat elküldi a központi kiszolgálónak és a válasz függvényében engedi be a felhasználót a rendszerbe (hitelesítés). Ezt követően a rendszer minden parancs kiadását vagy hozzáférési kísérletet felülvizsgál és a központi beállításoknak megfelelően engedélyezi vagy megakadályozza azokat (engedélyezés). A Cisco hálózati eszközökön lehetőség van helyi felhasználói adatbázisra támaszkodó AAA hitelesítés használatára. Ekkor az eszköz memóriájában található felhasználói név/jelszó párok kerülnek összevetésre az aktuális bejelentkezés során. (Watkins – Wallace [2008] és saját gyűjtés alapján)

A hálózati eszközök védelme

Azon túl, hogy erős jelszavakat és AAA megoldásokat használunk a hálózati eszközökbe való bejelentkezéshez, többféle módon lehet korlátozni a hozzáférést. Lehetőség van hozzáférés-vezérlő listákkal tetszőleges IP-címekre korlátozni a távoli eléréssel (telnet vagy SSH) próbálkozó felhasználókat. Bizonyos számú próbálkozás után letiltható egy időre a bejelentkezés lehetősége.

A forgalomirányítókon és kapcsolókon található nem használt interfészeket érdemes letiltani, így csírájában elfojthatók az ezeket kihasználó támadási kísérletek. Ugyancsak tanácsos kikapcsolni az eszközökön futó különböző szolgáltatásokat is, ha nem használjuk azokat. Ilyen szolgáltatások például a HTTP, HTTPS, Finger, DNS, kéretlen ARP, ICMP maszkolás, ICMP átirányítás, SNMP szolgáltatás, IP forrás útválasztás, BOOTP kiszolgáló, CDP, FTP és TFTP kiszolgáló vagy az NTP szolgáltatás. (Watkins – Wallace [2008])

A hálózati topológiák egyedi hibapontjainak (single point of failure) tekinthetjük például a tűzfalakat, forgalomirányítókat vagy IPS berendezéseket. A hálózat rendelkezésre állási idejének maximalizálásához ezeknek az eszközöknek fokozottan megbízhatóan kell üzemelniük. A megbízhatóság és a rendelkezésre állás, a hardveres tartalékok mellett, növelhető az úgynevezett redundancia protokollok segítségével. Ilyen protokoll például a szabványos VRRP (Virtual Router Redundancy Protocol), vagy a Cisco-specifikus HSRP (Hot Standby Router Protocol) és GLBP (Gateway Load Balancing Protocol) protokollok. Közös tulajdonságuk, hogy kettő vagy több forgalomirányító között automatikus feladat átadást valósítanak meg az aktív eszköz leállása esetén. (Hucaby [2006])

2.4.2 A kommunikációs kapcsolatok biztonsága

A következőkben a hálózati kommunikáció védelmének néhány jellemző problémájáról és az azokra kifejlesztett megoldásokról lesz szó, a teljesség igénye nélkül.

Kapcsolókat érintő LAN biztonság (Hucaby [2006])

Port Security: a kapcsolókat érintő MAC-cím csalásokból és MAC-cím tábla túlcsordulásokból eredő problémákra jelent megoldás a portbiztonság. A portbiztonság lehetővé teszi, hogy statikusan meghatározzuk egy interfész számára az azon engedélyezett állomások kommunikációját vagy beállíthatjuk a kapcsolót, hogy dinamikusan megtanuljon adott számú MAC-címet az interfészen. A beállított vagy megtanult forrás MAC-címeken kívül, a más forrás MAC-címmel rendelkező keretek eldobásra kerülnek. A port security szabályok megszegése esetén a kapcsoló letilthatja a portot (shutdown), vagy eldobhatja az ismeretlen forrás MAC-címmel rendelkező kereteket (protect, restrict).

Identitás alapú hálózati hozzáférés (802.1x): a felhasználók munkaállomásainak és hordozható gépeik hálózathoz történő csatlakoztatása általában egy kapcsolón vagy vezeték nélküli hozzáférési ponton keresztül történik meg. Az IEEE 802.1x szabvány olyan specifikációkat rögzít, melyek megteremtik a port-alapú azonosítás lehetőségét. A 802.1x egy adatkapcsolat rétegbeli protokoll, lényegében a felhasználó számítógépe és a hálózati kapcsoló vagy vezeték nélküli hozzáférési pont között definiálja az azonosítási feladatokat ellátó EAP (Extensible Authentication Protocol, Kiterjesztett Hitelesítési Protokoll) keretek beágyazásának módját. A felhasználói számítógép bekapcsolásakor nem fér hozzá szabadon a hálózathoz, előbb hitelesítenie kell magát. A hitelesítésért egy RADIUS kiszolgáló felelős. A hálózati kapcsoló csak továbbító szerepet kap a hitelesítési folyamatban. Amint a felhasználó hitelesítette magát, a kapcsoló a felhasználóhoz konfigurált VLAN-hoz rendeli (dinamikus VLAN hozzárendelés) a számítógépet és megkezdi a keretek feldolgozását. A hitelesítés előtt kizárólag EAPOL, CDP és STP forgalom haladhat át az adott kapcsoló porton. Vezeték nélküli hálózatok esetében a hozzáférési pont (AP) látja el a hitelesítő (authenticator) szerepét.

STP védelem: a kapcsolók hatékony működéséhez, a hurokmentes topológia kialakításához szükséges a feszítőfa protokoll (STP, Spanning Tree Protocol). Röviden szólva, az STP lehetővé teszi, hogy ha a kapcsolók között léteznek is redundáns fizikai összeköttetések,

logikailag hurokmentes legyen a topológia. Az STP protokollt érintő támadások kivédhetők a következő, Cisco Catalyst kapcsolóknál is használt biztonsági eljárásokkal:

- **Root Guard**: megakadályozza, hogy a nem megfelelő kapcsolók gyökérponti hídként (root bridge) üzemeljenek. Port szinten kell aktiválni, ekkor, ha egy porton olyan BPDU érkezik, amely azt eredményezné, hogy a port gyökérporttá váljon, akkor a port az ún. „root inconsistent" módra vált, és nem engedi át a hálózati forgalmat, amíg ehhez hasonló BPUD-k érkeznek rajta.
- **Portfast**: munkaállomásokhoz vagy kiszolgálókhoz csatlakozó hozzáférési kapcsolóportokon alkalmazható beállítás, amely felgyorsítja a port aktiválásának idejét, úgy, hogy a kapcsolóport kihagyja a figyelési (listening) és tanulási (learning) STP fázisokat, tehát a blokkoló (blocking) módból közvetlenül a továbbító (forwarding) módba vált.
- **BPDU Guard**: megakadályozza, hogy a portfast beállítással konfigurált kapcsolóportokhoz csatlakoztatott más kapcsolók miatt hurok alakuljon ki a topológiában (gyakorlatilag letiltja az interfészt).
- **BPDU Filter**: a hálózati hurkok megelőzésének másik módja. Globális konfigurációs módban alkalmazva, ha egy portfasttal beállított interfész BPDU-t fogad, akkor a kapcsoló eltávolítja a port portfast státuszát. Interfész szinten használva kiszűri a BPDU kereteket.

VLAN-ok, trönkök: a kapcsolóknál használt VLAN-ok (virtuális LAN) szegmentáló szerepe hatékonyságot és bizonyos szintű biztonságot eredményez, azonban léteznek kifejezetten olyan támadások, melyek a VLAN-ok közötti kommunikációt hivatottak elérni.

- **Switch spoofing (kapcsoló átejtés)**: a támadó egy felhasználói végpontra egy kapcsolót csatlakoztat, és arra készteti a vállalati kapcsolót (DTP keretek segítségével), hogy trönkvonalat alakítson ki vele. Ha sikerrel jár a trönkvonalon a kapcsoló összes VLAN-jának adatforgalma áthalad, így a támadó összegyűjtheti és elemezheti azokat. Ennek kivédésére ajánlott minden kapcsolóportnál expliciten beállítani, hogy az hozzáférési portként vagy trönkportként működjön.
- **Double tagging (dupla címkézés):** a kapcsolók egyik leggyakrabban használt trönkölési protokollja a 802.1q protokoll. A protokoll egy 4 bájtos mezőcsoporttal bővíti az Ethernet kereteket, melyben megjelöli, hogy a keretek melyik VLAN-ba

tartoznak. A címkézett kereteket csak a kapcsolók küldenek egymás között a trönkvonalakon, az elérési portokhoz csatlakozó munkaállomások nem alkalmazzák azokat (címkézetlen keretek). A kapcsolókon a natív VLAN beállítás határozza meg, hogy melyik VLAN-ba továbbítódjanak a címkézetlen keretek. A támadók az úgynevezett dupla címkézés (double tagging) segítségével képesek lehetnek kommunikálni más VLAN-okban található állomásokkal. Ezt röviden úgy teszik, hogy a keret külső címkéjében VLAN-ként a natív VLAN-t adják meg, a belső címke pedig a cél VLAN azonosítóját tartalmazza. Az efféle támadások kivédésére nem szabad felhasználói adatok továbbítására használni a natív VLAN-t, ezért egy olyan VLAN-t kell beállítani a kapcsolókon (üres VLAN), amelyik nincs beállítva egyetlen hozzáférési portnál sem.

DHCP Snooping: a DHCP csalásos támadások kivédésének módszere. A kapcsoló minden egyes portján beállítható, hogy az átengedheti-e a DHCP kérésekre válaszoló állomások üzeneteit (trusted/untrusted). Így kiszűrhetők a támadók által generált hamis DHCP válaszok, melyek például egy man-in-the-middle támadást készítenek elő.

Dynamic ARP Inspection (DAI): az ARP támadások során a támadó kéretlen (gratuitous) arp üzenetek segítségével módosítja saját MAC-címére, az állomások ARP táblájában az alapértelmezett átjáróhoz tartozó MAC-címet. A Dynamic ARP Inspection a DHCP Snooping beállítással együtt alkalmazva kivédheti a MAC-cím csalásos támadásokat. A kapcsoló a nem megbízható (untrusted) portokon beérkezett ARP üzenetek cím információit összeveti a DHCP Snooping által létrehozott IP-cím/MAC-cím táblázattal. Ha nincs egyezés a táblázat egyetlen bejegyzésével sem, akkor a kapcsoló eldobja az ARP üzenetet.

A forgalomirányító protokollok biztonsága

A forgalomirányítók különböző hirdetéseket küldenek egymás között (kivéve a statikus routingot), az alkalmazott útválasztó protokoll függvényében, így biztosítva a változások észlelését és az egymással való kommunikációt. A népszerű IGP protokollok (OSPF, EIGRP, RIPv2) támogatják a forgalomirányítási hirdetmények hitelesítését, de néhány régebbi változat nem (IGRP, RIPv1). (Stewart – Gough [2007])

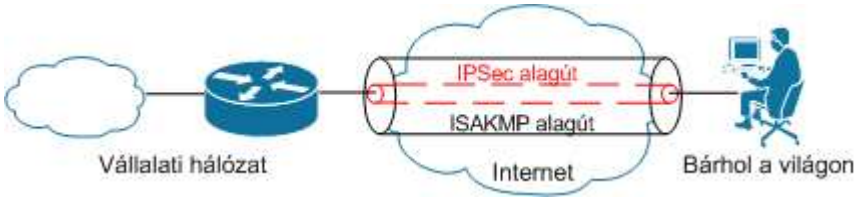
```
RouterA(config)#interface serial 0/0
RouterA(config-if)#ip ospf message-digest-key 1 md5 cisco
RouterA(config-if)#ip ospf authentication message-digest
RouterA(config-if)#
RouterA(config)#router ospf 1
RouterA(config-router)#area 0 authentication message-digest
```

6. ábra: OSPF hitelesítés konfigurálása MD5 használatával

VPN technológiák

A nyilvános kulcsú infrastruktúra és a különböző titkosítási eljárások lehetővé teszik, hogy nyilvános hálózatokon, az interneten keresztül tudjuk biztonságosan kiterjeszteni helyi hálózatunkat. A VPN technológiák (Virtual Private Network, Virtuális magánhálózat) ilyen feladatokat látnak el: egy nyilvános hálózaton biztonságos alagutat (tunnel) hoznak létre.

Kétféle VPN típus létezik. Egyik a távoli hozzáférést (remote access) megvalósító, elsősorban dinamikusan létrehozható csatlakozási igények esetén alkalmazott magánhálózat. Ilyeneket használnak például a távdolgozók a vállalati hálózatba való bejelentkezéshez. (7. ábra)



7. ábra: IPSec Remote Access VPN

A másik változat (site-to-site vagy telephelyközi) statikus összeköttetési igények esetén használt, főként telephelyi hálózatokat köt össze egymással, így a különböző földrajzi helyen lévő eszközök logikailag egy hálózatban képesek kommunikálni egymással, mivel a VPN alagút transzparens számukra. (8. ábra)

8. ábra: IPSec Lan-to-Lan VPN

Az IPSec a VPN technológiák egyik legfőbb szabványa. A szabványról több RFC dokumentum került kiadásra (például az RFC 2401), ami biztosítja a különböző gyártók egymással való kompatibilitását a VPN hálózatok kialakításában. Az IPSec a következő hálózatbiztonsági szolgáltatásokkal rendelkezik:

- az adatokat mindkét oldalon titkosítja az átvitel előtt, így biztosítva azok bizalmasságát (DES, 3DES, AES, SEAL, stb.)
- a fogadó oldal ellenőrzi a küldő által továbbított minden csomag hitelességét, ezáltal biztosítja az adatok integritását, sértetlenségét (HMAC-MD5, HMAC-SHA)
- a kommunikáló felek többféle hitelesítési módszer segítségével győződhetnek meg a másik kilétéről (osztott kulcs (PSK), RSA)

Az IPSec hátrányai között szerepel, hogy csak az IP csomagok és azok közül is csak az egyedi címzésű (unicast) csomagok átvitelére képes, ezért a nem IP-alapú protokollok, vagy a szórásos (broadcast) és a többes címzésű (multicast) IP forgalom átviteléhez a GRE (Generic Routing Encapsulation) alagút használata szükséges.

Egy másik egyre népszerűbb VPN megoldás az SSL alapú VPN. Az SSL VPN képes távoli hozzáférést biztosítani bármely internet eléréssel és web böngészővel rendelkező állomásról.

A VPN hálózatokat megvalósító céleszközök között szerepelnek az egyszerű VPN-képes SOHO routerek, a Cisco IOS rendszerű forgalomirányítói és kapcsolói, valamint a fejlett tűzfal és VPN koncentrátor berendezések (Cisco ASA, PIX). Szoftveres oldalról a hálózati operációs rendszerek úgy, mint a Windows Server változatok és a Linux disztribúciók is támogatják a VPN hálózatok kialakítását. A felhasználók általában az IPSec VPN kliensoldali alkalmazásokkal találkoznak. (Watkins - Wallace [2008] és Morgan, B. [2007] alapján)

2.4.3 Végponti eszközök védelme

A hálózatok létezésének célja a felhasználói végberendezések közötti kommunikáció megvalósítása. Végponti eszközöknek tekinthetjük a munkaállomásokat, a laptopokat, a kiszolgáló számítógépeket, a nyomtatókat, az okos telefonokat és a PDA-kat is. Ezek mindegyike valamilyen operációs rendszert futtat, amely interfészt biztosít az alkalmazások és a hardverek között. Az operációs rendszerek gyenge pontjai jelentik a végponti eszközök támadási felületét, ezért ezek megszüntetése a cél. A különböző szoftveres védelmi

alkalmazások mellett szó lesz a mobil eszközöknél kiemelten fontos titkosítási és fizikai védelmi eljárásokról is. (Watkins - Wallace [2008])

Frissítések és javító csomagok

Az operációs rendszerekhez, és a felhasználó alkalmazásokhoz kapcsolódó legtöbbet hangoztatott üzemeltetési ajánlás a frissítések és biztonsági javítócsomagok folyamatos telepítése. Vállalati környezetben kevésbé elterjedt az operációs rendszerek gyártója által kiadott frissítések automatikus, azonnali telepítése, az esetleges kompatibilitási hibák miatt. Ezekkel a feladatokkal a „patch management" témaköre foglalkozik az IT security világában. Alapszinten a következő fő lépésekből áll a patch management:

- A javítások azonosítása, beszerzése (időigényes, sok munkával jár)
- Tesztelési fázis (különálló, az élestől elszigetelt rendszerben)
- A kiválasztott frissítések telepítése (többnyire automatikusan, például Windows esetén WSUS)

Végpont védelmi szoftverek

Az antivírus programok, személyes tűzfalak és állomás alapú IPS szoftverek közvetlen védelmet biztosítanak a végponti számítógépeknek. A mai modern szoftverek gyakran egyesítik magukban mindhárom megoldás előnyeit. Vállalati környezetben alkalmazott komplex rendszer például a Cisco Security Agent vagy a McAfee Total Protection. Ingyenes változatok például a Comodo[16] vagy a Privatefirewall.

Antivírus rendszerek

Antivírus, más néven vírusirtó szoftvereknek nevezzük azokat az alkalmazásokat, melyek észlelik, elhárítják és eltávolítják az olyan kártékony szoftvereket (malware), mint a vírusok, férgek, trójai falovak. Manapság már a reklám és kémprogramok ellen is védelmet nyújtanak.

Számos észlelési stratégia alakult ki:

- vírusaláírás alapú (signature)
- heurisztikus védelem

[16] http://personalfirewall.comodo.com/

- gyanús viselkedés figyelése

Az első észlelési stratégia hatékony, de nem nyújt védelmet a legújabb fenyegetésekkel szemben, csak a már ismert programkódokat képes detektálni. A vírusirtók gyártói ezért jelentetnek meg naponta akár többször is aláírás adatbázis frissítéseket, melyek automatikusan települnek rendszerünkbe. A másik két észlelési forma sok esetben képes felismerni az új vírusokat. A heurisztikus keresési eljárások a fájlokban gyanús utasításokat keresnek (például törlést), virtuális környezetben emulálva vizsgálják egy fájl viselkedését vagy általános kódmintákat (generic signatures) használva próbálják megtalálni a vírusokat (gyakran tévesen riasztva a felhasználót).

Az antivírus szoftverek működhetnek rezidens módban (folyamatosan a memóriában futva), illetve lehetővé teszik az igény szerinti keresést is. Az automatikus keresés általában fájlműveleteknél, weboldalak betöltésekor vagy e-mailek forgalmazásakor következik be.[17]

Személyes tűzfalak és IPS szoftverek

A személyes tűzfalak hasonlóak a hagyományosan vett hálózati tűzfalakhoz. A felhasználó munkaállomásán futó szoftverek, melyek a konfigurált biztonsági házirendnek megfelelően engedélyezik vagy tiltják a hálózati forgalmat kimenő és bejövő irányba (de például Windows XP tűzfala nem képes kimenő irányba szűrni).

A személyes tűzfalak néhány jellemző szolgáltatása:

- riasztják a felhasználót a kapcsolódási kísérletekről
- figyelik a kapcsolódni kívánó alkalmazásokat
- nyomon követik az aktuális hálózati kapcsolatokat
- megvédik a számítógépet a port letapogatásos vagy ping felderítéses próbálkozásokkal szemben

Az állomás alapú IPS szoftverek (HIPS, Host based Intrusion Prevention System), a személyes tűzfalakhoz hasonló, proaktív biztonsági programok (a legtöbb gyártó terméke tűzfalas és IPS funkciókkal rendelkezik). A hálózati IPS (NIPS) eszközökkel szemben, melyekről a későbbiekben lesz szó, a HIPS szoftverek kizárólag azt a számítógépet védik, amelyre telepítve

[17] http://en.wikipedia.org/wiki/Antivirus_software

vannak. Viszont, mivel egy végponti eszközön működnek, képesek a titkosított kommunikációs csatornákon (például SSL) küldött adatok ellenőrzésére is. A hagyományos HIPS alkalmazások nem használnak aláírás adatbázisokat a kártékony programkódok felismeréséhez, így képesek az új veszélyek észlelésére is. E helyett, a személyes tűzfalakhoz hasonlóan, rögzíti az engedélyezett programokat (whitelist) és az azok által végezhető műveleteket. A listán nem szereplő programok alapértelmezés szerint nem megbízhatónak számítanak. Ez a tulajdonsága (hátránya) bizonyos szintű tudást követel meg az egyéni felhasználóktól, de vállalati környezetben ezt központi irányítás (policy) szabályozza.

Mobil eszközök védelme

A mobil eszközök védelme részben hasonló problémákat vet fel asztali társaikéhoz. Azonban a laptopok, PDA-k fizikai elmozdíthatósága miatt új problémák jelentkeznek. A felhasználókat tudatossá kell tennünk a veszélyekkel szemben (oktatással, a biztonsági szabályzat betartatásával). El kell érni, hogy mobil eszközeikre fokozottan vigyázzanak. Használjanak laptopjukhoz biztonsági rögzítő kábelt (Kensington lakat), vagy tartsák azt zárható helyen. A legtöbb igyekezet ellenére mégis eltűnik egy-egy ilyen eszköz, ezért gondoskodni kell a rajtuk tárolt adatok megfelelő biztonságáról.

A tárolt adatokhoz való hozzáférés korlátozható bejelentkezési jelszavak és egyéb hozzáférés szabályozó technikák mellett (birtoklás vagy tulajdonság alapú), az eszközön tárolt adatok titkosításával. A titkosításra számos megoldás született:

- a notebook alaplapján található TPM (Trusted Platform Module) modul hardveresen titkosítja (RSA kulcs) a merevlemez adatait, így a merevlemez más gépbe helyezve sem lesz használható
- szoftveres titkosítási megoldás az EFS (Encrypting File System) fájlrendszer titkosító használata, mely a felhasználóhoz tartozó SID[18] alapján végzi a fájlok titkosítását (Linux, Windows2000, XP Pro, Vista, Windows 7)
- ingyenes titkosító szoftver például a TrueCrypt[19], amely képes teljes meghajtók titkosítására és egy titkosított fájlban tárolva virtuális meghajtók kezelésére is

[18] A Windows NT vonalán kialakult, alfanumerikus biztonsági azonosító.

[19] http://www.truecrypt.org/

- a PDA-k és okostelefonok is felvértezhetőek adattitkosítási jellemzőkkel: SecuBox (Windows Mobile), Almenta (Symbian)

A notebook felhasználók nem minden esetben a biztonságos vállalati hálózathoz csatlakoznak. Annak a lehetőségét, hogy egy idegen hálózatra csatlakozva kerüljenek kártékony kódok a hordozható számítógépünkre, a már megismert végpont védelmi megoldások kombinált használatával kerülhetjük el. Biztonságos kommunikációs csatorna hozható létre a vállalati hálózattal nyilvános médiumokon keresztül a VPN technológiák alkalmazásával, melyekről már korábban volt szó. (ISC^2 CISSP [2008])

2.4.4 Az internet peremvédelmi zóna technológiái

A mélységi védelem fejezet során már említettük, hogy több különböző biztonsági megoldással hatékonyabb védelmi vonal hozható létre. Egy hálózat internet peremvédelmi területének nevezzük azt a részt, amely világot (pl. a szolgáltató által biztosított internet kapcsolat) összekapcsolja a szervezet belső hálózatával. A peremvédelmi zónában forgalomirányítók, tűzfalak és behatolás védelmi eszközök találhatóak. A támadóknak vagy a kártékony kódoknak át kell haladniuk ezen a védelmi vonalon a belső állomások eléréséhez. A hálózat ezen területén található forgalomirányító vagy tűzfal (VPN koncentrátor) valósítja meg a felhasználói vagy a telephelyek közötti VPN kapcsolatok végződtetését is. A tűzfalak segítségével létrehozhatók a külvilág számára elérhetőséget biztosító demilitarizált zónák is. A peremvédelmi lehetőségek száma tehát sokféle. Az itt alkalmazott technológiákról szól ez az alfejezet.

Tűzfalak

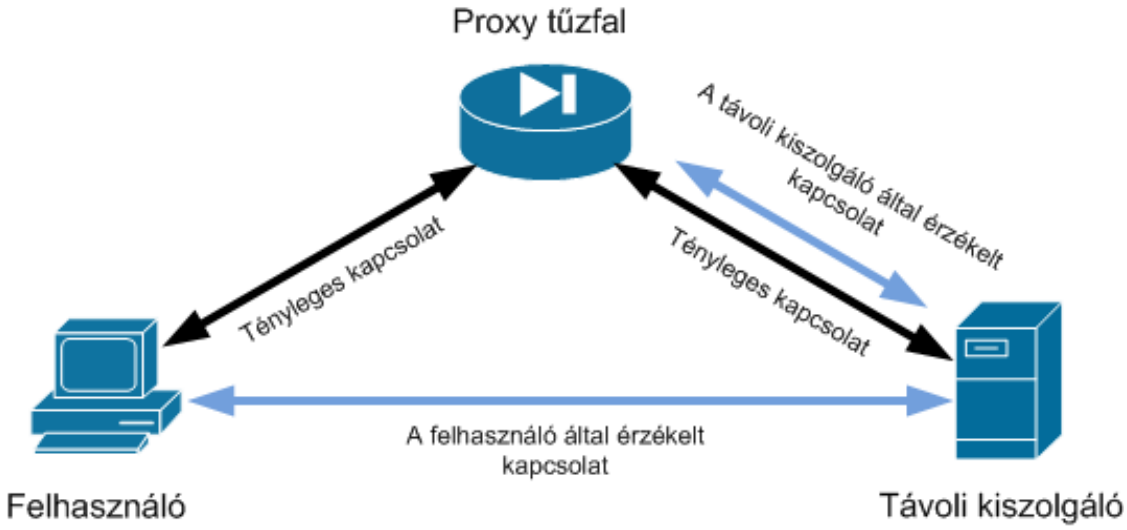
A korábban az építészetben és a járműveknél használt tűzfal kifejezés bekerült a számítógépes hálózatok fogalomkörébe. Gyakorlatilag a tűzfalak valósítják meg az adminisztratív biztonsági szabályzatot, megszűrve a be és kimenő forgalmat meghatározott szabályok alapján. A tűzfalak másik jellemzője, hogy elválasztják egymástól a megbízható és a nem megbízható hálózatokat, ezért azokat a különböző biztonsági tartományok közé kell elhelyezni.

Többféle tűzfaltípus létezik. A legegyszerűbb módszer a csomagszűrés, mely az OSI modell 3. és 4. rétegében található információk alapján szűr. (Forrás, cél IP-cím, portszámok,

protokoll.) Ilyen például a forgalomirányítóknál már megismert hozzáférés-vezérlő lista (ACL) is. Azonban az egyszerű csomagszűrő nem biztosít kellő védelmet, például a szabályos forgalom segítségével (HTTP) indított támadást nem szűri ki.

Sokkal hatékonyabb, dinamikus ellenőrzést végez a Stateful Packet Inspector (SPI) működésű tűzfal. Az SPI tűzfal az úgynevezett állapottáblában lévő kapcsolati információk alapján szűr. Az OSI modell 3., 4. és 5. rétegében működik. A statikus csomagszűréssel szemben, amely csak a csomagok fejlécében található információkat veszi figyelembe, az SPI nyomon követi a tűzfalon átmenő összes kommunikációt és figyelembe veszi a 4. rétegbeli szegmensek fejléc információit is, például a TCP fejléc SYN, RST, ACK és FIN jelzőket, illetve a kapcsolat állapotáért felelős további vezérlő információkat. Hátrányainak tekinthető, hogy mivel nem biztosít alkalmazásszintű védelmet, ezért a támadók kihasználhatják az engedélyezett hozzáféréseket, önmagukat engedélyezettként álcázva. Hátrányossága az is, hogy csak a TCP protokollnak van kapcsolat állapota, így az UDP vagy ICMP forgalmakat nem képes nyomon követni.

Teljesebb védelmet nyújtanak az alkalmazás átjáró tűzfalaknak is nevezett proxy tűzfalak. Ezek már egészen a 7. alkalmazási réteg szintjéig képesek vizsgálni az átmenő forgalmat. Két fajtájuk ismert: áramköri szintű proxy tűzfal és alkalmazás szintű proxy tűzfal. Ezek a tűzfalak közvetítőként működnek a forrás és a cél között (9. ábra). Ha a közvetítő úgy dönt, hogy a kapcsolat engedélyezett, akkor a kezdeményező gép nevében felépíti a kapcsolatot, és a felhasználónak úgy tűnik, mintha közvetlenül kapcsolódna a célállomáshoz (transzparens). A proxy tűzfalak negatív tulajdonsága, hogy az alapos vizsgálat és a nagyrészt szoftveres alapú szűrés miatt nem képesek nagy sebességgel működni, valamint az új alkalmazások és protokollok miatt szükség van a tűzfal adatbázisának rendszeres frissítésére.



9. ábra: A proxy tűzfalak közvetítő szerepe

Manapság már szinte minden gyártó tűzfala hibrid tűzfal a sebesség és a biztonság közötti kompromisszum megteremtése érdekében. A Cisco ASA tűzfala is alapvetően stateful működésű és e-mellett valósítja meg például az IM, P2P és egyéb protokollok alkalmazás szintű vizsgálatát.

A legtöbb tűzfal kihasználja a hálózati címfordítás (NAT, Network Address Translation) tulajdonságait. A hálózat biztonságát a NAT több jellemzője is pozitívan befolyásolja:

- a támadók számára nehezebbé válik kívülről a belső hálózat és a működő állomások feltérképezése
- bonyolultabbá teszi a SYN elárasztásos támadásokat, a port letapogatást vagy a csomagbeszúrást (man-in-the-middle)

Tartalomszűrés

Az internetre csatlakoztatott számítógépek használata során szükség van a tartalomszűrés valamilyen formájára. Tartalomszűrő lehet például a könyvtárakban és az iskolákban is egyre gyakrabban alkalmazott, pornográf vagy egyéb erkölcstelen webes tartalmakat blokkoló alkalmazások. Tartalomszűrésnek tekinthető az elektronikus levelezés világában jól ismert levélszemét (spam) szűrése, valamint a vírusok, férgek, trójai falovak és egyéb kártékony programok, valamint az ilyeneket tartalmazó weboldalak blokkolása. A tartalomszűrés megvalósítható állomásokra telepített szoftverekkel és központi eszközökkel is. Az előbbi

főként az egyedülálló, például otthoni felhasználók körében népszerű. A központi levélszemét és vírusellenőrzés a nagyobb vállalati környezetek esetében célszerű. Ilyen komplex védelmi megoldást nyújtanak például a Cisco Ironport megoldásai, de más gyártók: a McAfee és a Symantec is élen járnak a végponti védelmi megoldások terén.

IPS/IDS rendszerek bemutatása

A támadások, kártékony programok és vírusok nagyon gyorsan fejlődnek, napról napra újabbak születnek. A tűzfalak önmagukban nem mindig képesek reagálni az új típusú támadásokra, ezért szükség van olyan védelmi megoldásokra, melyek a forgalom elemzésével képesek azonnali jelzésre és beavatkozásra. (Watkins - Wallace [2008] és Thomas [2005] alapján)

A behatolás érzékelő (IDS, Intrusion Detection System) és behatolás gátló/megelőző rendszerek (IPS, Intrusion Prevention System) figyelik és elemzik a hálózaton átmenő csomagokat és riasztást küldenek a gyanús hálózati forgalom, vagy a potenciális támadások észlelésekor. Az IDS rendszerek passzív szerepet töltenek be, céljuk az észlelés és a riasztás. Az IDS berendezés számára egy kapcsoló másolatot készít a hálózati forgalomról. Veszély esetén riasztást küldhetnek és utasíthatják a többi hálózati eszközt, például a tűzfalakat, hogy reagáljanak a támadásra.

Az IPS eszközök ezzel szemben közvetlenül a hálózati forgalom útjába vannak telepítve (inline), észlelik a támadásokat és képesek azokat megállítani. Két vagy több interfész segítségével minden forgalom áthalad ezeken az eszközökön, így ezek már csomagszinten képesek észlelni a gyanús forgalmat, és a következő tevékenységeket végezheti el:

- Naplóbejegyzés létrehozása (Syslog, SDEE)
- A támadóhoz köthető minden további csomag eldobása
- A támadó TCP kapcsolatának újraindítása (TCP RST)
- A támadó IP-címének blokkolása

Ugyanaz a hálózati berendezés képes lehet IDS-ként vagy IPS-ként is üzemelni, illetve egyszerre mindkét szerepet is betölthetik, virtuális IPS/IDS kialakításával.

Az IDS/IPS rendszerek többféle elemzési módszer segítségével észlelik a támadásokat:

- **Mintázat alapú (signature) összevetés**: gyakorlatilag rögzített forgalomminták, bájtsorozatok gyűjteménye, folyamatosan összevetésre kerülnek a csomagokban található információkkal. Fejlettebb változata az állapotteljes (stateful) egyezés vizsgálat, amely nem csak különállóan vizsgálja a csomagokat, hanem megpróbál bizonyos sorozatokat, ismétlődéseket észlelni egy kapcsolat több csomagjában. A mintázat alapú észlelések hátrányai közé sorolható, hogy csak az ismert támadásokat képesek jelezni, és rendszeres aláírás-adatbázisfrissítést igényelnek.
- **Anomália alapú felismerés:** az anomália (szabálytalanság) alapú elemzés alapulhat statisztikai módszereken, mely során a normál hálózati működés idején felépül egy viszonyítási alap (baseline), amihez képest később összevetésre kerül a forgalom. Minden szignifikáns eltérés ettől a rögzített viselkedési profiltól riasztást válthat ki. Más anomália alapú észlelési módszer, ha magunk határozzuk meg a szabályosnak vélt hálózati aktivitást, és ezt egy szabályzatban (profilban) tároljuk. Anomália példák: sok sikertelen bejelentkezési kísérlet, szokatlan időpontban bejelentkező felhasználók, a rendszeridő tisztázatlan módosítása, újraindulások. (Ez a fajta észlelési módszer hajlamos a téves riasztásokra, mivel nehéz pontosan definiálni az elvárt működést.)

A hagyományos IPS megoldásokkal szemben hatékonyabb védelmet biztosítanak azok az eszközök, melyek kihasználják a Global Threat Correlation rendszert. Lényegében az IPS-ek egy a gyártó által létrehozott globális rendszerben együttműködnek és egy nagy virtuális elosztott adatbázisba regisztrálják az általuk felismert támadási forrásokat. Ezen adatbázist gépi algoritmusok és mérnökök elemzik, segítségével szinte percenként frissülő "veszélyforrás" adatbázist hoznak létre. Ezen veszélyforrás adatbázist az IPS-ek jellemzően 5-10-15 perces frissítéssel lemásolják és ez alapján előszűrést végeznek. A Cisco IPS Global Correlation így nagyobb átbocsájtó képességet tesz lehetővé, illetve "elhanyagolt" (rosszul beállított, nem frissített) IPS rendszereken magasabb védelmi szintet biztosít. (Megjegyzendő, hogy hasonló munkát végeznek például a Symantec Security Operations Center részlegében. (Warren – Streeter [2005]))

3. Az egységesített kommunikációs rendszerek biztonsági vonatkozásai

Ez a fejezet az egységesített kommunikációs rendszerek gerincét képező IP telefónia biztonsági kérdéseire keresi a választ. A tárgyalt témakörök Segyik István - IP-telefónia biztonság I., II. előadásai alapján készültek és elsősorban Cisco megoldásokra épülnek.

Bevezetésül érdemes összevetni egymással a hagyományos telefonos rendszerek biztonsági jellegzetességeit az őket fokozatosan leváltó, IP-telefóniás rendszerek biztonsági jellemzőivel. A kérdés nem egyszerű, hiszen a régi rendszerek kiforrottak, elkülönített fizikai hálózatot használnak, lehallgathatóságuk, blokkolhatóságuk fizikai hozzáférést igényel. A különböző alközponti gyártók termékei más-más protokollokat használnak, ezért a feltörésükhöz szükséges tudás nem általános. Talán meglepő, de ezzel szemben az adathálózatokon működő VoIP rendszerek semmivel nem biztonságosabbak alapesetben. A szolgáltatások blokkolhatóak, a hívások lehallgathatóak, ráadásul az interneten megannyi kész, gyorsan megtanulható szoftveres eszköz segíti a támadók munkáját. A korábbi telefonközpontos korszakban a támadók nem voltak motiváltak a hírnévszerzés, dicsekvés céljából történő támadások kivitelezésében, míg az IP-rendszerek eljövetelével megjelentek a lehallgatással, kapacitáslopással, szolgáltatás-blokkolással kérkedő esetek.

Az IP-telefónia bevezetése új biztonsági kihívások elé állítja a hálózati szakembereket, mivel az IP-hálózatok természetéből adódóan, a VoIP rendszerek távolról is használhatóvá és egyszerűbben hozzáférhetővé válnak a korábbi hagyományos telefonos rendszerekkel szemben.

3.1 Az UC rendszerek tipikus veszélyforrásai

3.1.1 Felderítés és feltérképezés

A kívülről kezdeményezett támadások előkészítő lépése, a katonai támadásokhoz hasonlóan, a célpont felderítése, rendszerének feltérképezése. Az illegális hozzáférés, lehallgatás mellett előkészületeket igényelnek a szolgáltatásmegtagadásos (DoS), bénulást okozó támadások is.

A támadók kezében számos lehetőség van rendszerünk megismeréséhez. A közösségi portálok (Iwiw, Facebook, MySpace) tömérdek hasznos információk, neveket, címeket árulnak el rólunk, kollegáinkról, alkalmazottainkról, melyeket felhasználva egy csak kicsit is merész támadó telefonon vagy személyes kontaktus során újabb információkat csalhat ki, például egy segítőkész telefonos asszisztenstől (social engineering).

A betelefonálásoknak lehet technikai jellegű célja is, például a bejelentkező interaktív hívásközpont (általában gépi női hang) által lejátszott hangmintákat elemezve (hangsúly, tónus, szöveg) nagy eséllyel határozható meg a szervezet által használt telefonos rendszer típusa, így a támadó a rendszer ismert gyengeségeit próbálja meg majd kihasználni. A különböző rendszerek alapértelmezett hangmintái megtalálhatóak az interneten. Használhatóak.

A felderítésez használható technikai eszközök ingyenesen elérhetőek javarészt Linuxra, de néhány a Windows rendszereket is támogatja. IP és port szkennelő program például az Nmap[20]. Kulcsrakész VoIP rendszerelemző, például a SiVus[21] és a SIPSCAN[22]. A port szkennelő alkalmazásokkal a hálózat aktív eszközein a jelzésrendszer és az adminisztrációs interfészek portjait célozzák meg. (Néhány tipikus port: SIP: 5060 UDP, H.323: 1719 UDP, 1720 TCP SCCP: 2000 TCP, Telnet: 21 TCP, SSH: 22 TCP/UDP, HTTP: TCP/UDP 80, TFTP: 69 UDP stb.) Ha sikerült egy válaszoló eszközt találni a hálózaton, „fingerprinting” (feltérképezés) eszközök segítségével, nagy valószínűséggel be lehet azonosítani a rajta futó rendszert (MAC-címek, bejelentkezési promptok, egyéb nyitott portok alapján).

[20] http://nmap.org/

[21] http://www.securityfocus.com/tools/3528

[22] http://www.hackingvoip.com/tools/sipscan.msi

A rendszerek felderítésének másik módja, amikor belülről szereznek meg információkat. Célja ennek is ugyan az, a DoS támadások, illegális hozzáférés, lehallgatás előkészítése. A szükséges információk (felhasználói nevek és jelszavak, IP-címek, portok protokoll verziók, programverziók) könnyebben megszerezhetőek a belső hálózat irányából, ezért fokozott figyelmet kell fordítani a belső szabályozásokra.

3.1.2 Lehallgatás

A hagyományos telefonos rendszerekkel ellentétben az IP-telefóniás rendszerek lehallgatásához nem kell fizikai közelségben lennünk a rendszerhez, a hangot hordozó csomagok a kábelhez való hozzáférés nélkül megszerezhetőek. A lehallgatás egyik módja, ha két telefon közötti közvetlen hálózati forgalmat átterelünk a saját számítógépünkre, melyet a már korábban említett man-in-the-middle támadás kivitelezésével tehetünk meg. Erre is léteznek kész eszközök, használatuk részletesen megtalálható az interneten. Az Ettercap[23] nevű alkalmazás több ilyen „mitm" támadási típust is ismer. Képes ARP mérgezéssel módosítani az állomások ARP táblájában lévő bejegyzéseket, ezután azok minden csomagot a támadó számítógépe felé küldenek, ami módosíthatja és továbbíthatja azokat az eredeti cél felé. Másik módszer az ICMP redirection (átirányítás) alapú támadás, amikor az állomásokkal elhiteti a támadó, hogy jobb útvonalat tud az internet felé. Ez a támadás egy ún. half-duplex „mitm" támadás (ha a másik fél egy eltérő hálózatban van), mert csak a kliens felől érkező forgalom halad át a támadó számítógépén, hiszen az elsődleges átjáró nem fogad el ICMP redirect üzeneteket egy közvetlenül csatlakozó hálózatra vonatkozóan. A harmadik támadási típus a korábban említett DHCP spoofing-ra épül. A támadó valós időben versenyez a hiteles DHCP kiszolgálóval, és megpróbál egy módosított alapértelmezett átjáróval rendelkező DHCP OFFER üzenet eljuttatni a DHCP klienseknek. Ez a módszer is half-duplex lehallgatást eredményez. Egyéb „mitm" módszer még a port stealing (port lopás).

Másik módszer a lehallgatásra, ha sikerül egy sniffer funkcióval rendelkező programmal (pl. Wireshark, Ettercap) egy állományba rögzíteni a forgalmat. Ezt követően például a Vomit nevű program (de a Wireshark vagy a Cain&Abel[24] is) képes a G.711 kodeket (tipikusan ezt

[23] http://ettercap.sourceforge.net/

[24] http://www.oxid.it/cain.html

használják a Cisco IP telefonok és a Microsoft Netmeeting is) használó hangrészleteket, lejátszható (wav) formátumúvá konvertálni.

3.1.3 A rendszer megbénítása

A denial of service támadások célja a szolgáltatások elérésének ellehetetlenítése, rendszerünk megbénítása. Az elárasztásos módszert alkalmazó általános technikák mellett (TCP SYN, UDP, ICMP flood) vannak VoIP specifikus módszerek. RTP csomagok és a jelzésprotokollok üzeneteinek (SIP esetén INVITE, REGISTER) generálásával is elérhető a telefonok vagy a teljes rendszer leállása.

Zavart és bénulást okozhat a VoIP végponti eszközöket kiszolgáló TFTP kiszolgáló kompromittálása, vagy az azon tárolt konfigurációs állományok módosítása. Ez utóbbi ahhoz vezet, hogy a telefonok valótlan címen keresik a hívásvezérlő központot (Callmanager).

Nem fix IP-címet használó környezetben, a hálózati címet adó DHCP kiszolgáló feltörésével telefonunk sosem kap vagy hibás IP-cím információkat kaphat, ami ugyancsak a szolgáltatás szüneteléséhez vezethet.

3.1.4 Jogosulatlan hozzáférés

Talán külön ki sem kellene emelni, annyira egyértelműek a hálózati eszközökhöz való illegális hozzáférés veszélyei. Egy kapcsoló feltörésével a támadó létrehozhat egy ún. SPAN portot (Switched Port Analyzer), amelyen keresztül a kapcsolón átmenő összes hálózati forgalmat elfoghatja, és utólag elemezve lehallgathatja a hívást.

A konfigurációs állományokat és IP-telefon firmware képállományokat (image) tároló TFTP kiszolgálók tartalmához való hozzáféréssel, olyan módosított konfigurációs fájlok vagy idegen kóddal fertőzött image-ek kerülhetnek a telefonokra, amelyek hibás működést vagy bénulást okozhatnak. A TFTP kiszolgálón lévő fájlok nevei gyakran utalnak a rendszerben lévő végponti eszközök pontos típusára (pl. cmterm-7911-sccp.7-2-1.exe – amely egy SCCP jelzési protokollt használó Cisco 7911-es típusú telefonra utal). A kiszolgálón található nevek kinyerhetőek például a TFTP Brute Force nevű programmal.

3.2 A veszélyforrásokra adható válaszok

A védelem nem csak biztonsági technológiák használatával (technikai kontrollok), hanem az ember tényezőkből eredő sérülékenységek felszámolásával és szabályok betartatásával is fokozható (adminisztratív kontrollok). A veszélyforrásokra adható védelmi megoldások egy részéről már volt szó az előző fejezet végén, ezért azok megemlítése mellett, csak az új módszerek ismertetésére kerül sor részletesebben. Az említett módszerekből részletesebben a Cisco Unified Communications Solution Reference Network Design c. dokumentum Voice security fejezetében olvashatunk.

3.2.1 Technikai biztonsági kontrollok

Elöljáróban annyit, hogy a biztonság fokozásához nem minden esetben van szükség költséges, új védelmi eszközök beszerzésére. A végpontok, kiszolgálók és köztes hálózati eszközök beépített biztonsági funkciókkal rendelkeznek, ismerni kell azok rendeltetését és tudni kell azokat megfelelően alkalmazni.

Az IP-telefóniás és a „hagyományos” adathálózati eszközök biztonságának első lépése, hogy be kell vezetnünk titkosított menedzsment és AAA funkciókat az eszközök adminisztrálásához.

LAN védelem

A biztonságos VLAN elkülönítés megvalósításával elejét vehetjük a belső felderítéses, lehallgatásos és DoS támadások kivitelezésének.

A VoIP rendszerek egyik hálózat tervezési elve, hogy az IP-telefonok hálózati forgalma egy logikailag elkülönített hang VLAN-t (voice VLAN) használjon. A telefonra fűzött PC adat VLAN-ja, a hívásokra használt hang VLAN-tól eltérő. Ezt biztosítja a hang és adat csomagok megfelelő szeparációját. Alapesetben a hardveres IP-telefon kapcsolóportja (a LAN kapcsolóhoz csatlakozó) minden forgalmat továbbít (megfelelő modell esetén) a telefonon lévő PC-port felé. A biztonság érdekében letiltható a telefonban, hogy a PC-felől érkező hang VLAN címkével ellátott forgalom eldobásra kerüljön (PC voice VLAN access), így a PC-portról nem lehet hozzáférni a hang VLAN hálózati forgalmához. Szoftveres telefonok esetén (például a Cisco IP Communicator) ez nem lehetséges, mert ekkor a PC-n lévő szoftveres IP-telefon által generált hang forgalomnak hozzá kell férnie a hang VLAN-hoz.

Ha nem megoldható a LAN kapcsolók fizikai védelme (valaki hozzáfér a kapcsolóportokhoz), akkor is biztosítható a kapcsolóportokhoz rendelt VLAN-ok biztonságos kiosztása. Ez 802.1x alapú azonosítással és dinamikus VLAN hozzárendeléssel kezelhető, a Radius kiszolgálón tárolt felhasználói név/VLAN azonosító adatbázis alapján. (VLAN Member Policy Server (VMPS) kiszolgálóval, MAC-cím alapján is működik).

Az illegális hozzáférés megelőzéséhez, a Cisco Catalyst kapcsolók rendelkeznek a Private VLAN funkcióval, mellyel olyan másodlagos VLAN-ok hozhatóak létre egy elsődleges VLAN-on belül, ami az alapvetően szórásos szegmenst, nem-szórásos, többes hozzáférésű közeggé alakítja át. Így egy adott VLAN-hoz tartozó portok forgalma elszigetelhető egymástól, fokozva a biztonságot. (Bővebben: Securing Networks with Private VLANs and VLAN Access Control Lists[25])

Kapcsolókhoz köthető egyéb biztonsági tanácsok:

- Használjuk a portbiztonság (port security) funkciókat!
- Alkalmazzunk VLAN ACL (VACL) szűrőlistákat, ahol szükséges!
- Használjuk a VLAN 1-et kizárólag STP célokra, minden másra hozzunk létre különböző VLAN-okat!
- Expliciten rögzítsük egy kapcsolóport trönk vagy hozzáférési port szerepét (a DTP-t tiltsuk le)!
- Alkalmazzuk a DHCP Snooping, Dynamic Arp Inspection, IP Source Guard funkciókat a man-in-the-middle támadások kivédéséhez!
- Az STP védelemhez használjuk a beépített BPDU Guard, Filter és Root Guard parancsokat!
- Alkalmazzuk a beépített Smartport makrókat a portok konfigurálása során (cisco-phone)!

A Callmanager biztonsági funkciói

A Cisco Unified Communications Manager elérése webes felületen történik. A rendszer támogatja a szerepkör alapú felhasználó kezelést. A rendszer adminisztrátoraihoz, vagy

[25] http://www.cisco.com/application/pdf/paws/10601/90.pdf

adminisztrátori csoportokhoz a különböző konfigurációs űrlapok szintjéig létre lehet hozni jogosultságokat.

A webes adminisztrációs felület HTTPS (HTTP over SSL) protokollon keresztül érhető el. A böngésző letölti és elfogadtatja a Callmanager által generált és aláírt (self signed) tanúsítványt.

A hívásvezérlő operációs rendszerének telepítésével egy külön nem menedzselhető állomás alapú IPS szoftver, a Cisco Security Agent is felkerül a kiszolgálóra. Ennek célja az ismert és ismeretlen támadások, a férgek és a vírusok elleni védekezés. A Callmanager jelenlegi 7-es verziója nem támogatja a távolról menedzselhető IPS alkalmazások és az antivírus programok használatát.

A nyilvános kulcsú infrastruktúrára épülő, fejlett biztonsági lehetőségek válnak elérhetővé a Communications Manager Certificate Authority Proxy Function (CAPF) szolgáltatásának alkalmazásával. A CAPF funkció lokális érvényű tanúsítványokat bocsát ki. Használatához szükség van legalább 2 hardveres biztonsági tokenre és a CTL kliens szoftverre. (A token egy USB felületű, a gyártó által aláírt tanúsítványt tartalmazó elektronikus tárolóeszköz; a CTL (Certificate Trust List) kliensben felvehetjük a megbízható állomások listáját, amely ezután minden telefonra letöltődik.) A CAPF szolgáltatás által biztosított védelmi funkciók összefoglalva:

- Hitelesítést biztosít a kiszolgálók és a végponti eszközök között
- Jelzésrendszer titkosítás: SIP és SCCP esetén TLS (SSL) alapú, H.323-nál IPSec alapú titkosítás
- A médiaforgalom titkosítása: Az SRTP protokoll (Secure Realtime Transport Protocol) 128 bites AES alapú adattitkosítást biztosít. A szimmetrikus kulcsú kódolás miatt szükség van a felek közötti biztonságos kulcscserére, ezt a ZRTP (Diffie-Hellman alapú) vagy a MIKEY valós idejű működésre tervezett kulcscsere protokollok végezhetik el. A csomagok integritásáért és hitelesítéséért a csomagokhoz fűzött HMAC-SHA1 alapú (32 vagy 80 bites) lenyomat felelős. (A Cisco telefonok, az IOS rendszerű média átjárók és a Cisco Unity (hangposta) kiszolgálók támogatják az SRTP-t.)
- Biztosítja a TFTP kiszolgálókon található tartalmak integritását és titkosságát. Digitálisan aláírja a telefonok működéséhez szükséges állományokat. A titkosítás

történhet a telefon publikus kulcsával, de tanúsítvány hiányában előre beállított szimmetrikus kulccsal is.

A telefonok biztonsága (phone hardening)

A végponti eszközök, jellemzően az IP-telefonok sokféle konfigurációs beállítással rendelkeznek. Ezek egy része bizonyos szolgáltatások miatt alapértelmezés szerint engedélyezve van. A tökéletes biztonságra törekedve, minden szükségtelen szolgáltatás le kell tiltani, úgy, mint a forgalomirányítóknál és a kapcsolóknál. A telefonok beállításai a Unified Communications Manager-ben távolról is testreszabhatók, de egyenként kézzel is konfigurálhatóak. A kérdéses konfigurációs beállításokról szól az alábbi lista:

- Olyan környezetben, ahol az IP-telefonokhoz bárki hozzáférhet (aulák, porták) hasznos lehet a telefon beállítások menüjének teljes letiltása, így a támadások előkészítésére használható információk (TFTP-kiszolgáló, hívásvezérlő IP-címe) elrejthetőek.
- A telefonok rendelkeznek egy egyszerű beépített web-kiszolgálóval, melyet a telefon IP-címének beírásával lehet elérni. Ez a weboldal eszközinformációkat, verziószámokat, és az össze konfigurációs beállítást tartalmazza. Ugyan ez az opció megkönnyíti a hibaelhárítási feladatokat, de túl sok hasznos információt biztosít a potenciális támadóknak.
- A kéretlen ARP üzenetek jelentette kockázatról már volt szó korábban. A telefonokban a 7-es CM verzió óta alapértelmezetten letiltásra kerül a kéretlen ARP üzenetek fogadása.
- A telefonokon található PC port teljesen letiltható, ezáltal olyan helyeken, ahol nincs külön számítógép a telefonra fűzve, elejét vehetjük az illegális hálózati hozzáféréseknek.
- A telefonok PC portjain kikapcsolható a CDP (a Cisco L2 információs protokollja) és az LLDP (szabványos L2 információs protokoll) protokollok támogatása. Erre akkor lehet szükség, ha a PC-n nem használunk telefonos vagy videotelefonos alkalmazásokat.

Peremvédelmi funkciók

Korábban már volt szó a peremvédelmi technológiákról, ezért az alábbiak kifejezetten az IP-telefóniás rendszerekhez köthető védelmi eljárásokról szólnak.

Az illegális hozzáférés kiküszöbölésének legalapvetőbb módszere a hozzáférés szűrése ACL-ekkel. Azonban az IP-telefóniás protokollok nagyszámú, dinamikusan választott portot használnak, melyek szabályozása statikus módszerekkel nem, de tűzfalak segítségével megoldható. A Cisco ASA, PIX vagy IOS-alapú tűzfalak képesek a VoIP protokollok (SIP, H.323, SCCP, MGCP, RTP, SRTP) megfelelőségi és alkalmazásszintű vizsgálatára.

Az ASA tűzfal, a hívásvezérlő központ CAPF szolgáltatásával együttműködve többféle módon segíthet növelni a rendszer biztonságát.

- Képes a LAN-on kívüli kommunikáció jelzésrendszerének (TLS alapú) és médiaforgalmának (SRTP) titkosítására, valamint hitelesítésére (digitális aláírásokkal vagy statikus kulcsokkal). Így például biztonságos kapcsolat hozható létre (külön lan-to-lan VPN nélkül) egy, az interneten elhelyezett hardveres telefonkészülékkel.
- Megoldja a szoftveres VoIP alkalmazásoknál az adat és hang a VLAN-ok közötti biztonságos kommunikációt.
- Felülírja a Callmanager felől érkező, telefonoknak szánt konfigurációs fájlokat, beleírja a publikus hívásvezérlő címét és olyan biztonsági beállításokkal egészíti ki, melyek védik a publikus, potenciális veszélyt jelentő támadásokkal szemben.
- Képes a konfigurációs állományok titkosítására.

(A proxy funkciókról részletesen a Cisco Unified Communications Manager Security Guide[26] című kézikönyvben olvashatunk.)

A meglévő IDS/IPS eszközök megfelelő hangolásával tovább fokozható a védelem. Elérhető olyan UC specifikus mintázat-gyűjtemény, amely az IP-telefonos rendszereket leginkább érintő támadások ismertetőjeleit tartalmazza (például SIP DoS támadás), ezért ezt ajánlott használni.

[26] https://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/7_0_1/secugd/sec701-cm.html

3.2.2 Adminisztratív biztonsági kontrollok

A támadások megalapozásához alkalmazott információgyűjtési módszerek kivédhetőek nem-technikai jellegű szabályozásokkal. Meg kell keresnünk a rólunk található, potenciális veszélyt jelentő információkat az interneten és gondoskodni kell azok felülvizsgálatáról és eltávolításáról. (pl. Iwiw profilok).

Jó biztonsági házirend fontosságáról már korábban volt szó. A belső támadások (lehallgatás) többsége megelőzhető a megfelelő szabályok rögzítésével és azok betartatásával. A házirendnek mindenképpen tartalmaznia kell egy a jelszavak használatáról szóló szabályzatot. Rendszeresen változtatott, erős jelszavak használatára van szükség, a nyers-erő alapú támadások kivédéséhez.

A felhasználók oktatásával felkészíthetjük őket a különféle emberi tényezőt kihasználó veszélyek, például szociális manipulációra épülő próbálkozások felismerésére és kezelésére.

4. Biztonsági felmérés és javaslattétel a gyakorlatban

Szakdolgozatom hátralévő részében egy valós környezetben végrehajtott, biztonsági felmérés előkészületeinek, menetének és eredményeinek dokumentálása található. A felmérés egy multinacionális vállalat, budapesti képviseletének épületében történt.

A biztonsági felmérés kiváltó oka egy Cisco Callmanager kiszolgáló által produkált rendellenesség volt, melynek hibás működéséből adódóan az egyik átjáró forgalomirányító folyamatosan ledobta a külső ISDN PRI kapcsolatot, így a helyi irányú hívások nem tudtak kimenni ezen a vonalon. Mint kiderült a jelenséget az eszköz szoftverének egy belső hibája produkálta, ami kikerülhető lett volna a megfelelő szoftver és hardver üzemeltetési előírások betartásával, lévén az eszköz rendszere 2 éve nem került frissítésre. A hiba feltárását követően a szervezet IT üzemeltetési vezetője megbízott hálózatuk biztonsági szemléjének kivitelezésére.

A fő cél a szervezet telekommunikációs hálózatának IT biztonsági szemléje, beleértve az ehhez kapcsolódó hardveres és szoftveres üzemeltetési, fizikai - és hálózatbiztonsági kérdések megtárgyalását. A projekt másodlagos célja a sürgős védelmi és megbízhatósági problémák orvoslása és javaslattétel a további teendőkre a megbízható és biztonságos üzemeltetés érdekében. Kifejezetten nem volt cél részletesen megvizsgálni a fizikai és környezeti biztonsági tényezőket, valamint egy bizonyos szinten túl nem vizsgáltam meg a szervezet munkaállomásainak és kiszolgálóinak biztonságát, hiszen ez nem tartozik a helyi IT üzemeltetés hatáskörébe (azokért az cég központi IT részlege felel).

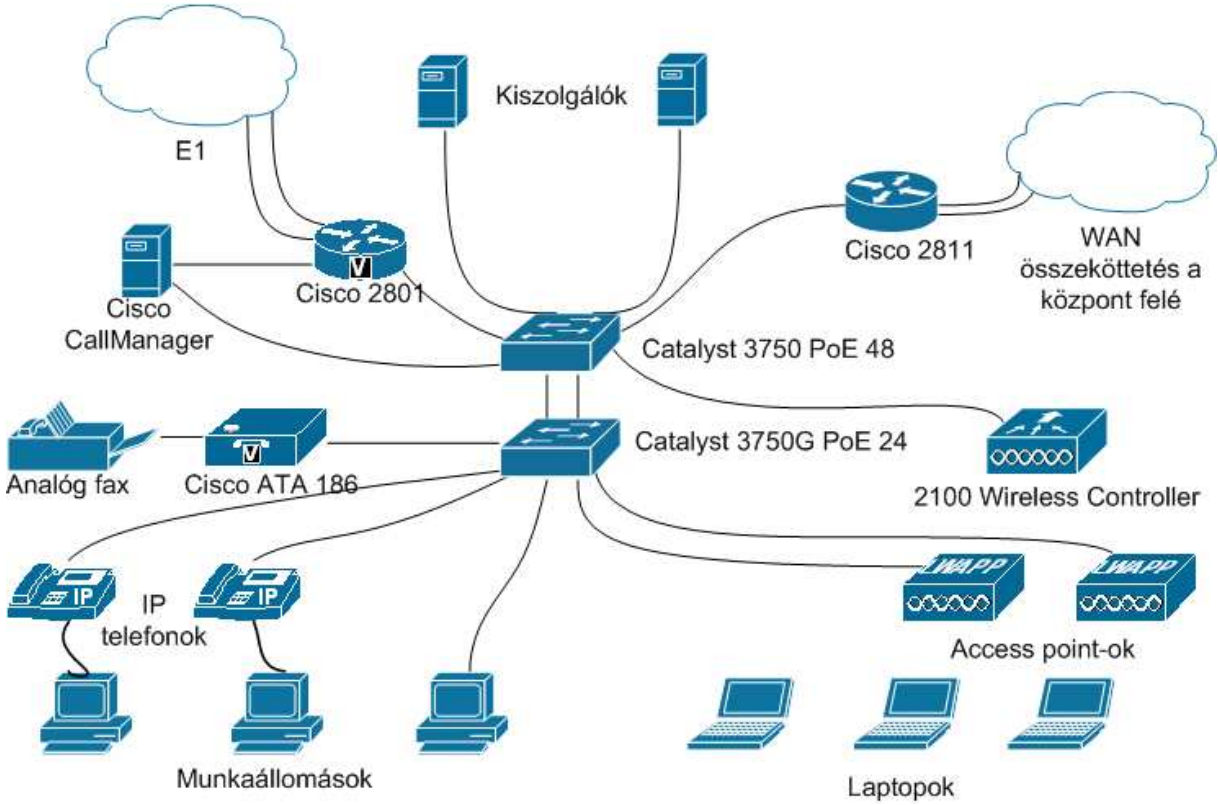
A felmérés elvégzését a következő jellemzők és támpontok segítették (ellenőrző lista):

- logikai diagram a szervezet hálózatáról
- az aktív hálózati eszközökön (forgalomirányítók, kapcsolók, tűzfalak) található IOS és firmware verziója (IPS/IDS signature verzió, Callmanager verzió, patchek száma)
- az eszközök hozzáféréséhez használt jelszavak erőssége, a jelszómenedzsment, egyéb hitelesítési módszerek (token, "biometrikus", egyszeri jelszavak, stb.)
- az eszközök hozzáférési vonalai (menedzsment hálózat)
- a hálózati adatforgalom szűrésére vonatkozó intézkedések, tűzfal házirendek
- naplózás, naplókövetés és időszinkronizáció

- az eddigi biztonsági szabályzat tartalma
- fizikai védelem, tűzvédelem és a megfelelő környezet biztosítása

4.1 Felmérés

A tényleges felmérést 2009. május 22-én történt. A helyszínen megtekintésre kerültek a kiszolgálóhelyiségben lévő hálózati eszközök, a kábelezés, az eszközök tápellátása és a környezeti viszonyok megállapítása. A nem technikai jellegű kérdésekre a helyi IT vezető válaszolt. A hálózati infrastruktúrát felmérve készült el a 10. ábra.



10. ábra: A vizsgált topológia

A redundáns klímával rendelkező kiszolgálóhelyiségben két rack-szekrénybe rendszerezve találhatóak az eszközök. A tápellátásért egy szünetmentes tápegység felel. Az egyik szekrényben kizárólag a kiszolgálók foglalnak helyet, míg a másikban találhatóak az UTP kábelrendező panelek és az aktív hálózati eszközök:

- egy Cisco 2811-es forgalomirányító, amely a vállalat központi hálózata felé biztosít redundáns, bérelt vonali WAN kapcsolatot
- egy Cisco 2801-es forgalomirányító, mely Voice Gateway feladatokat lát el, összeköttetésben áll a külső telefonos vonalakkal két E1 kapcsolaton keresztül
- egy Cisco Catalyst 3750 PoE 48 és egy Cisco Catalyst 3750 PoE 24 kapcsoló, melyek stackben üzemelve kiszolgálják a rájuk kapcsolt munkaállomásokat és IP telefonokat
- egy Cisco 7800as sorozatú kiszolgáló, melyen a Cisco Callmanager kiszolgáló fut
- egy a vezeték nélküli hozzáférési pontok vezérléséért felelős Cisco 2100-as vezeték nélküli kontroller
- három Cisco ATA 186 analóg konverter, melyek analóg faxokat csatlakoztatnak az adathálózathoz

Az eszközök és a csatlakozások külső szemrevételezését követően, megtekintésre és mentésre került az aktív eszközök konfigurációja és fontosabb állapotinformációi is. Ehhez legegyszerűbben a privilegizált módban kiadott ***show tech-support*** parancs használható (a parancs a 11.2-es IOS verzió óta elérhető[27]). A parancs egy rendkívül hosszú, de hasznos kimenetet eredményez, mivel egyetlen utasítás segítségével több diagnosztikai parancs kimenetét megtekinthetjük, és egyben lementhetjük. Az előbb említett parancs mellett érdemes a ***show cdp neighbors detail*** utasítás által eredményezett kimenetet is megőrizni, mely az adott eszközhöz közvetlenül csatlakozó Cisco eszközökről ad alapvető információt.

4.2 Kiértékelés és javaslattétel

A konfigurációk kiértékelésével feltárt kockázatok súlyosságát a már korábban ismertetett AS/NZS 4360 szabvány kvalitatív módszerének megnevezésivel jelölöm, külön-külön, minden esetben dőlten szedve. A jelölés segítségével fontosság alapján lehet sorba rendezni a feladatokat.

[27] http://www.cisco.com/en/US/docs/ios/12_3t/fun/command/reference/cfrgt_10.html#wp1098334

4.2.1 A Cisco Callmanager vizsgálata

A vállalatnál üzemelő Cisco 7800-as kiszolgálón futó Callmanager híváskezelő rendszerről a következőket lehetett tudni:

- Aktuálisan az 5.1-es főverzió van telepítve, mely már nem áll fejlesztés alatt, csak a támogatása biztosított. Azonban ennek is egy 2 éve kiadott, azóta nem frissített változata üzemelt, mely egy olyan ismert programhibát, amely hibás működést eredményez. A hiba miatt a Callmanager hibás MGCP profilt töltött le a Cisco 2801-es voice gateway forgalomirányítóra, így az nem kezelte megfelelően az ISDN PRI (E1) kapcsolatot, ami miatt a helyi irányú hívások nem az optimális költségű útvonalon mentek ki. *(Magas kockázat, sürgős beavatkozást igényel.)*
- A kiszolgáló rendszerét beépített állomás alapú IPS felügyeli.
- Erős jelszó: rendben, de rendszeres cseréje nincs megvalósítva. Rendszeres cseréjét házirendi szabályban kell rögzíteni, esetleg központilag adminisztrálni AAA segítségével. *(Alacsony kockázat, elhárítása javasolt, de nem igényel azonnali beavatkozást.)*
- Role Based Access control nincs megvalósítva, de mivel 1 személy menedzseli, ez nem is kritikus. Ugyanakkor a megkülönböztetett adminisztrátor felhasználói fiókok megléte a távoli támogatást (outsource) biztosító mérnököknek és a helyi rendszergazdának fontos lenne (például felülvizsgálati célokból). *(Alacsony kockázat, elhárítása javasolt, de nem igényel azonnali beavatkozást.)*
- A végfelhasználók számára fenntartott adminisztrációs interfész használatban van. Itt módosíthatják egyszerűen saját profiljukat (gyorstárcsázó, személyes telefonkönyv stb.). Ezen interfész védelme azonban nincs kellően szabályozva. Az alkalmazott jelszó erőssége és élettartama sem technikai, sem adminisztratív kontrollal nincs védve. Mivel itt személyes adatok védelméről beszélünk ez kritikus pont. Javasolt a jelszavak megfelelő szintű kezelésének megkövetelése vagy a céges Active Directory adatbázissal történő szinkronizáció. Az alkalmazott Active Directory rendszerben a jelszavak cseréjére és erősségére vonatkozó szabályok már megfelelőek (45 naponta kell megváltoztatni a jelszót, minimum 8 karakteres, a rendszer az utolsó 24 jelszót tárolja). Ezt a felhasználók már megszokták és elfogadták. Számukra is egyszerűbb lenne egyazon

biztonságos jelszó használata a telefóniás rendszerben és a Windows munkaállomásokon. *(Mérsékelt kockázat, mihamarabbi beavatkozást igényel.)*

- A naplózási funkciók alapbeállításban vannak, amely nem tesz eleget az elvárható auditálási követelményeknek. Központi Syslog kiszolgálón is tárolni kell a keletkező naplóüzeneteket. *(Mérsékelt kockázat, mihamarabbi beavatkozást igényel.)*
- A rendszerben a CAPF funkció nem aktív, így minden jelzésrendszer és média csomag titkosítatlanul kerül továbbításra. Mivel nincsenek interneten publikált telefonok és szoftveres telefonok az adat VLAN-on, VLAN szeparáció ugyanakkor van, továbbá a szervezet mérete meglehetősen kicsi és fizikailag is egy helyszínről beszélünk, a CAPF aktiválása nem létfontosságú. Bár a VLAN szeparáció nem megfelelő (még tárgyaljuk), annak növelése kielégítő biztonsági szintet eredményezhet. *(Mérsékelt kockázat, mihamarabbi beavatkozást igényel.)*
- A telefonok biztonsági profiljában a kéretlen ARP csomagok megfelelően tiltva vannak. A CDP és HTTP protokollok engedélyezve vannak, de a szervezet fent ismertetett tulajdonságait figyelembe véve, megfelelő VLAN szeparáció mellett ezen egyébként hasznos szolgáltatások tiltása nem növelné jelentősen a biztonsági szintet. *(Alacsony kockázat, elhárítása javasolt, de nem igényel azonnali beavatkozást.)*

4.2.2 A LAN kapcsolók biztonsága

Szoftverüzemeltetés

Ahogy a hívásvezérlő esetében, itt is probléma a szoftverek frissítésének elhanyagolása. A gyártó által kiadott biztonsági riasztásokat és frissítési javaslatokat az IT csoport erőforrás hiány miatt nem követi. A gyártói szoftver adatbázis ellenőrzése során kiderült, hogy az alkalmazott alverzió „deferred” státuszú, ami azt jelenti, hogy súlyos hiba derült ki benne (ami lehet, hogy soha nem lesz javítva), továbbá már nem patchelt és támogatott. *(Magas kockázat, sürgős beavatkozást igényel.)*

Adminisztratív hozzáférés vezérlés

- Erős jelszó alkalmazása: rendben, de rendszeres, központi cseréjéhez AAA-megoldásokra lenne szükség. *(Alacsony kockázat, elhárítása javasolt, de nem igényel azonnali beavatkozást.)*
- Nincs beállítva privilégium vagy CLI view szintű szerepkör alapú hozzáférés vezérlés, az adminisztrátorok megkülönböztetéséhez, de nem feltétlenül indokolt ebben a szervezeti környezetben. *(Alacsony kockázat, elhárítása javasolt, de nem igényel azonnali beavatkozást.)*
- Nincs titkosított adminisztrációs interfész. Jelenleg telnet alapú parancssor és HTTP alapú grafikus menedzsment interfészeket használnak, forráskorlátozás nélkül. SSH és HTTPS alapú hozzáférés beállítása ajánlott. *(Magas kockázat, azonnali beavatkozást igényel.)*
- Nincs beállítva figyelmeztető üzenet az adminisztrációs interfészekre történő belépéskor (***banner login, banner motd*** parancsok). Ez egy esetleges incidens esetén a támadó büntethetőségét is lehetetlenné teszi, mivel a hatályos jogszabályok alapján illegális hozzáférés elkövetése akkor valósul meg, ha a támadó erre figyelmeztetve lett (BTK 300/C §). *(Mérsékelt kockázat, mihamarabbi beavatkozást igényel.)*
- Egyéb hozzáférés védelmi metódusok, mint például a sikertelen belépési kísérletek naplózása és időbeni korlátozása nincs beállítva, ami potenciális lehetőséget biztosít egy brute force támadásra. A ***login block for***, ***login delay***, ***login quite mode access-class, login on-failure log, login on-success log*** parancsok használata javasolt minden vty vonalon. *(Magas kockázat, azonnali beavatkozást igényel.)*
- Az eseménynaplózás csak DRAM bufferbe történik, ami egy újraindítással elvész, így egy behatoló könnyedén eltűntetheti a nyomait. Helyette különálló (Syslog) kiszolgálónak elküldött naplózás javasolt a ***logging*** parancs segítségével. *(Magas kockázat, azonnali beavatkozást igényel.)*

A hálózati forgalom védelme

- A feszítőfa protokoll (STP) védelme maximálisan meg van valósítva.
- A portbiztonság (port security) helyesen be lett konfigurálva, így a CAM Flood[28] támadások ellen is védettek a kapcsolók.
- DHCP Spoofing védelem nem lett beállítva, a korábban említett ***ip dhcp snooping*** parancs használata javasolt. *(Mérsékelt kockázat, mihamarabbi beavatkozást igényel.)*
- Dynamic ARP Inspection funkció nem lett beállítva (***ip arp inspection*** parancs). A rendszer paramétereit tekintve a telekommunikáció szempontjából nem kritikus (az IP telefonkészülékek védelmi profiljában a kéretlen ARP tiltva van), de könnyen aktiválható hasznos funkció, amely jelentősen növelni a végponti eszközök védelmi szintjét. *(Alacsony kockázat, elhárítása javasolt, de nem igényel azonnali beavatkozást.)*
- 802.1x alapú dinamikus állomásazonosítás egyelőre nincs megvalósítva. Tekintve az infrastruktúra magas szintű fizikai védelmét és az alkalmazásokon megvalósított jogosultság kezelés magas szintjét, ez egyelőre nem kritikus. *(Alacsony kockázat, elhárítása javasolt, de nem igényel azonnali beavatkozást.)*
- A nem használt kapcsoló portok nincsenek letiltva. A fizikai körülmények miatt ez sem kritikus probléma, de általánosan javasolt eljárás. *(Mérsékelt kockázat, mihamarabbi beavatkozást igényel.)*
- A VLAN szegmentáció félig megvalósított. Pozitív, hogy külön-külön VLAN-okat használtak az adat és a telefóniás forgalomra. Továbbá pozitív, hogy a diagnosztikai üzenetekre használt 1-es számú VLAN nem használt más célra. A VLAN-ok közötti átjárhatóság ugyanakkor nincs szűkítve (Private VLAN, VLAN ACL, tűzfal), ami lehetővé teszi a telefóniás VLAN felderítését és illegális hozzáférési támadások indítását a hálózat más logikai szegmenseiből. *(Mérsékelt kockázat, mihamarabbi beavatkozást igényel.)*

[28] A kapcsoló CAM táblájának hamis MAC-címekkel történő telítése, miáltal a kapcsoló hub-ként kezd el működni.

4.2.3 A Cisco 2801 voice gateway biztonsága

A voice gateway forgalomirányító adminisztratív hozzáférés védelmi szintje teljes mértékben megegyezik a LAN kapcsolókéval. A korábban ismertetett MGCP-profil hiba elhárításával egy időben frissítésre került az eszköz szoftvere. A verzió frissítése jelenleg nem kritikus. *(Alacsony kockázat, szoftverüzemeltetési házirend szabály készítése javasolt, de nem igényel azonnali beavatkozást.)*

4.2.4 A vezeték nélküli hálózat biztonsága

A kommunikációs hálózat vezeték nélküli részét külföldről a cég központi IT csoportja menedzseli. Ezért teljes analízisre nem volt lehetőség, a konfigurációs állományt nem állt módomban ellenőrizni (a konzolos vonal jelszava nem volt elérhető). A rendszer biztonsága jelenleg kritikus hibát nem tartalmaz. NetStumbler-rel[29] történő analízissel és a helyi rendszergazda megkérdezésével a következő paramétereket mértem fel:

- WPA2 Pre Shared Key alapú titkosítás és authentikáció történik.
- Az alkalmazott Pre Shared Key megfelel az erős jelszavakkal szemben támasztott követelményeknek.

Az AP-kon a WLAN vezérlőnek köszönhetően dinamikus teljesítményszint szabályozás került megvalósításra, amellyel a környezetbe sugárzott jelszint a minimális értéken tartható, így a hálózat felderíthetőségének fizikai határai minimalizáltak.

Javaslatok a biztonság növelésére:

- EAP alapú dinamikus authentikáció (minimum PEAP vagy EAP-TLS). Amennyiben ennek infrastrukturális követelményei (korszerű AAA kiszolgáló- és ügyfélalkalmazások) nem valósíthatóak meg, akkor egy minimum 13 karakteres-, kis és nagybetűket, számokat, valamint speciális karaktereket egyaránt tartalmazó, pseudo-random pre-shared-key-ből származtatott authentikációs kulcs használata javasolt.
- Ajánlott a Wi-Fi-n csatlakozó állomások forgalmának külön VLAN-ba terelése (alkalmi felhasználók esetén vendég VLAN), továbbá ezen VLAN és más VLAN-

[29] http://www.netstumbler.com/

ok közötti forgalom minimum statikus szűrőlistákkal történő szűkítése. A maximális biztonságot belső tűzfal alkalmazása jelentené.

4.2.5 Általános fizikai biztonság

A fizikai biztonság terén kivetnivalót nem találtam. A cég területére történő belépés szigorúan ellenőrzött. Minden eltérő biztonsági szintű zóna elektronikus azonosító- és zárrendszerrel védett. Nem céges alkalmazottak csak a recepción keresztül léphetnek be és ki. Utóbbi különösen dicséretes, kevés helyen megvalósított szabály. A kijáratokat kamerák ellenőrzik, a vészkijáratot riasztórendszer védi. A kiszolgálóhelyiséget tűz- és rongálás biztos vastag lemez ajtó különíti el a többi szobától. A szoftverek, licencek, biztonsági kulcsok és egyéb kiemelt adathordozók tárolása tűzálló, biztonsági záras széfben történik.

4.2.6 Egyéb adminisztratív kontrollok áttekintő elemzése

A cég rendelkezik biztonsági házirenddel és annak ismeretére kötelezi a felhasználóit.

A felhasználók esetében a telefóniás rendszer végfelhasználói interfészéhez használt jelszavak frissítésére nincsenek kötelezve. Javasolt a korábban megemlített LDAP/Active Directory jelszó adatbázis szinkronizáció vagy a jelszavak változtatásának kötelezővé tétele.

A telekommunikációs rendszerben alkalmazott szoftverek rendszeres frissítésére nincs kidolgozott folyamat és nincs kijelölt felelős. Javasolt e folyamat kidolgozása, a felelős kijelölése vagy a tevékenység kihelyezése külső szakértő cég bevonásával.

4.2.7 Értékelés

A munka elsődleges célja az volt, hogy a rendelkezésre álló eszközök meglévő funkcióit felhasználva magasabb szintű legyen helyi LAN biztonsága, mely a javaslatok megvalósításával elérhető. Külön anyagi erőforrások rendelkezésre állása mellett, például egy tűzfal vagy IPS beszerzésével még jobban fokozható lehetne a hálózat védelme. A felmérés levezetéséhez és a javaslatok elkészítéséhez nagyon sok elméleti ismeretre, de még több gyakorlati tapasztalatra volt szükség. Számomra egyik sem állt maradéktalanul rendelkezésre, ezért nagyon sok segítséget kaptam külső témavezetőmtől a munka során, melyekért ismét köszönettel tartozom.

5. Összefoglalás

Az egységesített kommunikációs rendszerek, a különböző kommunikációs formákat összefogva, egyre nagyobb teret nyernek a vállalati szférában. Dolgozatom során igyekeztem bemutatni, milyen előnyökkel rendelkeznek az UC rendszerek, ismertettem a Cisco UC megoldásait, melyekkel eddigi munkám során ismerkedtem meg.

A kommunikációs megoldások mellett az IT biztonság és a hálózatbiztonság jelent számomra potenciális fejlődési irányt, ezért a legfontosabb tervezési és biztonsági technológiák bemutatására törekedtem a 2. fejezet során. Fontosnak tartottam, hogy az olvasó a veszélyforrások megismerésével meglássa, miért fontos adataink és hálózatunk védelme, ezért szorítottam helyet a dolgozatban napjaink leggyakoribb támadási technikáinak és korunk hackereinek ismertetésére. A fenyegetésekre adható technológiai megoldásokról is volt szó a fejezet végén. Természetesen minden említett védelmi megoldás részletes bemutatására a dolgozat terjedelmi korlátai miatt nem kerül sor, de nem is volt cél.

A harmadik fejezetben az egységesített kommunikációs rendszerek, azon belül kifejezetten a VoIP kommunikáció védelméről volt szó. A fejezet során a Cisco UC rendszerét vettem alapul. A jellemző veszélyek és támadások részletezését követően, bemutatásra kerültek veszélyekre adható válaszok és a rendszer nyújtotta biztonsági funkciók.

A dolgozat utolsó része egy, az eddigi ismeretekre alapozó, valós környezetben elvégzett biztonsági felméréssel foglalkozott. A biztonsági felmérés színhelyéül egy budapesti cég hálózata és UC rendszere szolgált. A munka a cég helyi IT vezetőjének kérésére történt. A körülmények kiértékelése mellett javaslatokat tettem a védelmi szint növelésére és meghatároztam a beavatkozás sürgősségét.

A dolgozatba fektetett munka során nagyon sok új dolgot tanultam meg, és remélem ebből minél többet sikerült átadnom az olvasónak. A szakirodalmak feldolgozása során, amint elkezdtem belemélyülni egy-egy témakörbe, világossá vált számomra, hogy mennyi mindent meg kell tanulnom még, ha a jövőben komolyabban akarok foglalkozni a témával.

6. Irodalomjegyzék

1. Cioara, J. - Cavanaugh, M. J. – Krake, K. A. [2009]: CCNA Voice Official Exam Certification Guide. Cisco Press, Indianapolis
2. Gregory, P. [2008]: Unified Communications for Dummies Avaya Custom Edition. Wiley Publishing, Inc., Indianapolis
3. Hucaby, D. [2006]: CCNP BCMSN Official Exam Certification Guide. Cisco Press, Indianapolis
4. ISC^2 [2008]: Official CISSP CBK Review Seminar Student Handbook. Pearson Custom Publishing, Boston
5. Morgan, B. [2007]: CCNP ISCW Official Exam Certification Guide. Cisco Press, Indianapolis
6. Porter, T. - Kanclirz, J. - Zmolek, A. - Rosela, A. - Cross, M. - Chaffin, L. - Baskin, B. - Shim, C. [2006]: Practical VoIP Security. Syngress Publishing, Inc., Rockland
7. Ranjbar, A. S. [2007]: CCNP ONT Official Exam Certification Guide. Cisco Press, Indianapolis
8. Stewart, B. D. – Gough C. [2007]: CCNP BSCI Official Exam Certification Guide. Cisco Press, Indianapolis
9. Thomas, T. [2005]: Hálózati biztonság. Panem Könyvkiadó, Budapest
10. Warren, P. - Michael S. [2005]: Az internet sötét oldala. HVG Kiadói Rt., Budapest
11. Watkins, M. - Wallace, K. [2008]: CCNA Security Official Exam Certification Guide. Cisco Press, Indianapolis

7. Egyéb források

1. Pintér Z. [2008]: Cisco Unified Communication a ROI mentén előadás prezentáció, Cisco Hálózati Akadémiai Napok, Szeged, 2008. október 17-19.
2. Segyik I. [2008]: IP telefónia biztonság I, II előadás prezentáció, Cisco Expo, Budapest, 2008. november 19-20.
3. Segyik I. [2007]: Security management előadás prezentáció

8. Internetes források

1. AS/NZS 4360:2004 szabvány
   http://www.ucop.edu/riskmgt/erm/documents/asnzs4360_2004_tut_notes.pdf
   Megnyitva: 2009. október 26.
2. Azonnali üzenetküldés
   http://en.wikipedia.org/wiki/Instant_messaging
   Megnyitva: 2009. szeptember 13.
3. Cisco MARS
   http://www.cisco.com/en/US/products/ps6241/index.html
   Megnyitva: 2009. november 18.
4. Cisco MCS kiszolgálók
   http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_models_home.html
   Megnyitva: 2009. november 18.
5. Cisco IP Communicator
   http://www.cisco.com/en/US/products/sw/voicesw/ps5475/index.html
   Megnyitva: 2009. november 18.
6. Cisco Unified Communications Solution Reference Network Design kézikönyv
   http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/uc7_0.html
   Megnyitva: 2009. október 20.

7. Cisco Unified Communications Manager Security Guide kézikönyv
https://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/7_0_1/secugd/sec701-cm.html
Megnyitva: 2009. október 22.

8. Cisco Unified 7900-as sorozatú IP-telefonok
http://www.cisco.com/en/US/products/hw/phones/ps379/prod_models_home.html
Megnyitva: 2009. november 18.

9. Cisco Unified Personal Communicator
http://www.cisco.com/en/US/products/ps6844/index.html
Megnyitva: 2009. november 18.

10. Cisco Unified 3500-as sorozatú videokonferenciás központok
http://www.cisco.com/en/US/products/hw/video/ps1870/tsd_products_support_series_home.html
Megnyitva: 2009. november 18.

11. Cisco VG200-as sorozatú átjárók
http://www.cisco.com/en/US/products/hw/gatecont/ps2250/index.html
Megnyitva: 2009. november 18.

12. Comodo - Ingyenes tűzfal és antivírus
http://personalfirewall.comodo.com/
Megnyitva: 2009. november 18.

13. E-mail történelem
http://www.multicians.org/thvv/mail-history.html
Megnyitva: 2009. szeptember 22.

14. Ettercap - Man-in-the-middle biztonsági program
http://ettercap.sourceforge.net/
Megnyitva: 2009. szeptember 22.

15. Fax technológia
http://en.wikipedia.org/wiki/Fax
Megnyitva: 2009. szeptember 13.

16. NetStumbler - Wi-Fi monitorozó alkalmazás
http://www.netstumbler.com/
Megnyitva: 2009. november 18.

17. Nmap - Hálózatbiztonsági szkenner
http://nmap.org/
Megnyitva: 2009. október 22.

18. Rövid leírások a VoIP biztonsági segédprogramokról
http://michaelboman.org/wiki/index.php?title=Category:VOIP_Security_Tools
Megnyitva: 2009. november 17.

19. SANS biztonsági házirend sémák
www.sans.org/resources/policies
Megnyitva: 2009 szeptember 28.

20. Securing Networks with Private VLANs and VLAN Access Control Lists
http://www.cisco.com/application/pdf/paws/10601/90.pdf
Megnyitva: 2009. október 14.

21. SIPScan - VoIP sebezhetőség tesztelő program
http://www.hackingvoip.com/tools/sipscan.msi
Megnyitva: 2009. szeptember 22.

22. SiVus - VoIP sebezhetőség tesztelő program
http://www.securityfocus.com/tools/3528
Megnyitva: 2009. szeptember 22.

23. TrueCrypt - Titkosító alkalmazás
http://www.truecrypt.org/
Megnyitva: 2009. november 18.

24. UC Security Best Practices
http://www.ucstrategies.com/uploadedFiles/UC_Information/White_Papers/Yedwab,_David/D%20Yedwab%20UC%20Security%20final%20092508.pdf
Megnyitva: 2009. szeptember 09.