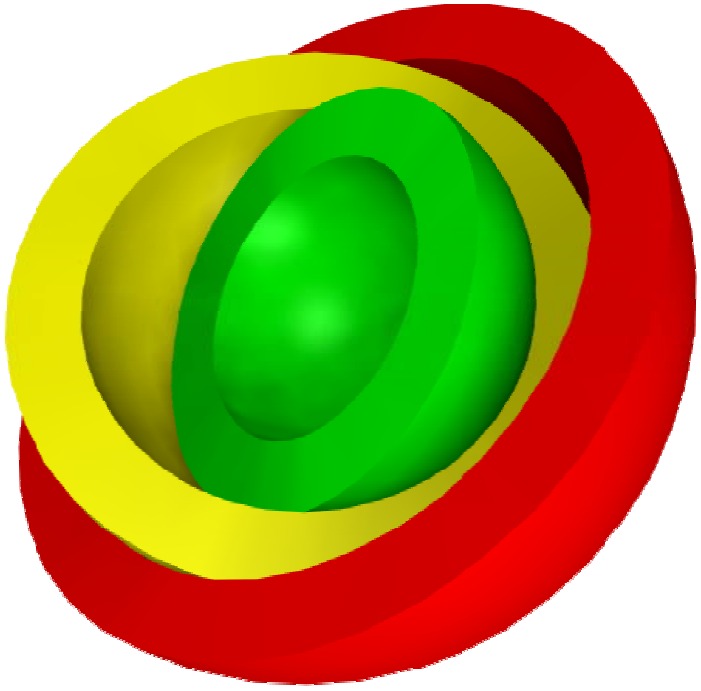
Az informatikai hálózati infrastruktúra biztonsági kockázatai és kontrolljai



Készítő:	MTA SZTAKI
Státusz:	*Harmadik mérföldkő lezárása; nyilvános!*
Utolsó mentés:	2006-05-14

A tanulmány elkészítésében és belső lektorálásában részt vettek: *Becz Tamás, Martos Balázs, Pásztor Szilárd, Rigó Ernő, Tiszai Tamás, Tóth Beatrix*

1 Bevezető

Jelen tanulmány az IHM-MTA Kutatási Program keretében végzett „*Internet védelmi rendszer struktúrájának kidolgozása*” című kutatási projekt (Sorszám: E4, Iktatószám: 4671/4/2003) részét képezi. A projekt fázisait magába foglaló mérföldkövek és a hozzájuk kapcsolódó határidők (kiemelve a jelen tanulmány által lefedni szándékozó részt):

- 1. mérföldkő: 1-2 kutatási fázis (Informatikai hálózati infrastruktúra biztonsági kockázatainak elemzése, és a kockázat-kezelési lehetőségek feltárása), lezárás: 2004. június 30.
- 2. mérföldkő: 3 fázis (Biztonsági mintarendszerek kidolgozása), lezárás: 2005. szeptember 30.
- **3. mérföldkő: 4 fázis (A biztonsági rendszerek üzemeltetési módszertanának kidolgozása, oktatási anyagok kidolgozása), lezárás: 2006. május 10.**

Az Informatikai Hálózati Infrastruktúra Biztonsága (továbbiakban – IHIB) magában foglalja a hálózat működéséért felelős hardver és szoftver elemeket, és ezeken felül számításba veszi a humán faktort és az egészet körülvevő adminisztratív jellemzőket is.

1.1 Röviden a tartalomról és a célokról

Az anyagban foglaltak segítséget kívánnak nyújtani a non-profit szervezetek (akadémiai intézmények, önkormányzatok) számára abban a nehéz munkában, hogy kialakítsák saját számítógép hálózatuk biztonságáért felelős szervezetüket – gyakorta alkalmazott betűszóval CERT, illetve CSIRT –. Ennek érdekében a jelen mérföldkőhöz kapcsolódó dokumentáció két jól elkülöníthető részre togolódik:

- Az első rész egy elképzelt CERT/CSIRT kialakításának alapelveit, továbbá az ott dolgozók alapvető tájékoztatását célzó minta-szabályzatot tartalmaz. Ez a szabályzat felsorolja mindazon alapvető intézkedést, amely egy tényleges incidens kezelő szervezet kialakításakor feladatként merül fel, és a lehetőségek szerint megoldási módokat, irányokat vázol fel az alapítási folyamat lebonyolítására.

  Természetesen ez a minta-szabályzat nem térhet ki valamennyi felmerülő feladat részletekbe menő szabályozására, de a szerzők megítélése és tapasztalatai alapján megbízható alapul szolgálhat a tényleges szabályzat kidolgozásához. E szerteágazó munkához az itt található minta-szabályzaton túl segítséget nyújtanak e kutatási munka megelőző szakaszaiban kidolgozott – és korábban már leadott – más dokumentumok is, amelyek a számítógép-hálózati incidensek értelmezésének, kezelésének, megelőzésének továbbá esetleges bekövetkezésüket követő adatgyűjtő / rögzítő / elemző munkának mibenlétével, a speciális szakterület fogalmainak megismertetésével, valamint az igénybe vehető további források felsorolásával foglalkoznak.
- E dokumentum második része egy terjedelmes oktatási anyag, amely a speciális területen – a hálózati incidensek kezelésében – már részleges ismereteket szerzett személyek számára nyújt rendszerezett fogalom magyarázatokat, valamint részletekbe menő ismeretanyagot. Az oktatási anyag – vetített bemutató ábrák (slide) formájában, amelyeket alkalmanként az előadó munkáját, illetve a megértést segítő jegyzetek egészítenek ki – végigvezet a hálózati incidenskezelés számos aspektusán, kezdve az alapelvek ismertetésétől, az incidenskezelő szervezetek működésének ismertetésén át, a terület specializált szabványainak és azok egymás közti viszonyainak bemutatásán keresztül az incidenskezelés és elhárítás technikai alapjainak és eszközeinek bemutatásáig.

Míg a kutatási feladathoz kapcsolódó korábbi tanulmányok közül az első bővebben ismertette az elméleti alapokat és az ezeken nyugvó gyakorlati alkalmazásokba adott betekintést, addig a második rész – és különösen a jelen harmadik rész – sokkal gyakorlatiasabb, így „szűkszavúbb”, ezáltal informatikai képzettséget vár el és feltételez a tárgyalt megoldások telepítése, alkalmazása és beállítása során.

A tanulmány két része miközben szoros összefüggésben van, ugyanakkor egymástól függetlenül is megismerhető és értelmezhető. Az olvasók bizonyos köre számára az egyes részek eltérő fontossággal bírnak, de elképzelhető, hogy mindkét rész megismerésére is szükségük lehet. Ezek megismerésének sorrendje azonban az igényeknek megfelelően tetszőleges lehet.

1.2 Szerzői jogi nyilatkozatok

A szerzői jogról szóló törvényi szabályok szellemében kell a tanulmánnyal eljárni mind a készítőkre, az átvevőkre és az olvasókra vonatkozóan. Hasonló módon az Adatvédelmi törvény ide vonatkozó paragrafusait is alkalmazni kell.

A szerzők nem vállalnak semmilyen felelősséget az anyagok téves felhasználásából, részben kiragadott vagy jogszerűtlen felhasználásából eredő károkért, és az általuk készített anyagokkal kapcsolatban is csak azt tudják vállalni, hogy legjobb szakmai tudásuk szerint állították össze azokat.

A tanulmány olyan linkeket (kapcsolódási pontokat) tartalmazhat, amelyek az Internet más és más oldalaira vezetnek. Ezen oldalak tartalmáért és szolgáltatóik adat-, valamint információvédelmi gyakorlatáért a szerzők nem vállalnak felelősséget.

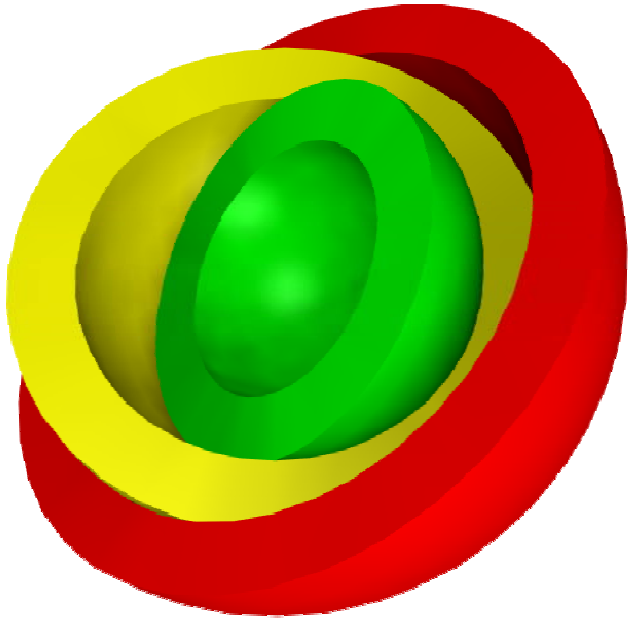
A tanulmányban említett konkrét rendszerek a védjegyet birtokló cég tulajdonában vannak, a példák csak az adott témakör szemléltetésére szolgálnak, azokból általános következtetéseket nem érdemes levonni.

A mellékelt CD csak egy példányban készült a tanulmányban használt fontosabb hivatkozások archiválására. A CD nem másolható, és tartalma nem tehető nyilvánossá, csak a tanulmányt olvasó használhatja segítségként, amennyiben az anyagban előforduló fontosabb hivatkozások nem lennének elérhetők a megadott címen, vagy nincs Internet-kapcsolata.

„Szervezet” CSIRT

alapszabályzat – kézikönyv

2006. május



A szabályzat kidolgozásában és lektorálásában részt vettek: *Becz Tamás, Martos Balázs, Pásztor Szilárd, Rigó Ernő, Tiszai Tamás, Tóth Beatrix*

Tartalomjegyzék

Táblázatok

Ábrák

1 Bevezető

1.1 A dokumentum státusza

Jelen szabályzat célja egyrészt egy elképzelt, a hálózati incidenskezelést feladatának tartó, és e területen tevékenykedő szervezet (továbbiakban: Szervezet) működési alapjainak leírása, másrészt az új belépők megfelelő tájékoztatása a „*miről kell tudni?*” kérdésekben.

A dokumentum felépítése szerint a következő fejezetekből áll:

- Rövidítések, fogalmak: a szabályzatban előforduló rövidítések feloldása,
- CERT-történeti áttekintés, hazai és nemzetközi körkép,
- A Szervezet által nyújtott szolgáltatások: a szolgáltatástípusok osztályozása és a vállalt szolgáltatások csoportosítása,
- Szervezeti struktúra: alá- és fölérendeltségek, felelősségi körök,
- Az infrastruktúra: erőforrások számbavétele, főbb rendszerek ismertetése,
- A napi tevékenység módja: rendszeres teendők részletezése,
- A Szervezet jogai, jogosultságai, kötelességei: a hazai és a nemzetközi lehetőségek az adott jogi keretek között,
- Anyagi feltételek biztosítása: a működés költségeinek biztosítása,
- Kapcsolattartás módjai: a többi Szervezettel való együttműködés és a kommunikáció követelményei,
- Hivatkozások: alapdokumentumok, melyek egyéb, a Szervezet számára kidolgozandó szabályzatoknak is hivatkozási alapja,
- Mellékletek: a szabályzatban hivatkozott és a szabályzathoz képest gyakran változó tartalmú adatlapok, bizonylatok stb. (minőségbiztosítási rendszerben külön nyilvántartási és verziószámmal rendelkező anyagok).

Ezek alapján a szabályzat célja, hogy alapinformációkat foglaljon össze a CERT/CSIRT-ekről egyrészt a működtetésében résztvevők, másrészt a szolgáltatásait igénybevevők számára. Az új belépők (pl. alkalmazottak, szervezetek) számára ez az elsők között elolvasandó dokumentum. A minőségbiztosítás szellemében ez az *alapdokumentum*, melyből indulva a többi dokumentum és bizonylat hivatkozási fája a Szervezetben felépíthető.

1.2 Helyzetkép és felmerült igények

Az informatika térhódításával és az egyre fontosabb rendszerek informatikai alapokra helyezett működésével az informatikai biztonság a mindennapok részévé vált. A felhasználók, a cégek és a mindenkori kormányzat is egyre fokozódó mértékben van kitéve különböző célzott vagy általános támadásoknak, melyek ellen védekezni kell (*megelőzés*), a támadásokat fel kell ismerni (*észlelés*), és a káros hatásokat is kezelni kell (*javítás*).

Miközben szinte mindenki ki lehet téve ugyanannak a veszélynek, a szükséges szaktudás nem várható el mindenkitől. A rendszerek többsége elsődleges feladatát akarja problémamentesen ellátni, és csak ezt a célt szolgálva foglalkozik a biztonsággal, ha tud arra erőforrásokat biztosítani. Sok esetben egy-egy kisebb rendszer csak közbülső lépcsőként szolgál egy nagyobb szervezet támadása során, így a veszélyelhárításban mindenkinek ki kell vennie részét. Ezt az összetett

védelmet egy központi szervezet által lehet hatékonyan megszervezni, koordinálni és a felügyelet alatt álló rendszereket figyelve a közösség biztonságát megfelelő szinten tartani.

E célból jönnek létre a számítógépes vészhelyzetekre reagáló egységek (CERT – Computer Emergency Response Team), illetve más néven a számítógép-biztonsági incidensekre reagáló egységek (CSIRT – Computer Security Incident Response Team). Jelen dokumentáció egy ilyen szervezet működésének alapjait írja le és szabályozza.

1.3 Történeti áttekintés

A CERT-ek jelentőségét az 1980-as évek végén ismerte fel a DARPA (Defense Advanced Research Projects Agency), amikor létrehozta a CERT koordinációs központot (CERT/CC) a Carnegie Mellon egyetem szoftvermérnöki intézetében 1988 novemberében. [CERT_FAQ]

A CERT/CC feladata volt az internetes biztonsági eseményekre történő reagálás, valamint egy olyan modell felállítása, mely alapján több hasonló szervezet jöhet létre. A regionális, technológiai, humán és egyéb tényezők miatt nem lehetséges uniformizált szervezet létrehozása, de a létrehozott szervezetek közötti együttműködés mégis a globális biztonságot szolgálhatja. Mindezen túl azonban tudomásul kell venni, hogy nem létezik olyan szervezet, amely minden támadást ki tud védeni, mindenhez tökéletesen ért és ehhez az erőforrásai is rendelkezésre állnak.

Mára több száz CSIRT jött létre a kereskedelmi, akadémiai, kormányzati vagy katonai szervezetek számára, melyek az internetes biztonsági eseményeket kezelik az alájuk tartozó szervezeten belül, és együttműködnek egymással. A működésnek és az együttműködésnek is megvannak az általános szabályai, melyeket az egyes CSIRT-ek alapszabályzatukban [RFC2350] rögzítenek. Fontos kiemelni, hogy a CSIRT-ek nem helyettesítik az olyan intézményeket, mint a katasztrófavédelem, rendőrség, vagy éppen a hírszerzés, de együttműködhetnek – és a jövőben mind inkább bizonyosan együtt is működnek – ezekkel az egységekkel is. Az együttműködés a hatályos jogszabályok (kiemelendő az adatvédelmi törvény) és a CSIRT szellemisége alapján alkotott saját szabályzat és etikai kódex szerint történik.

A nemzeti vagy kormányzati CSIRT-ek továbbá olyan „ernyőszervezetként” is működhetnek, amelyek országos hatáskörrel fogadják az informatikai biztonságra vonatkozó bejelentéseket, és továbbítják azokat azok felé, akikhez tartozik az eset kivizsgálása vagy a kérdések megválaszolása.

1.4 Más hazai CERT-ek

Jelen időpontban (2005. év vége) három hazai, CERT-feladatokat ellátó szervezetről tehetünk említést, melyek: a Magyar Nemzeti CERT (Hun-CERT), HUNGARNET CERT (NIIF-CSIRT) valamint, a magyar kormányzati CERT (CERT-Hungary). A szervezetek adatait a 10.7 Melléklet tartalmazza.

A *Hun-CERT* felhatalmazással bír az előforduló vagy előfordulással fenyegető mindennemű számítógépes biztonsági események közlésére a hazai Internet szolgáltatók felé. A támogatási szintek annak függvényében változnak, hogy az incidens vagy probléma milyen típusú, mennyire komoly, milyenek az összetevők típusai, mekkora az érintett közösség száma, és milyen erőforrások állnak rendelkezésre az adott időpontban a Hun-CERT számára, miközben minden esetben valamilyen válaszadás egy munkanapon belül megtörténik.

Az *NIIF-CSIRT* alá tartoznak azok az intézmények, melyeknek az NIIF az Internet szolgáltatója (egyetemek, felsőoktatási intézmények, néhány gimnázium, akadémiai kutatóintézetek és non-profit intézmények).

A *CERT Hungary* a kormányzati intézmények szervezete, és a többi – akár később megalakuló – CERT-ek ernyőszervezete.

1.5 A Szervezet

A Szervezet a megalakító intézmény, intézet, stb. szervezete. Feladatait ellátva a Szervezet a következő képet alakítja ki magáról, és elvárja, hogy munkatársai napi tevékenységük során is ezt a képet erősítsék:

(a) **Bizalmas partner:** *az általa kezelt adatok bizalmasságára igényes, és minden esetben védi azok hírnevét, akiknek a biztonsági események kezelése által az érzékeny adataihoz hozzáfér. Vitás esetekben szakértelmére alapozva a tények megállapítása által, a tanulságok levonásával azon munkálkodik, hogy a felek egyességre jussanak.*

(b) **Koordináló központ:** *koordinálja a biztonsági események kezelését, és figyelemmel kíséri az újonnan alakuló CERT feladatokat ellátó szervezetek munkáját is, hogy a hazai vonatkozás vagy érintettség esetében az eljárás hatékonyabb legyen, továbbá a nemzetközi kapcsolatok során szükséges adatszolgáltatások a lehetőségekhez mérten teljes körűek lehessenek.*

(c) **Szakértő központ:** *az események megfigyelése, kezelése, rendszerezése, elemzése folytán megszerzett tapasztalatai alapján a többi CERT, és a felhasználók széles tábora számára megkereséskor lehetőségeihez mérten segítséget nyújt vagy útbaigazít, oktatóanyagokat készít és elérhetővé tesz, cselekvést javasol, szakmai anyagokat előkészít, tervezeteket vagy megoldásokat véleményez olyan tevékenységek esetében, melyek az informatikai biztonságot érintik.*

1.5.1 Alapinformációk

Az általánosan elfogadott ajánlások szerint minden egyes CERT szervezet megalakulása előtt megfogalmazza céljait, küldetését, meghatározza az általa képviseltek körét, a szervezeti felépítést, erőforrásait és a támogatási forrásokat. Mindez a Szervezet esetében így néz ki:

(a) ***Képviseltek köre*** *(constituency)*: kiknek nyújt támogatást?

- A Szervezet elsősorban az alapító szervek és a kapcsolódó intézményeknek nyújt szolgáltatást. A teljes lista a 10.1 Mellékletben (A képviseltek köre) található.
- Ezen kívül a Szervezet együttműködve a többi hazai és külföldi CERT egységgel és a többi érintett szervezettel (magán, állami, akadémiai) a hozzá fordulókat a megfelelő szervezethez irányítja.
- Amennyiben valamilyen oknál fogva az adott bejelentés nem tartozik egyik szervezethez sem (pl. üzleti vonatkozás, amit a piaci szereplőkkel kell megoldani), vagy nem deríthető ki egyértelműen, hogy kihez továbbítható a bejelentés (pl. az adott országban nem működik ismert szervezet), úgy ezekben az esetekben sem szabad a bejelentést válasz nélkül hagyni. Üzleti érdekek sérelmét elkerülve ajánlhatók olyan keresőprogramok vagy adatbázisok, amelyekből tájékoztatás szerezhető. Ismert képviselet hiányában az adott ország diplomáciai képviseletén is lehet jelezni a bejelentés kivizsgálását, és kérni a megfelelő cél felé történő továbbítást. E példából is látható, hogy széleskörű együttműködésre van szükség (jelen esetben a Külügyminisztériummal), amely a Szervezet feladata, illetve vállalása.

(b) ***Küldetés*** *(mission)*: mi a szervezet küldetése?

- Az információs társadalom biztonságos fejlődésének érdekében az informatikai támadásokat megelőző, észlelő és javító eljárások alkalmazásával segíteni a társadalom számára létfontosságú intézmények biztonságát és az alapító intézmények munkája során előforduló informatikai fenyegetettségek kezelését.

- Együttműködni mindazokkal, akik Magyarország területén közvetett vagy közvetlen módon szintén ezen tevékenykednek, és útbaigazítani mindazokat, akik nem találják a problémáik kezelésére leginkább hivatott szervet.
- Hatással lenni a társadalom informatikai biztonság iránti hozzáállására és képzettségére, ezen belül külön odafigyeléssel a jövő informatikai szakembereire.
- A működés során szerzett és értékelt tapasztalatok során leszűrt következtetésekkel segíteni a magyarországi törvényhozókat – illetve alacsonyabb szintű döntéshozókat – annak érdekében, hogy azok munkájuk során a nemzeti szabályozást úgy alakíthassák, hogy az harmonikusan illeszkedjék a felmerülő igényekhez és nemzetközi elvárásokhoz.

(c) ***Szolgáltatások*** *(services)*: milyen típusú CERT lesz? (részletesebben ld. a 2. fejezetben)

- Az alapító intézmények informatikai hálózati rendszereinek biztonságot érintő eseményeinek monitorozása.
- Az alapító intézményektől érkező események fogadása, feldolgozása, rendszerezése.
- A begyűjtött események kezelése (megelőző, észlelő, javító intézkedések).
- A szükséges nem informatikai lépések megtétele.
- Tájékoztató, oktató, segítő információs bázis üzemeltetése (pl. segédanyagok közzététele, oktatásban való részvétel, hírlevél).
- Elemző munkák végrehajtása, a várható trendek, a régió sajátosságainak elemzése.

(d) ***Szervezeti felépítés*** *(organizational structure)*: melyek a strukturális összefüggések? (részletesebben ld. 3. fejezetben)

- A Szervezet az ISO minőségbiztosítási rendszerrel összhangban alkalmazza a szervezetet alkotókra vonatkozó szabályokat (csak beosztásokat fogalmaz meg, az egyes beosztásokat betöltő tényleges személyek adatait ld. a 10.9 Mellékletben).
- A munkaköri leírások tartalmazzák a munkakör betöltésének feltételét, és az ezek meglétét igazoló iratok körét. Mindezek a kötelességek és a felügyelő szerepek leírását tartalmazó iratokkal együtt a személyzeti dossziéban találhatók.
- Az új belépővel már a szerződésben/megbízásban közölni kell, hogy kik felett rendelkezik valamilyen szereppel, és kik alá tartozva végzi majdani munkáját.

(e) ***Infrastruktúra*** *(resources)*: mire van szükség a feladat ellátásához? (részletesebben ld. 4. fejezetben)

- Alapvető infrastruktúra elemek (épület, informatikai és telekommunikációs vonalak és eszközök).
- Számítástechnikai eszközök (gépek, nyomtatók) olyan összetételben, hogy a felmerülő bejelentéseket minél megfelelőbb környezetben lehessen vizsgálni (pl. többféle operációs rendszer egy-egy futó verziója legyen elérhető).
- Speciális elemek (pl. informatikai biztonsági eseményekre vonatkozó adatok beszerzését támogató eszközök, intelligens kártyák, biometrikus azonosítást végző eszközök stb.).

(f) ***Támogatás*** *(funding)*: milyen anyagi forrásokból gazdálkodik a szervezet? (részletesebben ld. 7. fejezetben)

- A Szervezet megalakulását és működésének megkezdését az alapító intézmény biztosítja/biztosította.

– A hosszú távú működés és ennek forrásai az indulást követő évben kerül pontos meghatározásra egy külön dokumentumban. Ezzel kapcsolatosan az már megállapítható, hogy – tekintettel az intézményi hatáskörre – a működés anyagi feltételeinek biztosítása intézményi források felhasználását indokolja.

2 A Szervezet által nyújtott szolgáltatások

A szolgáltatások jelenlegi és majdani körének egyértelmű meghatározása érdekében olyan csoportosítást célszerű alkalmazni, amelyben – egyértelmű azonosítók felhasználásával – a különféle tevékenységek besorolhatók. Az egyes szolgáltatásokhoz kidolgozandó eljárások, utasítások és egyéb dokumentumok erre az azonosítóra hivatkozva teszik egyszerűbbé a belső kommunikációt és a szolgáltatások karbantartását.

2.1 Osztályozás

A szolgáltatások három fő csoportba sorolhatók: így *reaktív*, *proaktív* és *minőség-menedzsment* csoportba tartozó szolgáltatásokról beszélünk:

(a) **Reaktív:** *ezek az alapvető szolgáltatások. A bejelentett eseményekre indított eljárások (ticket), a behatolás-érzékelők által jelzett események, a naplókból kiderülő támadásra utaló jelek vagy éppen egy széles körben terjedőben lévő kártékony kód alapján történő reagálások képezik e csoport alapját.*

(b) **Proaktív:** *segítő, oktató és útbaigazító szolgáltatások. Magukba foglalják a felkészülés és a védekezés körébe tartozó intézkedésekben történő segítségnyújtást. E szolgáltatások közvetve csökkenthetik az események számát és/vagy súlyosságát a felhasználók jobb képzettsége által.*

(c) **Minőség-menedzsment:** *a rendszer működésének javítására szolgáló szolgáltatások. Ezek a szolgáltatások függetlenek az incidenskezelés és a hagyományos informatikai, ellenőrzési vagy oktatási egységek tevékenységétől. Ha egy CSIRT felvállalja ezt a szolgáltatás-csoportot is, akkor az általános biztonság növelésében tud szerepet vállalni. A kockázatelemzés, fenyegetettség-vizsgálat, vagy a gyenge pontok feltérképezése említhető ebben a csoportban. Ezek általában proaktív szolgáltatások, de közvetett módon hatnak az események számának/súlyosságának csökkenésére is.*

Reaktív	Proaktív	Minőség-menedzsment
Jelzések és figyelmeztetések Incidenskezelés: Incidenselemzés, Helyszíni válaszadás, Válaszadás segítség, Válaszadás koordináció. Sérülékenység kezelés: Elemzés, Válaszadás, Válaszadás koordináció. Kártékony informatikai termékek (vírusok, kódok, fájlok, objektumok stb.) kezelése: Elemzés, Válaszadás, Válaszadás koordináció.	Értesítések Technológiafigyelés Biztonsági audit és értékelés Biztonsági eszközök fejlesztése Biztonsági eszközök, alkalmazások és infrastruktúrák konfigurációja és karbantartása. Behatolás figyelő szolgáltatás A biztonsággal kapcsolatos információk terjesztése	Kockázatelemzés Üzletmenet-folytonossági és katasztrófaterv Biztonsági tanácsadás Biztonsági tudatosság építése és növelése Oktatás és gyakoroltatás Termékek értékelése és/vagy tanúsítása

Táblázat 1. Szolgáltatások csoportosítása és besorolása

Az egyes szolgáltatásokhoz külön utasítások érhetők el a napi munkavégzés pontos leírására és előírására (ld. még 5 fejezetben).

2.1.1 Reaktív szolgáltatások

A Szervezet e csoportba sorolható szolgáltatásai a következők:

1. **Jelzések és figyelmeztetések:** olyan információk elterjesztését jelenti a védett szervezetek felé, amelyekben a Szervezet leír egy biztonsági problémát, és egyben megoldási javaslatot ad.
2. **Incidenskezelés:** a Szervezet megkapja, értékeli, elemzi és választ ad a jelentett incidensekre a védett szervezetek számára. A válaszadás a következő lépéseket foglalhatja magában:
   - A behatoló aktivitása által érintett, illetve fenyegetett rendszer, vagy hálózat védelme érdekében való beavatkozás,
   - Megoldások biztosítása, vagy stratégia kidolgozása a releváns figyelmeztetések függvényében,
   - Behatolók aktivitásának keresése és figyelése a hálózat más szegmenseiben,
   - Hálózati forgalom figyelése és szűrése,
   - Rendszerek újraépítése,
   - Rendszerek aktualizálása (patch-elése) és javítása,
   - Egyéb válaszok és módszerek kidolgozása.
3. **Incidenselemzés:** megvizsgálják a jelentett incidenst, vagy eseményt a rendelkezésre álló információk és támogató bizonyítékok alapján. Cél, hogy azonosítsák az incidens célpontját, a várható, vagy okozott kár nagyságát, az incidens természetét, és meghatározzák a megfelelő válaszadási stratégiát, vagy módszert. A Szervezet a kapott eredményeket felhasználja, hogy megértse, és biztosítani tudja a teljes és naprakész elemzéseket az érintett rendszerekről. Az elemzéseket a Szervezet felhasználja a támadás- és fenyegetettség-trendek előrejelzésére, illetve statisztikák készítésére. A szolgáltatás magában foglalhat két kiegészítő szolgáltatást is:
   - *Igazságügyi szakértés és bizonyítékgyűjtés*: olyan adatokat (rendszernaplók, behatolás-figyelő rendszer naplók stb.) gyűjt be a Szervezet, amelyek segítségével rekonstruálható az incidens menete, illetve megállapítható a behatoló kiléte.
   - *Nyomkövetés és bemérés*: a Szervezet megállapítja a támadó származási helyét, illetve azonosítja a támadás során felhasznált rendszereket. A bemérés során a Szervezet igyekszik azonosítani a támadó tényleges helyét és személyét is.

   Ezek a kiegészítő szolgáltatások szoros együttműködést igényelnek a belügyi szervekkel, az ügyészséggel, az Internet szolgáltatókkal, illetve egyéb érintett szervezetekkel is.
4. **Helyszíni válaszadás:** A Szervezet incidens esetén helyszíni segítséget nyújt a védett szervezetek számára a rendszereik visszaállításához. A Szervezet szakértői kiszállnak a helyszínre, és elemzik az eseményt az érintett rendszeren, majd segítséget adnak a helyi szakembereknek a helyreállításban.
5. **Válaszadás segítség:** A Szervezet incidens esetén segítséget nyújt a védett szervezetek számára a rendszereik visszaállításához telefonon, faxon, e-mailen vagy dokumentáció segítségével. A Szervezet továbbá technikai segítséget nyújt az adatok gyűjtésében, szakértőket nevez meg a témában, illetve helyreállítási stratégiákkal és leírásokkal látja el az érintett szervezetet.
6. **Válaszadás koordináció:** a Szervezet koordinálja azokat a szervezeteket, akiknek a válaszadásban, vagy az incidensben szerepük van (leggyakrabban az incidens áldozatai, a

támadásba bevont más site-ok, vagy szervezetek, illetve az elemzésbe és válaszadásba bevont szervezetek). A koordináció magába foglalja az áldozat szervezet informatikai támogatását ellátó szervezetet, az Internet szolgáltatóját, más CERT, vagy CSIRT szervezetet, illetve a hálózati és rendszer adminisztrátorokat. A koordináció feltétele, hogy a Szervezet rendelkezésére álljanak mindazok a kapcsolattartási információk, amelyek az érintett szervezethez kapcsolódnak (pl. 10.1 melléklet). A Szervezet a koordináció során statisztikai céllal információt gyűjt az incidensről.

7. **Sérülékenység kezelés:** a Szervezet információkat és jelentéseket kap a hardver és szoftver sérülékenységekről, elemzi e sérülékenységek természetét, mechanizmusát és hatásait. Megoldási stratégiákat fejleszt a sérülékenységek észlelésére és javítására. A sérülékenység kezelési szolgáltatásokat három csoportba sorolhatjuk:
   - *Elemzés*: a Szervezet technikai analízist és vizsgálatot végez a hardver és szoftver elemeken a sérülékenység szempontjából (a már ismert sérülékenységek vizsgálata, illetve az új sérülékenységek esetén annak vizsgálata, hogy a sérülékenység hol helyezkedik el, illetve hogyan lehet kihasználni). Az analízis kiterjed a rendelkezésre-álló forráskódok átvizsgálására „debugger" program[1] segítségével, illetve a sérülékenység teszt környezetben való reprodukciójára is.
   - *Válaszadás*: a Szervezet meghatározza a megfelelő válaszadást, hogy megelőzze, vagy javítsa az adott sérülékenységet. E szolgáltatás keretében a Szervezet kifejleszthet, vagy átvehet patch-eket, javításokat és metodológiákat, illetve figyelmezteti a védett szervezeteket és a többi CERT szervezetet a megelőző stratégiáról úgy, hogy figyelmeztetést bocsát ki. A szolgáltatás keretében a Szervezet szakemberei a helyszínen is elvégezhetik a szükséges patch-ek és javítások telepítését.
   - *Válaszadás koordináció*: a Szervezet értesíti az összes védett szervezetet a sérülékenységről és megosztja velük a javítási, illetve megelőzési javaslatait. A Szervezetnek meg kell győződnie arról, hogy a védett szervezetek sikeresen alkalmazták a szükséges intézkedéseket, és fel kell vennie a kapcsolatot a szoftver és hardver szállítókkal, más CERT szervezetekkel, technikai szakértőkkel, illetve minden érintettel, akik a mielőbbi sikeres megoldásban közreműködhetnek. Mindezek a kapcsolatfelvételek megkönnyítik a sérülékenységek felfedezését, és a sérülékenységi jelentések kibocsátását. A Szervezet koordinálhatja a különböző oldalakról érkező dokumentumok, patch-ek, javítások és metodológiák szinkronizálását valamint kibocsátását. A koordináció egyik fontos eleme, hogy a Szervezet minden esetben archiválja, és tudásbázisába beépítse a sérülékenységi és javítási információkat, illetve stratégiákat.
8. **Kártékony informatikai termékek kezelése:** Ilyenek mindazok a fájlok, objektumok és kódok, amelyek nagy valószínűséggel az informatikai rendszerek, illetve hálózatok elleni próbálkozások, vagy támadások segédeszközei, illetve maradványai. Ezek lehetnek többek közt vírusok, trójai programok, férgek, sebezhetőséget kiaknázó script-ek és segédeszközök lehetnek. A Szervezet információkat és másolatokat kap ezekről a kártékony informatikai termékekről, majd átvizsgálja őket. A vizsgálat során elemzi természetüket, mechanizmusukat, verziójukat és használatuk módját, majd válaszadási stratégiát fejleszt ki észlelésükre, eltávolításukra és az ellenük való védekezésre. A szolgáltatást három részre oszthatjuk:
   - *Elemzés*: a Szervezet technikai vizsgálatot és elemzést végez a kártékony informatikai terméken, melynek során azonosítja a termék típusát és struktúráját, összehasonlítja a

[1] Egyes licenc-szerződések ezt tiltják, így erre figyelemmel kell lenni.

már regisztrált termékekkel, hogy megállapítsa a hasonlóságokat és a különbözőségeket, illetve visszafejti a kódot, hogy megállapítsa a termék célját és funkcióját.

– *Válaszadás*: a Szervezet meghatározza a megfelelő lépéseket, hogy azonosítsák és eltávolítsák a kártékony informatikai termékeket a rendszerekről, illetve lépéseket tesz a termékek informatikai rendszerekbe való bejutása ellen.

– *Válaszadási koordináció*: a Szervezet egységesíti és megosztja a különböző forrásból származó technikai és egyéb vizsgálatok és elemzések eredményeit, illetve a válaszadási stratégiákat a védett szervezetekkel, a többi kutatóval, a CERT szervezetekkel, a szállítókkal és a többi biztonsági szakemberrel. A Szervezet mindezek mellett archiválja, és tudásbázisában rögzíti a termékek hatásait, illetve a megfelelő válaszadási stratégiákat.

2.1.2 Proaktív szolgáltatások

A Szervezet e csoportba sorolható szolgáltatásai a következők:

1. **Értesítések:** Az értesítések – többek között – magukba foglalják a behatolási figyelmeztetéseket, sérülékenység figyelmeztetéseket és biztonsági tanácsokat. Az értesítéseken keresztül a Szervezet informálja a védett szervezeteket a közép és hosszú távú hatással bíró új fenyegetésekről, úgymint az újonnan észlelt sérülékenységekről és behatoló eszközökről. Az értesítések segítségével a védett szervezetek felkészülhetnek, hogy megvédjék rendszereiket és hálózatukat az új kártékony informatikai termékektől, mielőtt azokat bárki alkalmazná ellenük.
2. **Technológiafigyelés:** a Szervezet figyelemmel kíséri az új technikai fejlesztéseket, behatoló aktivitásokat és kapcsolódó trendeket, hogy meghatározhassa a jövőbeni fenyegetettségeket. A figyelés kiterjedhet jogi és törvényi szabályozásokra, szociális és politikai fenyegetettségekre, illetve a veszélyes technológiákra is. A Szervezet a tevékenység során folyamatosan figyeli a biztonsággal foglalkozó levelezési listákat és Internet helyeket, az aktuális híreket, illetve tudományos, technológiai, politikai és kormányzati újságcikkeket, hogy összegyűjtse a védett szervezetek számára fontos, biztonsággal kapcsolatos információkat. Az információgyűjtés során a Szervezet folyamatosan kommunikál a megfelelő szervekkel, hogy mindig ellenőrzött és korrekt információk birtokába jusson. A szolgáltatás végterméke értesítés, javaslat, illetve összefoglaló lehet, amely közép és hosszú távú biztonsággal kapcsolatos problémákra fókuszál.
3. **Biztonsági audit és értékelés:** a Szervezet részletes átvilágítást és elemzést végez a védett szervezetek biztonságáról. Az átvilágítás alapja lehet a szervezet biztonsági szabályozása, illetve egyéb biztonsági szabványok (pl. MSZ EN ISO 17799). Különböző típusú biztonsági átvilágítások és értékelések lehetségesek:
   – *Infrastruktúra átvilágítás*: manuálisan áttekintik a hardver és szoftver konfigurációkat, útválasztókat, tűzfalakat, szervereket és asztali számítógépeket, annak érdekében, hogy megállapítsák, mennyire felelnek meg a szervezet biztonsági előírásainak, illetve egyéb biztonsági szabványoknak.
   – *„Best practice" átvilágítás*: az alkalmazottakkal, valamint a rendszer és hálózati adminisztrátorokkal készített interjúk alapján megállapítják, hogy mennyire felelnek meg a követett gyakorlatok a szervezet biztonsági szabályozásának, illetve a biztonsági szabványoknak.
   – *Tesztelés*: sérülékenység-, illetve víruskereső szoftver segítségével megvizsgálják, mely rendszerek sérülékenyek, illetve fertőzöttek.

   – *„Attack and Penetration" tesztelés*: automatikus tesztelő szoftver segítségével megvizsgálják a szervezet hálózatának támadhatóságát.

   Mindezekhez a vizsgálatokhoz az adott szervezet felső vezetésének jóváhagyása szükséges, mert egyes vizsgálati metódusok sérthetik a szervezet biztonsági politikáját. Ezt a szolgáltatást a Szervezet kiadhatja, megfelelő képesítésekkel és garanciákkal rendelkező, külső szervezet számára is.
4. **Biztonsági eszközök, alkalmazások és infrastruktúrák konfigurációja és karbantartása:** a Szervezet meghatározza, vagy megfelelő segítséget nyújt ahhoz, hogy hogyan konfigurálhatók és üzemeltethetők biztonságosan egyes eszközök, alkalmazások, illetve az informatikai rendszerek általában, a védett szervezeteknél, vagy magánál a Szervezetnél. A Szervezet megadja a konfigurációs és üzemeltetési változásokat a biztonsági eszközök és szolgáltatások tekintetében, mint a behatolás-észlelő szoftverek, a hálózat tesztelő és monitorozó szoftverek, szűrők, tűzfalak, VPN-ek és az azonosító mechanizmusok.
5. **Biztonsági eszközök fejlesztése:** a Szervezet fejlesztheti új, a védett szervezetekre specifikált biztonsági eszközöket és szoftvereket is. Mindezek a fejlesztések kiterjedhetnek olyan biztonsági script-ekre és program komponensekre is, amelyek kiterjesztik, illetve növelik a védett szervezetek biztonsági szintjét.
6. **Behatolás figyelő szolgáltatás:** a Szervezet átvizsgálja a védett szervezetnél üzemelő behatolás észlelő szoftver napló állományát, és kidolgozhat olyan új szabályokat és reakciókat, amelyeket a feltárt támadások ellen a leghatékonyabbnak gondol. A folyamat során értékeli a meglévő érzékelők működésének megfelelőségét, és új érzékelőket építhet be, ha erre szükség van.
7. **A biztonsággal kapcsolatos információk terjesztése:** a Szervezet ezzel a szolgáltatással a védett szervezetek számára nyújt olyan átfogó, hasznos és könnyen kezelhető információkat, amelyek segítségével növelhető a biztonság a szervezeteknél. Ezek az információk kiterjednek:
   – A CERT kapcsolati-információira,
   – A jelzések, figyelmeztetések és értesítések archívumára,
   – Az aktuális „best practice" dokumentációra,
   – Az általános informatikai biztonsági segédletekre,
   – A szabályozásokra, szabványokra és ellenőrző listákra,
   – A patch fejlesztésekre és terjesztési információkra,
   – A szállítói linkekre,
   – Az incidensekkel kapcsolatos aktuális statisztikákra és trendekre,
   – Az egyéb biztonságot növelő információkra.

2.1.3 Minőségmenedzsment szolgáltatások

A Szervezet e csoportba sorolható szolgáltatásai a következők:

1. **Kockázatelemzés:** a Szervezet a védett szervezetek számára értékes információkkal szolgálhat a kockázatelemzésük elvégzése során, azaz segíthet reálisan értékelni a szervezeteket érintő tényleges informatikai kockázatokat. A kockázatok értékelése mellett a Szervezet megadhatja a kockázatkezelési módszereket és stratégiákat is.

2. **Üzletmenet-folytonossági és katasztrófaterv:** a Szervezet a védett szervezetek számára értékes információkkal szolgálhat üzletmenet-folytonossági, illetve katasztrófaterveik elkészítéséhez. Ideális esetben a Szervezet maga is része a védett szervezetek katasztrófa terveinek, mint értesítendő, illetve beavatkozó szervezet.
3. **Biztonsági tanácsadás:** a Szervezet segít a védett szervezeteknek növelni a biztonsági szintjüket a biztonsági tanácsadás szolgáltatás során, amely magában foglalja a biztonsági és egyéb szabályzataik értékelését, új szoftver, illetve hardver elemek biztonságos konfigurálását.
4. **Biztonsági tudatosság építése és növelése:** a Szervezet képes meghatározni azokat a területeket a védett szervezet üzemelési rendjében, ahol a biztonsági tudatosságot ki kell alakítani, illetve fejleszteni kell. Mindezek segítségével elérhető, hogy a védett szervezetek alkalmazottai megértsék a biztonság szükségességét, ezáltal a napi operatív tevékenységet kevesebb kockázattal fogják végrehajtani. A Szervezet által közreadott cikkek, kiadványok és egyéb információs anyagok fejlesztik a védett szervezeten kívüliek biztonsági tudatosságát is.
5. **Oktatás és gyakoroltatás:** szemináriumokon, tanfolyamokon, illetve kiadványokon keresztül a Szervezet oktató tevékenységet is folytat, hogy megismertesse a védett szervezetek munkatársait, saját munkatársait, illetve minden érdeklődő felet a biztonsági problémákkal, illetve a védekezés lehetőségeivel és módszereivel. Az oktatott témák többek között:
   - Incidensek jelentése,
   - Megfelelő válaszadási metódusok,
   - Válaszadási stratégiák és eszközök,
   - Védelmi stratégiák és eszközök,
   - Egyéb olyan információk, amelyek segítik a megelőzést, a felfedezést, a válaszadást és a védelmet.
6. **Termékek értékelése és/vagy tanúsítása:** a Szervezet, a szállítókkal együttműködve, biztonsági szempontból értékeli a szoftvereket, hardvereket és szolgáltatásokat, ezáltal elősegítve a védett szervezeteket a megfelelő eszközök és szolgáltatások kiválasztásában. A Szervezet, a megfelelő jogosítványok megszerzése után akár tanúsíthatja is mindezeket.

2.2 Jelentések, statisztikák

A munka hatékonyságát és a terhelést felmérendő, rendszeres időközönként statisztikákat kell készíteni a bejelentett és tudomásra jutott biztonsági eseményekről.

Az incidensek kezelésére szolgáló eszköz – az RTIR, Request Tracker for Incident Response – segítségével lehetőség nyílik különböző, a jegyek adatain alapuló statisztikák készítésére. A különféle statisztikák részletes listája az 4.4.5 fejezet végén található. Az adatok elemzésének célja, hogy felmérje a szervezet munkájának hatékonyságát, ill. segítsen feltárni a hibákat és a szűk keresztmetszeteket. Az adatok elemzésével különböző tendenciák is megfigyelhetők, amelyek szintén segítenek a szervezet működésének javításában. Különösen a következő értékek változását érdemes figyelni:

- Jegyek létrejötte, és megoldása/válasz küldése között eltelt idő. Ezen adatok segítségével felmérhető a szervezet terheltsége.
- A kiugró megoldási idejű jegyekből a komoly problémák természetére lehet következtetni.

- A jegyek típusonkénti megoszlásának vizsgálatával meg lehet határozni, hogy milyen szakemberek bevonására milyen gyakran van szükség.
- Az újra megnyitott jegyek száma és az elvégzett munka alapossága között is lehet összefüggéseket találni.
- Hosszútávon a bejelentések számának növekedéséből a szervezet fejlődésének ütemére, külső megítélésére lehet következtetni (ha csökken, akkor valami nem jó).
- A bejelentések rövidtávú ingadozását, és annak esetleges ciklikusságát is érdemes nyomon követni.

2.3 Témacsoportok

A Szervezet munkatársai általánosan magas szinten értenek az informatikai biztonsági kérdések megoldásához (horizontális tudás), de szükség van egy-egy területen speciális szaktudásra (vertikális tudás). A Szervezeten belül nem megoldható esetekben külső szakértők és szakemberek kerülnek alkalmazásra (ld. 10.10 melléklet).

A témacsoportok a védett intézményekben előforduló rendszerektől függően alakulnak. Az informatikai biztonsági problémák általánosak, mégis egyes operációs rendszereket vagy alkalmazásokat jobban kell védeni, vagy több támadás éri, mint egy másikat. A különböző sebezhetőségeket rendszerező internetes katalógusokban is lemérhető, hogy melyek a támadásoknak jobban vagy kevésbé kitett rendszerek.

Az operátorok között lenniük kell a Linux és Windows rendszerekhez vertikális tudással értő embereknek is. Hasonló módon lennie kell vírusokhoz, útválasztókhoz, Web-szerverekhez stb. értő ember(ek)nek is. A pontos lista a felügyeltek infrastruktúráján múlik.

Új rendszer felmerülése esetén (pl. intelligens kártya elterjedése a Kormányzatban) fel kell mérni a várható esetek számát, és a szerint biztosítani hozzáértő alkalmazottat vagy szakértőt (bővítve a mellékletbeli listát).

2.4 Kapcsolódó területek, egyéb szolgáltatások

Az éles működés közben kiderülhet, hogy nagyobb számban érkeznek olyan megkeresések, melyek e szabályzat írásának időpontjában nem láthatók előre, ezért jelenleg ezeket az eseteket az egyéb szolgáltatások közé kell sorolni. Amennyiben a Szervezet a működési területéről olyan bejelentést kap, amely az aktuális szabályzat szerint nem sorolható be, de hosszú távon tanácsos lenne, úgy ezeket is be kell építeni a szolgáltatások közé. Például, ha az aktuális szabályzat nem rendelkezik a munkaállomásokra kötött chipkártya olvasókat érő támadások kezeléséről, de pár éven belül ezek az eszközök megjelennek a szolgáltatási körbe tartozó intézményeknél, és egyre több bejelentés érkezik ezekkel kapcsolatban, akkor ki kell egészíteni az érintett szabályzatokat (pl. digitális aláírás használata, jelszó/PIN használat, kártyák fizikai tárolási szabályai stb.).

A jelenleg közvetlenül kapcsolódó területek, és a figyelembeveendők rövid listája:

- *Mentés és archiválás*: a mentések védelme több szempontból is fontos, mivel visszatöltéskor azok lesznek az éles adatok, vagy illetéktelen kézbe kerüléskor az adatok bizalmassága közvetlenül, a rendszer sértetlensége pedig közvetve is sérülhet (kikövetkeztethető beállítások, adatok stb. alapján).

  A mentést végezhesse a műszak kijelölt operátora, az ellenőrzést végezhesse egy másik operátor, de a mentett adatokba ne tekinthessenek bele. A tárolás legyen védett helyen (kiemelten fontos mentés esetén – pl. havi teljes mentés – az adathordozókat külső

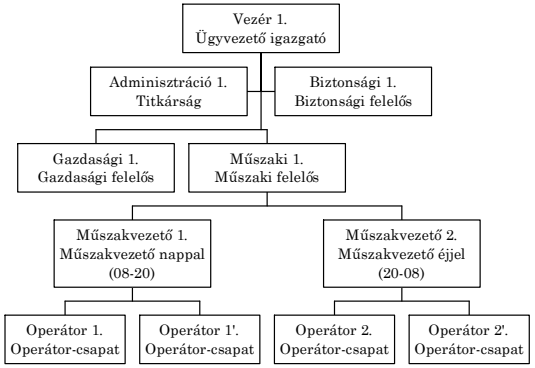
helyszínen kell tartani[2]). Archiválás esetén még foglalkozni kell az archiválási idővel is, majd annak lejártakor a biztonságos és az adatvédelmi szabályoknak megfelelő megsemmisítéssel is.

– *Tartalékrendszer*: akár helyi RAID rendszerről van szó, akár távoli éles tartalékrendszerről (ld. lábjegyzet), gondoskodni kell a tükrözés és a tartalékrendszer felé irányuló információk biztonságáról, és szükség esetén azok használatbavételi módjáról (pl. átállás/átkapcsolás menete).

[2] Az éles rendszerről is lehet folyamatos tükrözés, és ezt is tanácsos megfelelő külső helyszínen üzemeltetni.

3 Szervezeti struktúra

A feladatokból adódóan többféle tudású és beosztású személyre bontható a kívánatos szervezeti struktúra. Minden egyes dolgozó munkaköri leírásában legalább három elemnek szerepelnie kell: munkakör betöltésének feltétele (az igazoló iratok mellékelve a személyzeti dossziéban), felettes valamint beosztott viszonyai és kapcsolatai. Ezek szerint a szervezeti felépítés a következő:



Ábra 1. Általános szervezeti felépítés

3.1 A beosztások rövid leírása

Az ábrán látható beosztások részletesebb magyarázata[3]:

– Vezér 1. (ügyvezető igazgató): a szervezet vezetője, hosszabb vagy rövidebb távolléte esetén a megfelelő kérdésekben a felelősökre delegálhat bizonyos döntési felelősségeket.

– Adminisztráció 1. (titkárság): adminisztratív feladatok ellátása (de nem érintkezik a bizalmas iratok tartalmával).

– Biztonsági 1. (biztonsági felelős): biztonsági kérdésekben előkészít, javasol, ellenőriz, de a döntéseket az igazgató jóváhagyása és aláírása/elrendelése alapján viszi végbe, és neki tartozik jelentési kötelezettséggel, a többieknek csak értesítési kötelezettséggel (pl. operátorral végrehajtatott biztonsági beállításról, belső átvilágítás tervéről, előre be nem jelentett ellenőrzésről stb.).

– Gazdasági 1. (gazdasági felelős): a gazdasági ügyeket intézi, alá tartozhat a titkárság, de a pénzügyekben (pl. munkatársak bére) csak az igazgatónak tartozik jelentési kötelezettséggel.

– Műszaki 1. (műszaki felelős): A műszaki feladatokat igazgatja, közvetlenül a műszakvezető, közvetve pedig az operátorok felettese. Az operátorokat közvetlenül is utasíthatja, de erről a műszakvezetőt is tájékoztatnia kell.

– Műszakvezető 1-2. (műszakvezető éjjel/nappal): A műszaki felelőstől kapott utasítások alapján végzi feladatát az adott műszakban az oda beosztott operátorokkal. Más műszak operátorai felett azok műszakvezetőjén keresztül gyakorolhat felettesi pozíciót.

[3] A Szervezetben dolgoznia kell legalább egy Igazságügyi szakértőnek, aki a nyomozószervekkel tartja a kapcsolatot olyan esetekben, amikor a két szervezetnek szüksége van a másikra.

Műszakvezetők közötti szakmai viták esetén a műszaki felelőssel kötelesek egyeztetni, és a megegyezés vagy utasítás alapján eljárni. Műszakvezető és műszaki felelős szakmai vitájában (szükség esetén a biztonsági felelős véleményének meghallgatásával) az igazgató dönt. A műszakvezetők egyben rendszermérnöki szinten képzettek az informatikai biztonsági kérdésekben, így az operátorok által megoldatlan kérdésekben is el tudnak járni[4].

– Operátor 1-2. (és 1'-2' operátor csapatok): Közvetlenül a műszakvezető, közvetve a műszaki felelős vezetése alatt állva végzi feladatát. Különböző műszakokban történő munkavégzés esetén időszakos felettese az adott műszak vezetője, de állandó felettese a műszaki felelős. A biztonsággal kapcsolatos tevékenységekben a biztonsági felelős utasításait kell végrehajtania, amennyiben azok a szabályzatnak nem mondanak ellent. Ellentmondás esetén a hierarchiát követve a műszakvezető – műszaki felelős – igazgató vonalat követve kell megegyezésre jutni.

  Az 1' és 2' csapatok elképzelhetők közös tartaléknak is, vagy olyan csoportnak, akik éppen továbbképzésen vagy szabadnapon vannak stb., de vészhelyzetben vagy csupán nagyobb terhelés esetén szükség lehet rájuk.

3.2 Szakértők és szakemberek

A szervezetben lévőkön kívül szükség van olyan *szakértőkre* (pl. igazságügyi szakértők, CISA vizsgás auditorok stb.), akik *egy-egy bonyolultabb* esetben segítenek a szakmai munkában. Az eseti szükség miatt ezekkel a szakértőkkel keret-megállapodás alapján folyik a kapcsolattartás akkor, amikor kimondottan rájuk van szükség (pl. bírósági ügy esetében, vagy egy audit módszertana miatt).

A *szakemberek* csoportja olyan egy-egy adott területen speciális és mély tudással rendelkező emberekből áll, akik *egy speciális szaktudást igénylő* ügyben tudják segíteni a Szervezet csapat munkáját. Hosszabb távú együttműködés igényének esetén akár határozott idejű félállású munkatársakká is válhatnak.

Mindkét csoportba tartozó emberekről naprakész listákat (szakterület és névszerinti listákat ld. a 10.10 mellékletben) kell vezetni, hogy szükség esetén minél előbb elérhetők legyenek. Önkéntes bejelentkezési alapon bárki által elérhető internetes adatbázist is fenn lehet tartani, hogy szükség esetén kit lehet megkeresni.

3.2.1 Beérkező feladatok osztályozása

Minden bejelentés a feldolgozás vagy megoldás során elérhet egy olyan pontra, amikor a szervezeten belül az operátori szintnél feljebb kerül, mert ott van meg a megfelelő szaktudás a megoldásra. Ebben az esetben kerülhet sor külső szakértők bevonására is (operátor közvetlenül nem adhatja ki külsősnek számító szakértőnek a bejelentést).

A szakértők elérési adatai (ld. 10.10 melléklet) alapján kereshetők fel a bejelentés adatainak bizalmasságát és sértetlenségét megtartó módon (titkosított formában vagy csatornán szabad közvetíteni az adatokat olyan kiegészítéssel, mely sértetlenségüket is ellenőrizhetővé teszi).

Az adatok mellett szerepelnie kell az elvárt visszajelzési határidőnek, és a kiküldés célba érkezéséről másik csatornán is meg kell győződni (pl. e-mail-ben küldött anyag esetén telefonos rákérdezés). A kiküldés egyidejűleg helyi másolatot is képezzen, hogy a kiküldés ténye és adatai is elérhetők legyenek később.

[4] Nem feltétel a jó kommunikációkészség, ezért a kapcsolattartás ekkor is a szakképzett operátorok által végzendő.

3.2.2 A szakértői adatbázis

A szakértők éves felülvizsgálatra kerülnek, amikor is ellenőrzésre kerül, hogy szakértői jogosítványuk még érvényes-e, és évente egyszer a Szervezet által a szakértőiknek szervezett szakmai szemináriumon kötelesek részt venni.

Új felvétel esetén a szakértőnek igazolnia kell, hogy a megcélzott szakterületen rendelkezik-e a megfelelő tudással és erkölcsi bizonyítványt tud csatolni kérelméhez. A szakmai igazolás lehet más szervezetnél megszerzett szakértői szintű jogosítvány (pl. igazságügyi szakértő, CISA vizsga, bírósági eseti szakértő stb.) vagy olyan meggyőző kérelem, mely alapján a szervezet vezetője a műszaki felelős javaslata alapján dönt az illető szakértői listára történő felvételéről.

A meggyőző kérelem azt jelenti, hogy az illető a terület elismert szakértője egyetemi oktatóként, doktori fokozatot szerzett a területen, publikációs listája alapján vagy eddig végzett munkái okán. A függetlenség elvének őrzése miatt óvatosan kell eljárni a céges elkötelezettségű szakértőkkel és felvételi kérelmükkel. A listára kerülésük nem tiltott, ha az adott szakterületen valóban megfelelő tudással vagy igazolással rendelkeznek, de megkeresésükkor figyelni kell arra, hogy az adott bejelentés és a szakértő elkötelezettsége jelenthet-e összeférhetetlenségi problémát. Egyértelműen nem eldönthető esetben a bejelentéstevőt is be kell vonni, hogy hozzájárul-e a bejelentés adott szakértőhöz való továbbítására. Amennyiben nem, úgy a rendelkezésre álló erőforrásokkal és emberanyaggal kell megoldani a bejelentés kezelését.

A szakértők véleményével a szervezetnek is egyet kell értenie, ha ez alapján jár el a továbbiakban, így a későbbi reklamációkkal kapcsolatban a szervezetnek kell eljárnia, nem vonhatja ki magát a szakértő és a bejelentő közötti kommunikáció átadásával.

Adott szakértő listáról történő levételéről a szervezet saját hatáskörében dönt (szervezeten belül bárki kezdeményezheti, de a műszaki felelős véleménye alapján a szervezet vezetője dönt).

3.3 Belső oktatás

A minőségbiztosítási rendszernek megfelelően rendelkezni kell a munkatársak belső oktatási tervéről (előzetes féléves terv), és ennek részévé kell tenni a szervezeten belül felgyülemlő tapasztalatok megbeszélését és terjesztését az operátorok között. Ezáltal válik lehetségessé a különböző műszakok során szerzett tapasztalatok elterjedése[5] is. Ld. még 5.4.1 T6 pontját.

Az új belépők számára is biztosítani kell oktatást, melynek végeztével tett sikeres vizsga esetén kerülhet az adott operátori munkakörbe a munkatárs. Az év során a szakmai szint és a csapattréning erősítése érdekében játékos helyzetgyakorlatok vagy célfeladatok által motivációs tényezőkkel támogatva külön feladatok kiadása is ajánlott, mely nem a versenyszellemet, hanem az egymáshoz rendelt csapatok szakmai tudását gyarapíthatja[6].

A napi teendők között szerepel a különböző biztonsági eseményeket taglaló hírforrások (elektronikus és papíralapú) áttekintése és kivonatolása. Ezt végezheti a műszak elején kijelölt operátor, de a kijelölés ne essen mindig ugyanarra az operátorra (ajánlatos a hetente történő csere).

3.4 Keresztkontroll

Az esetleges tévedéseket ki lehet deríteni, de a minőségbiztosítás része is az, ha valamilyen keresztkontroll vagy jóváhagyás/megerősítés megoldás kerül alkalmazásra írott anyagok és szakmai tevékenységek esetében.

[5] Biztonsági szempontból alkalmazható a műszakösszetételek szándékos változtatása, így az információáramlás is könnyebb lesz a különböző műszakokban szerzett tapasztalatok tekintetében.
[6] Irányadók a kooperatív tanulási módszertanok, melynek egyik fő eredménye a tudásszintek emelése és felzárkóztatása.

Bárki készítsen olyan írott anyagot, mely kikerül a szervezet honlapjára, másik szervezetbeli személy által ellenőrzésre és elolvasásra kell kerülnie. Az ellenőrzést (pl. adott parancsok helyesek, valóban az történik, ami a leírásban szerepel) végezheti azonos vagy alacsonyabb szinten dolgozó is, de az elolvasás (kvázi bírálat) felettes által kerülhet elvégzésre majd jóváhagyásra. Javítás vagy újabb verzió esetén is ez az eljárás követendő, kiemelve, hogy az előző verzióhoz képest mi került javításra vagy átírásra.

A keresztkontroll „intézménye" része a minőségbiztosítási rendszernek is, ahol a szabályzatok, bizonylatok és minden ügyfeleket érintő tevékenység valamilyen módon ez alá van vonva. A tevékenységeknek van felelőse, végrehajtója és ellenőrzője, jóváhagyója vagy elfogadója.

4 Az infrastruktúra

Jelen esetben közvetlenül az infrastruktúrába tartozónak értjük az informatikai eszközöket, míg közvetetten az informatikai eszközök működéséért felelős eszközök is ide tartoznak, így ezek is említésre kerülnek.

4.1 Informatikai eszközök

A szolgáltatás ellátáshoz megfelelő eszközparkra és terhelésnövekedés vagy vészhelyzet esetén megfelelő módon és időben igénybe vehető tartalékeszközökre van szükség.

Az eszközpark alkotóelemei a szerverek (pl. adatbázis, Web, E-mail), a kliensek (nem homogén rendszer, többféle operációs rendszerrel és alkalmazás-felszereltséggel). Mivel ezek a szerverek érzékeny adatokat kezelnek, ezért fontos minden adatkezelési ponton az adatvédelmi szabályok betartásán túl az ügyfelek tájékoztatása (pl. telefonos bejelentéskor figyelemfelhívás a beszélgetés rögzítéséről, Web-szerveren adatvédelmi nyilatkozat), hogy adataik milyen módon kerülnek kezelésre.

4.2 Informatikai rendszert kiszolgáló eszközök

Az informatika maga is kiszolgáló tevékenységet folytat, de az informatikát is ki kell szolgálni, hogy kiszolgáló tevékenységét elláthassa.

A kiszolgáló eszközök három fő csoportját különböztethetjük meg:

- *Energiaellátás*: szünetmentes tápegységek, tartalék rendszerek, túlfeszültségvédők, egyéb zavartalan ellátást biztosító eszközök.
- *Kommunikáció*: telefon (mobil és vezetékes), fax, személyi hívó, CB-készülék[7], melyeken előnyben kell részesíteni a titkosított kommunikációra képes változatokat.
- *Adatkezelés*: hordozók (papír – ld. dokumentumkezelés, rack, pendrive, CD/DVD – írható, újraírható, ZIP-drive, DAT-kazetta, memóriakártya stb.) és megsemmisítők (különböző hordozók esetén különböznek a megsemmisítők is).

4.2.1 Biztonsági megoldások

Külön kell foglalkozni a biztonsági eszközökkel, mert ezek a kiszolgáló tevékenység mellett a védelmi tevékenységeket is befolyásolják. Nem a „security by obscurity" (titok általi biztonság) elve alapján kell kezelni a biztonsági megoldásokat, azonban megfontoltan kell megállapítani azok körét, akik az adott megoldás részleteit ismerik[8]. Az informatikai biztonsági szabályzatból mindenki számára ki kell derülnie, hogy munkavégzésével kapcsolatosan mire kell figyelemmel lennie, és mit kell betartania.

A kiszolgáló biztonsági megoldásokat a következők szerint csoportosítjuk (néhány példával illusztrálva):

- *fizikai védelem*: a szervezet környezete (épület, megközelíthetőség, valószínű fizikai káresemények, mint árvízveszély vagy éppen tömegdemonstráció közeli helyszínen), belső védelem (elektromágneses és egyéb kisugárzás és lehallgatás elleni árnyékolás és védelem, beléptető rendszer, zónarendszer, iratmegsemmisítők),

[7] Nem biztos, hogy mindegyik forma el is érhető és alkalmazásban van.
[8] A „need to know" elve alapján mindenki annyit tudjon, ami szükséges és elégséges a munkavégzéshez. A hierarchikus elvet (minél magasabban van a céges hierarchiában, annyival több jogosultsága legyen) *kerülni kell*!

– *logikai védelem*: tűzfal és vírusvédelmi megoldások, egyéb biztonsági megoldások (jelszótárolók, titkosított kommunikációt biztosító alkalmazások),

– *adminisztrációs védelem*: biztonsági-, jelszó-, üresíróasztal-politika, iratmegsemmisítés módja.

4.3 Tárolás

Az adattárolás több formában is megvalósulhat, így az infrastruktúrában fontos szerepe van akár élő, akár archivált adatról van szó. Az adattárolás szerteágazó és különleges szabályok alapján fedhető le teljes mértékben, ebben a részben csak az alapelveket rögzítjük.

Az adatkezelésben az adatvédelmi törvény[9] az irányadó, de a szervezet speciális szolgáltatásai és ügyfélköre miatt egyéb jogszabályok is figyelembeveendők (ld. 6 fejezet).

A munka során minden alkalmazott köteles betartani az üresíróasztal-politikát, ami *„egy mélyebb filozófiát takar, nevezetesen azt az elvet, hogy a munka során előkerült és használt információk biztonságáért a munkavégző személy a felelős, és ezt a felelősséget nem hagyhatja figyelmen kívül, amikor – akár csak pár percre – magára hagyja a munkakörnyezetet”*.[10] Ezzel a „betekintés-jellegű” támadások ellen is védekezünk, valamint a rendre nevelés pozitív hatásait is erősítjük. A politika része az eszközök használata is, hiszen egy csak munkahelyen alkalmazandó eszközre (rack-es háttértár, telefon, token, digitális aláírásra alkalmas kártya stb.) is vonatkozik az elv.

Külön kiemelendő a háttértárak tárolása, hiszen a saját munkaállomásban használt külön elzárható háttértárak esetén azok napi felvétele és leadása is csak pontosan szabályozott módon történhet. Ezen túlmenően az ilyen háttértáron lévő telepített rendszerek használata is ebbe a szabályzatba sorolható azzal a különbséggel, hogy ezek a rendszerek nem mindig egyazon felhasználó által kerülnek használatra.

A dokumentumkezelésben a minőségbiztosítási rendszer is segít, így az iktatás, a verziószámok, a dokumentum-kísérőlapok, a kiosztási lista és egyéb elemek a rendszerezettségen túl a biztonság megőrzését is segítik.

A fentebb már említett tokenek, kártyák és egyéb hasonló eszközök esetében (a belépőkártya kivételével) a munkakezdés előtti felvétel és munkavégzés utáni leadás rendszer alkalmazása miatt ezeknek az eszközöknek a tárolása úgy működik, hogy a felvételhez és a leadáshoz szükséges egy felelős aktív részvétele, de a tulajdonos jelenléte nélkül ő sem tudja ezeket az eszközöket magához venni (pl. kétkulcsos láda alkalmazása).

4.4 RTIR – Az incidenskezelő eszköz

Nyilvánvaló, hogy a beérkező bejelentéseket valamilyen rendszerrel kezelni kell, amely bizonyos automatizmusokat vezet be, annak érdekében, hogy a munka elvégzését megkönnyítse azáltal, hogy segít a történések dokumentálásában, a bejelentések osztályozásában, a régebbi adatok keresésében, ill. olyan integrált eszközöket bocsát rendelkezésre, amelyek segítenek a probléma gyors megoldásában.

Ezt a funkcionalitást a Best Practical Solutions által fejlesztett és karbantartott *Request Tracker for Incident Response* (továbbiakban RTIR) szoftver biztosítja. Az RTIR a Request Tracker-re épülő incidenskezelő eszköz, amelyet a JANET CERT-tel együttműködve fejlesztenek[11], kifejezetten a CERT-ek igényeihez igazítva. Mivel a munka nagy része ebben a rendszerben zajlik,

[9] 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról
[10] Forrás: Biztostű portál (`http://www.biztostu.hu`)
[11] JANET = Egyesült Királyság oktatási és kutatói számítógép-hálózata.

szükségszerű felépítésének, működésének, szolgáltatásainak, logikájának ismerete. Ennek a fejezetnek célja ezek számbavétele.

4.4.1 Ismertetés

Az RTIR egy webes felületen, bármilyen modern böngészőből elérhető rendszer. Alapját az un. „jegy” (*ticket*) képezi. Minden jegy egy adott problémához tartozó adatokat, ill. a rendszer által hozzá rendelt egyéb jellemzőket (metadata), – pl. tulajdonos, fontosság – tartalmaz, természetesen az egyes jegyek között különböző kapcsolatok lehetségesek.

A rendszer alapvető működési logikája igen egyszerű:

Ha beérkezik egy bejelentés, akkor az automatikusan rögzítésre kerül, majd emberi beavatkozás segítségével el kell dönteni, hogy a jegyet fel kell-e dolgozni, vagy el kell utasítani. Ha a bejelentésben vázolt problémát meg kell oldani, akkor lehetőség van arra, hogy ezt hozzácsatoljuk egy már létező esethez.

A jegyek fontosabb tulajdonságai az alábbiak:

– *Megfigyelő (watcher)* – Valaki, akinek valamilyen köze van a jegyhez. A következő szerepkörökbe sorolhatjuk őket:
  - Tulajdonos (owner) – Az a személy, aki felelős a jegyért és annak megoldásáért. Minden jegynek csak egy tulajdonosa lehet.
  - Bejelentő (requestor) – Valaki(k), aki(k) kért(ek) valamit; tulajdonképpen a jegy létrehozója.
  - CC – Akik másolatot kapnak a jegyre adott összes válaszról. Nem szükségszerűen van joguk dolgozni a jegyen (pl. A bejelentő osztályvezetője).
  - AdminCC – Olyan CC, aki a megjegyzésekből is kap másolatot, és általában joga van dolgozni a jegyen.
– *Státusz (Status)* A jegy osztályozására szolgál, értéke a következők valamelyike lehet:
  - Új (new) – újonnan létrehozott jegy, amihez még senki nem ért hozzá.
  - Nyitott (open) – a jegyen valaki dolgozik.
  - Várakozó (stalled) – rajtunk kívülálló okok miatt (pl. válaszra várakozás külső féltől) éppen nem történik semmi a jeggyel. Amint valaki frissíti a jegyet, megint nyitottra fog változni az állapota.
  - Megoldott (resolved) – a jegy megoldásra került.
  - Visszautasított (rejected) – a felvetett probléma nem kerül megoldásra (pl. mert nem a mi hatáskörünk), de valami miatt mégis érdemes megtartani a rendszerben. Mondjuk valaki valamilyen képtelenséget kér, a jegyet nem kell megoldani, de az adatbázisban nyoma marad a kérésének.
  - Felhagyott (abandoned) – Olyan jegy, amelyen annak ellenére, hogy nem került megoldásra, nem folyik további munka, vagy, mert a megoldásra irányuló törekvések kudarcba fulladtak, vagy mert előző tulajdonosuk valamilyen oknál fogva nem tudja tovább kezelni.
  - Törölt (deleted) – Olyan jegy, amelynek semmi keresnivalója nincs a rendszerben – pl. spam.

Az RTIR rendszerben a jegyek osztályozására az un. sorok szolgálnak. Minden sor egyfajta gyűjtőhelye az azonos típusú jegyeknek. A rendszerben négy különböző sor található, ezek rendre a következők:

- *Bejelentések (Incident reports)* – Ebbe a sorba kerülnek az új bejelentések. Emberi beavatkozással kell eldönteni, hogy új jegyként átkerüljön-e a problémák közé, hozzá kell csatolni egy már létező problémához, vagy valamilyen módon el kell dobni
- *Problémák (Incidents)* – A megoldásra váró problémák. Minden ilyen jegy tulajdonképpen gyűjtőhelye a hozzá kapcsolódó összes bejelentésnek, blokknak, vizsgálatnak. Ilyen módon tulajdonképpen ezek a jegyek jelentik a rendszer szívét, a másik három sor némiképp alárendelt feladatot játszik, a problémák megoldásában felmerülő feladatok állapotának áttekinthető dokumentálására valók
- *Vizsgálatok (Investigations)* – Ha egy probléma megoldásához vizsgálatra kell felkérnünk külső felet, akkor egy, ebben a sorban létrehozott, az eredeti jegyhez kapcsolódó jegyen keresztül tehetjük meg
- *Blokkok (Blocks)* – Amennyiben egy probléma kapcsán hálózati szabályozásra (pl. hálózat blokkolására) van szükség, a megfelelő jegyek itt kerülnek létrehozásra. Mivel az RTIR feladata az adatok kezelése, nem várható el tőle, hogy egy tetszőleges hálózathatár védelmi rendszert automatikusan tudjon frissíteni, ezért az ebbe a sorba bekerülő jegyeket a sor AdminCC mezőjében megadott hálózatüzemeltetési csoportnak is meg kell kapnia, hiszen az ő feladatuk ezeknek a kéréseknek a végrehajtása.

4.4.2 A jegyek életútja a rendszerben

Az elméleti alapok tisztázása után érdemes megvizsgálni, mi is történik egy jeggyel, amíg a rendszerben tartózkodik. A folyamat könnyebb megértése érdekében az alábbi szöveges ismertetés mellett célszerű az „Ábra 2. Bejelentések kezelésének folyamata” folyamatábrát is tanulmányozni.

Az első lépés egy jegy életében természetesen a keletkezése. Az RTIR rendszerbe alapvetően két úton kerülhetnek új jegyek:

- *E-mailben történő bejelentés*: Amennyiben valaki bejelentést küld a rendszer beállított e-mail címére, a rendszer részét képező un. e-mail gateway automatikusan létrehoz egy jegyet a bejelentések sorban (ill. egy új felhasználót a bejelentőnek, ha még nincs).
- *Egyéb úton történő bejelentés*: Ha a bejelentés telefonon – vagy más úton – történik, akkor azt kézzel kell bevinni a rendszerbe. Akkor is meg kell ezt tenni, ha a probléma már ismert, hiszen:
  - Bejelentés nem hagyható figyelmen kívül.
  - A bejelentő így automatikusan értesülhet a problémával kapcsolatos minden őt is érintő információról

Miután a jegy bekerült a bejelentések közé, „új” állapotban várakozik addig, amíg valaki meg nem vizsgálja. Ekkor először azt kell eldönteni, hogy szükséges-e a jeggyel foglalkozni. Ha nem, mert nem tartozik a szervezet hatáskörébe, spam stb., akkor az indok megjegyzésben (vagy, ha szükséges válaszban) történő megjelölése után el kell utasítani.

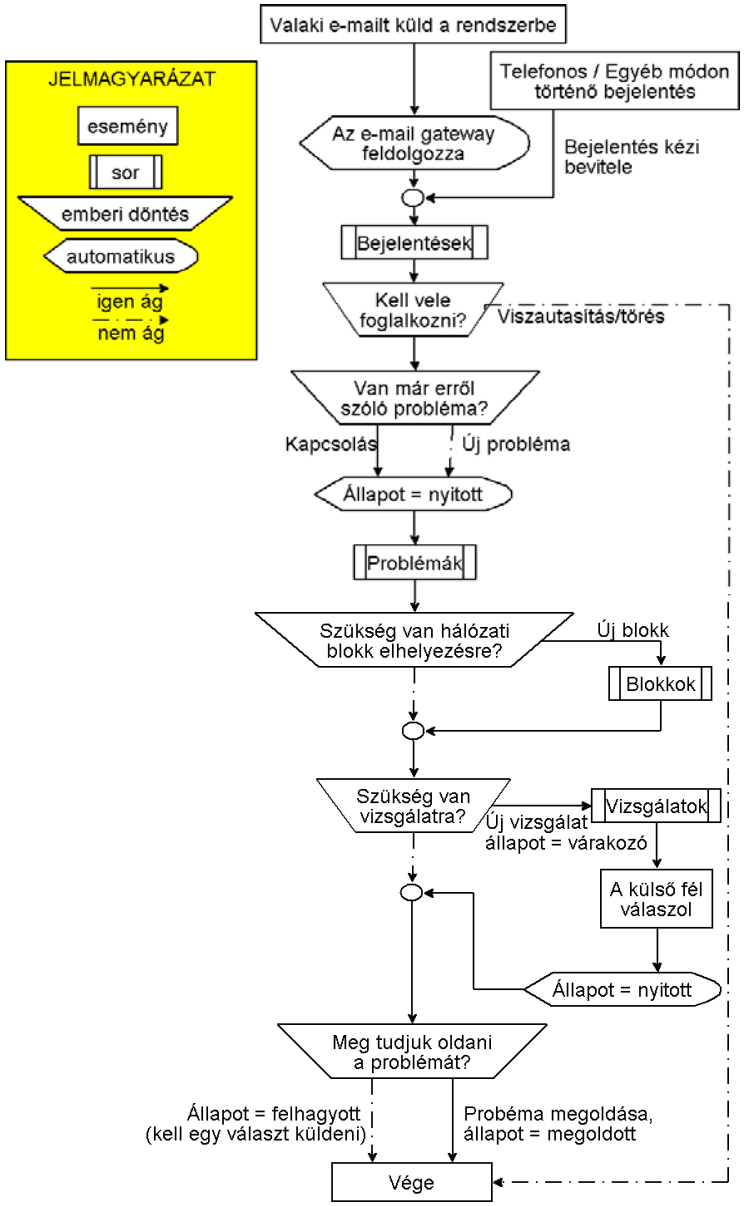
Amennyiben a bejelentést fel kell dolgozni, a következő eldöntendő kérdés, hogy ismert-e már a probléma (esetleg egy már ismertet egészít ki újabb információkkal), vagy sem. Az első esetben hozzá kell csatolni az ismert problémához, az utóbbiban pedig új problémát kell számára létrehozni. (Megjegyzendő, hogy bár lehetőség lenne közvetlenül a bejelentésekkel történő munkára, a

rendszer logikája azt diktálja, hogy így legyenek a jegyek kezelve, mivel ellenkező esetben a rendszerben tárolt adatok átláthatatlanná válnának.)

Innen kezdődik a tulajdonképpeni problémamegoldás, amelynek keretében az első lépés annak eldöntése, hogy a hálózat védelme szempontjából szükséges-e blokkok elhelyezése. Ha igen, akkor az adott problémához kapcsolódóan kell készíteni egy új jegyet a Blokkok között.

Ezután meg kell vizsgálni a problémát, és ha szükséges, külső fél vizsgálatát kell kérni, a Vizsgálatok sorban létrehozott jeggyel. Ekkor a probléma felfüggesztett állapotba kerül, egészen addig, míg válasz nem érkezik a külső féltől.

A problémakezelés végén, a jegyet le kell zárni, vagy a további munkát fel kell adni (ha a probléma megoldása sikertelen volt). Természetesen elképzelhető, hogy egy már lezárt jegyről kiderül: a probléma mégsem oldódott meg. Ilyenkor a jegy újra megnyitható és ismételten végighaladhat a problémamegoldás folyamatán.



Ábra 2. Bejelentések kezelésének folyamata

4.4.3 A rendszer használatának folyamata

Mint látható, egy jegy életútja a rendszerben viszonylag egyszerű, könnyen követhető folyamat, azonban a rendszert használóknak nem csak egy jeggyel kell dolgozniuk, ezért szükséges a rendszer használatakor alkalmazott munkafolyamat áttekintése is. Ehhez az „Ábra 3. A bejelentések kezelésének munkafolyamatai” folyamatábra nyújt segítséget. Természetesen ez az ábra csak egy lehetséges lépéssorozatot mutat be, hiszen a való életben szükség lehet az itt bemutatottól eltérő lépésekre is, ha a helyzet úgy kívánja, ill. az ábra bizonyos pontjaiból adott esetben át lehet ugrani annak egy másik pontjára, azonban ennek ábrázolása már az érthetőség rovására menne, ill. szükségtelen is, hiszen a rendszer logikáját ismerő számára (remélhetőleg) az értelmezés nem jelent problémát.

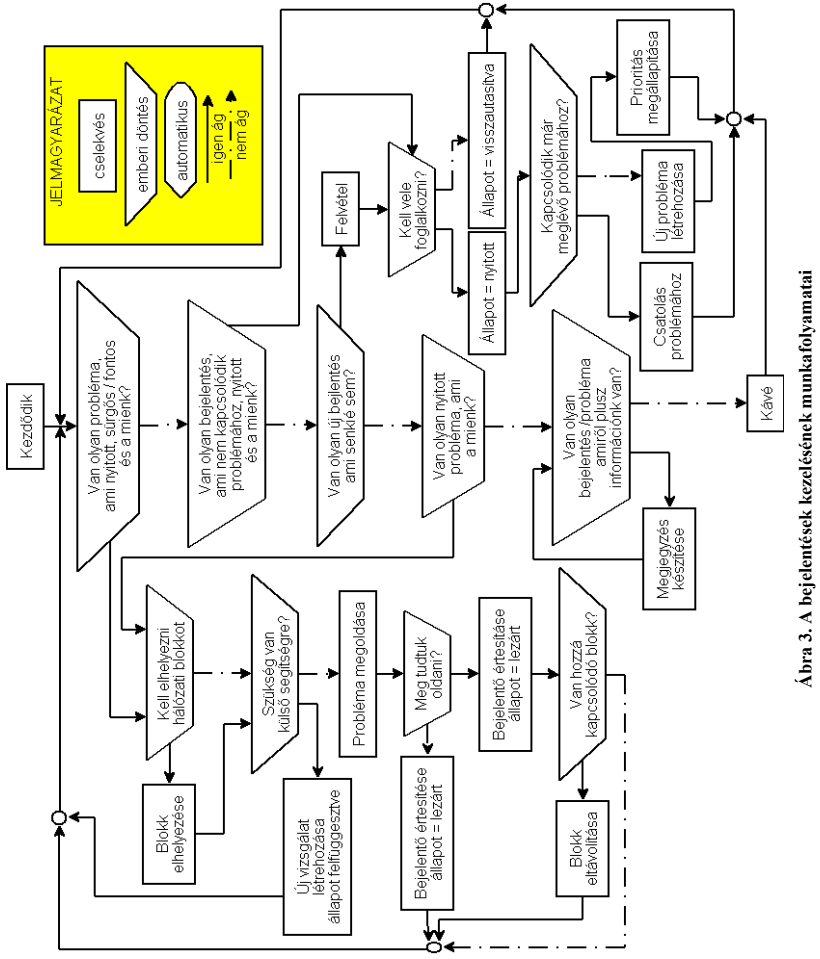
Könnyen felismerhető, hogy a folyamatok szervezésének fő szempontja a munkák sorrendjének meghatározása. A lényeg a fontos esetek mielőbbi megoldása, és a többi problémára történő lehető leggyorsabb reagálás, majd megoldás biztosítása. Ennek megfelelően először, ha ilyenek vannak, azokkal a problémákkal kell foglalkozni, amelyek megoldása a mi felelősségünk, és fontosak, vagy már közelít a határidejük. A problémával foglalkozó részmunkafolyamat (az ábra bal oldala) természetesen szinkronban van a jegy életútját bemutató folyamattal, csak ezúttal az ember, nem pedig a jegy szempontjából került ábrázolásra.

A következő azoknak a bejelentéseknek a vizsgálata, amelyek még senkihez sem rendeltek, ill. valamilyen oknál fogva még nem kerültek besorolásra. Ezekről el kell dönteni, hogy kell-e velük foglalkozni, ha igen, akkor ismert problémához kapcsolódnak-e? Amennyiben igen, úgy hozzá kell csatolni a bejelentéseket ezekhez, ha nem, akkor új problémát kell létrehozni, és meg kell határozni a hozzá tartozó prioritást (bővebben ld. 5.2).

Bár elsőre logikátlannak tűnhet a bejelentések osztályozásának előre vétele a problémamegoldásokkal szemben, azonban ez biztosítja, hogy a problémákkal kapcsolatos összes információ a lehető leggyorsabban bekerüljön a rendszerbe, egyrészt a pótlólagos információval megkönnyítve a megoldást, másrészt segít abban, hogy egy esettel lehetőleg csak egyszer kelljen foglalkozni.

A bejelentések osztályozása után a saját problémák vizsgálata következik, a már megismert irányelvek alapján.

Amennyiben sem kezeletlen bejelentés, sem foglalkozást igénylő probléma nincs, úgy még mindig ott a lehetőség mások jegyeinek átnézésére, hátha meg lehet könnyíteni a többiek munkáját.



Ábra 3. A bejelentések kezelésének munkafolyamatai

4.4.4 Kommunikáció a rendszerrel

Az RTIR rendszer részét képezi egy e-mail gateway program, aminek az a feladata, hogy a rendszerbe érkező, ill. onnan kimenő leveleket eljuttassa az MTA-hoz (Mail Transport Agent). E program képes arra, hogy a beérkező levelet egy adott jegyhez társítsa. Ezt két módon kísérli meg elérni. Egyrészt úgy, hogy a levél tárgyában szerepelteti a jegy számát, így a rendszerrel kommunikálni akaró ember közvetlenül is hivatkozhat erre, másrészt pedig a levél fejlécébe tesz „In-Reply-To:", ill. „RT-Ticket:" fejléceket, hogy minél biztosabban azonosítani tudja, melyik jegyhez tartozik a hozzászólás. Az RTIR természetesen vizsgálja, hogy kinek van joga, egy adott jegyhez hozzászólni.

Mindezen túl lehetőség van arra is, hogy a rendszerbe ne csak a bejelentő küldhessen további e-mail-eket, hanem megjegyzéseket ill. válaszokat is küldhetünk a külön ezekre a célokra beállított e-mail címekre.

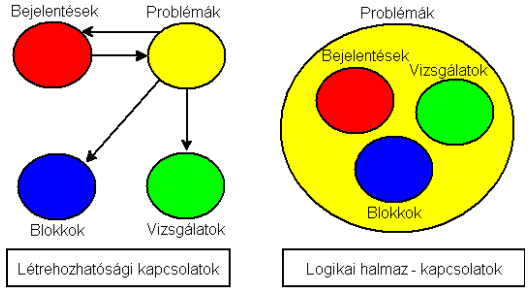
4.4.5 A rendszer szolgáltatásai

Az alábbiakban röviden áttekintjük azokat a „kényelmi" szolgáltatásokat, amelyeket az RTIR nyújt. Ennek a fejezetnek nem célja, hogy e szolgáltatások használatát ismertesse, csupán hogy ezek meglétéről, ill. funkciójáról tájékoztatást adjon. A használat részletesebb ismertetése külön anyagban érhető el.

Az egyik legfontosabb szolgáltatás a „Jegytörténet": egy jegy megtekintésekor láthatóvá válik az összes esemény, amely a múltban történt vele. Tehát látszik a jegy összes frissítése, állapotváltozása, ill. bármely járulékos adat megváltozása.

A rendszer másik fontos tulajdonsága a jegyek közötti kapcsolatok kezelése. Lehetőség van a jegyek közötti kapcsolatteremtésre, szülő – gyerek kapcsolatok kiépítésére. Ez azzal az előnnyel jár, hogy a szülő jegyből gyorsan elérhető a hozzá kapcsolódó összes gyermek, illetve, hogy ezeknek bizonyos tulajdonságait a rendszer automatikusan átállítja a szülő megváltoztatásakor. Pl. egy probléma lezárásakor lezáródik az összes olyan bejelentés, ami hozzá kapcsolódik. Furcsa lehet, hogy a rendszerben mindig a probléma sorba tartozó jegy a szülő, holott a legtöbb ezek közül egy bejelentésből jön létre, ami pedig mindig gyerek. Azonban a probléma bejelentésből történő létrehozása tulajdonképpen csak az adatok átmásolása, az elvégzendő munka minimalizálását segítendő.

A rendszer logikája miatt a különböző jegytípusok egymásból való létrehozhatósága korlátozva van. A megengedett eseteket az alábbi, egyszerű ábra mutatja be:



Ábra 4. Jegytípusok keletkezési lehetőségei

Mint látható, vizsgálatokból és blokkokból nem lehet semmit sem létrehozni, hiszen ezek mindig egy adott problémához kapcsolódnak. Ez az oka annak is, hogy nem hozhatók létre bejelentésekből sem.

Az RTIR lehetőséget biztosít több jegy egybeolvasztására is. Ilyenkor a beolvasztott jegyre vonatkozó kéréseket, hivatkozásokat automatikusan átirányítja az új jegyre, megőrizve ezzel az adatok konzisztenciáját. Ennek a folyamatnak az ellentéte is elérhető, vagyis egy jegyet kétfelé is lehet választani. Erre például akkor lehet szükség, ha egy bejelentő e-mailben több probléma is felvetődött, vagy egy problémáról kiderül, hogy két megoldandó feladatra bontható.

Ugyancsak a gyors munkát segítik elő az integrált keresési funkciók. A rendszer a potenciális adatokból a felhasználói felületen linket készít, így gyorsan elérhetővé válnak a kapcsolódó jegyek az összes sorban. Az RTIR tartalmaz beépített *whois* és *traceroute* szolgáltatásokat is. A rendszerben ezek eredménye is megjelenik, de a szolgáltatások emellett természetesen külön is elérhetők.

Nagy mennyiségű adatfeldolgozás mellett mindenképp szükséges statisztikai adatok generálása is, hogy a munka eredményessége mérhető legyen. E feladat két módon is megoldható. Az egyik az RTIR részét képező jelentés generátor, amely szöveges vagy HTML formátumban közöl adatokat egy adott időszak alatt beérkezett és megoldott/meg nem oldott bejelentésekről, ill. ezek szolgáltatási idő-intervallum szerinti megoszlásáról. A másik eszköz egy beépülő statisztikai modul, amely táblázatos és grafikus formában a következő adatokat gyűjti össze:

- Egy sorra nézve a létrehozott / megoldott / törölt jegyek száma, napi bontásban.
- Az új /nyitott / felfüggesztett jegyek jelenlegi száma, soronként.
- A létrehozott / megoldott / törölt / felfüggesztett tulajdonságú jegyek közül valamelyiknek a több sorra vonatkoztatott adatai, napi bontásban.
- Egy sorra nézve a létrehozott / megoldott / törölt jegyek száma, napi bontásban az elmúlt héten.
- A jegyek megoldásának átlagos ideje, napi bontásban.
- Egy sorra vonatkoztatott megoldási idő eloszlás.

4.4.6 Kötegelt vizsgálatkérés

A hálózati incidenskezelés világában gyakran szükséges, hogy egy probléma kapcsán számos külső féllel lépjünk kapcsolatba. Ha pl. egy új féreg kezd terjedni, szinte biztos, hogy rengeteg jelentés fog befutni egyrészt a zaklatottaktól, másrészt a behatolás-érzékelő eszközöktől. Hasonló a helyzet egy DDoS (megosztott szolgáltatásmegtagadásos támadás) kivizsgálása kapcsán is. Ezekben az esetekben egy sablon e-mail elküldésére van szükség számos e-mail címre, ráadásul ezek a címek legtöbbször nem is állnak közvetlenül rendelkezésre, hanem egy whois adatbázisból kell őket megkeresni IP cím alapján. E feladat manuális végrehajtása időigényes feladat.

Ahhoz, hogy ezek az e-mailek beleilleszkedjenek az RTIR rendszerbe, mindegyikhez létre kell hozni egy problémát és egy vizsgálatot, ami tovább növeli a felesleges robotolással eltöltött időt. A rendszernek ezért van olyan szolgáltatása, amely mindezeket elvégzi helyettünk. Megadott IP címek alapján kikeresi a whois adatbázisból egy adott mezőből az értékeket, de közvetlenül e-mail címek is megadhatóak. A kimenő levelekbe változók helyettesíthetők be, ami lehetővé teszi címenként a releváns információk beágyazását.

Mivel a publikus whois adatbázisokban elég nehéz kiválasztani egy mezőt, ami minden esetben tartalmazza az eset kapcsán értékes e-mail címet, a saját ügyfeleinkre vonatkozó adatokat érdemes egyéni, jól meghatározott mezőkkel ellátott adatbázisban tárolni.

4.5 Egyéb eszközök

Az RTIR egy meglehetősen komplex rendszer, ezért működése több egyéb szoftverre épül, az alábbiakban ezek számbavétele következik:

- *HTTP szerver*: mivel az RTIR webes felületen működik, szükség van olyan felületre, amin keresztül elérhetővé válik. A szerverrel szemben követelmény, hogy rendelkezzen mod_perl vagy FastCGI modullal. Mivel a világ egyik legrobosztusabb http kiszolgálója az Apache, továbbá a fejlesztők is ezt használják, mindenképpen ennek a használata javasolt.
- *Adatbázis szerver*: Mint szinte minden nagyobb mennyiségű adattal dolgozó program, az RTIR is relációs adatbázisban tárolja az információkat. Jelenleg a Mysql, Postgresql, Oracle, Informix és SQLite platformok támogatottak, azonban ezek közül az utolsó három jelenleg még csak béta állapotú, továbbá a program fejlesztése elsődlegesen Mysql környezetben zajlik, így ennek használata javasolt.
- *Levelező kiszolgáló*: Ahhoz, hogy a rendszerből kifelé, ill. az abba befelé áramló leveleket kezelni lehessen, szükség van egy MTA-ra (Mail Transport Agent). Mivel gyakorlatilag az összes – Unix-szerű rendszeren futó – MTA biztosít sendmail kompatibilis illesztő-felületet, az RTIR-nek pedig erre van szüksége, ezért csaknem bármelyik MTA használható. A választásnál érdemes azonban figyelembe venni, hogy ajánlott a spam és vírusszűrők használata (lásd később), amit szintén az MTA-n keresztül praktikus megoldani.
- *Kéretlen levelek szűrése*: Az Internetet egyre súlyosabban érinti a mindenhova eljutó kéretlen levelek áradata. Különösen súlyosan érint ez olyan e-mail címet, amely széles körben ismert, márpedig a Szervezet levelezési címe ilyen. Így feltétlenül szükséges a beérkező levelek automatikus szűrésére. Erre alapvetően két módszer használható. Az első olyan szűrők használata, amelyek az e-mailek tartalma alapján próbálják meghatározni, hogy egy levél spam-e. A másik megoldás a megerősítés kérésén alapszik. Ennek értelmében, ha olyan e-mail címről jön levél, ami a rendszerben még nem ismert, akkor az addig nem kerül továbbításra, amíg a küldő nem erősítette meg, hogy ő küldte a levelet. Ezt azonban elég egyszer megtennie, és címe bekerül az adatbázisba, ami után már küldhet levelet. Ez a módszer biztosabb, mint a tartalomelemzés, de két kisebb hátránya is van. Az egyik, hogy – bár minimális, de – járulékos feladatot ró a másik félre. A másik hátrány az, hogy egy ismert cím nevében küldött levél átjut a szűrőn. A legbiztosabb megoldást a vázolt két megoldás együttes használata jelentheti.
- *Vírusszűrő*: Hasonlóan a kéretlen levelekhez, rengeteg vírusos levél is terjed az Interneten, amelyeknek rendszerbe jutását meg kell akadályozni. Erre is alkalmazható olyan szoftver, ami a levél tartalmát vizsgálja vírusok után kutatva, azonban a fentebb leírt megerősítésen alapuló módszert használva a kéretlen levelek szűrésére, erre a megoldásra gyakorlatilag nincs szükség, hiszen a vírusos e-mailre nem fog megerősítő válasz érkezni, ilyen szempontból a spam és a vírus egyformán kezelhető.
- *Tűzfal*: A rendszert meg kell védeni az illetéktelen külső behatolásoktól. Mivel – rendes körülmények között – az RTIR-t futtató rendszer jól behatárolható szolgáltatásokat nyújt a külvilág felé, ezért egy csomagszűrő, állapotfigyelő tűzfal segítségével jól védhető. A legtöbb UNIX-szerű operációs rendszer kínál erre saját megoldását.
- *Biztonsági másolatok*: Az adatbázisról készülő biztonsági másolatok készítésére az RTIR-ben nincsen külön megoldás, hiszen az adatbázis kezelők mindegyike rendelkezik saját megoldással, ami viszonylag egyszerűen használatba vehető. Mindenképp

szükséges az adatbázis rendszeres biztonsági mentése, amit célszerű földrajzilag is elkülönülten őrizni. (ld. még a 2.4 fejezetet!).

5 A napi tevékenység módja

A napi tevékenységek közé tartozik a támogatásnyújtás, a kommunikáció, a munkarend betartása, és a remélhetőleg ritkán, de mégis bármelyik nap bekövetkezhető katasztrófaterv szerinti riasztás és annak a rendje. Mindez szabályozott módon folyhat.

5.1 A támogatásnyújtás módjai

A CERT működésének egyik alapja a megfelelő kapcsolattartás mind a bejelentéseket tevőkkel, mind a többi CERT-tel. Ehhez arra van szükség, hogy a kommunikáció ne „ad hoc" alapon működjön, hanem jól szabályozott keretek között. A keretek meghatározásának alapját a kommunikációs csatornák definiálása jelenti. Meg kell határozni, hogy kivel, mikor és milyen formában lehet vagy kell kommunikálni.

Alapvetően kétféle kommunikációs csatorna különböztethető meg: be- és kimeneti. A bemeneti csatornák célja, hogy a rajtuk keresztül érkező bejelentések bekerüljenek az incidenskezelő rendszerbe. Ezek a bejelentések lehetőleg tartalmazzák a probléma megoldásához szükséges összes információt. Az egyes bejelentés-típusokhoz kapcsolódó bekérendő információkat a 10.4 melléklet tartalmazza.

5.1.1 Bemeneti csatornák

A bemeneti csatornák a következők lehetnek:

(a) *Telefonos bejelentés*: Amennyiben egy bejelentés telefonon keresztül érkezik, az operátor feladata, hogy az összes szükséges információra rákérdezzen, majd ezt a bejelentést az incidenskezelő rendszerben rögzítse. Ennek – a rendszer logikája szerint – az adatok áttekinthetőségének érdekében akkor is be kell kerülnie a bejelentések közé, ha a hiba egyedinek látszik, (ld. 10.4 fejezet). Ezekben az esetekben különösen fontos ügyelni arra, hogy az udvarias kommunikációra vonatkozó szabályok betartásra kerüljenek, hiszen a szervezetről kialakult képet az operátorok modora nagyban befolyásolja. A későbbiekben a bejelentéseket tároló jegyről egyértelműen eldönthető, hogy telefonos adatfelvétel során keletkezett-e.

(b) *E-mailben történő bejelentés*: Ezek a bejelentések automatikusan bekerülnek az incidenskezelő rendszer adatbázisába, az operátorok ezen keresztül értesülnek az új bejelentésről. Ez egyrészt kényelmessé teszi az ilyen bejelentések kezelését, másrészt viszont problémát rejt magában, mert a bejelentésben lévő adatok hiányosak lehetnek. Ennek elkerülésére két mód kínálkozik: a megelőzés, és a javítás. A megelőzés fő eszköze a bejelentő űrlapok, ill. ezek mind szélesebb körben történő használata. Ennek ellenére elkerülhetetlen, hogy olyan levelek kerüljenek a rendszerbe, amelyek elégtelen mennyiségű információt tartalmaznak. Ebben az esetben a bejelentő részére el kell küldeni az űrlapot (javítás), továbbá e levélben lehet kérni plusz információkat, ill. fel lehet hívni a figyelmet az űrlap bizonyos – a bejelentés szempontjából releváns – mezőire, amennyiben ez szükségesnek látszik.

(c) *Személyes bejelentés*: Abban az esetben, ha a bejelentő személyesen keresi fel az operátorokat, a kezelés módja ugyanaz, mint a telefonos bejelentés esetében, azonban ezek a bejelentések a szervezet megítélésében még kényesebbek, ezért különös figyelemmel kezelendők. Továbbá megvan az a hátulütőjük, hogy a bejelentő nincs az incidens kezelésére alkalmas helyszínen, ezért a szükséges (plusz) információkat esetleg nem tudja szolgáltatni. Ebben az esetben szükséges az információ megszerzésének mikéntjéről és időpontjáról egyeztetni.

(d) *Webform*: A Webes bejelentéshez használatos űrlap, mely a szükséges információkat tartalmazza. A minta a 10.4 mellékletben szerepel. A webform-ok alkalmazása kétirányú előnnyel jár. Egyrészt a bejelentő személy munkáját az űrlap nagymértékben segítheti azzal, hogy számos adat esetében csupán előre adott válaszok közül kell választania, továbbá az űrlap elküldése – elektronikus levél formájában – csak akkor történik meg, ha a bejelentő valóban minden fontos információt tartalmazó mezőt tartalmilag és alakilag helyesen kitöltött. Az űrlapok alkalmazásának előnye a Szervezet szemszögéből vizsgálva abban jelenik meg, hogy az egységes tartalmú elektronikus levelek operátorok általi feldolgozása egyszerűbb, gyorsabb, egyértelműbb lehet, mint az egyedi levelek osztályozása, amely a beérkező levélben – esetlegesen hiányosan – jelenlévő információ kikeresését igényli.

(e) *Egyéb módon történő bejelentések*: Bármilyen egyéb formában érkező bejelentés (pl. fax, esetleg postai levél) törekedni kell arra, hogy az összes releváns információ a rendszerbe kerüljön, majd tájékoztatni kell a bejelentőt az előnyben részesített „szabványos" bejelentési csatornákról.

5.1.2 Kimeneti csatornák

A kimeneti csatornák arra szolgálnak, hogy a szervezet kapcsolatot tartson fenn a bejelentőkkel, társszervezetekkel, állandó vagy eseti együttműködő partnerekkel, ill. arra, hogy a nyilvánosságnak szánt adatait közzétegye.

Ezek a csatornák a következők:

(a) *E-mail*: Az elektronikus levél valószínűleg a leggyakrabban használt kimeneti kommunikációs forma. Nagy előnye hogy nem követeli meg a felektől az egyidejűséget, továbbá egyszerűen továbbítható rajta gyakorlatilag bármilyen adat. Van azonban egy hátránya is: megbízhatatlansága. Nem tudni, mennyi idő alatt érkezik meg egy levél a címzetthez, ha egyáltalán megérkezik. Emiatt a magas prioritású, fontos ügyekben nem használható – legalábbis önmagában semmiképpen sem. Ráadásul előnye egyben hátránya is, hiszen a nem közvetlen, visszaigazolás nélküli kommunikáció nem minden esetben megfelelő. A hitelesség és letagadhatatlanság biztosítása érdekében minden kimenő e-mailt elektronikusan alá kell írni, továbbá – ha a benne lévő információk ezt szükségessé teszik – titkosítani is kell (ld. még 8.7)

(b) *Telefon*: Főként akkor kell használni, ha az adott kérdés megköveteli a megbízható átvitelt, vagy a közvetlen, azonnali kommunikációt, vagyis amikor az e-mail nyújtotta szolgáltatások nem elegendőek. (Természetesen a két forma kombinálható is.) E módszer alkalmazása – a felek személyes ismeretsége esetén – fokozza a probléma feldolgozása kapcsán fontos szerepet betöltő „bizalmi faktort" is, amely bizonyos intézkedések megtételét gyorsíthatja, vagy egyáltalán lehetővé teheti. Ügyelni kell azonban arra, hogy a telefon olyan – biztonsági szempontból – nyílt adatátviteli csatorna, amely minősített adatkezelést igénylő információk átvitelére általában nem alkalmazható. A telefon alkalmazása – nemzetközi hívás esetén – felvet(het)i még az időzónák kérdését is. Ezt akkor lehet figyelmen kívül hagyni, ha a hívott fél – a Szervezethez hasonlóan – ugyancsak 24/7 üzemben dolgozik.

(c) *Postai küldemény*: Használatára csak akkor van szükség, ha a kommunikációnak kötelezően papíralapúnak kell lennie, mert azt az adminisztrációs rendszer, vagy a külvilággal történő kommunikáció megköveteli.

(d) *Publikálási csatornák*: A tapasztalatok és a szakmai tudás alapján a szervezet publikációkat tesz közzé, melyek maximálisan figyelembe veszik az adatvédelmi törvényeket (az ügyfeleket nem érheti kár ügyükre vonatkozó adat nyilvánosságra kerülésével). A csatornák többfélék lehetnek:

- *Tudományos (elemző)*: az informatikai biztonság területén kutatói szemszögből nézve elért eredmények, és az incidens-kezelés témakörébe tartozó kutatás-fejlesztés (K+F) szakmai cikkei sorolhatók ebbe a csoportba.
- *Oktató (megelőző)*: az átlagos képzettségű felhasználó számára is érthető és alkalmazható tanácsok, leírások és segédanyagok köre.
- *Hírközlő (tényszerű)*: a megtörtént, vagy a trendekből várható események és a lehetséges védekezések tényszerű puszta hírközlő csatornája (pl. sajtótájékoztató, ld. 5.4.2 d. pontját).

5.2 Prioritások

Ahhoz, hogy a felmerülő problémák optimális úton kerüljenek megoldásra, meg kell határoznunk fontosságukat. Erre a besorolásra nem kerülhet sor szubjektív alapon, mindenképpen valamilyen objektív besorolási rendszerre van szükség. Ahhoz hogy egy ilyen kialakításra kerüljön, meg kell határozni, hogy milyen szempontok járulnak hozzá a fontossághoz. Esetünkben ezek a következők:

- *Érintettek köre*: Különbséget kell tenni az alapján, hogy a probléma által érintettek bele tartoznak-e a szervezet által képviselt körbe, vagy nem. A képviseltek között is fel lehet állítani fontossági sorrendet.
- *Érintettek száma*: Ugyancsak mérvadó, hogy egy ember problémájáról van-e szó, egy kisebb csoportéról, netán az egész képviselt kört érintő veszélyekről.
- *Probléma súlyossága*: Meghatározandó, hogy a probléma fennállása milyen következményekkel jár, és ezek mekkora hátrányt ill. mennyi kárt okoznak az érintetteknek.
- *Érintett szolgáltatások száma*: Nyilvánvalóan nem mindegy, hogy egy adott probléma hány szolgáltatás használhatóságát érinti.
- *Bejelentés óta eltelt idő*: Ahhoz, hogy egy incidens ne jusson „jogtalan" előnyhöz egy másikkal szemben, valamilyen módon figyelembe kell venni a korukat, vagy a számukra kitűzött határidőt.

E szempontok figyelembevételével kell tehát kialakítani egy olyan rendszert, amely alapján meghatározható, hogy milyen sorrendben kell foglalkozni a megoldandó esetekkel. Ezt a következő besorolási elvek valamelyike alapján lehet megtenni:

- *Prioritási sor*: A problémákat kategóriákba kell sorolni (pl. levelezést, vagy weboldalt érintő problémák), és ezekből – a fenti szempontok figyelembevételével – kialakítani egy sort, amely alapján aztán a feladatok elvégzésének sorrendje meghatározásra kerül.
- *Fixpontos rendszer*: A különböző szempontokat kell felbontani csoportokra, és a csoportokhoz pontértéket kell rendelni. Egy probléma prioritása az őt érintő pontértékek összege lesz.
- *Változópontos rendszer*: Kezdetben úgy működik, mint a fixpontos rendszer, azonban az idő múlásával a pontok valamilyen szisztéma szerint (pl. az utolsó válasz óta eltelt idő) növekszenek (ill. esetenként csökkennek).
- *Vegyes rendszer*: A problémákat kategóriákba soroljuk, azon belül viszont valamely pontozásos rendszerrel történik a sorrend megállapítása.

A prioritások többféle szempont szerint kerülhetnek meghatározásra (ld.: Hivatkozások/(c) 3.7.6 fejezet táblázatát). A Szervezet számára kialakított táblázat a 10.3 mellékletben található.

5.3 Incidensek életciklusa (RTIR támogatás)

A beérkező és választ igénylő jelentésekre a vállalt határidőn belül (általában 24 óra) választ kell küldeni. Az incidens beérkezésétől annak lezárásáig terjed az incidens aktív életciklusa. Passzív életciklus alatt értjük a mentés és archiválás alatti időszakot. Az életciklus az incidens törlésével érne véget, de ez ritkán fordul elő, pl. akkor, ha kiderül, hogy téves volt a bejelentés vagy a rögzítés, de ebben az esetben is adott idő után kerül végleges törlésre az incidens, mert kiderülhet, hogy a tévesnek minősítés volt téves…

Egy incidens megoldása sem jelentheti az életciklus végét, mivel későbbi előfordulás esetén is foglalkozni kell az adott problémával, még akkor is, ha egy pont ilyen incidens már megoldásra került, és az adott bejelentés már lezárt.

Az életciklus-szemlélet szerint egy incidens a következő állapotokkal rendelkezhet:

- *Keletkezik*: nem kell okvetlen megtörténnie egy incidensnek ahhoz, hogy a rendszerbe kerüljön; az incidenskezelésre való felkészülés állapota így is elkezdődhet (pl. egy operációs rendszerben talált súlyos hiba nyilvánosságra kerülése és a hiba kihasználása időben nagyon távol is lehet egymástól, de a hiba és a potenciálisan okozható incidens felvehető a rendszerbe[12]).

  Az incidens így lehet *talált* (a Szervezet talál rá valamilyen forrásban vagy módon), *észlelt* (a Szervezet észleli aktív munkája vagy az érzékelők által) vagy *bejelentett* (a Szervezet bejelentést kap az incidensről).

- *Kezelés alatt álló*: ekkor kezdődik a bejelentés 4.4.2 fejezetben részletezett élete.

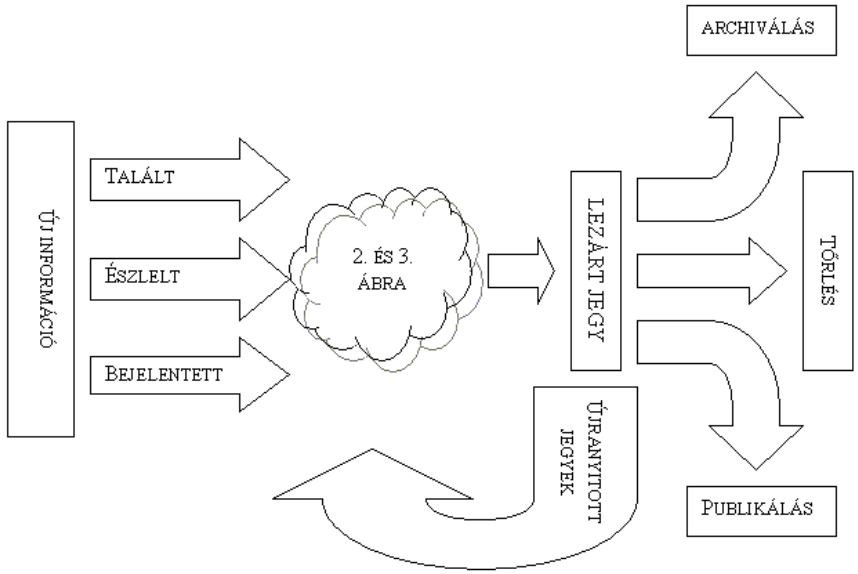
- *Tárolt*: mentett (tudás-/adatbázisban), archivált (későbbi visszakeresés, visszatöltés esetére) vagy publikált (pl. Web-szerveren).

- *Újra felbukkanó*: (ekkor van szerepe az eltárolt jegynek, és a hozzá kapcsolódó teendőknek és lehetőségeknek a bejelentés kezelésében).

- *Megszűnő/törölt*: ez csak akkor következhet be, amikor az adott bejelentésben szereplő adatok nem érintenek még működő rendszereket (pl. az adott operációs rendszer, alkalmazás vagy protokoll már nem érhető el működő változatban)[13].

A fenti állapotokat szemlélteti és foglalja össze a következő ábra:

[12] Az incidens első éles megjelenésekor már elérhetők lehetnek az incidenskezelés teendői is.
[13] Ebben az esetben is lehet tanulsága az adott eseménynek, mely más esetben is alkalmazható az újabb technológiákban is, ezért a törléssel nagyfokú körültekintéssel kell eljárni, és vélhetően elég ritka lesz a törölt bejelentés.



Ábra 5. Az incidensek életciklusa

5.4 Munkarend

A Szervezet munkatársai a megfelelő munkarend szerint végzik a segítségnyújtást. A munkarend szabályozza, hogy miként épülnek fel az egyes műszakok, hogyan történik a váltás a műszakok között stb. A szervezeti felépítés alapján (ld. 3.1 fejezet) adott, hogy ki kinek a beosztottja vagy felettese, és ez alapján ki kitől miként fogadhat és fogad el utasításokat.

Alapelv, hogy minden váltott műszakban dolgozó munkatárs úgy végzi munkáját, hogy az átadás és az átvétel zökkenőmentes legyen. A (minőségbiztosítási) szabályok ennek szellemében alakulnak ki. A napi munkavégzésen kívül vannak más időszakonként végzendő feladatok is, melyek nem átadás-átvétel alapúak, hanem „elvégezve-ellenőrizve” rendszerűek.

5.4.1 Tevékenységek és időszakok

Nem minden tevékenységnek lehet meghatározni az időszakát. Például a vészhelyzet bármikor előfordulhat, de mégsem napi tevékenység a katasztrófaterv végrehajtása. A katasztrófaterv szerint vészhelyzet esetén előre meghatározott írott riasztási rend alapján kell a megfelelő munkatársakat vagy vezetőket értesíteni és bevonni a munkába.

A riasztási rendben szereplő adatok érvényessége fontos tényező a vészhelyzetben. A riasztási rendben szereplők kötelessége, hogy jelentsék, ha elérési adataikban változás állt be, de adott időközönként így is ellenőrizni kell, hogy vészhelyzet esetén a riasztási rendben szereplő adatok alapján az illetékes ember valóban elérhető lenne-e. Ajánlatos évente egy vészhelyzet-gyakorlat lefolytatása, és negyedévente az adategyeztetés/ellenőrzés elvégzése.

Egyes feladatok naponta, mások akár évente egyszer végzendők, de az „éves munkarend” részét képezik. A következő táblázat az általános tevékenységeket és azok gyakoriságát foglalja össze:

Kód	Leírás	Időszak
T1	Beérkező események kezelése, mely egyben a napi munkavégzés dokumentálása is lehet. Elektronikus formában a telefonos bejelentések is a munkavégzés dokumentálását segítik, de a rögzítés rendszere az adatvédelmi irányelvek alapján működik, ezért az így keletkezett adatok archiválásánál az érzékeny adatok kezelését meg kell oldani (pl. kiszűrni, vagy csak megfelelő jogosultságú személy számára biztosítani az elérést).	naponta
T2	Jelentések készítése: – a munka során felmerülő igények szerint – összesített adatok alapján	egyedi, havonta
T3	Mentés és archiválás (évente legalább egyszeri visszatöltés-teszteléssel[14]): – napi mentés biztonságos környezetben és adathordozóra – a hetedik napi mentés egyben heti mentés – havi teljes mentés	naponta, hetente, havonta
T4	Vészhelyzet: leírása adott, gyakorlása évente legalább egyszer	eseti
T5	Adategyeztetés (riasztáshoz): – változás esetén bejelentés alapján (érintettnek kötelező) – évente személyes egyeztetéskor (operátornak kötelező)	egyedi 3 havonta
T6	Oktatás, tanfolyam: – éves oktatási terv alapján belső és külső oktatás – kimenő csatornán – ld. 5.1.2 fejezet (d) pontja – részvétel szakmai szemináriumokon, konferenciákon (oktatási tervvel összhangban, de éves vagy többéves[15] naptár alapján)	egyedi

Táblázat 2. Tevékenységek és időszakok

5.4.2 Kommunikáció az ügyfelekkel

A bejelentések útja az 4.4.2 fejezetben került részletezésre, míg a titoktartási szabályokat külön dokumentum tartalmazza, melyet minden belépő tudomásulvétel után aláír, de a kommunikáció tekintetében még ki kell emelni a következőket:

(a) *Válaszidő*: a bejelentésekre előzetesen (szabályzatban, honlapon) kijelentett időtartamon belül válaszolni kell. A bejelentés súlyosságától és várható hatásától függően kell az erőforrásokat biztosítani, de mindenképpen ajánlatos a 24 órán belüli válaszadás felvállalása.

(b) *Válaszok*: a bejelentés-típustól függően alkalmazhatók a típusválaszok is, de ezek idővel alakulnak ki (pl. másik CERT-hez irányítás, vagy nem a szervezet hatáskörébe tartozó bejelentések kezelése stb.), bővülnek, változnak, így itt csak tudni kell róla, hogy léteznek típuslevelek.

(c) *Jogosultságok*: meg kell határozni, hogy a szervezeti felépítés szerint kinek van jogosultsága adott külső féllel kommunikálni (pl. operátor által tájékoztatott rendszergazda, vagy műszaki felelős által tájékoztatott osztályvezető). A szakember a szakembert érti meg jobban, a vezető a vezetővel szeret inkább egyeztetni. A bejelentések felvétele és kezelése operátori feladat, de a válaszok és teendők kommunikálása vezetői feladat lehet, amennyiben a bejelentő beosztása is vezető.

(d) *Média*: kizárólag a legfelsőbb vezető vagy annak megbízásából valamelyik középvezető nyilatkozhat. Minden egyéb információszolgáltatás felelősségre vonást von maga után.

(e) *Publikáció*: a szervezeten belüli munka kapcsán vagy annak adatai alapján készült publikációk a felettes jóváhagyásával nyújthatók be (ide értendő már a puszta címmel történő előzetes jelentkezés jóváhagyása is).

(f) *Döntés-előkészítés*: A Szervezet helyzetéből adódó lehetséges speciális feladata a működése során tapasztaltak nemzeti szabályozásra (törvények, rendeletek stb.) kihatható események döntéshozók (törvény/rendelet előkészítők) felé jelzése (ld. még 6.2). E kommunikáció lényege, hogy a Szervezet felhívja a döntéshozók figyelmét azon területekre, amelyeken a hazai szabályozás jelentősen eltér a nemzetközi gyakorlattól, illetve amely területeken a szabályozás idejétmúlt, esetleg hiányos. Különösen igaz ez a megállapítás akkor, ha a Szervezet valamely esemény kezelése során a megoldásban érintett partnertől ez irányú kifejezett kérést kap vagy kapott.

5.4.3 Miben segíthetnek az ügyfelek?

A szolgáltatási körbe tartozó ügyfelek felé a következő tízparancsolatot kell kommunikálni, és ez alapján kezelni a bejelentéseiket, felhívva figyelmüket arra, hogy ezek betartásával a segítségnyújtás hatékonyabb lehet. Közös érdek a következők alkalmazása:

1. Mindent dokumentáljanak. — Az incidenssel kapcsolatos minden információ hasznos lehet a további munka során.
2. Keressenek segítőtársat az incidenskezeléshez. — Például az egyik intézkedik, a másik dokumentálja a munkát.
3. Elemezzék a bizonyítékokat. — Meg kell győződni arról, hogy valójában mi történt (pl. jellemző jelenségeknek utána kell nézni internetes keresőkkel, intézményen belüli kollégákat meg kell kérdezni, elérhető dokumentációkban utána kell nézni, mi okozhatta a tapasztalt jelenséget).
4. Értesítsék az érintett alkalmazottakat. — A vezetőket és az illetékeseket (helyi szabályzat vagy katasztrófa-terv szerint) tájékoztatni kell, de diszkrét módon csak azokat, akiket szükséges és olyan csatornákon, melyek biztonságosak.
5. Állítsák meg a támadást, amennyiben még folyamatban van. — A legegyszerűbb lehetőség a hálózati kapcsolat megszakítása[16], más esetben a tűzfal vagy az útválasztó átállítása lehet a megfelelő megoldás a nem kívánt forgalom kiszűrésére.
6. Gyűjtsenek bizonyítékokat. — Az érintett rendszerről mentés (teljes lemez /image/, nem puszta fájl-mentés), a naplóállományokról másolat hasznos lesz a későbbiekben.
7. Takarítsák ki a rendszert. — Minden vírus, vagy egyéb kártékony alkalmazást ki kell tisztítani a rendszerből. Amennyiben teljes mértékű a kompromittálódás, úgy az alapoktól újra kell telepíteni a rendszert, vagy vissza kell tölteni mentésből a legutolsó még jól működő változatot.

[14] A mentés és archiválás azért készül, hogy szükség esetén használható legyen, tehát nem egyirányú feladat.
[15] A rendszeres nevesebb konferenciák akár több évre előre is betervezhetők.
[16] Egyes esetekben a támadó kilétének kinyomozása érdekében ez nem tanácsos, ráadásul így észleli a támadó, hogy támadását észlelték, így a hálózati kapcsolat megszakítása csak a szabályzatban foglaltak szerint történhet (pl. csak felsővezető vagy biztonsági felelős engedélyezheti).

8. Azonosítsák és csillapítsák a sebezhetőségeket. — Az incidens vélhetően valamilyen sebezhetőségen keresztül következett be, így meg kell előzni, hogy ugyanezt kihasználva újra előfordulhasson.
9. Legyenek bizonyosak, hogy a rendszer újra normális működésű. — Bizonyosodjanak meg róla, hogy az adatok, alkalmazások és szolgáltatások normális módon elérhetők és működnek.
10. Készítsenek összegző jelentést. — Ennek részleteznie kell az incidenskezelés eljárását, és kitérhet arra is, hogy mi történt, és milyen módon lehetett volna elkerülni az incidens bekövetkeztét, csökkenteni a károkat, vagy gyorsabban megoldani a problémát.

A szolgáltatási körbe tartozók más-más mértékig tudják ezeket a pontokat teljesíteni, így a fentiek közül annyit teljesítsenek, amennyit tudnak, a többiben a Szervezet segít nekik.

6 A Szervezet jogai, jogosultságai, kötelességei

A Szervezet működését a hazai és nemzetközi jogszabályok keretein belül végzi, és minden egyéb jogosultságot a szolgáltatási körébe tartozóktól vagy azok felügyeleti szervétől kaphat. Ezeket a jogosultságokat írásban kell rögzíteni, és a megfelelő vezetői szinten aláírással hitelesíteni.

6.1 Irányadó jogszabályok

A pontos jogszabályi környezet teljes ismertetése nem része az alapszabályzatnak, de kiemelhetők azok az érvényben lévők, melyeket figyelembe kell venni a működés során. Ezeket jól foglalja össze az Informatikai Biztonság Részstratégia [MITS_IBRS] 1. melléklete, de szélesebb körben az „Internet joggal” foglalkozó gyűjteményes Web-lap is elérhető (`http://internetjog.lap.hu`). Néhány jogszabályt azonban tételesen is érdemes kiemelni:

- Adatvédelmi törvény (1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról)
- Államtitokról és szolgálati titokról szóló törvény (1995. évi LXV)
- Cybercrime egyezmény (Számítástechnikai Bűnözésről Szóló Egyezmény, Convention on Cyber-crime 2001), melyet Budapesten írtak alá[17]
- Hacker törvény, azaz a „300/C” (2001. évi CXXI. törvény a Büntető Törvénykönyvről szóló 1978. évi IV. törvény módosításáról)
- [ENISA] létrehozásának szabályozása (Regulation (Ec) No. 460/2004 of the European Parliament and of the Council of 10 March 2004, establishing the European Network and Information Security Agency)

Az ebben a fejezetben hivatkozott forrásokban felsoroltakon kívül létezhetnek még olyan szabályok, melyek újként jelennek meg, vagy régebbieket módosítanak, így az érvényes és a működést befolyásoló jogszabályokat folyamatosan figyelni kell. Erre a feladatra a Szervezet által megbízott jogász szakembert kell alkalmazni, aki a szükséges belső oktatásokat is megtartja az alkalmazottak számára.

EU csatlakozásunk után a CSIRT-ek számára készített tanulmány [CSIRT_trv] következő kiadásába már Magyarország is bekerül, így a többi ország törvénykezési rendszerével is összehasonlíthatjuk a hazai rendszert és a szabályok által lefedett, vagy éppen le nem fedett területeket (ld. az idézett tanulmány 1. táblázatát).

6.2 Jogosultságok és kötelességek

Az irányadó jogszabályok alapján a jogosultságokhoz szükséges a működési terület meghatározása és a szolgáltatási körbe tartozók megnevezése. Ezzel kapcsolatban a következő alaptételek fogalmazhatók meg:

- A működési terület elsősorban az alapító intézményhez tartozó intézmények, így a működési terület ezen intézmények által meghatározott területre terjed ki.
- A Szervezet az ország EU tagsága okán – valamint az ENISA-ban betöltött szerepünk miatt is – együttműködik a többi európai CERT-tel.

[17] Albánia, Andorra, Ausztria, Azerbajdzsán, Belgium, Bulgária, Horvátország, Ciprus, Csehország, Dánia, Észtország, Finnország, Franciaország, Görögország, Grúzia, Hollandia, Izland, Írország, Lettország, Liechtenstein, Litvánia, Luxemburg, Lengyelország, *Magyarország*, Macedónia, Málta, Moldávia, Nagy-Britannia, Németország, Norvégia, Olaszország, Oroszország, Örményország, Portugália, Románia, San Marino, Spanyolország, Svédország, Szlovákia, Szlovénia, Svájc, Törökország, Ukrajna.

– A nemzetközi terrorizmus-ellenes küzdelemben vállalt szerepünk miatt az EU határain kívül is együttműködünk a többi hasonló szervezettel.

– A Szervezet az alapító intézményen belül működve biztonsági központként (Point-of-Contact) működve fogadja a bejelentéseket.

– Az adatvédelmi törvények betartásával információ-gyűjtést végez az országos informatikai biztonsághoz kapcsolódó adatokról, informatikai biztonsági szakértőkről (önkéntes bejelentkezés, ld. 10.10 melléklet), potenciális veszélyekről (védendő elemekről).

– Az információk alapján végzett elemzésekből származó adatokkal támogatva javaslattétellel él a döntéshozók felé, akár törvénymódosítás előkészítéséhez szükséges szakértői tevékenység által is.

– A szolgáltatási körébe tartozó informatikai rendszereket ért támadás kapcsán a támadás közvetlen forrásánál a nyomozáshoz szükséges információkat elkérheti (törvény által erre jogosultakkal és a szolgáltatókkal együttműködve), a közvetett források esetében segítséget és együttműködést kér a közvetlen forrás felderítésének érdekében.

– A felügyelt informatikai rendszerekben a felügyelet mértékétől és az incidenstől függően aktív beavatkozást hajt végre (pl. beállítások változtatása, rendszer frissítése, kiegészítése, vagy akár a hálózatelérés blokkolása).

Több pontban a jogosultságok egyben kötelességek is, tehát nemcsak jogosult az incidensek kezelésében, de kötelessége is megtenni azt, vagy legalább a megfelelő helyre továbbítani a bejelentést.

7 Anyagi feltételek biztosítása

A Szervezet működéséhez szükséges anyagi feltételek több forrásból származnak vagy származhatnak. Mivel a szolgáltatási körbe főként az alapító intézmény tartozik, ezért a megalakulást döntően az alapító intézmény finanszírozza.

Az oktatási, kutatási tevékenységén keresztül felsőoktatási, kutatóintézeti, míg a nemzetközi kapcsolatain keresztül külföldi partnereivel is olyan helyzetbe kerülhet, amikor pályázatokon való részvételre, vagy nyertes pályázati munkában való együttműködésre hívják meg. Ebben az esetben a Szervezet az alaptevékenység ellátása után fennmaradó erőforrásaival vehet részt ezekben a munkákban és kooperációban, de a részvétel anyagi vonzatait (utazások, emberi erőforrások) és bevételeit (pályázati támogatások és/vagy alvállalkozói munkadíjak) legalább nullszaldóval kell zárni. Nagyobb EU finanszírozású projektek esetében ez a tevékenység nettó bevételeket jelenthet.

Az ország EU-béli helyzeténél fogva a frissen csatlakozott és a leendő csatlakozók számára a Szervezet helyi központ (center of expertise) szerepet is betölt, így ilyen irányú pályázatokból és anyagi támogatásokból is részesedik, illetve a régió országai számára is végezhet szolgáltatási körébe eső munkát. Az ilyen feladatok különösen érzékenyek az adatvédelemre, titoktartásra, nemzetbiztonsági vonzatokra, így az ez irányú feladatvállalás előtt a megfelelő szervezetekkel egyeztetni szükséges.

Régióközpontként jelentősek lehetnek a hosszabb szemináriumok, vagy konferenciák szervezése által elérhető bevételek, míg regionális felkészítő és vizsgaközpontként az oktatás alá sorolható bevételek is számottevők lehetnek.

Fontos kiemelni, hogy a Szervezet bevételeit és kiadásait olyan elven kezeli, hogy ne intézményi támogatásból finanszírozzon külföldi projektekben való részvételt, hanem a pozitív bevételek esetében a hazai igényeket elégítse ki (pl. elnyert EU pályázatokba hazai kutatókat és intézményeket von be a munkába).

Összegezve, a működés során a Szervezet bevételi forrásai a következő főbb csoportokba sorolhatók:

– alapító intézményi támogatás,

– pályázati (kutatás-fejlesztés, meghirdetett hazai vagy nemzetközi pályázatokon vagy projektekben való részvétel),

– nemzetközi (EU támogatások, régióbeli megbízások),

– piaci (szabad erőforrások függvényében piaci szolgáltatások, aktív incidenskezelés, tanácsadás, oktatás témákban).

A pontosabb (számszerűsített vagy képlettel meghatározható) összegek a működés során alakítandók ki, amikor tapasztalati adatokon alapulhat egy olyan számítás, hogy a szabad erőforrások milyen költségátalányokkal értékesíthetők a piaci területeken. Ezeket a számításokat éves felülvizsgálatokkal és azok tapasztalatai alapján kell pontosítani, vagy új szolgáltatások bevezetésével a nemzetközi tapasztalatokra hagyatkozva a honi sajátosságokat figyelembe véve kialakítani. Mindezt a *Szervezet üzleti terve* foglalhatja magába.

Egyes publikációk azt állítják, hogy nem határozható meg pontosan egy-egy incidens kezelésének költsége, míg több olyan tanulmány is elérhető, melyek erre kísérletet tesznek. Az alapkérdések megválaszolása után következhet az összegek meghatározása és a költségszámítás, mely számos paramétertől függ (régió megfelelő szakembereinek bére, telekommunikációs költségek, alkalmazott eszközök megoldásra fordított időarányos ára stb.), de a kérdések ezektől függetlenek:

– Kik dolgoztak a válaszadáson vagy az incidens kivizsgálásán?

- Mennyi időt fordítottak rá?
- Hány ember nem tudta a munkáját végezni az incidens miatt?
- Mennyi hasznos munkaórát vesztettek a kieséssel?
- Mennyi a munkaórák díja (dolgozók száma * órabér)?
- Mennyi állandó többletköltség kerül kifizetésre a dolgozók felé (biztosítások, betegállomány stb.)?

A [SF_kolts] cikkben található bővebb leírás és hivatkozás további hasznos céltanulmányokra, melyek alapján a konkrét számítások elvégezhetők. A költségelemzéshez értékes alapadatokat szolgáltathat a Szervezet munkáját segítő nyilvántartó rendszer részeként üzemelő statisztikai modul.

A költségek esetén jelentős összeget emészt fel az alkalmazottak tudásának szinten tartása és a kapcsolattartás a többi szervezettel, melynek keretében a konferencia-részvételek és utazások képviselik a nagyobb összeget (ld. még 8.5 pont).

A Szervezet tevékenységével olyan képet kell kialakítson magáról, hogy megbízható és naprakész információkat képes szolgáltatni az Internet biztonság témakörében. Hosszú távon ez azt eredményezi, hogy a piac az információkat keresni fogja, ezáltal a Szervezet a szolgáltatásait képes lesz profitorientáltan (pl. tagdíj, szolgáltatási csomagok értékesítése, előfizetett hírlevél, oktatás stb.) értékesíteni a piac érdekelt szereplői számára.

8 Kapcsolattartás módjai

8.1 Bevezetés

Az intézményi számítógépes infrastruktúra a világ hálózataival szoros összeköttetésben áll. A hálózati támadások nem ismernek országhatárokat, ezért az infrastruktúrának megbízhatónak, biztonságosnak és bizonyos mértékig „öngyógyítónak” kell lennie.

A lehetséges támadások – amelyek irányulhatnak a hálózati infrastruktúra feltérképezésére, gyenge pontjainak felderítésére, a szolgáltatások akadályozására, hátsó ajtók betelepítésére – idejében való felderítése és az arra adandó gyors válasz nemegyszer azon múlhat, hogy milyen kapcsolata van a Szervezetnek a nemzetközi incidenskezelő csoportokkal és szervezetekkel (ld. 10.8 melléklet).

8.1.1 A kapcsolattartás céljai

- Együtt kell működni a *nemzetközi* számítógépes hálózatbiztonsági szervezetekkel az információs infrastruktúra védelme és a biztonsági kultúra terjesztése érdekében.
- Szorosabb kapcsolatot kell kiépíteni és fenntartani *az Európai Unió hálózatbiztonsággal* foglalkozó intézményeivel. Figyelemmel kell kísérni az EU e téren végzett jogalkotását és a hazai szabályozástól való eltéréseit.
- Különös figyelmet kell fordítani a alapító intézményhez hasonlatos külföldi *CERT*-ekkel való kapcsolattartásra, közös problémák feltárására, megoldására.
- Az incidensek kezelése során szükségessé válhat az *egyes, illetékes hálózatbiztonsági csoport* felderítése (ismerni kell fellelhetőségük, ellenőrzésük módját).

8.2 Nemzetközi hálózatbiztonsági szervezetek, társulások

A Szervezet célja, hogy aktív tagja legyen a CERT-eket tömörítő szervezeteknek és kapcsolódjon ilyen társulásokhoz. Az alábbiakban – a FIRST-öt kivéve – csak a legfontosabb európai tömörüléseket soroljuk fel.

8.2.1 FIRST

Az 1990-ben alakult FIRST (Forum of Incident Response and Security Teams), az incidenskezelő csoportok szövetsége, amely a számítógépes incidensek kezelését és az incidensek megelőzését tűzte ki célul. Ennek érdekében:

- technikai információkat, eszközöket, eljárásokat, folyamatokat és helyes gyakorlatokat fejlesztenek ki és terjesztenek,
- támogatják a biztonsági termékek, eljárások és szolgáltatások fejlesztését,
- elősegítik incidenskezelő csoportok alapítását, bővítését,
- tudásukkal, ismereteikkel egy védett és biztonságos elektronikus környezet megteremtésére törekednek.

A FIRST-ben teljes (full) és pártoló (liaison) tagok vannak. A belépés során a kérelmezésen túl [FIRST_mem] a tagok közül ajánló(ka)t kell szerezni. Az éves tagdíj jelenleg 240$ illetve 900$.

8.2.2 TERENA TF-CSIRT és Trusted Introducer

A TF-CSIRT projektet az európai CERT-ek részére a TERENA (Trans-European Research and Education Networking Association) Technikai Programjának támogatásával [TF_CSIRT] indították útjára az alábbi célokkal:

- fórumot biztosítson a tapasztalatok és ismeretek kicseréléséhez,
- kísérleti szolgáltatásokat nyújtson az európai CERT-ek számára,
- szabványokat és eljárásokat határozzon meg az incidensekre adandó válaszokhoz,
- támogassa az új CERT-ek létrehozását és biztosítsa a CERT munkatársak továbbképzését,
- közös kezdeményezéseket valósítson meg,
- az Európai Unió és más döntéshozó szervezetek, valamint az európai CSIRT-ek között közvetítő szerepet töltsön be.

A TF-CSIRT Trusted Introducer elnevezésű projektje az európai CERT-ek nyilvántartását végzi. A CERT-eknek háromféle státusza lehet: „bejegyzett", „akkreditálásra készülő" és „akkreditált". A bejegyzéshez csak egy formalap kitöltése szükséges, a további szintek elérésének már feltételei vannak. [CSIRT_lev]

8.2.3 EGC CSIRT

Az európai kormányok CSIRT csoportja, az EGC 2002-től kezdve hat taggal működik (Finnország – CERT-FI, Franciaország – CERTA, Hollandia – GOVCERT.NL, Nagy-Britannia – UNIRAS, Németország – CERT-Bund, Svédország – SITIC). Céljuk a kormányzatokat érintő incidensek közös kezelése. Évente négy alkalommal tanácskoznak. Együttműködnek a TF-CSIRT-tel is, de nem kívánják, és nem is tudják azt a szerepet betölteni, mint az APCERT Ázsiában, vagyis hogy a földrész egyetlen CERT kapcsolati pontja legyenek. [EGC]

8.2.4 eCSIRT.net

2002. júliusa és 2003. decembere között az 5. keretprogram jóvoltából több európai CSIRT kapott támogatást egy kísérleti projekt megvalósításához. A projekt a CSIRT-ek hatékony együttműködését, az incidenseket érintő adatok cseréjét, a statisztikai adatok gyűjtését és egy tudásbázis kialakítását célozta meg.

A projekt sikeresen lezárult, és a projekt keretében felállított IDS szenzorok európai hálózata azóta is folyamatosan gyűjti a támadásokra vonatkozó adatokat további elemzés céljából. [CSIRT_sen]

A résztvevők listája: CSIC/IRIS-CERT (E), DFN-CERT (D), INFN/GARRnet CERT (I), Stelvio b.v. (NL), NASK/CERT-Polska (PL), PRESECURE Consulting GmbH (D), RENATER/Le CERT Renater (F), UKERNA/JANET-CERT (UK), UNI-C/DK-CERT (DK)

8.2.5 EISPP

Az EISPP-t (The European Information Security Promotion Program) szintén az 5. keretprogram támogatta. [EISPP] Az EISPP nemcsak a biztonsággal kapcsolatos tudás terjesztését célozta meg, hanem az információ tartalmának és szétosztásának módját próbálta meghatározni, elsősorban a kis- és középvállalkozók felé. A 2002 júniusában megindult projekt 2003 végén fejeződött be. A projektet a CERT-IST vezette, részt vett benne többek között esCERT és a Siemens-CERT.

8.2.6 ENISA

Az Európa Parlament és Tanács 460/2004. számú rendeletében 2004. március 10-én létrehozta az Európai Hálózat- és Információbiztonsági Ügynökséget, az ENISA-t (European Network and Information Security Agency). [ENISA]

Az ENISA elsősorban a következő tevékenységekre összpontosít:

1. tanácsokkal látja el a tagállamokat és a Bizottságot az informatikai biztonság területén fellépő problémák megoldásánál.
2. elősegíti az iparral folytatott tárgyalásokat, hogy biztonságos hardver és szoftver termékek kerüljenek gyártásba,
3. összegyűjti és elemzi az incidenseket és a felmerülő veszélyeket Európában,
4. segíti a kockázatelemzési és kockázatkezelési eljárások kialakítását, hogy határozottabban lehessen fellépni az informatikai biztonságot érintő fenyegetésekkel szemben,
5. támogatja az informatikai biztonság különböző területein munkálkodó szervezetek/egyének tudatosságának fejlesztését, együttműködését, különösen a PPP viszonylatában.

A CERT-ek az ENISA minden tevékenységében, de elsősorban a harmadik pontban érdekeltek.

8.3 Az incidensekkel kapcsolatos szabványtervezetek

Sajnos, ma még nem áll rendelkezésre mindenki által elfogadott szabványos eljárás arra, hogy a CERT-ek információikat egymás között kicseréljék, az incidensre vonatkozó adatokat valamilyen előírt módon gyűjtsék és közzétegyék. Sokan belátják, hogy a feladatok szabványosítása egyszerűsítené a csoportok közti kommunikációt, s ezért egyre több ebbe az irányba mutató kezdeményezés lát napvilágot.

A Szervezetnek figyelemmel kell követnie a szabványtervezetek alakulását, így megismerheti az aktuális trendeket, véleményt tud alkotni azok alkalmazhatóságáról, tapasztalatait az illetékesekhez eljuttatva befolyásolni tudja a végleges változat kialakulását. A következőkben néhány szabványosítással foglalkozó csoport munkáját mutatjuk be.

8.3.1 INCH WG (IETF Incident Handling Working Group)

A munkacsoportot [INCH_WG] feladata egy olyan adatformátum definiálása, amelyet a CERT-ek majdan az incidensre vonatkozó információk kicserélésénél használhatnak. Munkájuk előzménye a TERENA TF-CSIRT projektje keretében meghatározott IODEF formátum. Ez az új formátum tartalmazni fogja:

- az incidensben szerepet játszó forrás – és célrendszert, viselkedésük elemzését,
- a bizonyítékokat,
- az incidens vizsgálatának és elemzésének sémáját,
- egyéb olyan adatokat, amelyek megkönnyítik az információcserét (pl. adat érzékenysége).

Az adatformátumot a következő kommunikációkban alkalmazzák:

- a CSIRT-hez a hatáskörébe tartozó szervezetek részéről történő bejelentéseknél,
- a CSIRT és az incidensek vizsgálatába bevont felek (rendőrség, érintett felek) közti kommunikációban,
- CSIRT-ek közti együttműködésben.

8.3.2 IETF Intrusion Detection Workgroup (IDWG)

Az IDWG [IDWG] csoport célja, hogy olyan adatformátumot és adatkicserélési eljárásokat hozzon létre, amivel az incidenseket érzékelő rendszerek (IDS-ek) közötti információcsere emberi beavatkozás nélkül megvalósulhat. Tehát az INCH-csel szemben itt a hangsúly a rendszerek közti kommunikáción van (A definiált adatformátum neve: IDMEF).

Az IODEF és az IDMEF összehangolásával a Terena TF-CSIRT programja foglalkozott. Röviden összefoglalva: az IODEF-től elvárják, hogy az IDMEF-fel kompatibilis legyen, és képes legyen az IDMEF üzeneteket értelmezni, a másik irányú kompatibilitás nem követelmény, vagyis az IDS-eknek nem kell értenie az IODEF üzeneteket.

8.3.3 Common Advisory Interchange Format (CAIF)

A CAIF [CAIF] a biztonsággal kapcsolatos tanulmányok struktúrájának meghatározására, tárolására és továbbítására szolgál. (A biztonsággal kapcsolatos dokumentum elnevezésére az angolban az „advisory" szót használják, ami egy számítógépes biztonsági probléma leírását, vagy megoldását jelenti.)

A formátum meghatározásánál a kibocsátó, a terjesztő és legfőképpen az olvasó szempontjait vették figyelembe (olvasó: ki küldte a tanulmányt, autentikus-e, érdekes-e az olvasó számára, várnak-e választ; a terjesztő: szabadon vagy csak korlátozottan terjeszthető, konvertálható). A formátum a kötelező alapelemek mellett szabad-szöveges elemeket is tartalmaz(hat), és XML alapú.

8.3.4 Automated Incident Reporting (AirCERT)

Az AirCERT [AirCERT] a biztonságot érintő eseményekre vonatkozó információk szétosztására alkalmas elosztott, skálázható rendszer. Segítségével az IDS-ek által generált információk továbbíthatók. A rendszer többféle formátum (IODEF, IDMEF és SNML) továbbítására képes.

8.3.5 Bizonyítékok gyűjtésének és tárolásának irányelvei (RFC 3227)

Az IETF RFC-i között ez a dokumentum [RFC3227] a „best practice", azaz a helyes gyakorlat besorolását kapta. A dokumentum célja, hogy iránymutatást adjon az [RFC2828] szerint „security event" címszó alatt definiált biztonsági esemény gyűjtésére és archiválására.

8.4 Információforrások a sebezhetőségekről

A Szervezetnek naprakész információkkal kell rendelkeznie az Interneten jelentkező sebezhetőségekről, több host-ot érintő, vagy nagyobb károkat okozó támadásfajtákról, megszűntetésük lehetséges módjairól. E feladat ellátásához nyújt segítséget a Hivatkozások rész utolsó bekezdésében említett hasznos információforrások cím alatti lista. Néhány nevesebb elem (levelezési listák, weblapok, konferenciák stb.) elérhető a 10.6 mellékletben.

8.5 Konferenciák, rendezvények

Az intézményi CERT tagjainak – mint bármely más CERT csoport tagjainak – a konferenciákon való részvétel a személyes kapcsolatok építését, ápolását jelentheti, a továbbképzést biztosítja, felhívja a figyelmet az új tendenciákra, új kutatási eredményekre, a készülő vagy életbe léptetett szabványokra. Ezért aztán különösen fontos, hogy a tagok évente néhány konferenciára eljussanak[18].

[18] A konferenciákon való megjelenés (előadással vagy látogatóként) szabályozott, az ott folytatott tárgyalásoknál be kell tartani az érzékeny adatokra vonatkozó szabályokat. A kapcsolatok kezdetén a Szervezet hivatalos és engedélyezett formátumú és adattartalmú kétnyelvű névjegyeit kell használni.

A konferencia kiválasztása függ a rendezvény fő témájától, a konferencia színhelyétől, de figyelembe kell venni, hogy kiknek ajánlják a részvételt, és milyen haszonnal járhat a Szervezet munkájában, ha azon képviselteti magát. (ld. 10.6.3 melléklet)

8.6 Oktatás, kutatás, továbbképzés

A CERT csoportok képzése/továbbképzése kiemelten fontos a sikeres védekezésben. Nagyon sok információ érhető el az Internetről, ezek tudatos gyűjtése és rendszerezése *részben* pótolhatja a profi szervezetek által nyújtott képzést. A tanuláshoz az alábbi segédeszközök alkalmazhatók:

- *Tanulmányok (advisories)*: azokat az anyagokat hívják így, amelyek a számítógépes biztonság egy adott kérdését alaposabban elemzik. Ezek általában hosszabb életű dokumentumok, aktualitásukat sokáig megőrzik.
- *Konferencia-előadások*: ld. 8.5 pont.
- *Műhelymunkák (workshop)*: közvetlenségük miatt néha hasznosabbak a konferenciáknál. A kis létszámú csoportban a kérdések alaposabban elemezhetők, mélyebb információk szerezhetők. A TERENA TRANSIT projekt (ld. 8.2.2) példaként szolgálhat, ahol a CSIRT csoportok munkatársai – korlátozott létszámban – évente kétszer ingyenes továbbképzésen vehetnek részt.
- *Helyzetgyakorlatok*: alapos előkészítő munkát igényel. A csoport tagjai előtt egy rövid helyzetképet ismertetnek, majd ezután kérdésekre kell válaszolniuk. A jelenlévők a kérdésekre adandó választ megbeszélhetik, és úgy alakíthatják ki végleges álláspontjukat. A gyakorlat során kitűnik, hogy mit tehet a csoport egy adott helyzetben, ezt hogyan lehet a biztonsági irányelvekkel, eljárásokkal egyeztetni, milyen hiányok vagy esetleges ellentmondások vannak a kérdéses helyzet és a rögzített irányelvek, eljárások között (ld. Hivatkozások/(a) B szcenáriók). Mintahelyzetek lehetnek: intézményen belülről induló spam, feltört szerver, külső DDoS támadás, vírusterjedés stb.
- *Könyvek*: a szakirodalom főként külföldi forrásból, angolul érhető el, de akad néhány hazai munka és fordítás is, gyakran egyetemi jegyzet formájában is.
- *Tanfolyamok/vizsgák*: a tanfolyamok kiválasztása több tényező függvénye, úgymint:
  - kit képeznek (vezető, technikai személyzet),
  - milyen témában, és célból,
  - milyen előismereteket feltételeznek a résztvevőről,
  - távoli eléréssel (on-line módon), vagy a helyszínen tanul,
  - kíván-e valamilyen bizonyítványt megszerezni.
- *Egyéb ismeretek*: ide tartoznak a jogi és közgazdasági ismeretek mellett az olyan speciális ismeretek, melyeket céltanfolyamokon lehet megszerezni. Ezek közül a legfontosabb az operátoroknak tartandó tréning, amely keretében a kommunikációs és problémakezelő készségük (telefonos, személyes, E-mail-es) fejleszthető.

A megszerzett tudást többnyire akkor ismertethető el, ha a külvilág felé dokumentummal is igazolható. A Szervezet által támogatott, javasolt, vagy előnyben részesített tanfolyamok és vizsgák a 10.11 mellékletben kerültek felsorolásra.

Külön témakör a kutatások és fejlesztések (K+F) területe, amely többnyire kutatóintézetekhez és felsőoktatási intézményekhez kapcsolódik. A Szervezet támogatja azokat a kutatásokat, melyek

közvetlenül számára is hasznos eredményeket hozhatnak (pl. honey pot rendszerekkel végzett kutatások, titkosító algoritmusok erősségének vizsgálata, korszerű adatvédelmi megoldások stb.).

A Szervezet a támogatandó témakörökről és a konkrét támogatásokról éves terv keretében dönt, de megvizsgál minden olyan megkeresést, melyben a Szervezetre partnerként számítanak más intézetek leendő, vagy folyamatban lévő munkák során.

8.7 CSIRT-ek közti biztonságos kommunikáció

A Szervezetnek különösen figyelmet kell fordítania saját és partnerei biztonságának megőrzésére. Ennek során az alábbi hét tényezőre kell ügyelni:

1. Titkosság/bizalmasság (confidentiality) — csak ahhoz az információhoz férhessen hozzá valaki, ami számára engedélyezve van, máshoz nem;
2. Elérhetőség (availability) — bárki elérhesse azt az információt és akkor, amikor szüksége van rá;
3. Sértetlenség (integrity) — az információ maradjon az, amilyennek eredetileg szánták/tervezték;
4. Hitelesség (authenticity) — az információ forrását biztosan azonosíthassuk;
5. Kizárólagosság (exclusivity) — csak a cél(személy) tudja az információt használni;
6. Magánélet sérthetetlensége (privacy) — garantálni kell az egyének vagy szervezetek érdekeinek védelmét;
7. Elkötelezettség (obligation) — mindenki a lehető legnagyobb gondossággal járjon el.

8.7.1 Titkosítás és digitális aláírás az elektronikus kommunikációban

A CERT-ek közti, a csoporton belüli, illetve a csoport és harmadik fél közti kommunikáció sokféleképpen megvalósítható (telefon, fax, e-mail), azonban a bizalmas és az érzékeny adatok kommunikálásakor titkosítás és digitális aláírás használata szükséges. Biztonságos fax, telefon nem mindig áll rendelkezésre a harmadik félnél, de az elektronikus levelezéshez többnyire rendelkezésre állnak azok a technikák, amelyekre támaszkodni lehet.

E célra két, széles körben használatos, szabadon elérhető megoldás az OpenPGP és az S/MIME. Bár funkciójukban hasonlóak, a két protokoll lényegesen különbözik:

Service/Protocol	OpenPGP/GnuPG	S/MIME v3
Signature	DSA (2048)	DSA (2048)
Public key	El-Gamal (4096)	DH (1024)
Encryption	3DES	3DES / (RC2)
Hash	SHA-1 (160)	SHA-1 (160)
Message Format	Binary	binary, CMS
Certificate Format	Binary	binary, X.509 (v3)
Mime signed	multipart/signed with ASCII armor	multipart/signed CMS
Mime encryption	Multipart/encrypted	application/pkcs-7-mime

Táblázat 3. OpenPGP és S/MIME tulajdonságok

Bővebb információ az IETF RFC oldalain található. [RFC_crypt] A népszerű e-mail kliensek legalább az egyik szabványt plug-in-ként ismerik.

8.7.2 Kriptográfiai kulcsok és tanúsítványok

Az S/MIME és a PGP/GPG aszimmetrikus (nyilvános-titkos kulccsal történő) kódolást használ, tehát a CERT egészének és a tagoknak is rendelkezniük kell egy ilyen kulcs-párral. Ennek megszerzéséhez a következő lépések megtétele szükséges:

- kulcs-pár generálása (DH vagy RSA),
- a titkos kulcs biztonságos tárolása és megőrzése,
- a nyilvános kulcs közzététele (tanúsítványszerzés után).

A generált nyilvános kulcs elfogadtatásához tanúsítványt kell szerezni, vagyis igazolni kell, hogy a nyilvános kulcs és a tulajdonos összetartozik. Kétfajta tanúsítványi rendszer alakult ki, a bizalmi harmadik félen (Trusted Third Parties), és a bizalmi hálózaton (Web-of-trust) alapuló. Mindkét megoldás alkalmazható, de az előbbi törvény alapján is támogatott[19].

Nincs egyértelmű gyakorlat arra nézve, hogy a CERT-ek használják-e a titkos kulcsukat más nyilvános kulcsának aláírására. A CERT/CC egyetlen más kulcsot sem ír alá, míg a CERT-NL néhány igazán megbízható embernek aláírja a kulcsát. A kormányzati CERT-nek ez utóbbi megoldás javasolható.

A FIRST konferenciákon (ld. 10.6.3.1) kulcsaláíró összejövetelt szoktak szervezni, amikor a felek a személyesen végzett ellenőrzés alapján aláírják egymás kulcsait.

8.7.3 Kulcskezelés

A kulcskezelés jelentőségét nem lehet eléggé hangsúlyozni. A mindennapi gyakorlat során az alábbiakat kell megoldani:

- *A kulcsokat teljes életciklusuk alatt kezelni kell*. A kulcskezelés nemcsak a kulcs generálását jelenti, a kulcsokat alkalmas módon kell tárolni, importálni, menteni, visszaállítani, és szükség esetén visszavonni, felfüggeszteni, vagy éppen megsemmisíteni.
- *A kulcsokhoz való hozzáférést szabályozni kell*. Biztosítani kell, hogy se egy ember, se egy csoport ne veszélyeztethesse a rendszert, ezért rögzíteni kell, hogy ki, milyen esetben, milyen kulcskezelési feladatokat végezhet.
- *Lehetővé kell tenni a szintekre bontást*. A napról-napra növekvő kulcsszám mellett fontos szempont, hogy a megfelelő biztonsági szinten a megfelelő erősségű kulccsal történjen meg az aláírás.
- *Földrajzilag távol lévő kulcsok kezelése*. A Szervezetnek a kulcs helyétől függetlenül képesnek kell lennie a kulcsok kezelésére.

[19] 2001. évi XXXV. törvény az elektronikus aláírásról.

9 Hivatkozások

A hosszú Web-es hivatkozások (csak sortöréssel férnek el) TinyURL (►) rövidített hivatkozással is rendelkeznek.

[AirCERT] AirCERT – Automated Incident Reporting

http://aircert.sourceforge.net/

[CAIF] CAIF – Common Advisory Interchange Format

http://cert.uni-stuttgart.de/files/caif/requirements/split/requirements.html

► http://tinyurl.com/6jtc8

[CERT_FAQ] The CERT® Coordination Center FAQ

http://www.cert.org/faq/cert_faq.html

[CSIRT_lev] Klaus-Peter Kossakowski, Don Stikvoort: A Trusted CSIRT Introducer in Europe, M&I/Stelvio, Amersfoort, The Netherlands (Version 2.0, February 27. 2000)

http://www.ti.terena.nl/about_ti/ti-v2.pdf

[CSIRT_sen] eCSIRT.net statisztika az érzékelők jelentései alapján

http://www.ecsirt.org/service/ids-sensor-data.html

[CSIRT_trv] Dr. Andrew Rathmell, Dr. Lorenzo Valeri (Project Managers), Neil Robinson (Project Coordinator), Andrea Servida (Project Officer): Legislative Procedures of Computer and Network Misuse in EU Countries – Study for the European Commission, Directorate-General Information Society (2002)

http://www.cordis.lu/ist/directorate_d/trust-security/eeurope.htm

► http://tinyurl.com/5mpd9

http://europa.eu.int/information_society/eeurope/2005/doc/all_about/csirt_handbook_v1.pdf

► http://tinyurl.com/7xhnr

[EGC] EGC – European Group of CERTs

http://www.bsi.bund.de/certbund/EGC/index_en.htm

[ENISA] ENISA (European Network and Information Security Agency)

http://www.enisa.eu.int/

[FIRST_mem] FIRST Membership process

http://www.first.org/membership/process.html

[EISPP] EISPP – The European Information Security Promotion Program

http://www.eispp.org/

[IDWG] IDWG – Intrusion Detection Workgroup of IETF

http://www.ietf.org/html.charters/idwg-charter.html

http://www.terena.nl/tech/task-forces/tf-csirt/iodef/docs/iodef-idmef-xmldtd-00-rfc.html

► http://tinyurl.com/4x5u3

[INCH_WG] INCH WG: Incident Handling Working Group of IETF

http://www.ietf.org/html.charters/inch-charter.html

http://www.ietf.org/internet-drafts/draft-ietf-inch-rid-01.txt

► http://tinyurl.com/49os9

[MITS_IBRS] Magyar Információs Társadalom Stratégia – Informatikai Biztonsági Részstratégia

http://193.6.108.12/anyagok/stea/Mits/e-biztonsag/IBRS_hazai.pdf

► http://tinyurl.com/6oqwz

[RFC2828] R. Shirey: Internet Security Glossary, May 2000

http://www.ietf.org/rfc/rfc2828.txt

[RFC2350] N. Brownlee, E. Guttman: Expectations for Computer Security Incident Response, June 1998.

http://www.ietf.org/rfc/rfc2350.txt

[RFC2350_h] Az RFC2350 magyar nyelvű változata, elérhető a Hun-CERT honlapján:

http://www.cert.hu/szabaly/4RFC2350/rfc2350-hun-cert-hun.html

► http://tinyurl.com/4st7e

[RFC3227] D. Brezinski, T. Killalea: Guidelines for Evidence Collection and Archiving, February 2002

http://www.ietf.org/rfc/rfc3227.txt

[RFC_crypt] RFC2440: OpenPGP Message Format

RFC3156: MIME Security with OpenPGP

RFC2631: Diffie-Hellman Key Agreement Method

RFC2632: S/MIME Version 3 Certificate Handling

RFC2633: S/MIME Version 3 Message Specification

RFC3369: Cryptographic Message Syntax

RFC3852: Cryptographic Message Syntax (CMS) Algorithm

http://www.ietf.org/rfc/rfc<szám>.txt

[RTIR] RTIR: RT for Incident Response. Nyílt forrású incidenskezelő rendszer a CERT-ek igényeihez

http://www.bestpractical.com/rtir/

[SF_kolts] David A. Dittrich: Developing an Effective Incident Cost Analysis Mechanism (last updated June 12, 2002)

http://www.securityfocus.com/infocus/1592

[TF_CSIRT] TF-CSIRT Term of Reference (TSec(04)084rev2, Approved by the TTC on 15 September 2004):
http://www.terena.nl/tech/task-forces/tf-csirt/TSec_04_084.pdf
► http://tinyurl.com/4kblz

Egyéb felhasznált (a-c) és ajánlott (d-j) irodalom:

(a) Tim Grance, Karen Kent, Brian Kim: Computer Security Incident Handling guide, NIST Special Publication 800-61, 2004 január
http://csrc.nist.gov/publications/nistpubs/index.html

(b) Myriam Dunn and Isabelle Wigert (edited by Andreas Wenger and Jan Metzger): Critical Information Infrastructure Protection, Swiss Federal Institute of Technology, 2004
http://www.isn.ethz.ch/crn/_docs/CIIP_Handbook_2004_web.pdf

(c) Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle, Mark Zajicek: State of the Practice of Computer Security Incident Response Teams (CSIRTs), Technical Report, CMU/SEI-2003-TR-001
http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03tr001.pdf

(d) Handbook for Computer Security Incident Response Teams (CSIRTs)
http:/59/www.sei.cmu.edu/pub/documents/03.reports/pdf/03hb002.pdf

(e) State of the Practice of Computer Security Incident Response Teams (CSIRTs)
http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03tr001.pdf

(f) Organizational Models for Computer Security Incident Response Teams (CSIRTs)
ftp://ftp.sei.cmu.edu/pub/documents/03.reports/pdf/03hb001.pdf

(g) Forming an Incident Response Team
http://www.auscert.org.au/render.html?it=2252&cid=1938

(h) CSIRT Services
http://www.cert.org/archive/pdf/CSIRT-services-list.pdf

(i) Computer Security Incident Handling Guide (NIST)
http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

(j) Steps for Creating National CSIRTs
http://www.cert.org/archive/pdf/NationalCSIRTs.pdf

Elektronikus segédeszközök és hírforrások: nem a szabályzat része, de a Szervezet Web-szerverén és az intraweben is elérhetővé kell tenni egy jól strukturált és rendszeresen karbantartott listát (pl. Hivatkozások/(a) 131-146. oldal F. és G. mellékletek). A külső vagy belső forrásból érkező javaslat alapján csak a felelős jóváhagyásával lehet változtatni a listát.

10 Mellékletek

A mellékletek szerepe, hogy a szabályzathoz képest gyakrabban változó, vagy eljárásokat tartalmazó részeket „kiemelhető” formában fogja össze.

Az ISO minőségbiztosítási rendszer szellemében a mellékletek külön azonosítóval és ezen belül verziószámmal rendelkeznek, így változás esetén az adott azonosítójú melléklet kerül cserére, eggyel nagyobb verziószámmal beemelve az új változatot. Ez a rendszer megengedi, hogy újabb mellékletek is bekerüljenek, de ekkor meg kell hivatkozni a szabályzatban, illetve megszűnő mellékletek legyenek, de ekkor ezek azonosítója nem adható ki más mellékletnek (jelezni kell, hogy volt, de megszűnt).

10.1 A képviseltek köre

E táblázat szolgál arra, hogy a Szervezet működési területéhez tartozó intézmények, csoportok, szervezetek stb. legfontosabb – elsősorban a kapcsolatfelvételhez szükséges – adatait összefoglalja. A táblázat szükség esetén újabb oszlopokkal bővíthető.

Intézmény	Kapcsolattartó	Elérési adatok	Megjegyzés
Alapító intézmény	*név és/vagy beosztás*	*telefon / e-mail*	*Operátor / műszaki felelős keresse…*
XY részleg			*Z Internet-szolgáltató*
Piaci szereplők			*Szerződésszám*

Táblázat 4. Képviseltek köre

10.2 Egy-egy tipikus hibabejelentés szokásos kezelése

Minél több bejelentés érkezik a Szervezethez, annál inkább kialakulnak a bejelentések típusai, és a típusválaszok is.[20] Ez a melléklet ezeket foglalja magába.

10.2.1 Téves bejelentés

Nem a megfelelő helyre történt a bejelentés, ezért a bejelentő figyelmét felhívva a megfelelő helyre kell irányítani, a rendelkezésre álló legpontosabb adatok megadásával (ld. a mellékletek között is a megfelelő táblázatokat).

10.2.2 Nem hatáskörbe tartozó bejelentés

A bejelentés a hasonló szervezetek körébe sem tartozik (pl. szervizre tartozó problémák, otthoni Internet-szolgáltatóra tartozó ügyek stb.), így akár a legpontosabb adatok megadása nélkül (kerülni kell a marketinget, de ha egy adott céghez köthető a megoldás, akkor megemlíthető a név), de szükséges tájékoztatni a bejelentőt, hogy nem a megfelelő szervezethez fordult, és milyen irányba lépjen tovább.

10.2.3 Felveendő bejelentések

Minden olyan bejelentés, mely közvetlenül vagy közvetve a Szervezethez tartozó intézmények (ld. 10.1 részben felsoroltakat) biztonságát érinti.

Más szervezetek által alkalmazott űrlapok mintái megtalálhatók a CSIRT-ek kívánatos működését leíró anyagban (Hivatkozások/(c) 213-266 oldalak). Ezek közül is kiemelhető a SANS által közzétett űrlap-csomag (Incident Handling Forms): `http://www.sans.org/score/`

Egy alapminta megtalálható a 10.3 fejezetben, melyet nemcsak a Web-en bejelentők tölthetnek ki, de ezt használhatják a Szervezet operátorai is a telefonos – vagy más formában – érkező bejelentések rögzítéséhez.

10.2.4 Hibabejelentő fák

Ezek a fák az idővel felgyülemlő tapasztalatok alapján a Szervezeten belül alakítandók ki, de mintaként ajánlható a Hivatkozások/(a) dokumentumban a 105. és 113. oldalaktól (A. és B. szcenáriók) azok a leírások, melyek a jellegzetesebb incidensekre térnek ki részletesebben.

10.3 Prioritások meghatározása

A prioritások felosztásánál a színkód és a szint neve (azonosító vagy sorszám) tulajdonképpen másodlagos szereppel rendelkezik. A felosztás egyértelműsége, és az egyes szintekhez kapcsolódó tevékenységek összessége a fontos. Az egyes prioritások az idő függvényében egy adott bejelentés esetében változhatnak is.

A 5.2 fejezetben leírtakhoz tartozó prioritási táblázat:

[20] Beszélgetés szövege, e-mail formátum, kötelező és opcionális elemek, általános és specifikus esetek – idővel bővül, iterálódik a bejelentések számától és típusaitól függően.

Szint	Leírás	Mi tartozik bele? Hogyan kezelendő?
0	*Semleges*, a beérkezett eseménnyel nem foglalkozik a Szervezet, de ekkor is rögzíti a bejelentést	Nem tartozik a tevékenységi körébe a probléma kezelése (pl. hardver-kompatibilitási gondok, biztonságot nem érintő alkalmazói beállítások, téves vagy hamis megkeresések stb.)
1	*Alap*, a beérkezett eseményre egyszerű megoldás adható (pl. írott anyag vagy egyszerű és hamar elvégezhető beállítások)	Az esemény lokális probléma, és egyszerű úton, rövid időn belül orvosolható (pl. jelszóváltoztatás, megfelelő paraméter beállítás, vírusfigyelő frissítése)
2	*Közepes*, a beérkezett eseményre összetettebb megoldás adható, szükség esetén helyszíni kiszállás szükséges	Az incidens megoldásán túl az újra előfordulás ellen el kell végezni több feladatot (frissítés, vírusirtó telepítés és beállítások több különböző szinten és rendszerelemben), melyekhez nem elégséges írott dokumentáció vagy rövid leírás biztosítása.
3	*Nagy*, az esemény külső szakértők bevonását is igényelheti, a probléma speciális, és a tudásbázisban nincs ismert ellenszere	Minden új és gyorsan terjedő támadás, melynek nem ismert a teljes mértékű megoldást jelentő ellenszere, és félő a hálózati kapcsolatok megszakadása, a rendszerek rendelkezésre-állásának erős romlása. Szükség esetén a Szervezet intézkedik a hálózati kapcsolatok felfüggesztéséről, amennyiben nem tudja elkerülni a támadás hatásában ugyanezt az állapotot, és a hálózati kapcsolat fenntartása nagyobb károkat okozhat később, mint a kapcsolat megszakítása.
4	*Kiemelt*, vészhelyzet, katasztrófa az adott rendszerre vagy kapcsolataira	A katasztrófatervben részletezett események, melyekre a tervben foglaltak szerint kell reagálni (riadólánc, élet és kármentés, tartalékrendszer stb.) Nagy valószínűséggel a hálózati kapcsolatok megszakításával vagy megszakadásával járó esemény.

Táblázat 5. Prioritási szintek meghatározása

10.4 Hibabejelentő űrlapok

Ajánlott minták szerepelnek a Hivatkozások/(c) dokumentum 123. oldal C.1 és C.2 részeiben (rövidebb és hosszabb űrlap-minta). Ajánlatos az űrlapok számának korlátozása, és inkább egy vagy két űrlappal megoldani a bejelentések kezelését. Ezeken lehetnek olyan sorok, melyek előre elkészített menüt is kínálnak (pl. incidens típusa, a bejelentést tevő intézmény stb.).

A mindenkor aktuális web-form, és az azt kezelő alkalmazás elérhető a Szervezet honlapján/szerverén, míg ez a melléklet csak szöveges mintát mutat egy ilyen űrlapra az [RFC2350_h] alapján:

A CERT/CC által kifejlesztett űrlapot használjuk az incidensek bejelentésére. Ha úgy érzi, hogy számítógépét vagy hálózatát támadás érte, kérjük, adja meg az alábbi adatokat és juttassa el hozzánk.

A *-gal megjelölt sorokat feltétlenül töltse ki.

Név és szervezet

1. Név *
2. Szervezet neve *
3. Ágazat (pl. bank, oktatási intézmény, közigazgatás) *
4. Elektronikus levelezési cím *
5. Telefonszám *
6. Egyéb adat

Érintett gép(ek)

7. Host-név és IP cím *
8. Időzóna (Magyarországon CET, ld. http://wwp.greenwichmeantime.com/time-zone/index.htm)
9. A host funkciója (lehetőleg pontosan adja meg) *

A támadó gép(ek)

10. Host-név és IP cím
11. Időzóna
12. Kapcsolatot felvették?
13. Az incidens által okozott kár becsült költsége (ha ismeretes)
14. Az incidens leírása (tartalmazza a dátumot, a bejutás módját, a támadó által használt eszközöket, a megtámadott gép operációs rendszerének és érintett alkalmazásoknak a verziószámát, a feltett javításokat, a sebezhetőségeit, a támadás módjáról feljegyzett adatokat (naplófájlok), és minden további lényeges információt): *

10.5 Elektronikus eszközök

Leltár szerepet is betöltő lista az eszközök egyedi azonosítóival (külső forrásból ideiglenesen a Szervezetben lévő és saját eszközöket jól látható megkülönböztető jellel kell ellátni a Szervezetben tartott időre), fizikai helyével, tulajdonosával vagy felügyelőjével. A jelzés ésszerű módon alkalmazandó, így a szervertől a hajlékony lemezig mindenen a megfelelő jelzésrendszer kerüljön alkalmazásra, hogy az eszközök hovatartozása szemmel azonosítható legyen.

A nyilvántartásba tartozik minden olyan eszköz, mely a szolgáltatásban közvetlenül vagy közvetve részt vesz a számítógépektől a telekommunikációs eszközökön át az iratmegsemmisítőkig.

Az eszközök adatai mellett szerepelnie kell egy várható időpontnak, amikor az adott eszköz cserére szorul, és ez alapján egy meghatározott időpontnak, amikor a pótlásáról vagy felújításáról gondoskodni kell a beszerzési eljárás elindításával. Nem engedhető meg, hogy kulcsfontosságú rendszerelem esetében az új elem később kerüljön üzembeállításra, mint ahogy az aktuálisan használt elem kivonásra kerül az üzemszerű működésből.

A minőségbiztosítási rendszer részeként a leltárral összhangban vezetett nyilvántartás a következő táblázatformába foglalható[21]:

[21] A hajlékonylemezek, CD stb. esetében elégséges a fizikai megjelölés, leltárba csak akkor kell felvenni, ha az adattartalma ezt megkívánja (pl. speciális telepítőkészlet).

Név, típus	Azonosító (leltári szám)	Fizikai hely	Tulajdonos vagy felügyelő	Kivonás / pótlás
PC1, személyi számítógép	*XYZ 1234*	*Titkárság*	*AB*	*2007. június / 2007. április*

Táblázat 6. Elektronikus eszközök – nyilvántartás

10.6 FAQ és hasznos információforrások

A FAQ (GYIK) egy idővel gyarapodó kérdés-válasz gyűjtemény. Mintaként elérhető példa:

- Hivatkozások/(a) 139. oldaltól H. pont
- CERT/CSIRT FAQ: http://www.cert.org/csirts/csirt_faq.html

A hasznos információforrások egy folyamatosan változó lista (ld. 577. oldal utolsó bekezdés), ezért itt csak egy minta szerepel az aktuálisan leghasznosabb forrásokról.

10.6.1 Levelezési listák

10.6.1.1 Bugtraq

A Bugtraq a SecurityFocus-on működtetett moderált lista, témája a számítógépes biztonságot érintő sebezhetőségek elemzése: a sebezhetőség mibenléte, a sebezhetőséget kihasználva hogyan törhető fel egy rendszer vagy alkalmazás, hogyan lehet javítani az érintett programot. A statútum részletesen felsorolja, hogy milyen jellegű leveleket vár:

- számítógépet illetve hálózatot érintő sebezhetőségek (UNIX, Windows, vagy bármilyen más rendszer),
- feltöréshez alkalmazott programok, script-ek, vagy azok részletes leírása,
- javítások, a sebezhetőségek elkerülésére,
- bejelentések, tanácsok, figyelmeztetések,
- számítógép- és hálózatbiztonságra vonatkozó ötletek, tervek vagy munkák,
- egyes gyártóknál alkalmazott eljárások a témába vágó információs anyagai,
- egyéni tapasztalatok a gyártókról, biztonsági szervezetekről,
- incidensekről tanácsok vagy informális anyagok,
- új vagy frissített biztonsági eszközök.

A SecurityFocus-on további, a témába vágó listák találhatók, például a tűzfalakról, honey pot-ról, IDS-ről, számítógépes bűntett kivizsgálásáról stb.

`http://www.securityfocus.com/archive`

10.6.1.2 Full disclosure

A lista a sebezhetőséggel kapcsolatos mindenféle információval foglalkozik. A levelező partnerektől például feltörésnél alkalmazott kódokat és technikákat, evvel kapcsolatos szoftver-

eszközöket, ilyen tárgyú bejelentéseket taglaló cikkeket vár. A lista témájába vágó leveleket nem moderálják. Az archívum 2002 júliusától kezdve letölthető, így a feliratkozás nem szükséges.

http://lists.netsys.com/pipermail/full-disclosure/

10.6.1.3 Penetration testing (Pen-test)

A listát elsősorban hálózat-auditálással foglalkozó szakembereknek szánták, de biztonsági hibákkal és azok kihasználásával foglalkozó levelek is találhatók itt. Ugyancsak a SecurityFocus szerverén érhető el.

http://www.securityfocus.com/archive/101

10.6.1.4 LogAnalysis

A LogAnalysis lista elsősorban rendszeradminisztrátorok fóruma, ahol a log-fájlok konfigurálásáról, kezeléséről, biztonságos tárolásáról esik szó.

http://sisyphus.iocaine.com/pipermail/loganalysis/

Két további weblap, ahol sebezhetőségekkel, incidensekkel kapcsolatos listák találhatók: SecLists.Org, Neohapsis.com.

http://seclists.org/

http://archives.neohapsis.com/

10.6.2 Weblapok

10.6.2.1 Common Vulnerabilities and Exposures (CVE)

A CVE az ismert sebezhetőségeket és biztonsági hibákat tartalmazza. A sebezhetőségek egyértelmű azonosítása, a szabványos leírás nagy előrelépés volt, amely elősegíti a különféle rendszerek átjárhatóságát. A CVE hivatkozást sok IDS rendszer használja, példaként említhető a Snort.

A szolgáltatást a Department of Homeland Security alapította. Egy biztonsági rés bejelentésekor az egy ideiglenes CVE számot kap. Amennyiben az Editorial Board megtárgyalta és jóváhagyta a listába kerülést, akkor a CVE bejegyzés véglegessé válik. A lista tartalma (jelöltek is) kereshető név és kulcsszó alapján, kereshető egy alkalmazáshoz tartozó összes bejegyzés, valamint a teljes lista le is tölthető.

http://www.cve.mitre.org/

10.6.2.2 CERT/CC Incident Notes and Advisories

A CERT/CC az egyik legnagyobb központ, amelyik Internet biztonsági problémákkal foglalkozik. A Carnegie Mellon University, Software Engineering Institute keretén belül működik. A munkatársak – többek között – biztonsági problémákat elemeznek, technikai dokumentumokat adna ki stb. 2004 februárjáig jelentettek meg incidensekre vonatkozó tanulmányokat és megjegyzéseket, azóta ez a tevékenység az US-CERT-hez került át.

http://www.cert.org/incident_notes/

10.6.2.3 US-CERT

Az US-CERT-et, az USA nemzeti biztonsági csoportját 2003. szeptemberében alapították, a US Department of Homeland Security támogatásával. Pontosabban a minisztériumon belül a National Cyber Security Division (NCSD) részleghez tartozik. A CERT/CC incidenskezelő tevékenységét átvéve 2004. januárja óta ez a szervezet gyűjti és teszi közzé a biztonsági riasztásokat. Kétfajta riasztást kezel: az ún. „technical cyber security alert (TA04-nnnn)”-t a szakemberek számára, és a laikusoknak szánt „cyber security alert (SA04-nnnn)”-t. Egy-egy incidensre vonatkozó riasztás

többnyire mindkét kategóriában megjelenik, eltérés az incidensek részletezésében, a leírás szakmai alaposságában mutatkozik (a szám évenként változik, míg az ’nnnn’ szekvenciális sorszámozást jelent).

http://www.us-cert.gov/cas/techalerts/index.html

10.6.2.4 SANS (SysAdmin, Audit, Network, Security Institute)

A SANS weblapjain lévő információk közül az ISC Storm-ot érdemes kiemelni, ami tulajdonképpen egy korai figyelmeztető rendszer. Az egyes portokon folyó tevékenységek és ezek trendjének nyomon-követésével észleli a kiugrásokat, s a váratlan tendenciákra még a biztonsági hiba feltárása előtt felhívja a szakemberek figyelmét. Az adatokat országonként is összesíti, így területi trendek is elemezhetők. Ingyenes on-line folyóiratára bárki feliratkozhat (@RISK).

http://isc.sans.org/

http://www.sans.org/

10.6.2.5 SecurityFocus

A fontosabb levelezési listáknál már szóba került a SecurityFocus. Ide a sebezhetőségeket tartalmazó adatbázisa miatt került. Az adatbázis kereshető a gyártó, az elnevezés, a Bugtraq azonosító, a CVE azonosító és kulcsszavak szerint is. Egy-egy sebezhetőség leírása nagyon részletes, tartalmazza a közzététel dátumát, Bugtraq azonosítót, bejelentőt, az érintett rendszereket verzió szinten, a biztonsági rés kiküszöbölhetőségének módját, hivatkozásokat stb.

http://www.securityfocus.com/

10.6.2.6 iDefense

Az iDefense-t az Infrastructure Forum Inc. alapította 1988-ban azzal a céllal, hogy segítse a felhasználókat az információs vagyonukat, számítógépeiket, hálózatukat, az Internet-elérésük működőképességét fenyegető veszélyek elkerülésében vagy legalábbis kezelésében.

Négy szolgáltatást nyújtanak: kutatásjelentéseket, rosszindulatú kódokról szóló tanulmányokat, sebezhetőségeket, és a teljes Internet-világot érintő fenyegetéseket leíró anyagokat tesznek közzé.

http://www.idefense.com/application/poi/display?type=vulnerabilities

10.6.2.7 Gyártók honlapjai

Ha bármilyen biztonsági résről egy rendszergazda tudomást szerez, akkor a gyártó honlapját érdemes először megnézni. A legtöbb esetben a gyártó a cég honlapján a ”/security” cím alatt teszi elérhetővé biztonsággal kapcsolatos anyagait. Ezen túl azonban egy-egy – az adott operációs rendszerrel foglalkozó, de nem a gyártó által üzemeltetett – biztonsági oldalt is érdemes figyelemmel kísérni, mert a népszerűbb operációs rendszerek esetében sokszor a gyártó lapján még el nem érhető információk is megtalálhatók ezeken. Csak a példa kedvéért:

http://www.nl.debian.org/security/

http://www.linuxsecurity.com/docs/

http://www.microsoft.com/security/

http://www.windowsecurity.com/

10.6.3 Konferenciák

Az alábbi lapok mindegyike biztonsággal foglalkozó konferenciákat gyűjt össze. Az első hivatkozást azért lehet kiemelni, mert a biztonsággal foglalkozó konferenciákat kulcsszavakkal látja el.

`http://www.ee.oulu.fi/research/ouspg/sage/conferences/`

`http://www.cs.ucsd.edu/users/mihir/confs.html`

`http://homelandsecurity.osu.edu/conferences.html`

`http://www.cl.cam.ac.uk/Research/Security/conferences/all.html`

`http://www3.ca.com/securityadvisor/newsinfo/team.aspx?q=60000`

`http://www.allconferences.com/Computers/Security/`

A fenti forrásokból viszonylag egyszerű eszközökkel *rendezvénynaptár* készíthető és készítendő. A rendezvények témájának Interneten keresztüli figyelése is megmutatja, hogy milyen irányba fejlődik a hálózatbiztonság, milyen új eszközök jelentek meg, honnan és kitől lehet további információt szerezni.

10.6.3.1 Nevesebb konferenciák

FIRST (ld. 8.2.1) – `http://www.first.org/conference/`

Rendszeres évi konferenciájuk, az „Annual FIRST Conference on Computer Security Incident Handling”, a CERT csoportok találkozója. Ezen kívül tavasszal és ősszel még egy-egy technikai kollokviumot is szerveznek, de ezekre csak FIRST tagok lehetnek hivatalosak.

SANS (ld.10.6.2.4) – `http://www.sans.org/conference/archive/`

A SANS számos rendezvényéből kiemelkedik a SANS Annual Conference, amit ők maguk is „megakonferenciának” neveznek. Állandó helyszín az Egyesült Államok.

ISACA (ld. 10.11 táblázatban) – `http://www.isaca.org`

Az ISACA története egészen 1967-ig nyúlik vissza, amikor egy kis csoport – egyre kritikusabban szemlélve szervezetük számítógépes rendszerének működését – összeült és egy információs útmutatót készített. A csoport 1969-ben intézményesült, EDP Auditors Association néven. Az ISACA-nak ma már mintegy 100 országban 35,000 tagja van, akik a legkülönfélébb információtechnológiai pozíciókat töltik be, például információbiztonsági szakértő, informatikai vezető, belső auditor. Ezek a pozíciók átfogják az ipar minden ágazatát, beleértve a banki, a kormányzati szférát, és a magánszektort.

Az ISACA három nevezetes konferenciát szervez:

- Computer Audit, Control and Security Conference (CACS)
- Network Security Conference
- Information Security Management Conference

HISEC (Nemzeti adatvédelmi és adatbiztonsági konferencia) – `www.hisec2004.hu`

2003-ban kelt új életre ez a magyar konferencia. A 2004-es témák: Common Criteria és a Magyar Informatika Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS); biometria és elektronikus szavazás; kriptográfia; adatvédelmi átvilágítás és audit elmélete és gyakorlata; mobil fizetés és intelligens kártya; hálózat- és IT biztonság aktuális kérdései; elektronikus aláírás.

10.6.3.2 Underground…

A fiatal érdeklődők és tehetségek egyes csoportjai különböző rendezvényeken vagy hírcsoportokban (news) találkoznak, melyeken sokszor olyan információk is elérhetők, melyek a tudományos és egyéb konferenciák egyikén sem. A több éves hagyományokkal megrendezésre kerülő összejövetelek aktuális információira rá kell keresni a következő néhány „kulcsszó” alapján:

- Hacking Extreme (Hex 2005), elődei: HIP97, HAL2001 – Hollandia
- Chaos Computer Club – Németország
- DefCon, HOPE, Geek, H2K2, Alt2600 – Egyesült Államok
- Hacktivity – Magyarország

Ezek mellett ázsiai forrásokra is figyelemmel érdemes lenni, mert nemcsak az ottani kutatók és kormányok támogatják az elektronikus hadviselést[22], hanem arra is volt példa, hogy európai vagy amerikai konferenciáról elutasított előadás ázsiai konferencián kapott helyet, majd később elismerő szavakat, mert az adott sebezhetőség igaznak bizonyult.

10.6.3.3 Saját rendezvények

Azokban az esetekben, amikor a konferencia évente más és más helyszínen (országban) kerül megrendezésre megfontolandó a hazai pályázat beadása. Ebben az esetben a részvétel szélesebb körnek lehet elérhető, és a kapcsolatépítés is könnyebb.

A kisebb rendezvények magában foglalhatnak egy adott témában megrendezett szemináriumot akár egyetlen előadóra építve az eseményt. A potenciális előadó személyére és a szeminárium témakörére minden alkalmazott tehet javaslatot a műszaki felelős felé, aki előzetesen felmérheti az előadó meghívásának lehetőségeit, de a hivatalos felkérés csak a felsővezetőtől származhat.

Az alkalmazottak minden egyéb felkérésnek a felsővezető jóváhagyásával tehetnek eleget, de a Szervezet támogatja felsőoktatási tevékenységüket (oktatás, szakdolgozók témavezetése stb.), mivel ez jó csatorna a fiatal tehetségek felfedezésére.

[22] A Zrínyi Miklós Nemzetvédelmi Egyetemen évek óta létező szakirány.

10.7 Hazai CERT-ek elérési adatai

(Az alábbi adatok a 2006. április végi állapotot tükrözik.)

Megnevezés	Kapcsolattartó	Elérési adatok	Megjegyzés
Magyar Nemzeti CERT (Hun-CERT):	Becz Tamás, Martos Balázs, Rigó Ernő, Tiszai Tamás, Tóth Beatrix,	MTA-SZTAKI 1111 Budapest, Kende u. 13-17. Tel: +36-1-279-7190 (09:00-16:00) Fax: +36-1-466-7503 E-mail: cert@cert.hu PGP-KeyID: 0x59B9E495 Lenyomat: B368 6C6B F4A6 5693 9721 B271 F8EC 9F54 59B9 E495	
HUNGARNET CERT (NIIF-CSIRT):	Farkas István Máray Tamás Mohácsi János, Németh Ervin,	NIIF-CSIRT NIIF/HUNGARNET 1132 Budapest, Victor Hugó u. 18-22 Tel: +36-1-279-6030 (08:00 – 18:00) E-mail: csirt@mail.ki.iif.hu	
Kormányzati CERT (CERT Hungary):	Dr. Suba Ferenc Szekeres Balázs Birkás Bence	CERT-Hungary 1061 Budapest, Munkácsy Mihály u. 16. Tel: +36-1-301-2080 Fax: +36 1 353 1937 PGP Key lenyomat: 2E13 1DC5 0C31 51F0 E658 C670 89B3 CCF1 F3A0	
Szervezet			

Táblázat 7. Hazai CERT-ek elérési adatai

10.8 Külföldi CERT-ek adatai

A melléklet legalább évente egyszer felülvizsgálatra és frissítésre kerül. A külföldi CERT-eket jelző térkép többféle méretben elérhető a CERT honlapján: `http://www.cert.org/csirts/images/csirts-big3.gif`

(Az alábbi adatok a 2005. október végi állapotot tükrözik.)

Név	Hivatalos név	Ország	Típus	Webcím	CERT/CC	FIRST	TI
AAB GCIRT	ABN AMRO Global CIRT	Hollandia	banki	http://www.abnamro.com/	*	*	
AboveSecCERT	Above Security Computer Emergency Response Team	Kanada	cég	http://www.abovesecurity.com/	*	*	
ABUSE TP S.A.	Tpnet	Lengyelország	cég	http://www.tpnet.pl/abuse-english.html	*		*
ACERT	Army Emergency Response Team	USA	katonai	----	*	*	
ACIRT	Accenture CIRT	USA		----	*	*	
ACOnet-CERT	ACOnet.CERT	Ausztria	felsőoktatás	http://cert.aco.net/	*	*	*
AFCERT	Air Force CERT	USA	légierő	----	*	*	
AMC-CERT	Academic Medical Center	Hollandia	egészségügyi	http://www.amc.uva.nl/cert/	*		
Apple	Apple Computer	USA	cég	----	*	*	
APSIRT					*		
ARCcert	The American Red Cross Computer Emergency Response Team	USA	egészségügyi.	----	*	*	
ArCERT	Computer Emergency Response Team of the Argentine Public Administration	Argentína	kormányzati	http://www.arcert.gov.ar/en/	*	*	
ART	"@stake" Response Team	USA	cég	http://www.atstake.com/	*	*	
AT&T	AT&T	USA	cég	----	*	*	
AusCERT	Australian Computer Emergency Team	Ausztrália	nemzeti	http://www.auscert.org.au/	*	*	
Auth-CERT	Aristotle University	Görögország	felsőoktatás	http://www.auth.gr/			*
Avaya-GCERT	Avaya Global Computer Emergency Response Team	USA	cég	----		*	
B1CSIRT	Bank One Computer Security Incident Response	USA	banki	----		*	
BadgIRT	University of Wisconsin-Madison	USA	felsőoktatás	http://www.doit.wisc.edu/security/	*	*	
BCERT	Boeing CERT	USA	cég	----	*	*	
BE-CERT					*		
BMO ISIRT	BMO InfoSec Incident Response Team	Kanada	banki	----	*	*	
Brasil Telecom					*		
BT SBS	BT Secure Business Services	Nagy-Britannia			*		*

Név	Hivatalos név	Ország	Típus	Webcím	CERT/CC	FIRST	TI
BTCERTCC	British Telecommunications CERT Co-ordination Centre	Nagy-Britannia	cég	----	*	*	*
CAIS/RNP	Brazilian Research Network CSIRT	Brazília	kutatói hálózat	http://www.cais.rnp.br/	*	*	
CanCERT	EWA-Canada / Canadian Computer Emergency Response Team	Kanada	nemzeti	http://www.cancert.ca/Home/Default.php		*	
CARNet CERT	Croatian Academic and Research Network CERT	Horvátország	nemzeti	http://www.cert.hr/	*	*	*
CAT	Cable & Wireless Cyber Attack Team	USA	cég		*	*	
CCERT					*		
CC-SEC	Cablecom Security Team	Svájc	ISP	http://www.cablecom.ch/	*	*	*
Cdn CIRCC	Canadian Computer Incident Response Coordination Centre	Kanada	kritikus infrastruktúra	http://www.ocipep-bpiepc.gc.ca/	*	*	
CERN-CERT	CERN, European Nuclear organization	Svájc	kutatóintézet		*		*
CERT Polska	Computer Emergency Response Team Polska	Lengyelország	Internet felhasználók	http://www.cert.pl/	*	*	*
CERT.PT	NRES CERT	Portugália	kutatói hálózat	http://www.cert.pt	*		
CERT/AQ					*		
CERT/CC	CERT Coordination Center	USA	Internet	http://www.cert.org/	*	*	
CERTA	CERT-Administration	Franciaország	kormányzati	http://www.certa.ssi.gouv.fr/	*	*	*
CERT-Bund	CERT-Bund	Németország	szövetségi kormányzati intézmények	http://www.bsi.bund.de/certbund/	*	*	*
CERTBw	Computer Emergency Response Team Bundeswehr	Németország	Védelmi Minisztérium		*	*	*
CERTCom	CertCom AG	Németország	cég	http://www.certcom.de/			*
CERT-FI		Finnország	országos	http://www.ficora.fi/englanti/tietoturva/certfi.htm	*		*
CERT-IDC	CERT Internet Data Center	Hollandia		http://www.energis-idc.net			*
CERT-IN					*		
CERT-IST	CERT Industries, Services & Tertiaire	Franciaország	ipar, felsőoktatás, szolgáltatás	http://www.cert-ist.com/	*	*	*
CERT-IT	CERT Italiano	Olaszország	olasz Internet site-ok	http://security.dico.unimi.it/	*	*	*
CERT-KUN	CERT Katholiek Universiteit Nijmegen	Hollandia	felsőoktatás	http://www.kun.nl/cert	*		*
CERT-LEXSI	Laboratori d'Expertise en Securité Informatique	Franciaország	l cég	http://www.lexsi.com	*		*
CERT-Renater	CERT-Renater	Franciaország	Kutatási és Oktatási Minisztérium	http://www.renater.fr/Securite/CERT_Renater.htm	*	*	*
CERT-RUG	Computing Center, University of Groningen		felsőoktatás	http://www.rug.nl/rc/security	*		*
CERT-UU	Utrecht University	Hollandia	felsőoktatás	http://www.cs.ruu.nl/cert-uu/	*		*
CERT-VW	CERT-VW	Németország	cég		*	*	*
CESNET-CERTS		Csehország	akadémiai hálózat	http://www.cesnet.cz/			*
CGI CIRT	CGI Computer Incident Response Team	Kanada	CGI, minisztériumok, magánipar	http://www.cgi.ca/	*	*	

Név	Hivatalos név	Ország	Típus	Webcím	CERT/CC	FIRST	TI
CIAC	US Department of Energy's Computer Incident Advisory Capability	USA	Energiaügyi Minisztérium	http://ciac.llnl.gov/	*	*	
CiART					*		
Cisco Systems	Cisco Systems	USA	cég	http://www.cisco.com/security/	*	*	
Cisco-PSIRT	Cisco Systems Product Security Incident Response Team	USA	cég		*	*	*
Citigroup CIRT	Citigroup CIRT	USA	cég		*	*	*
CLCERT	Chilean Computer Emergency Response Team	Chile	.cl alatti felhasználók, szervezetek	http://www.clcert.cl/		*	
CNCERT/CC	National Computer Network Emergency Response Technical Team / Coordination Center of China	Kína	.cn domain	http://www.cert.org.cn/	*	*	
ComCERT	Commerzbank CERT	Németország	banki	http://www.commerzbank.com/	*	*	*
Cornell Univ					*		
CounterCERT	Counterpane First Team	USA	multi cég	http://www.counterpane.com		*	
CSE	Communications Security Establishment	Kanada	cég	http://www.cse-cst.gc.ca/en/about_cse/about_cse.html	*	*	
CSIRT ABM AMRO REAL					*		
CSIRT Santander Banespa					*		
CSIRT Unicamp					*		
CSIRT USP					*		
CSIRT.DK	Danish Computer Security Incident Repsonse Team	Dánia	TeleDenmark felhasználói	http://www.csirt.dk/	*	*	*
CTR/DPF					*		
CYPRUS	Cyprus Academic Research Network	Ciprus	akadémiai hálózat		*		*
DANCERT	Delivery of Advanced Network Technology to Europe, Ltd.	EU	Európai kutatói hálózata	http://www.dante.net/safeflow.html	*	*	*
dbCERT	Deutsche Bank Computer Emergency Response Team	Németország	banki	http://www.db.com/	*	*	
dCERT	debis Computer Emergency Response Team	Németország	cég		*	*	*
DFN-CERT	DFN-CERT	Németország	nemzeti	http://www.cert.dfn.de/eng/	*	*	*
DIRT	DePaul Incident Response Team	USA	felsőoktatás	http://dirt.depaul.edu/	*	*	
DK-CERT	Danish Computer Emergency Tam	Dánia	nemzeti	http://www.cert.dk/	*	*	*
DND CIRT	Department of National Defence	Kanada	minisztériumi	http://www.first.org/about/organization/teams/dnd_cirt/	*	*	
DoD-CERT	US Department of Defense CERT	USA	Védelmi Minisztérium	http://www.cert.mil/	*	*	
E-CERT	Energis Computer Emergency Response Team	Nagy-Britannia	cég	http://cert.energis2.net/	*	*	*
EDS	EDS	USA	cég	http://www.eds.com/	*	*	
EForensics	eForensics	USA	ügyészség?		*	*	

Név	Hivatalos név	Ország	Típus	Webcím	CERT/CC	FIRST	TI
ELN-FIRST					*		
EnCIRT	Encase Computer Incident Response Team	USA	cég	http://www.GuidanceSoftware.com		*	
ESACERT	ESA Computer and Communications Emergency Response Team	Olaszország	EU űrkutatás	http://www.esacert.esa.int		*	*
EsCERT-UPC	CERT for Technical University of Catalunya	Spanyolország	felsőoktatás	http://escert.upc.es/	*	*	*
ETISALAT-CERT	ETISALAT Computer Emergency Response					*	
EUCS-IRT	University of Edinburgh	Nagy-Britannia	felsőoktatás		*		*
FCC CIRT					*		
FedCIRC					*		
Foundstone	Foundstone FIRST Team	USA	cég		*	*	
FRS-CERT	Federal Reserve System National Incident Response Team	USA	szervezet	http://www.frsnirt.org/	*	*	
FSC-CERT	CERT of Fujitsu-Siemens Computers	Németország	cég		*	*	
FUNet CERT	Finnish University and Research Network CERT	Finnország	akadémiai hálózat	http://www.csc.fi/suomi/funet/cert/index.html.en	*		*
GARR-CERT	GARR Network	Olaszország	akadémiai hálózat	http://www.cert.garr.it/	*		*
GD-AIS	General Dynamics – AIS	USA	cég			*	
GE					*		
GI REACT					*		
GIST	Google Information Security Team	USA	cég		*	*	
GNS-CERT	GNS-CERT	Németország	cégek	http://www.gnsec.net		*	*
Goldman Sachs	Goldman, Sachs and Company	USA	cég		*	*	
GOVCERT.NL	GOVCERT.NL	Hollandia	kormányzati	http://www.govcert.nl/	*	*	*
GRNET-CERT	Greek Research and Technology Network	Görögország	akadémiai hálózat	http://cert.grnet.gr	*		*
GTCERT	Georgia Institute of Technology CERT	USA	felsőoktatás	http://www.gatech.edu/itis/security/home.html	*	*	
Guardent					*		
HEANETCERT	HEANET CERT	Írország	akadémiai hálózat	http://www.heanet.ie/cert.html	*		*
HKCERT	Hong Kong Computer Emergency Response Team Coordination Centre	Kína	területi	http://www.hkcert.org	*	*	
HOUSECIRT	US House of Representatives Computer Incident Response Team	USA	képviselőház	http://www.house.gov/ushcert/	*	*	
HP SSRT	HP Software Security Response Team	USA	cég		*	*	
Hun-CERT	Hungarian Internet Service Provider	Magyarország	Internet szolgáltatók	http://www.cert.hu	*		*
IBM MSS	IBM Managed Security Services	USA	cég	http://www-1.ibm.com/services/continuity/recover1	*	*	
IBM-ERS	IBM Emergency Response Services, Europe	USA	cég	http://www.ers.ibm.com/	*		*
IDCERT					*		

Név	Hivatalos név	Ország	Típus	Webcím	CERT/CC	FIRST	TI
IIJ-SECT	IIJ Group Security Coordination Team	Japán	Internet szolgáltató		*	*	
ILAN-CERT	Israeli Academic CERT	Izrael	akadémiai		*	*	*
IP+CERT	IP-Plus CERT	Svájc	cég	http://www.ip-plus.net/	*	*	*
IRIS-CERT	IRIS-CERT	Spanyolország	kutatói hálózat	http://www.rediris.es/cert/	*	*	*
IRS CIRT	IRS (Internal Revenue Service) Computer Security Incident Response Team	USA	cég		*	*	
Isnet CERT		Izland		http://www.cert.isnet.is/			*
ISS	ISS	USA	cég (biztonság)		*	*	
IU-CERT	Indiana University CERT	USA	felsőoktatás	http://www.itso.iu.edu/	*	*	
JANET-CERT	JANET-CERT	Nagy-Britannia	akadémiai hálózat	http://www.ja.net/CERT/cert.html	*	*	*
JPCERT/CC	JPCERT Coordination Center	Japán	Internet közösség	http://www.jpcert.or.jp/	*	*	
JPMC CIRT	JPMorgan Chase Computer Incident Response Team	USA	cég		*	*	
JSOC	Japan Security Operation Center	Japán	cég	http://www.lac.co.jp/security/	*	*	
KCSIRT	KENNISNET CSIRT	Hollandia	iskolai hálózat		*	*	*
KMD IAC	KMD Internet Alarm Center	Dánia	cég	http://www.kmd.dk/	*	*	*
KPN-CERT	Computer Emergency Response Team of KPN	Hollandia	cég	http://www.kpn-cert.nl	*	*	*
KrCERT/CC	CERT Coordination Center – Korea	Korea	országos	http://www.certcc.or.kr/	*	*	
LITNET CERT	LITNET CERT	Litvánia	akadémiai hálózat	http://cert.litnet.lt	*	*	*
LuxCERT		Luxemburg	országos	http://www.cert.lu/	*		*
MARCERT					*		
MCI	MCI, Inc.	USA	cég			*	
MCIRT	Metavante Computer Incident Response Team	USA	cég		*	*	
MCIWorldCom					*		
Micro-BIT	Micro-BIT Virus Center	Németország	felsőoktatás		*	*	
MIT Network Security	Massachusetts Institute of Technology Network Security Team	USA	felsőoktatás	http://web.mit.edu/net-security/	*	*	
MLCIRT	Merrill Lynch Computer Security Incident Response Team	USA	cég		*	*	*
MODCERT	MOD Computer Emergency Response Team	Nagy-Britannia	védelmi minisztérium	http://www.mod.uk/cert/	*	*	*
MOREnet					*		
Motorola					*		
MSCERT	Microsoft Product Support Services Security Team	USA	cég	http://www.microsoft.com/technet/security/	*	*	
mtCERT		Málta	cég				*
MYCERT	Malaysian Computer Emergency Response Team	Malajzia	országos	http://www.mycert.org.my/	*	*	

Név	Hivatalos név	Ország	Típus	Webcím	CERT/CC	FIRST	TI
NAI					*		
NARIS					*		
NASIRC	NASA Incident Response Center	USA	ügynökség	http://www-nasirc.nasa.gov/	*	*	
NAVCIRT	Naval Computer Incident Response Team	USA	Tengerészeti minisztérium	http://infosec.nosc.mil/	*	*	
NBSO/Brazillian CERT	NIC BR Security Office - Brazilian Computer Emergency Response Team	Brazília	országos	http://www.nbso.nic.br/	*	*	
NCIRC CC	NATO Computer Incident Response Capability - Coordination Center	Belgium	NATO			*	
N-CIRT					*		
NCSA-IRST	National Center for Supercomputing Applications IRST	USA	kutatóközpont	http://www.ncsa.uiuc.edu/people/ncsairst/	*	*	
NIHIRT	NIH Incident Response Team	USA	egészségügyi		*	*	
NIIF-CSIRT	Hungamet CERT	Magyarország	akadémiai hálózat	http://csirt.niif.hu	*		*
NIRT	National Incident Response Team, Cabinet Secretariat	Japán	kormányzati és kritikus infrastruktúra	http://www.bits.go.jp/	*	*	
NIST	NIST IT Security	USA	szabványügyi hivatal		*	*	
NN FIRST Team	Nortel Networks FIRST Team	Kanada	cég	http://nortelnetworks.com		*	
NORDUnet	NORDUnet	Dánia	skandináv kutatói hálózat	http://www.nordu.net/	*	*	*
NU-CERT	Northwestern University	USA	felsőoktatás	http://grumpy.acns.nwu.edu/nu-cert/	*	*	
NUSCERT	NUS Computer Emergency Response Team	Szingapúr	felsőoktatás	http://security.nus.edu.sg/	*	*	
OGCBS	Executive Agency of the Office of Government Commerce	Nagy-Britannia		http://www.ogcbuyingsolutions.gov.uk/	*		*
Ontario IPC	Ontario Information Protection Centre	Kanada	tartományi kormányzat			*	
ORACERT	Oracle Global Incident response Team	US	cég		*	*	
OS-CIRT	Open Systems AG Computer Incident Response Team	Svájc	cég	http://www.open.ch/	*	*	*
OSU-IRT	the Ohio State University Incident Response Team	USA	felsőoktatás		*	*	
OxCERT	Oxford University IT Security Team	Nagy-Britannia	felsőoktatás	http://www.ox.ac.uk/it/compsecurity/oxcert/	*	*	*
PAKCERT					*		
PCERT					*		
PERMALAN	perComp Malware Analysis Team	Németország	cég	http://www.percomp.de		*	
PHCERT					*		
POL34-CERT	Polish Scientific Broadband Network CERT	Lengyelország	akadémiai	http://cert.pol34.pl	*		*
PRE-CERT	PRE-CERT	Németország	cég	http://www.pre-secure.de/	*	*	*
PruCERT					*		
PSU	Pennsylvania State University	USA	felsőoktatás		*	*	
Q-CIRT	QinetiQ Computer Incident Response Team	USA	cég?	http://www.qinetiq.com/	*	*	*

Név	Hivatalos név	Ország	Típus	Webcím	CERT/CC	FIRST	TI
RADIANZ	RADIANZ	USA	cég	http://www.radianz.com/	*	*	
RBC FG CSIRT	RBC Financial Group CSIRT	Kanada	banki	http://www.radianz.com/	*	*	
RBSG	Royal Bank of Scotland, Investigation and Threat Management	Nagy-Britannia	banki	http://www.rbs.co.uk/		*	
RHNet CERT		Izland	felsőoktatás		*		*
RM CSIRT	ROYAL MAIL CSIRT CC	Nagy-Britannia	posta			*	
RU-CERT	Computer Security Incident Response Team RU-CERT	Oroszország	országos	http://www.cert.ru/Eng/	*	*	*
RUS-CERT	Rechenzentrum Universitat Stuttgart CERT	Németország	egyetemi	http://cert.uni-stuttgart.de/	*	*	*
Rutgers CIRT					*		
SAIC-IRT	Science Applications International Corporation - Incident Response Team	USA	cég			*	
SBACERT	Small Business Administration	USA			*	*	
SBS	Secure Business Services	Nagy-Britannia	British Telecom	http://www.btignitesolutions.com/solutions/securit		*	
S-CERT	CERT of the German Savings Banks Organization	Németország	banki	http://www.s-cert.de/	*	*	*
Secu-CERT	SECUNET CERT	Németország	cég		*	*	*
SGI	Silicon Graphics, Inc.	USA	cég	http://www.sgi.com/support/security/	*	*	
SIAPI-CERT	Siapi Networks Eleno, Morell & Sanchez Asociados S.L		cég		*		*
SI-CERT	Slovenian CERT	Szlovénia	akadémiai hálózat	http://www.arnes.si/en/si-cert/	*	*	*
Siebel	Siebel Security Team	USA	cég		*	*	
Siemens-CERT	Siemens-CERT	Németország	cég		*	*	*
SingCERT	Singapore CERT	Szingapúr	országos	http://www.singcert.org.sg/	*	*	
SITIC	Swedish IT Incident Centre	Svédország		http://www.sitic.se	*		*
SPRINT	SPRINT	USA	cég		*	*	
Stanford	Stanford University Information Security Services	USA	felsőoktatás	http://security.stanford.edu/		*	
SUN	Sun Microsystems, Inc.	USA	cég		*	*	*
SUNet-CERT	SUNet-CERT	Svédország	felsőoktatási hálózat	http://www.cert.sunet.se/	*	*	*
SUNSet					*		
SURFnet-CERT	SURFnet-CERT	Hollandia	kutatói hálózat	http://cert.surfnet.nl/	*	*	*
SWISS ReCERT					*		
SWITCH-CERT	Swiss Education and Research Network CERT	Svájc	akadémiai hálózat	http://www.switch.ch/cert/	*	*	*
SymCERT	Symantec Computer Emergency Response Team	USA	cég	http://www.symantec.com/	*	*	
T-Com-CERT	Deutsche Telekom AG CERT	Németország			*		*
TDBFG CSIRT	TDBFG Computer Security Incident Response Team	Kanada	banki			*	

Név	Hivatalos név	Ország	Típus	Webcím	CERT/CC	FIRST	TI
Telekom-CERT	Internal CERT for Deutsche Telekom	Németország	cég		*	*	*
TeliaCERTCC					*		
TESIRT	TELMEX Security Incident Response Team	Peru	országos	http://www.telmex.com/pe/tesirt/		*	
ThaiCERT					*		
TRCERT		Törökország	kormányzat		*		*
TS/ICSA FIRST	TruSecure Corporation					*	
TS-CERT	TeliaSoneraCERT CC	Svédország	cég			*	*
TWCERT/CC	Taiwan Computer Emergency Response Team/Coordination Center	Taiwan	országos	http://www.cert.org.tw/	*	*	
TWCIRC					*		
U.S. Coast Guard CIRT					*		
UB-FIRST	UB-First	USA	felsőoktatás	http://www.buffalo.edu/	*	*	
UCERT	Unisys CERT	USA	cég		*	*	
Uchicago Network Security	The University of Chicago Network Security Center	USA	felsőoktatás	http://security.uchicago.edu/	*	*	
UGaCIRT	The University of Georgia Computer Incident Response Team	USA	felsőoktatás	http://www.uga.edu/compsec/	*	*	
UNAM-CERT	UNAM-CERT	Mexikó	felsőoktatás	http://www.unam-cert.unam.mx/	*	*	
UNINETT CERT	UNINETT CERT	Norvégia	felsőoktatás	http://cert.uninett.no/	*	*	*
UNIRAS	HM Government CERT / UK National Infrastructure Security Co-ordination Centre (NISCC)	Nagy-Britannia	kormányzati	http://www.uniras.gov.uk/	*	*	*
US-CERT	United States Computer Emergency Readiness Center	USA	nemzeti infrastruktúra	http://www.us-cert.gov	*	*	
USPS	United States Postal Service Computer Incident Response Team	USA	posta		*	*	
UU-IRT	Universitet Uppsala Incident Response Team	Svédország	felsőoktatás	http://www.irt.uu.se	*		*
UvA-CERT	University of Amsterdam, Informatiseringscentrum	Hollandia	felsőoktatás	http://ic.uva.nl/cert/	*		*
VeriSign	VeriSign	USA	cég		*	*	
VISA-CIRT	VISA-CIRT	USA	cég		*	*	
WebPlus ISP	WebPlus Internet Serrvice Provider	Oroszország	cég	http://support.wplus.net/security/	*		*
WFCSIRT	Wells Fargo Computer Security Incident Response Team	USA	banki	http://www.wellsfargo.com/	*	*	

Táblázat 8. Külföldi CERT-ek adatai

10.9 A Szervezet beosztottjai

A személyek feladatairól részletek a 3. fejezetben találhatók.

Beosztás	Személy	Elérési adatok	Megjegyzés
Vezér 1. (ügyvezető igazgató):			
Adminisztráció 1. (titkárság):			
Biztonsági 1. (biztonsági felelős):			
Gazdasági 1. (gazdasági felelős):			
Műszaki 1. (műszaki felelős):			
Műszakvezető 1-2. (műszakvezető éjjel/nappal):			
Operátor 1-2. (és 1'-2' operátor csapatok):			heti beosztástól függő, hogy ki melyik csapatban van

Táblázat 9. Beosztásokat betöltő személyek adatai

10.10 Szakértők és szakemberek listája

A szakértők és szakemberek szerepéről részletek a 3.2 fejezetben találhatók. A szakterület- és a névszerinti táblázatok a következők:

Szakterület	Személy	Elérési adatok	Megjegyzés

Táblázat 10. Szakértők és szakemberek szakterület szerinti listája

Személy	Szakterület	Elérési adatok	Megjegyzés

Táblázat 11. Szakértők és szakemberek névszerinti listája

10.11 Külső tanfolyamok és vizsgák

A következő táblázat a biztonsági szakemberek részére megszerezhető, nevezetesebb bizonyítványokat[23] mutatja be (a szürkék gyártófüggők), és azt jelzi, hogy ezek közül a Szervezet mit tart támogatandónak (T), javasoltnak (J) vagy előnyösnek (E):

Kiállító	Bizonyítvány neve	Szervezet hozzáállás
Brainbench	Internet Security Network Security Security Industry Knowledge	
American Society for Industrial Security (ASIS)	Certified Protection Professional	
Computing Technology Industry Association	Security+	
Information System Audit and Control Association (ISACA)	CISA (Certified Information System Auditor)	
International Webmaster Association (IWA)	Certified Web Professional (CWP) Security Specialist CIW Security Analyst	
Information Systems Security Certifications Consortium	Certified Information Systems Security Professional (CISSP) System Security Certified Practitioner (SSCP)	
SANS Institute	GIAC Security Essentials Certification (GSCE) GIAC Security Engineer (GSE)	
Security Certified Program	Security Certified Network Professional (SCNP) Security Certified Network Architect (SCNA)	
TruSecure	TruSecure ICSA Certified Security Associate (T.I.C.S.A.) TruSecure ICSA Certified Security Expert (T.I.C.S.E.)	
Checkpoint	Certified Security Administrator (CCSA) Certified Security Expert Plus (CCSE Plus)	
Cisco	Cisco Security Specialist	
IBM/Tivoli	IBM SecureWay Firewall for Win NT	
Microsoft	MCP Exam 70-220: Security Design MCP Exam 70-227: Installing… ISA server…	
RSA's Certified Security Professional Program	RSA Certified Administrator (RSA/CA) RSA Certified System Engineer (RSA/CSE) RSA Certified Instructor (RSA/CI)	
Symantec Certification Program	Symantec Product Specialist (SPS) Symantec Certified Security Engineer (SCSE) Symantec Certified Security Practitioner (SCSP)	

Táblázat 12. Tanfolyam- és vizsgabizonyítványok és kiadó szervezetek

[23] Itthon elérhető még az NJSZT (többféle), az NHH (digitális aláírás) és az Igazságügyi (többféle) szakértői igazolvány megszerzése. Ezek közül az utóbbi megszerzése támogatott, a többi előnyt jelent egy alkalmazott számára.

11 Rövidítések, fogalmak

Az egyes szakkifejezések megtalálhatók a Fogalomtárban (http://www.fogalomtar.hu). Az anyagban szereplő kifejezések és rövidítések:

3DES – (Triple) Data Encryption Standard
AirCERT – Automated Incident Reporting CERT
APCERT – Asia-Pacific CERT
ASCII – American Standard Code for Information Interchange
CACS – Computer Audit, Control and Security Conference
CAIF – Common Advisory Interchange Format
CB – Common Band (radio)
CC, BCC – Carbon copy, Blind carbon copy
CERT – Computer Emergency Response Team
CERT/CC – Computer Emergency Response Team / Coordination Center
CET – Central European Time
CGI – Common Gateway Interface
CISA – Certified Information Systems Auditor
CMS – Cryptographic Message Syntax
CSIRT – Computer Security Incident Response Team
CVE – Common Vulnerabilities and Exposures
DARPA – Defense Advanced Research Projects Agency
DH – Diffie-Hellman
DoS, DDoS – Denial of Services, Distributed Denial of Services
DSA – Digital Signature Algorithm
EGC – European Group of CERTs
EISPP – The European Information Security Promotion Program
ENISA – European Network and Information Security Agency
FAQ – Frequently Asked Questions
FIRST – Forum of Incident Response and Security Teams
GIAC – Global Information Assurance Certification
GPG – GNU Privacy Guard
GYIK – Gyakran Ismételt Kérdések
HTML – HyperText Markup Language
HTTP – HyperText Transfer Protocol
IBRS – Informatikai Biztonsági RészStratégia
IDMEF – Intrusion Detection Message Exchange Format
IDS – Intrusion Detection System
IDWG – IETF Intrusion Detection Workgroup
IETF – Internet Engineering Task Force
INCH WG – IETF Incident Handling Working Group
IODEF – Incident Object Description and Exchange Format
IP – Internet Protocol

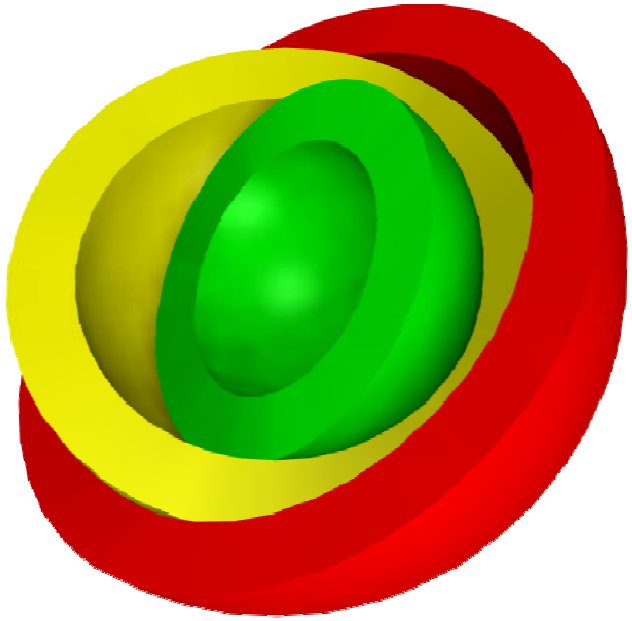
ISACA – Information Systems Audit and Control Association
ISC – Internet Storm Center
IT – Information Technology
MIBÉTS – Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma
MIME – Multipurpose Internet Mail Exchange
MITS – Magyar Információs Társadalom Stratégia
MTA – Mail Transport Agent
NCSD – National Cyber Security Division
NIIF – Nemzeti Információs Infrastruktúra Fejlesztési Program
PGP – Pretty Good Privacy
PIN – Personal Identification Number
PPP – Public-Private Partnership
RAID – Redundant Array of Inexpensive Disks
RFC – Request For Comments
RSA – Ron Rivest, Adi Shamir, Leonard Adleman
RTIR – Request Tracker for Incident Response
SANS – SysAdmin, Audit, Network, Security Institute
SHA-1 – Secure Hash Algorithm 1
SNML – Simple Network Markup Language
SQL – Structured Query Language
TERENA – Trans-European Research and Education Networking Association
URL – Uniform Resource Locator
VPN – Virtual Private Network
XML – eXtensible Markup Language

* * *

Hálózati incidenskezelés

oktatási anyag

2006 május



Az oktatási anyag kidolgozásában és lektorálásában részt vettek: *Becz Tamás, Pásztor Szilárd, Rigó Ernő, Tiszai Tamás, Tóth Beatrix*

1 Bevezetés

Jelen dokumentum egy – a hálózati incidenskezelés témakörében kidolgozott – oktatási anyaghoz kapcsolódó előadási bemutató-anyag, illetve a bemutató megtartásához, valamint az egyes oldalak értelmezéséhez segítséget nyújtó megjegyzések gyűjteménye.
Maga az oktatási anyag egy összesen 6 órányi előadást tartalmazó tanfolyam – tutorial – keretei között megismertethető, a hálózati incidenskezelés területén meglehetősen széles ismereteket közlő tananyag. A vetíthető ábrákon bemutatott tananyag a következő főbb fejezetekre oszlik:

- Bevezetés
- Az internetes veszélyeztetettségről

  A veszélyeztetettségek alapvető fogalmait taglaló, a későbbiekben hivatkozott fogalmakat bevezető és értelmező fejezet.
- Magyar és nemzetközi CSIRT-ek

  A hálózati incidenskezeléssel foglalkozó speciális szervezetek – CERTek, CSIRTek – feladatait ismertető, a meglévő ilyen szervezetek jellemzői bemutató fejezet.
- Hálózatbiztonsági szabványok

  A speciális szakterület és a kapcsolódó rokon területek legelterjedtebb szabványait, azok logikai felépítését és egymáshoz viszonyított kapcsolatait bemutató fejezet.
- Megelőző intézkedések
  - 1. rész: Technológia

    A hálózati incidensek elkövetése során felhasznált és támadott alapvető megoldások, protokollok, valamint a támadások esélyét csökkentő megelőző intézkedések körét számbavevő fejezet.
  - 2. rész: Audit és management

    A hálózati incidensek felfedését, az esetleges incidensek megelőzését biztosító módszereket, eszközöket, eljárásokat bemutató fejezet.
  - 3. rész: Visszaható intézkedések

    Az incidensek következményeit mérséklő, illetve bekövetkezésüket speciális megoldásokkal elhárító vagy lassító eszközök alapjait bemutató fejezet. Itt kerül ismertetésre néhány olyan eszköz és módszer is, amely a bekövetkezett incidensek kezelését, a nyomok rögzítését, dokumentálását célozza.

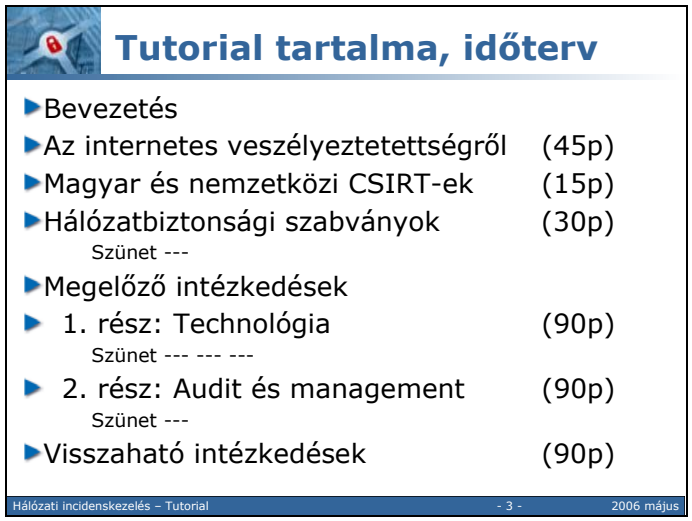
Az itt következő előadási anyag tényleges felhasználhatóságát, érthetőségét és előadásához szükséges valódi időtartam ellenőrzését a szakterület elismert, évtizedes hagyományokkal rendelkező éves konferenciája – a Network Shop – 2006. évi rendezvénye során tartott Tutorial szekció keretében megtartott előadáson ellenőriztük. Tapasztalataink szerint a csaknem 200 oldalnyi vetíthető ismeretanyag a hallgatóság elismerését vívta ki, amely alapján feltételezhető, hogy más, a szükséges számítógéphálózati alapismeretekkel rendelkező érdeklődő közönség számára is hasznos információkat tartalmaz.

1.

A tutorial célja, hogy áttekintést adjon a kis és közepes méretű, Internet-eléréssel is rendelkező, IP alapú hálózatok fizikai és management-szintű védelmi lehetőségeiről, valamint az üzembe állított védelmi és behatolásérzékelő rendszerek által felfedett incidensek kezeléséről. Az előadás során kitérünk az incidensek nyomán esetlegesen hátramaradó információk, bizonyítékok gyűjtésének és elemzésének módszereire is.

2.

3.



Bevezetés
– rövid tartalmi áttekintés, időzítés ismertetése

Az internetes veszélyeztetettségről
-- mit is nevezünk veszélyeztetettségnek
-- forrásai, céljai, módszerei definíciói

Magyar és nemzetközi CSIRT-ek
-- fogalom értelmezése, jelentése, régi és új rövidítések
-- CSIRT-ek szerepe, feladataik
-- más nemzetközi szervezetek

Hálózatbiztonsági szabványok
-- milyen ajánlások születtek a világban eddig a tématerületen
-- BS7799, Common Criteria, Cobit, stb.

Megelőző intézkedések
-- mit tehetünk előzetesen a veszélyeztetettség elkerülésére

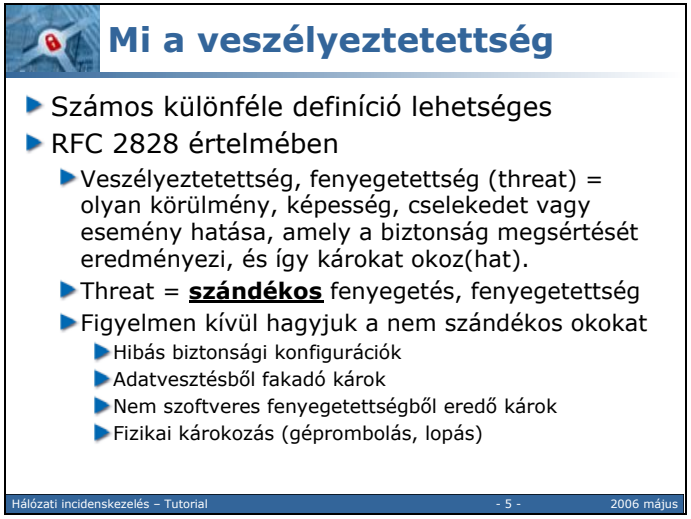
1. rész: Technológia
-- forgalomszűrés, tűzfalak szerepe
-- titkosítás, hitelesítés
-- jogosultságellenőrzés, hozzáférésvédelem

2. rész: Audit és management
-- önmegtámadás, önellenőrzés (Nessus)
-- szoftverfrissítés, verziókövetés
-- célszerű fizikai/logikai struktúra megválasztása
-- adminisztratív eszközök, elosztott biztonsági szolgáltatások

Visszaható intézkedések
-- behatolásjelzés (Honeynet, Snort)
-- forensic eszközök és alkalmazásuk
-- incidenskezelő rendszerek (RT-IR)

4.

5.



Számos különféle definíció lehetséges, amelyek a fenyegetettséget (threat) különféle szempontból definiálják

Az RFC 2828 (Internet Security Glossary, 2000) a fenyegetettséget is definiálja.

Hosszabban kifejtve: olyan körülmény, képesség, cselekedet vagy esemény hatása, amely a biztonság megsértését eredményezi, és így károkat okozhat.

Röviden: támadás az (informatikai) biztonság ellen.

Jelen esetben csak a szándékos fenyegetettségeket vizsgáljuk

Figyelmen kívül hagyjuk a nem szándékos (és nem informatikai) fenyegetettségeket:

-- hibás konfiguráció okozta problémák

-- adatvesztésből fakadó károk

-- nem szoftveres fenyegetettségek, pl. villámcsapás, áramkimaradás

-- fizikai károkozás, géprombolás, adathordozó lopás

6.

Veszélyek osztályozása

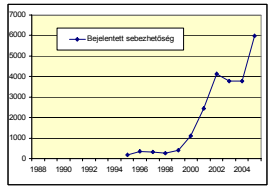
- Sok különféle besorolás létezik, tekintsünk egy viszonylag egyszerű osztályozást:
  - Tényleges veszélyeztetettség
    - Szerverek, tűzfalak, egyéb programok már felfedett veszélyeztetettségei (nyilvánosan ismert hibák)
      - Az okozott kár mértéke alapján további csoportosítás is ismert
  - Potenciális veszélyeztetettség
    - Rejtett (nem ismert) veszélyeztetettségek
      - Általában csak penetráció tesztekkel fedezhetők fel
      - Ha rendszerünket teljesen ismernénk, tényleges veszélyek lennének
  - Információs veszélyeztetettség
    - A rendszer mikéntjéről begyűjthető adatok (info leakage)
      - Futó szolgáltatások, IP-címek, portok, oprendszer verziók, stb.
      - A rendszer fontos részleteire lehet belőlük következtetni
      - Későbbi támadásokhoz adatokat szolgáltathat

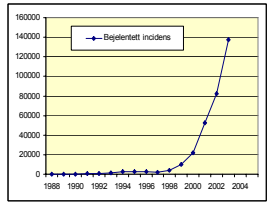
7.

Fontos ez a probléma? (1)

- A fenyegetettségek száma meredeken nő (forrás: CERT/CC)
- A felkészülési idő gyorsan csökken

  (egyre hamarabb kihasználják a felismert hibát)





Szükséges-e a hálózati biztonság kérdésével foglalkozni. Néhány beszédes adat:

A felismert támadási lehetőségek száma meredeken emelkedik.

A bejelentett incidensek száma exponenciálisan nő, miközben egy-egy incidens egyre több gépet érint(het). Vagyis az alsó ábrán látható görbe NEM a megtámadott gépek számát, hanem a bejelentett incidensek számát jelzi, miközben egy incidens sokszor gépek százait-ezreit érinti.

A sebezhetőség felismerése/publikálása, majd az ezt kihasználó támadás bekövetkezése között eltelt idő (a felkészülési idő) gyorsan csökken. Korábban ez

8.

Fontos ez a probléma? (2)

- Adatok egy konkrét hálózat vizsgálatáról:
  - 438 gép automatikus biztonsági ellenőrzése
  - 1676 súlyos biztonsági hiba (3,8 / gép)
  - 3192 biztonsági rés (7,2 / gép)
- Ugyanezen hálózat forgalmi elemzése:
  - Egyértelmű, automatikus támadás: 700.000/hó
  - IP címenkénti próbálkozás: 66/óra
  - Sebezhetőség típusonkénti próbálkozás: 20/óra
- **Célkitűzés:** a fenyegetettség megszüntetése, de legalább jelentős csökkentése

Hálózati incidenskezelés – Tutorial - 8 - 2006 május

A SZTAKI hálózatának automatikus eszközökkel (Nessus) végrehajtott egy korábbi vizsgálata rengeteg már ismert sebezhetőség jelenlétét tárta fel. A 438 gépen a dián látható számú súlyos biztonsági hiba, illetve kevésbe veszélyes biztonsági rés volt detektálható. A vizsgálat során az automata a hálózatra vonatkozó semmilyen előzetes információval nem rendelkezett, vagyis egy hacker/cracker által végrehajtott intelligens (ember általi) támadás során a „siker” szinte bizonyos.

A forgalom elemzése (Snort) azt mutatta, hogy a hálózatot havi több száz ezer automatikus, robotok által végrehajtott, egyértelműen azonosítható támadás éri.

A támadások feloszthatók egyrészt a támadás tárgya (IP cím, vagyis konkrét gép), másrészt a támadás módja (a kihasználni szándékozott biztonsági hiba) alapján.

Mindezek alapján kijelenthető: a problémát kezelni kell!!!

9.

Mit tehetünk?

Védekezzünk!

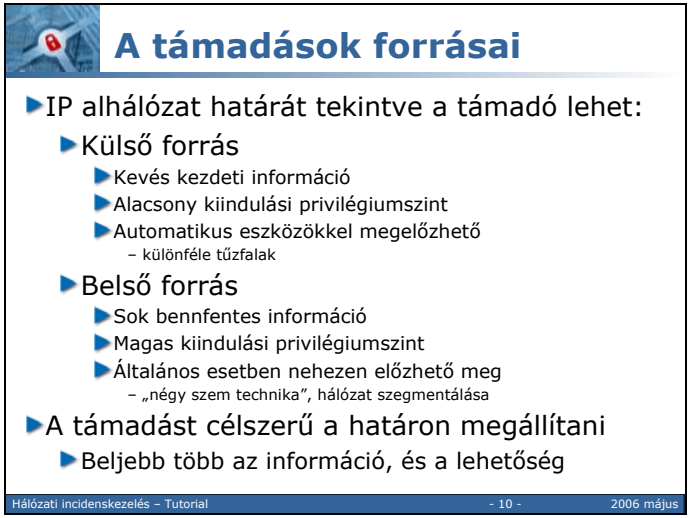
- A védekezés érdekében ismernünk kell
  - A támadások forrásait
  - A támadások céljait
  - A támadások törvényszerűségeit
  - A támadások módszereit és eszközeit
  - A támadások kockázatát

A fentiek ismeretében, a rendszerezés után tehetünk megelőző, szisztematikus lépéseket a fenyegetettségek mérséklésére, a káros hatások csökkentésére.

Hálózati incidenskezelés – Tutorial - 9 - 2006 május

Miről lesz szó... valahogy arról is kell beszélni, hogy ezek ellen a dolgok ellen „harcolunk”, és ehhez szeretnénk segítséget nyújtani az elkövetkező szekciókban.

10.



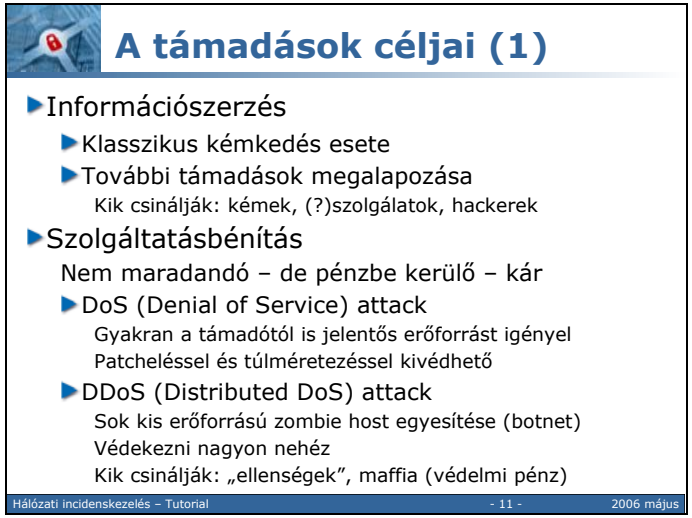
Egy általános értelemben vett, internetes kapcsolattal rendelkező, IP alapú hálózatot alapvetően két forrásból, a hálózat és az Internet közti határvonal szempontjából belső és külső csatlakozási pontról érhetnek támadások. E két forrás, vagy két szint közt az alapvető különbség a támadást kivitelező program vagy személy rendelkezésére álló információk mennyiségében és a támadás kiindulópontjául szolgáló rendszer vagy egyéb hálózati csatlakozási pont privilégiumszintjében rejlik.

A szakirodalomban ([SANSPenStud], [SANSPenTest]) az említett két szint (külső, belső) között még számos további átmeneti szintet is megkülönböztetnek, de végső következtetésként levonható, hogy a külső szintről a belső felé haladva az információmennyiség és a privilégiumszint is folyamatosan nő, vagyis a feltételezett támadó dolga folyamatosan egyszerűsödik, ebből következőleg a támadás által okozható kár mértéke és a károkozás kockázata folyamatosan növekszik.

Kevés olyan, speciálisan tervezett (például a katonai és komoly üzleti, banki körökben elterjedt, nem csak a számítástechnikában működőképes, „négy szem” technikát alkalmazó), rendszer létezik, ahol a legbelső szintre való behatolás nem ruházza fel teljes jogkörrel a támadó szoftvert vagy személyt, ezért célszerű a támadást lehetőleg a külső szinten megakadályozni.

Az előzőekben leírtakból következőleg azért is érdemes a külső szintre koncentrálni, mert az ott alkalmazható alapvető támadási módszerek befelé haladva csak bővülnek, a védekezési módszerek csak fogynak, azzal a kiegészítéssel, hogy befelé haladva a védekezések hatékonysága, a támadásokkal ellentétes arányban, folyamatosan csökken a támadások számára rendelkezésreálló információ mennyiségének növekedése miatt.

11.



A támadások sosem céltalanok, mindig a támadó hasznát és szándékait szolgálják. A célokat a következőképp csoportosíthatjuk:

Információszerzés

A legtöbb támadás során előfordul, hogy a támadás indítója új információkhoz jut a támadott rendszerrel kapcsolatban: ha mást nem tud meg, legalább azt, hogy a kipróbált támadási forma sikerrel járt-e az adott rendszeren, vagy nem, sok esetben ez is fontos információ lehet. Az információszerzés ilyen esetekben általában a további támadások előkészítését segíti és általában a támadó saját céljait szolgálja.

Előfordul azonban az is, mikor a megszerzett információ nem a támadó saját céljait, hanem megbízójának, vagy leendő vásárlójának céljait szolgálja, ilyenkor az információszerzés által okozott kár közvetlenebbé válik, ez a klasszikus kémkedés esete.

Szolgáltatásbénítás

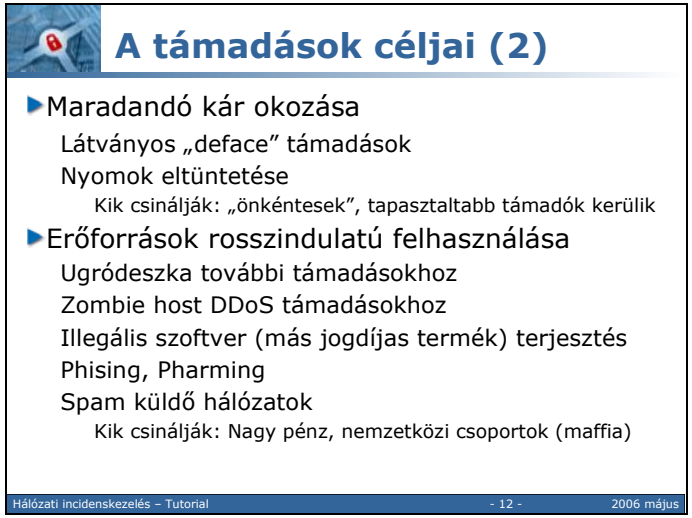
A szolgáltatásbénításról (Denial of Service, DoS) beszélhetünk úgy is, mint közvetlen hatásait tekintve átmeneti károkozásról. Általában akkor használják, ha maradandó károkozásra nincs könnyű mód, mivel általában a szolgáltatásbénítás az egyszerűbb műveletek közé tartozik.

Az ilyen esetekben a támadó célja a támadott rendszer – általában – publikus szolgáltatásainak használhatatlanná tétele mások számára. Ez egyszerű esetben okozhatja például egy weboldal elérhetetlenségét, de összetettebb helyzetben a támadó számára új lehetőségek nyílhatnak további támadások véghezvitelére (például egy azonosító, hitelesítő szolgáltatás bénítása esetén).

A szolgáltatásbénításos támadások során nem ritkán előfordul, hogy a támadás erőforrásigénye messze alatta marad a megtámadott rendszer által felemésztett erőforrásoknak (például kereséseket, bonyolult műveleteket indít egy távoli gépen), esetleg elegendő egyetlen támadás egy szolgáltatás végleges blokkolásához (ilyen volt az

egyes Intel processzorok „F00F bug” néven elhíresült hibája), ilyenkor egyszerűbb a támadó dolga. Ha azonban a megtámadott rendszer megfelelően nagy teljesítményű, és a támadás nem túl hatékony, elképzelhető, hogy a támadó rendszere önmagában nem képes a szolgáltatás teljes mértékű leterhelésére. Ilyen esetekben alkalmazzák az elosztott szolgáltatásbénítást (Distributed DoS, DDoS), melynek során a támadó több forrásgépről, azok teljesítményét összesítve, párhuzamosan indíthat támadást célja ellen.

12.



A maradandó károkozás általában a legnyilvánvalóbb eredményekkel járó támadási forma. Ezekben az esetekben a hiányzó adatok, a módosított tartalmú (ún. „deface”-elt) weboldal jórészt rögtön felfedezhetők, de előfordulnak kifinomultabb adatmegsemmisítési esetek is, mint például egy rendszer naplóbejegyzéseinek törlése, ahol az eltűnt információk nem feltétlenül éreztetik hiányukat. A tapasztaltabb támadók általában kerülik a maradandó károkozást (lásd.: . ábra), mivel ilyen esetekben a közvetlen haszon általában elhanyagolható, viszont nagy a felfedezés valószínűsége.

Erőforrások rosszindulatú felhasználása

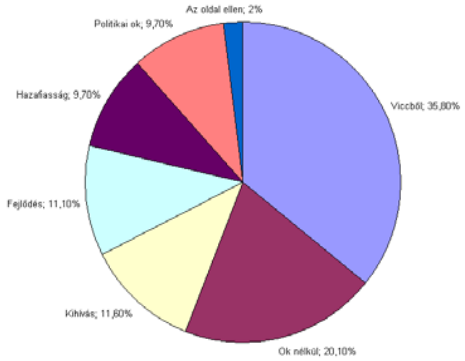
Ez a támadási forma azonosítható talán legkevésbé az élet más területein is elkövethető rosszándékú cselekedetekkel. A támadó mindenféle eltulajdonítás és közvetlen károkozás nélkül utasításainak követésére bír egy erőforrást (sok esetben egy egész hálózati hostról van szó). Az erőforrás jogos felhasználója általában fel sem fedezi a támadás sikerességét, a támadó pedig a birtokába jutott erőforrást elosztott szolgáltatásbénításra, kéretlen üzleti tartalmú levelek küldésére, jelszóadatbázisok feltörésére, megszemélyesítéses támadásokra vagy bármilyen más célra felhasználhatja.

Phising = social engineering egy formája, hamisított honlapon érzékeny információk begyűjtése

Pharming = DNS meghamisítása, hogy egy adott név ne a valódi gépre, hanem annak rosszindulatú másolatára mutasson

13.

Deface támadások okai



Forrás: zone-h.org

14.

A támadások törvényei (1)

- A támadásokkal kapcsolatban néhány törvényszerűség ismerhető fel

  Forrás: Qualys (www.qualys.com)

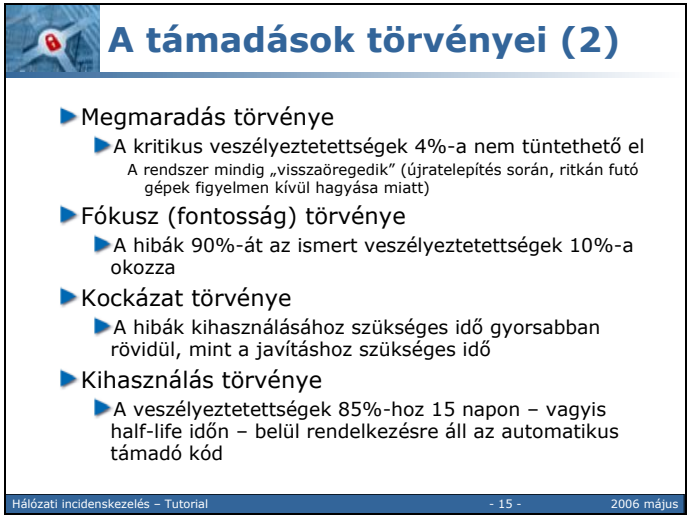
- Fél-élettartam (half-life) törvénye
  - A rendszerkomponensek felének patch-elési ideje

    Változás 2004-ről 2005-re

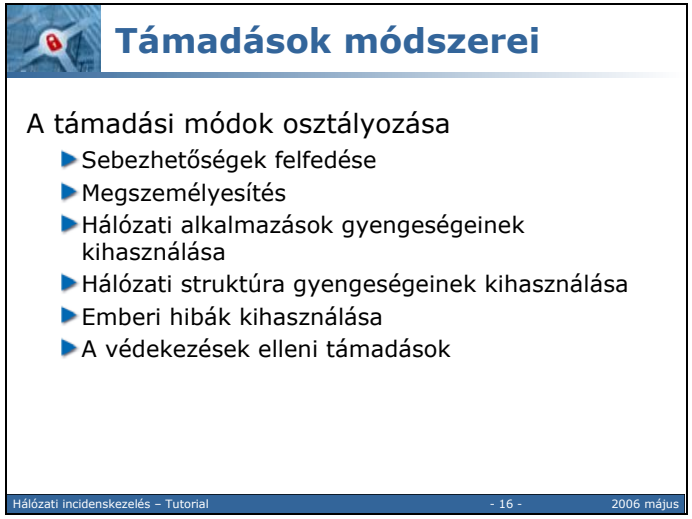
    külső rendszerek felének kijavítási ideje: 21 → 19nap

    belső rendszerek felének kijavítási ideje: 62 → 48nap
- Gyakoriság törvénye
  - Az elterjedt/súlyos veszélyeztetettségek 50%-át egy éven belül újak veszik át

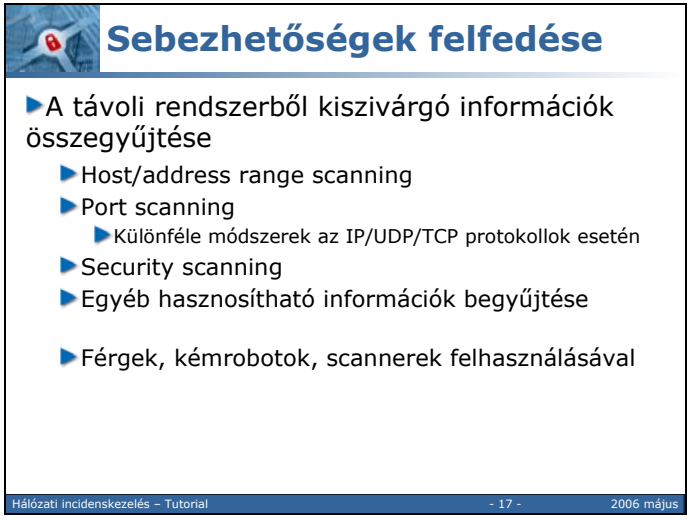
15.


A támadások törvényei (2)
Megmaradás törvénye
A kritikus veszélyeztetettségek 4%-a nem tüntethető el
A rendszer mindig „visszaöregedik” (újratelepítés során, ritkán futó gépek figyelmen kívül hagyása miatt)
Fókusz (fontosság) törvénye
A hibák 90%-át az ismert veszélyeztetettségek 10%-a okozza
Kockázat törvénye
A hibák kihasználásához szükséges idő gyorsabban rövidül, mint a javításhoz szükséges idő
Kihasználás törvénye
A veszélyeztetettségek 85%-hoz 15 napon – vagyis half-life időn – belül rendelkezésre áll az automatikus támadó kód
Hálózati incidenskezelés – Tutorial - 15 - 2006 május

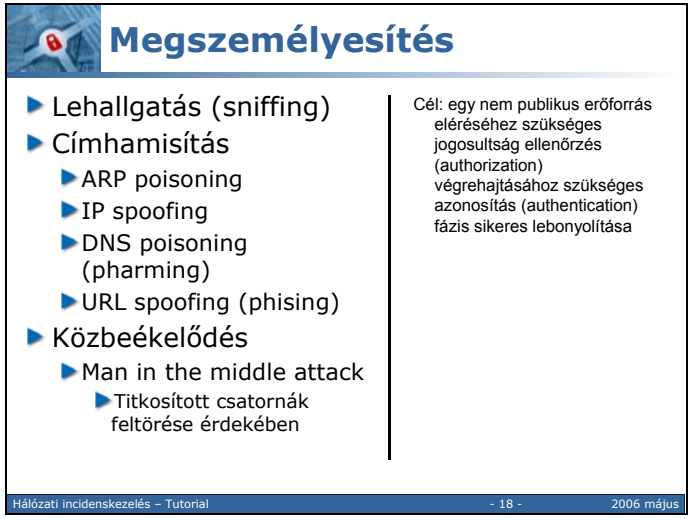
16.


Támadások módszerei
A támadási módok osztályozása
Sebezhetőségek felfedése
Megszemélyesítés
Hálózati alkalmazások gyengeségeinek kihasználása
Hálózati struktúra gyengeségeinek kihasználása
Emberi hibák kihasználása
A védekezések elleni támadások
Hálózati incidenskezelés – Tutorial - 16 - 2006 május

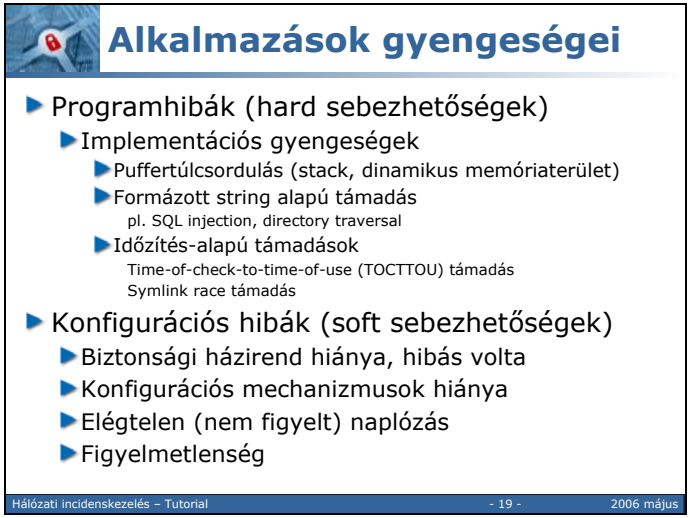
17.


Sebezhetőségek felfedése
A távoli rendszerből kiszivárgó információk összegyűjtése
Host/address range scanning
Port scanning
Különféle módszerek az IP/UDP/TCP protokollok esetén
Security scanning
Egyéb hasznosítható információk begyűjtése
Férgek, kémrobotok, scannerek felhasználásával
Hálózati incidenskezelés – Tutorial - 17 - 2006 május

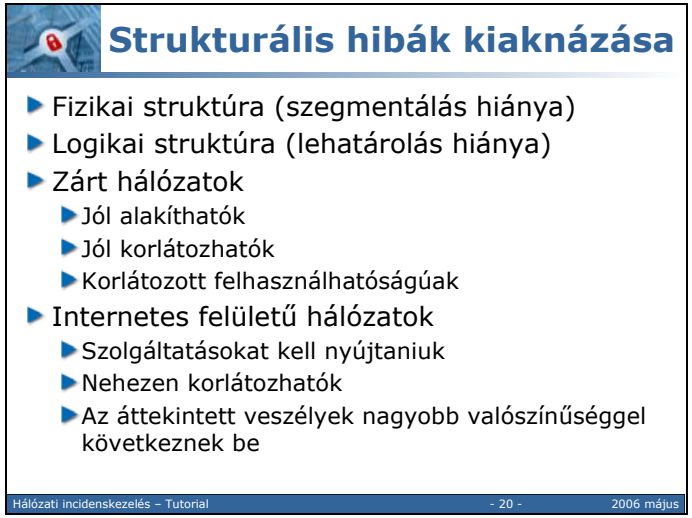
18.


Megszemélyesítés
Lehallgatás (sniffing)
Címhamisítás
ARP poisoning
IP spoofing
DNS poisoning (pharming)
URL spoofing (phising)
Közbeékelődés
Man in the middle attack
Titkosított csatornák feltörése érdekében
Cél: egy nem publikus erőforrás eléréséhez szükséges jogosultság ellenőrzés (authorization) végrehajtásához szükséges azonosítás (authentication) fázis sikeres lebonyolítása
Hálózati incidenskezelés – Tutorial - 18 - 2006 május

19.


Alkalmazások gyengeségei
Programhibák (hard sebezhetőségek)
Implementációs gyengeségek
Puffertúlcsordulás (stack, dinamikus memóriaterület)
Formázott string alapú támadás
pl. SQL injection, directory traversal
Időzítés-alapú támadások
Time-of-check-to-time-of-use (TOCTTOU) támadás
Symlink race támadás
Konfigurációs hibák (soft sebezhetőségek)
Biztonsági házirend hiánya, hibás volta
Konfigurációs mechanizmusok hiánya
Elégtelen (nem figyelt) naplózás
Figyelmetlenség
Hálózati incidenskezelés – Tutorial - 19 - 2006 május

20.


Strukturális hibák kiaknázása
Fizikai struktúra (szegmentálás hiánya)
Logikai struktúra (lehatárolás hiánya)
Zárt hálózatok
Jól alakíthatók
Jól korlátozhatók
Korlátozott felhasználhatóságúak
Internetes felületű hálózatok
Szolgáltatásokat kell nyújtaniuk
Nehezen korlátozhatók
Az áttekintett veszélyek nagyobb valószínűséggel következnek be
Hálózati incidenskezelés – Tutorial - 20 - 2006 május

21.

Emberi hibák kihasználása

- A támadásra kiszemelt rendszerről hasznos adatok begyűjtése nem technikai eszközökkel (social engineering)
  - Legális adatbányászat is eredményes lehet
  - Fondorlatos adatgyűjtés, rászedés
  - Zsarolás, lelki/fizikai erőszak
  - Megvesztegetés
  - Szakemberek szándékos „túlterhelése”
  - Elkeseredettség, ellenszenv kihasználása
  - Egyéni akciók, bosszú (tipikusan belső támadások)

22.

Védekezések elleni támadás

- Automatikus biztonsági beavatkozás ellenérdekű kihasználása DoS attack-re
  - Jelszóhiba miatti kitiltás
  - Távoli IP cím kitiltása
  - Víruskereső megtévesztése (túlterhelése)
- Indirekt támadások
  - Figyelem elterelés hamis riasztásokkal
  - Kifárasztás sorozatos oktalan riasztásokkal
  - Rendszermentések támadása
    pl. kompromittált mentés felhasználásának kieszközölése

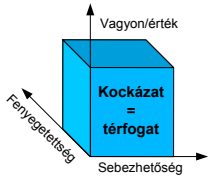
23.

A támadások kockázata

- A támadások kockázatot jelentenek
- A kockázat teljesen nem szüntethető meg
- A kockázatokat elemezni kell – és lehet...
  - Sokszor csak relatív kockázati értékek mérhetők
  - Elemzéssel a kockázat/költség alacsonyan tartható
  - A legégetőbb problémákra koncentrál(hat)unk
  - „Kockázati kocka” fogalma

$$R = \sum p_t * d_t \quad \forall t \in T$$

R = kockázat
T = veszélyforrások halmaza
p_t = t bekövetkezési valószínűsége
d_t = t bekövetkeztekor elszenvedett kár

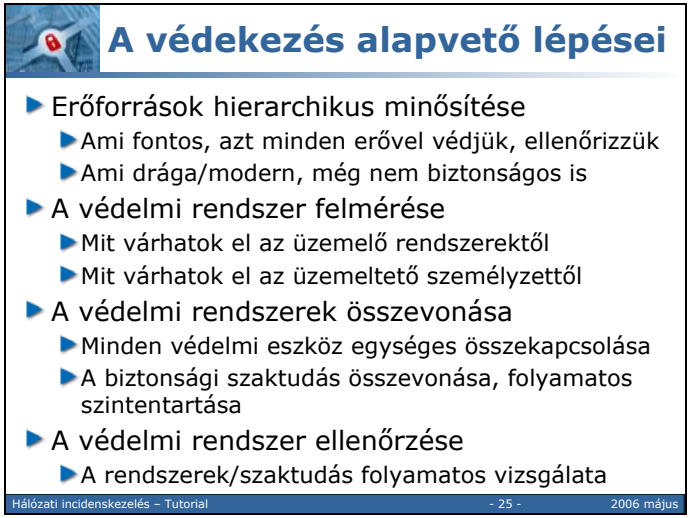


24.

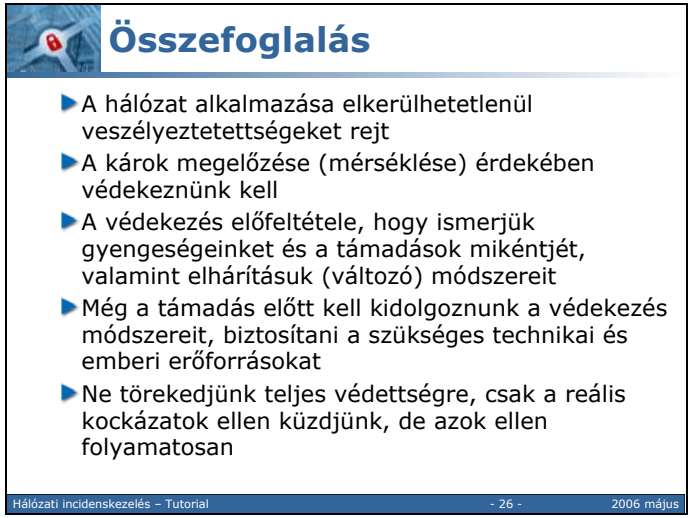
Biztonsági kockázat-elemzés

- Minden ismert kockázatra válaszoljuk meg az alábbi kérdéseket („5M kérdés”):
  - A kockázatot kiküszöbölő intézkedés:
    - Milyen problémát old meg? (leírt célok!)
    - Mennyire jól oldja meg? (hatékonyság)
    - Milyen új problémát vet fel? (egymásra hatás)
    - Milyen költségeket generál? (közvetett is van...)
    - Megéri (a fentiek tükrében)? (foglalkozzunk vele?)
- Néhány megszívlelendő jótanács:
  - A biztonság nem termék, hanem eljárás!
  - A biztonság nem állapot, hanem folyamat.
  - A biztonság nem a kockázat elkerülése, csak annak kezelése.
  - Nincs teljes biztonság, csak tudatos kockázatvállalás.

25.


A védekezés alapvető lépései
Erőforrások hierarchikus minősítése
Ami fontos, azt minden erővel védjük, ellenőrizzük
Ami drága/modern, még nem biztonságos is
A védelmi rendszer felmérése
Mit várhatok el az üzemelő rendszerektől
Mit várhatok el az üzemeltető személyzettől
A védelmi rendszerek összevonása
Minden védelmi eszköz egységes összekapcsolása
A biztonsági szaktudás összevonása, folyamatos szintentartása
A védelmi rendszer ellenőrzése
A rendszerek/szaktudás folyamatos vizsgálata
Hálózati incidenskezelés – Tutorial - 25 - 2006 május

26.


Összefoglalás
A hálózat alkalmazása elkerülhetetlenül veszélyeztetettségeket rejt
A károk megelőzése (mérséklése) érdekében védekeznünk kell
A védekezés előfeltétele, hogy ismerjük gyengeségeinket és a támadások mikéntjét, valamint elhárításuk (változó) módszereit
Még a támadás előtt kell kidolgoznunk a védekezés módszereit, biztosítani a szükséges technikai és emberi erőforrásokat
Ne törekedjünk teljes védettségre, csak a reális kockázatok ellen küzdjünk, de azok ellen folyamatosan
Hálózati incidenskezelés – Tutorial - 26 - 2006 május

27.

Hasznos linkek, referenciák

- http://zone-h.org
  the Internet thermometer
- http://isc.sans.org
  Internet storm center
- http://www.qualys.com
  veszélyeztetettségi törvények, egyéb ajánlások
- http://www.securitydocs.com
  biztonsági dokumentumok, tanulmányok (white paper)
- http://www.cert.hu
  hálózatbiztonsági tanulmány, egyéb információk

28.

Hun-CERT
HUNGARIAN NATIONAL COMPUTER EMERGENCY RESPONSE TEAM

Magyar és nemzetközi CSIRT-ek

29.

Miről lesz szó?

- CSIRT fogalma, célja, története
- CSIRT létrehozása, típusai
- CSIRT működésének feltételei, elemei
  - Szolgáltatások
    - Incidenskezelés
- Hazai és nemzetközi CSIRT szervezetek
- Projektek, trendek
- Szabványosítások
- Zárómegjegyzések
- Hasznos linkek

30.

CERT/CSIRT fogalma

- CERT (Computer Emergency Response Team) fogalma
- CSIRT célja:
  - Segítsen az incidensek megelőzésében
  - Az incidensek által okozott kárt minimalizálja
  - Hosszú távú segítséget nyújtson az incidenskezelésben
- Szinonimák: CSIRT, IRT, CSIRC, CIRT, CIRC, SERT, SIRT

CSIRT olyan szervezet vagy csoport, amely szolgáltatást nyújt és támogatást ad a számítógépes incidensek megelőzésében illetve a számítógépes incidensekre adott válaszlépésekben egy megadott kör részére.

Általában a CSIRT-ek:

- a helyi számítógépes/hálózati biztonsági problémák bejelentésére szolgáló kontakt pont
- ahol azonosítják és elemzik a bekövetkezett eseményt, beleértve annak hatását és lehetséges veszélyeit, fenyegetéseit
- keresik a megfelelő megoldást
- a megtalált választ, információkat, tanulságokat megosztják a szervezet embereivel
- hosszútávú megoldásokat keresnek az incidensek elkerülésére

A CERT szó szerinti fordításban: számítógépes szükségállapottal, kényszerhelyzettel foglalkozó csapat, ez egy kicsit megtévesztő, mert leszűkíti a tevékenységet, ugyanis nemcsak vészhelyzetben tevékenykednek. Korábban ezt az elnevezést használták, most inkább a CSIRT jött divatba. A CSIRT (Computer Security Incident Response Team) jelentése: számítógépes incidensekre adandó válaszokkal foglalkozó csapat.

Megjegyzem, hogy az "incidenskezelés"-t a továbbiakban tágabb értelemben használjuk, tehát ez a fogalom nem azonos azzal, hogy egy adott számítógépes/hálózati biztonsági eseményt megoldunk, annál több, olyan folyamatok összessége, amelyben

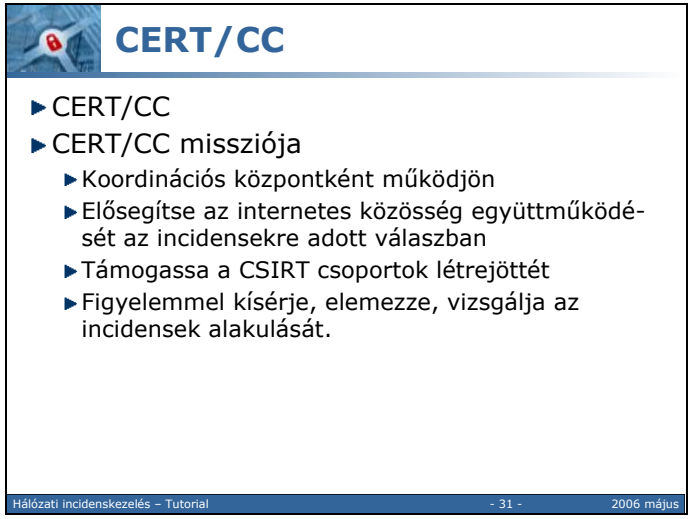
- benne van az incidensekre vonatkozó figyelmezetés,
- az incidensek felderítésében, elemzésében való csapatmunka,
- az együttműködés és a koordináció,
- a megelőzést segítő intézkedések.

Szinonimák: CSIRT – Computer security incident response team, IRT – incident response team, CSIRC – comp. Sec. Inc. Response Capability, CIRC – comp. Inc. Response capability, SERT – security emergency response team

(A CSIRT kifejezés főleg Európában terjed, talán aa TERENA (Trans European Research and Education Networking Association) hatására).

Fontos megjegyzés: Nincs univerzális csodaszer az informatikai biztonságra, a CSIRT csak egy aspektus. Emellett a biztonságos konfiguráció, a tudatosság, külső és belső védelem, szakértők, megfelelően biztonságos rendszerek... mind, mind kellenek.

31.

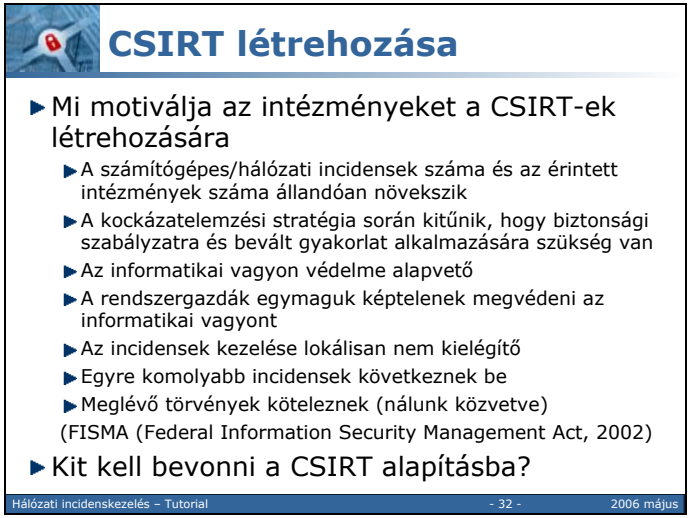


Talán az első CERT a CERT/CC volt. A CERT koordinációs központot 1988 novemberében hozta létre a DARPA (Defense Advanced Research Porject Agency), az USA Védelmi hivatalának kutatásokért felelős részlege. Az alkalmat a Morris féreg megjelenése kínálta, amely demonstrálta, hogy mennyire sebezhető az internet. Helyileg a Carnogie Mellon University-n, a Software Engineering Institute-ben (SEI) van.

A Morris féregről: a nevet a szerzőről kapta. 1988-ban kb 60000 gép volt az Internetre kötve. A gépeken lévő biztonsági lyukakról már akkor is tudtak, de nem vették komolyan. A féreg ezeket a biztonsági lyukakat használta ki: a sendmail (levelező szerver) -be beépített „hibakereső” funkción, mint hátsó ajtón keresztül hatolt be (első biztonsági lyuk), és ezek után a sendmail jogosultságával tevékenykedhetett a gépen. A sendmailt abban az időben szinte mindenki rendszergazdaként indította (második biztonsági lyuk). Ezenkívül a gépek egymásban megbíztak, tehát egy másik gép rendszergazdáit rendszergazdai jogosultsággal beengedték (harmadik biztonsági lyuk). A becslések szerint az akkori 60000 gépből 6000 gép, azaz 10 % fertőződött meg. 2006. januárjában 394 millió host van az Interneten, egy hasonló méretű hiba végzetes lenne.

A CERT/CC ma már koordinációs központként működik, céljai a dián olvashatók.

32.



Ezen a dián azt elemezzük, **mi indokolja** a CSIRT-ek létrehozását. A legfőbb indokok fent olvashatóak.

Két megjegyzés:

1.) Alapvető hiba, hogy a rendszergazdák oldják meg a biztonság kérdését. Kétségtelen, hogy a biztonsági eszközök beállítás, a helyes konfigurálás stb. az ő feladatuk, de egy sor olyan munka létezik, ami kívül esik a feladatkörükön pl. tudatosság növelése, oktatás

2.) A törvények is köteleznek a nagyobb biztonság elérésére. Magyarországon még csak közvetve, pl. „1992. évi LXIII. törvény a személyes adatok védelméről

és a közérdekű adatok nyilvánosságáról”,” 2003. évi XLVIII. törvény” az elektronikusan tárolt adatokra is vonatkozik.

Az USA-ban talán konkrétabb szabályozások vannak:

- Gramm Leach Billey törvény 1999, ami arra kötelezi a pénzintézeteket, hogy az ügyfelek személyi adatait védjék és informatikai biztonsági programjaik legyenek;
- vagy az egészségügyi adatok védelméről szóló HIPAA törvény,
- de a leginkább a FISMA (Federal Information Security Management Act, 2002), amely arra kötelezi a szövetségi intézményeket (agencies), hogy incidenskezelő csoportokat hozzanak létre.

Kik hozzák létre a CSIRT-eket?

A CERT létrejöttéhez felsőbbszintű döntés kell, de a kezdeményezés alulról szokott indulni. Tehát a CERT-ek létrehozásában fő szerepet játszhat:

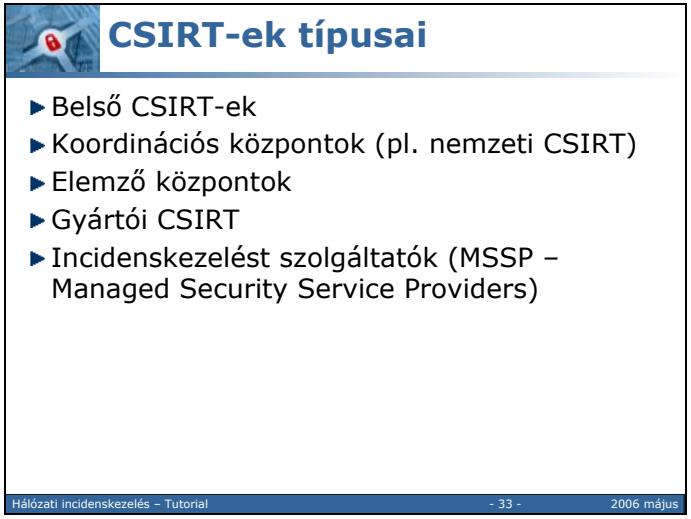
- az informatikáért felelős vezető
- a biztonságért felelős vezető
- a szervezet vezetői

- projektvezetők, projekttagok

A CERT-ek alapításába be kell vonni:

- a szervezet jogi képviselőjét
- személyzeti vezetőjét
- a biztonsági felelősöket
- rendszer- és hálózatadminisztrátorokat
- felső vezetést
- kockázatkezelésért vagy auditálásért felelős embereket, ha vannak

33.



Mivel minden CSIRT más-más körülmények között működik, mindegyik különbözik. Azonban a következő típusokat lehet megkülönböztetni.

- Belső CSIRT-ek: a saját szervezet részére végeznek incidenskezelést, ez a szervezet lehet bank, egyetem, önkormányzat stb. (pl. NIIF CSIRT a kutatói hálózat, Hun-CERT az Internet szolgáltatók részére)
- Koordinációs központok: az incidenskezelést koordináló és összehangoló központ, munkáját több CSIRT számára végzi el. Ilyenek például pl. az nemzeti CSIRT-ek. Nálunk a CERT-Hungary.
- Elemző központok:különböző forrásokból nyert információk alapján az incidens-aktivitás trendjét és formáit elemzik, összegzik. Ilyen pl. a BME-n a víruslabor.
- Gyártói CSIRT-ek: a gyártó által gyártott termékekre specializálódott CSIRT-ek.
- Incidenskezelést szolgáltatók: külső cégek, akik más szervezetek részére nyújtanak incidenskezelést. Bármilyen más tevékenységhez hasonlóan az incidenskezelést is ki lehet szervezni („outsourcing”).

34.

A következő 3 dián végigmegyünk azokon az elemeken, ami egy CSIRT működéséhez szükséges.

Ha segítségre van szükségünk, akkor vegyük elő pl. az RFC2350-t, egy „helyes gyakorlat” státuszú RFC-t. Nagyon sok információ található még a NIST lapjain, ld. utolsó diák egyike.

Körültekintően kell eljárni a célok meghatározásában! Ha azok nem világosak, akkor a CSIRT által végzett munka is ad-hoc jellegű. A célok megfogalmazásában legyünk reálisak, vegyük figyelembe a rendelkezésre álló erőforrásokat (eszközök, emberek, anyagi háttér...), a célok között állítsunk fel prioritási sorrendet. Célok lehetnek például:

- a helyi hálózat/számítógépek biztonságának növelése;
- a szervezet segítése a megelőző biztonsági tevékenységben,
- a biztonsági tudatosság növelése,
- a biztonság területén a helyes gyakorlat terjesztése,
- a biztonsági problémák feltérképezése

Célközönség (fennhatóság) alatt azokat az embereket és eszközöket értjük, akikért és amelyekért a CSIRT a tevékenységét végzi.

A korlátok kijelölési is idetartozik: hol vannak az adott intézmény telephelyei, szobái (földrajzi határok); hogyan közelíthetők meg ezek; mi az az eszközpark amit felügyelünk; hol van a hálózat határa, amitől kezdve már nem mi felügyeljük a rendszert; kik azok az emberek, akiknek a bejelentését elfogadjuk?...

A célközönség meghatározása egyes esetekben triviális: pl. egy kisvállalkozás esetén a kisvállalkozás minden munkatársa és számítógépe lehet ez a kör. Egy nagy egyetem esetén már nem olyan egyszerű a kérdés: a CSIRT csak a rendszer- és hálózatgazdákkal álljon kapcsolatban vagy az egyetem minden hallgatójával és tanárával?

A célközönség meghatározása döntően befolyásolja a jövőbeni munkát, hogy pl. milyen szintű figyelmeztetéseket köröznek, milyen szintű tanácsokat adnak...(Ez a kérdés különösen nehéz pl. egy koordinációs központ esetén, mint amilyen a nemzeti CSIRT)

35.

Szervezeti kérdések: A dián látható első két kérdés szorosan összefügg. A CERT/CC által végzett felmérések szerint rendszerint az Információtechnológiai részleghez szokták besorolni a CSIRT-et. Ugyanakkor az ISO 17799 szabványt szerint a CIO számoljon be a CSO -nak, és az feleljen CEO-nak. (CIO -> CSO -> CEO)

CIO: chief information officer

CSO: chief security officer

CEO: chief executive officer

A szervezeti kérdések azért fontosak, mert a CSIRT és az IT részlegnek együtt kell működnie számos esetben: CSIRT javaslatot tehet a belső és külső védelemre (pl. tűzfalak, vírusírtók, IDS-ok kiválasztása, telepítése; de nemcsak az eszközök, hanem a folyamatok megváltoztatásra is javaslatot tehet.

Szervezési kérdés az is, hogy hogyan tarthatja a kapcsolatot a célközönséggel: milyen információt adhat ki, milyen információkat kell kiadnia, a kapcsolatot milyen formában tarja (email, hirdetőtábla), megbízható vagy nyílt hálózaton stb.

Finanszírozás: szükséges Montecuccoli: „Mi kell a háborúhoz? Pénz, pénz és pénz”

Mennyibe kerül egy incidenskezelés, mennyit fordítanak a védelemre erről az hivatkozásban szereplő FBI/CSO jelentésben olvashatunk.

Döntési jogosultság: Tisztázni kell, hogy milyen jogosultsága van a CSIRT-nek, mint csoportnak és mikor, kinek, milyen jogosultsága van a CSIRT-en az egyes csoporttagoknak. El kell különíteni azokat a jogokat, amelyben a CSIRTnek

- teljes szabadsága van: pl. egy rendszergazdának megmondhatja, hogy húzza le a gépét a hálózatról, vagy ő maga lehúzhatja,
- megosztott a felelőssége: amikor részt vesz a döntéshozásban. Például egy patchet (javítást)-t fel kell tenni, addig lehúzzák-e a hálózatról az adott gépet.

- nincs döntéshozási jogosultsága: tegyenek fel egy javítást

Csoport nagysága, összetétele: nagyon változó, kevés főállású személyzet, inkább egy adott terület szakértői félállásban; gyakorlata legyen, kommunikációképes,

36.

37.

A szolgáltatások három nagy csoportját különböztetjük meg:

Reagáló intézkedések: ezek azok a szolgáltatások, amelyeket valamilyen esemény vagy kérés indít el. Ilyen eseményre példa: egy feltört host, a hálózaton terjedő rosszindulatú kód, az IDS által észlelt esemény.

Megelőző intézkedések: segítséget nyújtanak vagy valami információt közölnek arról, hogy hogyan előzhető meg egy támadás, egy váratlan esemény. Ezekkel a szolgáltatásokkal a később *bekövetkező incidensek számát csökkenthetjük*.

A biztonságot javító szolgáltatások: Ezek a szolgáltatások távolabb állnak az incidens-kezeléstől, és ezeket a *szervezeten belül más részlegek is megvalósíthatják*. Ha a CSIRT részt vesz vagy ő maga nyújtja ezeket a szolgáltatásokat, akkor a CSIRT szempontjai is érvényesíthetők az egész szervezet biztonságának növelésében. Tehát ez is megelőző intézkedés, de csak közvetve csökkenti a bekövetkező incidensek számát.

Az első oszlop elemei:

Riasztások: egy meglévő problémára hívjuk fel a figyelmet, és megmondjuk, hogymit kell tenni rövid időn belül (pl. egy javítás feltevése)

Incidenskezelés I. a következő diát.

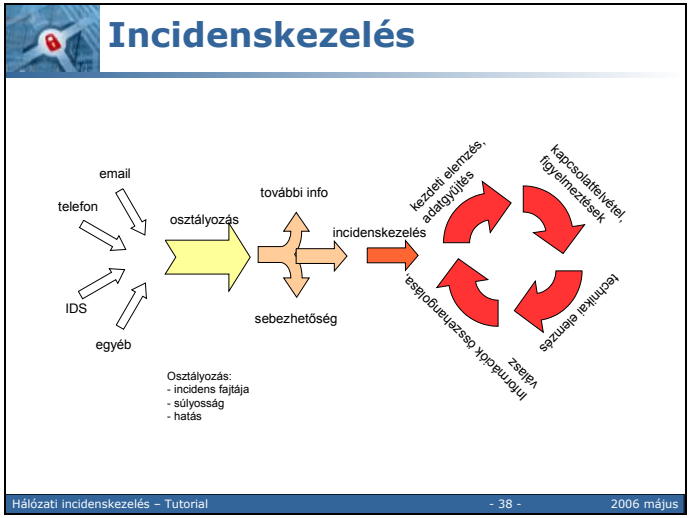
Sebezhetőségek kezelése: belső vagy külső forrásból egy olyan hardver/szoftver biztonsági hibáról, gyengeségről értesülünk, amelyet egy rosszindulatú ember kihasználhat. Az elemzés során megbizonyosodhatunk, hogy a gyengeség/hiba valóban létezik. A válasz: javítás megkeresése, telepítése; de lehet, hogy csak a sebezhetőség elkerülésére kapunk javaslatot. PL. MS IE hibáknál: csak megbízható oldalakat látogassunk. Koordinálás: a sebezhetőséggel kapcsolatos információ terjesztése.

Kártékony informatikai elemek: olyan a rendszerben található fájl vagy objektum, amit a hálózat vagy a rendszer támadására lehet felhasználni – ide sorolja a vírust, férget, trójait, ismeretlen scriptet.

Megelőző szolgáltatások: Bejelentés (sebezhetőség, támadásfajtás ismertetése); Technologiai figyelmeztetés (új technológiai fejlesztések figyelemmel kísérése); Az informatikai vagyon felértékelésére és auditálására vannak szabványok, eljárások, ezek használata (OCTAVE: Operationally Critical Threats, Assets and Vulnerability Evaluation, CRAMM, FIRM); Szűrők, tűzfalak, VPN stb alkalmazások, saját patch szolgáltató szerver építése, gyors visszaállítási eszközök előkészítése.

Harmadik oszlop: magáért beszél

38.



A fenti ábra az incidenskezelés folyamatát mutatja be. A CERT/CC ábrája ez, ettől különböző módszerek is alkalmazhatunk.

1. Az incidensekről **beérkező hí**r sokféle módon juthat el a csoporthoz:

e.mail, web-felületen történő bejelentés, tűzfal vagy IDS-ek okozta riasztás, telefon, fax... Számos kérés eldöntésre kerül: saját felhasználóinktól érkezett-e, foglalkozunk-e evvel...?

2. Ha kérés beérkezett, a következő lépés a **kategorizálás**.

A bejelentés után a következő lépés az osztályozás, akár egy kórházban: van-e elég információnk az esetről, incidensről lehet-e egyáltalán szó vagy egyéb biztonságot érintő bejelentés (pl. egy sebezhetőséget fedeztek fel)?

Osztályozás módjai: incidens típusa (felhasználó veszélyeztetése, root veszélyeztetése, szolgáltatásmegtagadás, felderítés, vírus, hoax...) Mekkora az incidens kiterjedése (egy gép, teljes hálózat?

Súlyosság: emberi életet veszélyeztet (kórház), pénzügyi veszteséget okozhat, CSIRT rendszert érinti, az infrastruktúrát veszélyezteti, valamilyen tevékenységet korlátoz.

Hatás: sikeres-e a támadás vagy csak kísérlet; az érintett vagy veszélyeztetett rendszer nagysága, a támadás összetettsége

Valószínűleg incidens: - akkor dönteni kell, kinek kell szólni, mennyire sürgős a beavatkozás?

3. Lehet, hogy a **döntést még nem lehet meghozni**, mert kiegészítő információkra lenne szükség. Ekkor visszacsatolás történik a bejelentőhöz.

4. **Incidens történt**: akkor a CSIRT megkapja a feladatot. (Azon belül ki?).

- kezdődik az adatok elemzése, egyéb adatok gyűjtése illetve bekérése. Ha - esetleg – bírósági eljárásról lesz szó, nagyon körültekintően kell a bizonyítékok gyűjtését végezni, minden lépésünket rögzíteni kell (írásban vagy szóban). Mentés készítése.

- dönteni kell, hogy kit értesítsünk és kivel vegyük fel a kapcsolatot. (pl. a hálózatról lehúzzuk a gépet, az illető főnöknek tudni kell erről; egy adott témához értő szakértő szükséges, meg kell keresni; hálózatadminisztrátor vagy ISP értesítése is szükséges lehet; újabb áldozatot fedezünk fel, s az illető még nem tudja, hogy áldozat – őt is.)(Kérdés: a támadó beazonosításakor értesítsük-e az intézményét, őt stb.
- elkezdődhet a technikai elemzés, optimális esetben tudjuk: ki a támadó, milyen sebezhetőséget használt ki, milyen kárt okozott
- Milyen további lépéseket kívánunk tenni: rendszer helyreállítása, feljelentés, figyelmeztetés a többi felhasználónak, CSIRT-nek...

39.

Hazai CSIRT szervezetek

- Hungary CERT – magyar **állami,** önkormányzati és üzleti szféra
  http://www.cert-hungary.hu
  IHM, Közháló, NETI Kft., Nemzeti Hírközlési Hatóság, NT Kht., Polgári Légiközlekedési Hatóság, Puskás Tivadar Közalapítvány
- Hun-CERT – Internet Szolgáltatók Tanácsa
  http://www.cert.hu
- NIIF CSIRT – magyar kutatói hálózat
  http://csirt.iif.hu/

Hálózati incidenskezelés – Tutorial - 39 - 2006 május

A CERT-Hungary a Puskás Tivadar Alapítvány keretein belül működő Magyar Kormányzati Hálózatbiztonsági csoport, 2005. januárjában alakult. Az állami, önkormányzati és üzleti szférát egyaránt kiszolgálja, de elsősorban a kormányzati szféra támogatására jött létre. Különösen a felsorolt szervezetek részére nyújt szolgáltatást.

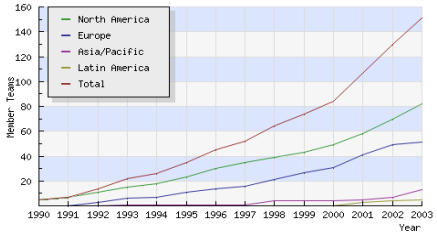
Hun-CERT: 2002. januárjában indult, az Internet szolgáltatók részére nyújt szolgáltatást.

NIIF CSIRT: az első volt, de hol működött, hol nem. Ez attól függött, hogy ki az aki felvállalta ezt a szerepkört. Pásztor Miklós nevét feltétlenül meg kell említeni, mint a biztonsággal kapcsolatos munkák elindítóját. S ma már újra elmondható, hogy létezik a NIIF CSIRT.

40.

Nemzetközi CSIRT-ek (1)

- FIRST (Forum of Incident Response Teams)
  - Tagok



  - Éves konferencia
  - Technikai kollokvium évente 3x

Hálózati incidenskezelés – Tutorial - 40 - 2006 május

A FIRST az incidenskezelő csoportok legnagyobb szervezete. 1988-ban alakult, néhány héttel a CERT/CC előtt, szintén a Morris féreg kapcsán, az USA-ban. 1989 októberében, a Wank féreg megjelenése után kitűnt, hogy a biztonsági incidensekkel foglalkozó csoportok között javítani kell a kommunikációt és a koordinációt. Azóta a FIRST célja a CSIRT csoportok összefogása.

(Wank féreg a VMS/DEC rendszereket fertőzte, de nem a TCP/IP, hanem a DECNet-en keresztül. A jelszókezelés gyengeségeit használta ki, módosította a .com fájlokat, új azonosítót generált...)

Tagjai között mindenfajta CSIRT van: kormányzati, oktatási, katonai, gyártói, kereskedelmi. A tagok létszámának alakulása látható az ábrán. Magyar tagja még nincs, elsősorban a fizetendő tagdíj miatt, de a CERT-Hungary már elindította az eljárást.

1989 óta minden évben megrendezik a FIRST konferenciát, amelyik az egyik legnagyobb találkozója a biztonsági szakembereknek. 2004-ben Budapesten tartották az összejövetelt.

41.

A TERENA az európai kutatói hálózatokat tömörítő szervezet. Ennek ellenére az ún. „Trusted Introducer” listán nemcsak a kutatói hálózatokhoz tartozó CSIRT-eket gyűjti maga köré, hanem minden CSIRT-et. A CSIRT-eknek két státuszuk van, kezdetben nem akkreditált, majd bizonyos feltételek után akkreditált státuszt kapnak. Magyarországról mindhárom szervezet tag, de a CERT-Hungary 2006. február óta akkreditált tag is..

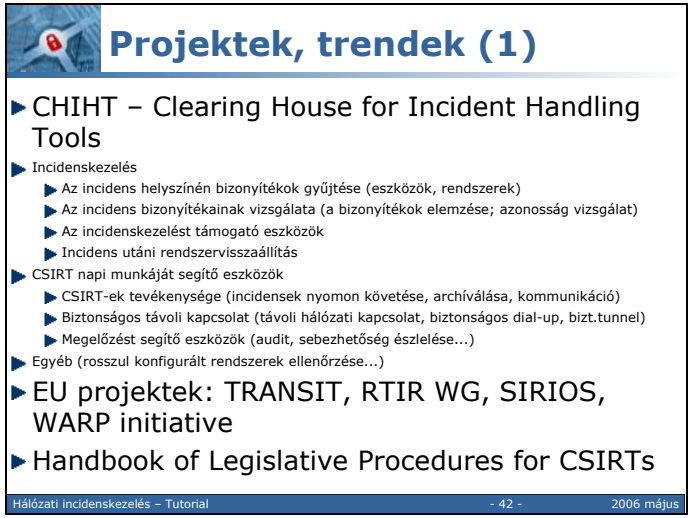
ENISA: nem igazán a CSIRT-ek szervezete, az ügynökséget az Európai Parlament és a Bizottság 2004-ben hozta létre. Az ügynökség feladata:

- a biztonsági incidensek és a kockázatok adatainak gyűjtése és elemzése
- európai szinten a különböző szereplőkkel (PPP) történő együttműködés a biztonság területén
- biztonsági tudatosság növelése, kockázatkezelési eljárások és a „helyes gyakorlat” elterjesztése
- biztonsági szabványok kifejlesztése a termékekre, szolgáltatásokra

A tavalyi tevékenységéről szóló beszámoló azt mutatja, hogy a TERENA-val karöltve az európai CSIRT mozgalom támogatását felvállalta.

A további két szervezet közül az EGC együttműködés a CERT-Hungary számára fontos.

42.



CHIHT: ennek a projektnek a keretében az Incidenskezelő csoportok számára hasznos eszközöket, iránymutatásokat, dokumentumokat gyűjtik össze. Tehát eszközök találhatók a fentebb felsorolt témákhoz.

TRANSIT: CSIRT csoportok képzése

http://www.ist-transits.org/

2002-2005 között az Európai Unió támogatásával folyt az ún. TRANSIT projekt, évente 2-szer tanfolyamot szerveztek a biztonsági szakembereknek. Miután 2005 júliusában befejeződött a TRANSIT projekt, ugyanakkor nagyon jó visszhangja volt ennek, a TERENA és a FIRST között szorosabb kapcsolat alakult ki az oktatás kapcsán. A FIRST a TRANSIT oktatási anyagokat átveszi, és ennek alapján Latin-Amerikába és Ázsiában is tanfolyamokat szervez. Ezenkívül hármas támogatással (TERENA, FIRST, ENISA) közös „training workshop”-okat terveznek. 2006. márciusában már Vilniusban volt ilyen tanfolyam.

RTIR WG:incidensek kezelése elektronikusan

http://www.terena.nl/activities/tf-csirt/rtir.html

SIRIOS – inicdenskezelésre szolgáló eszközökkel foglalkozik(Tools for incident handling)

http://www.cert-verbund.de/sirios/

WARP: Warning, Advice and Reporting Point

http://www.warp.gov.uk/

Handbook of Legislative Procedures for CSIRTs: 2002-ben az EU Bizottság megbízásából készült el a fenti címmel egy kiadvány. A dokumentum két részből áll:

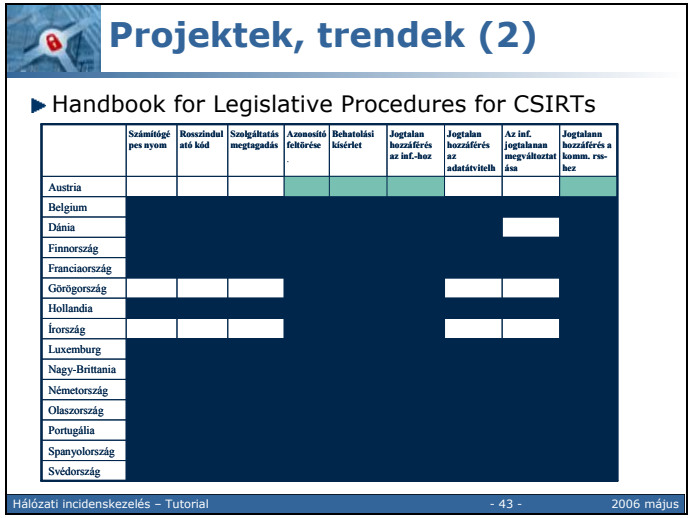
- az első rész a rosszindulatú használat fajtáit és biztonsági incidenseket kategorizálja, átnézi a nemzetközi szabályozást (Számítógépes bűnözésről szóló egyezmény, amit itt

Budapesten írtak alá), az incidensek jogi szempontból történő vizsgálatának elveit mutatja be,

- a második rész pedig a számítógépes bűnözésnek büntethetőségét ismerteti az egyes országokban .

Az eredeti dokumentum az 15 országára vonatkozik, jelenleg bővítik a kötetet.

43.



Szerintem a számítógépes bűnözéssel kapcsolatos jogi információkra egyre nagyobb szükségük lenne a CSIRTeknek.

A számítógépes bűnözés egyik alapproblémája, hogy a szabályozás az egyes országokra érvényes, de a hálózat nem ismeri az országhatárokat. Az EU evvel a kézikönyvvel próbál segíteni a kérdésen. Az első könyv, ami 2002-ben készült, még 15 országra vonatkozott. Most folyik a második változat készítése, ami mind a 25 országra vonatkozik.

A fenti ábrán a vízszintes oszlopban az incidensek osztályozása látható, a függőleges oszlopban az egyes országok láthatók.

A színek jelentése:

- Fehér: nincs jogi szabályozás
- Szürke: adminisztratív szankció van
- Fekete: büntető szankció van

<u>További információk:</u>

Handbook of Legislative Computer Security Incident Response Teams

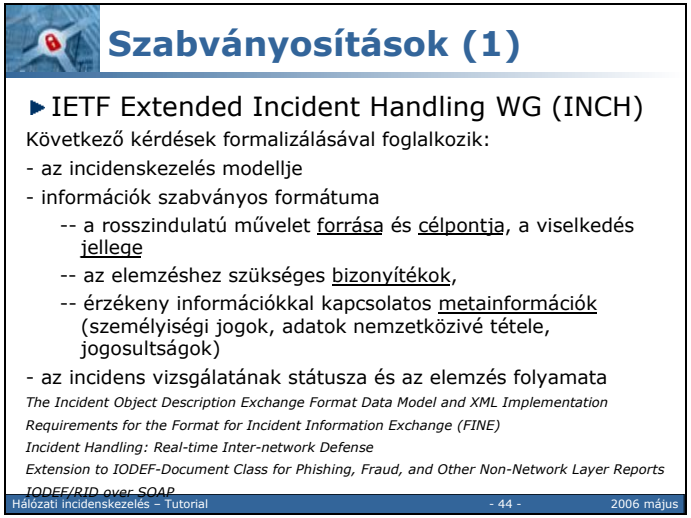
Eredeti anyag:

http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03hb002.pdf

Új anyag:

http://www.csirt-handbook.org.uk/app/index.php?&table_name=app_countries&function=search&where_clause=&page=1&order=country&order_type=ASC

44.



Jobb lenne a „szabványosítási kísérletek” fogalmat használni.

Az INCH csoport célja egy adatformátumok definiálása, amely elősegíti, hogy a biztonsági incidensekről szóló információt lehet elektronikus lehessen kezelni.

A feladatok közé tartozik tehát annak szabványosítása, hogy hogyan nézzen ki a modell és milyen legyen az üzenet szabványos alakja, például a következő esetekben:

- a beérkező jelentés (amit a felhasználóktól kapnak)
- a egyéb személyektől (pl.technikai személyzettől, más CSIRT-ektől) beérkező információ
- elemző központból érkező információ

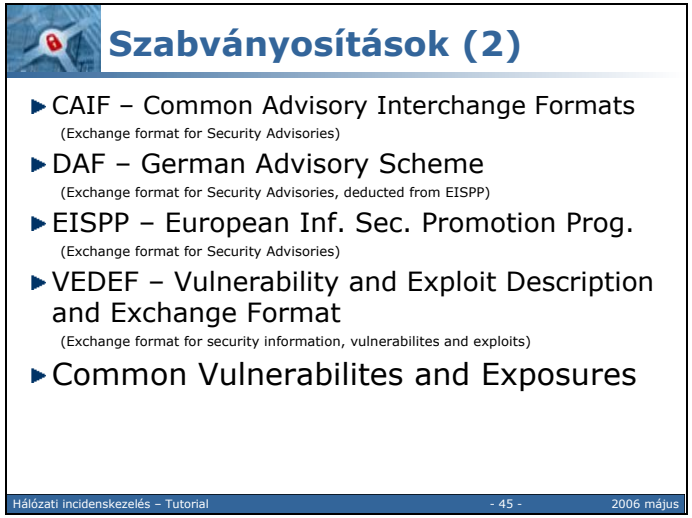
A szabványosított formátum a ma még emberi erőforrás-igényes kommunikációs folyamatokat fogja segíteni. A csoport a következő kérdések formalizálásával és átvitelével foglalkozik:

- . a rosszindulatú felhasználás forrása és célpontja, a viselkedés elemzése
- az elemzéshez szükséges bizonyítékok,
- az incidens vizsgálatának státusza és az elemzés folyamata
- érzékeny információkkal kapcsolatos metainformációk (személyiségi jogok, adatok nemzetközivé tétele, jogosultságok)

Az alul felsorolt IETF dokumentumok még ún. Draft-ok, tehát nem elfogadott anyagok.

Ezt a munkát az európaiak indították el IODEF (Incident Object Description and Exchange Format) néven, amely csoport munkáját folytatta az IETF most már INCH néven.

45.

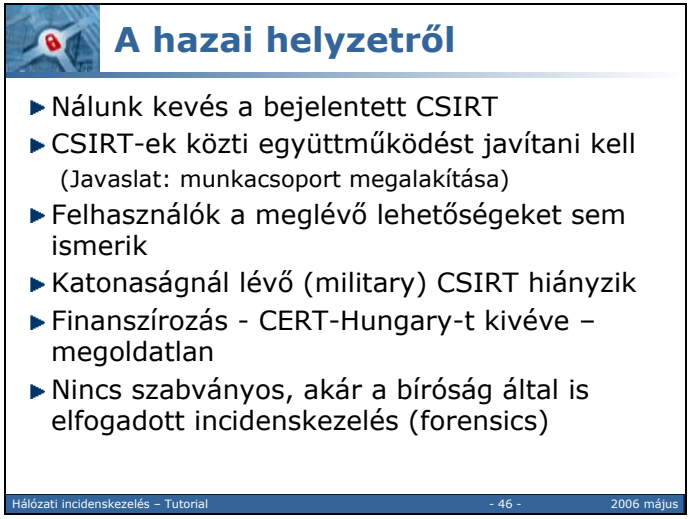


Mindenféle európai szabványosítási kísérleteket megpróbáltam összeszedni, amelyek az adatcserére vonatkoznak.

Az utolsó talán a legelfogadottabb kísérlet:

CVE: sebezhetőségek és kitettségek http://cve.mitre.org

46.



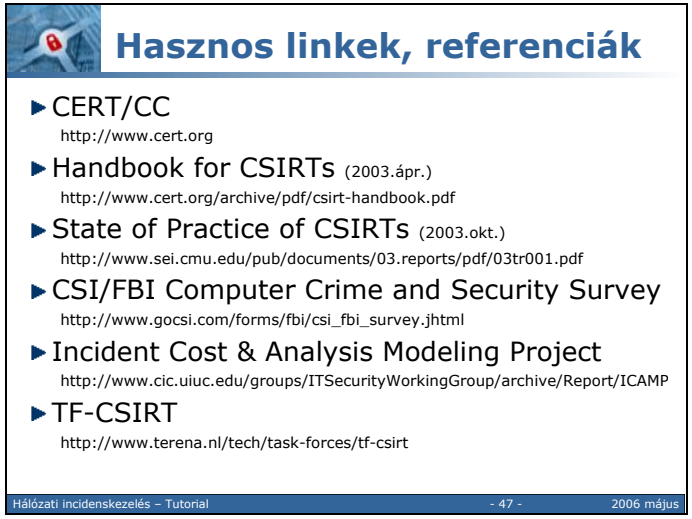
Sokfajta biztonsági csoport működik nálunk: vírusközpontok, rendszergazdák,... de ezek nem valamilyen kellően szabályozott formában dolgoznak, nemzetközi szervezetekben nem vesznek részt.

Szemben a külföldi példákkal, a magyar férgek megjelenése – Maya Gold, Zafi – nem késztette összefogásra a hazai szakértőket. Mindenki a saját területén dolgozik. Valamilyen szervezett forma (pl. Az IHM vezetésével egy munkacsoport) javíthatna a helyzeten. S a CERT Hungary lehetne az a szervezet, ami jobban összefogja a munkát.

Felhasználók nem ismerik a CSIRT-eket. A felhasználók alatt a rendszergazdák is értendők.

Nagyon sok helyen a katonasághoz kötödik a CERT (nyilván a hírszerzéssel is összefüggésben). Itt a keleti blokkban pl. a lengyeleknél vannka jól működő katonai (kormányzathoz kapcsolódóan) és civil csoportok.

47.

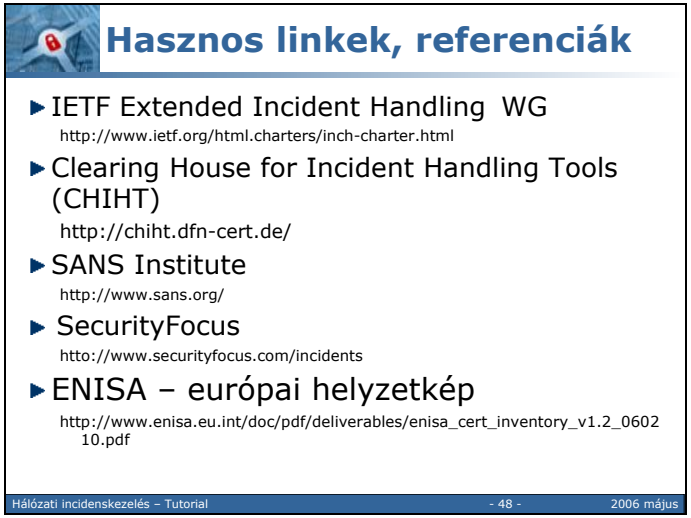


További linkek:

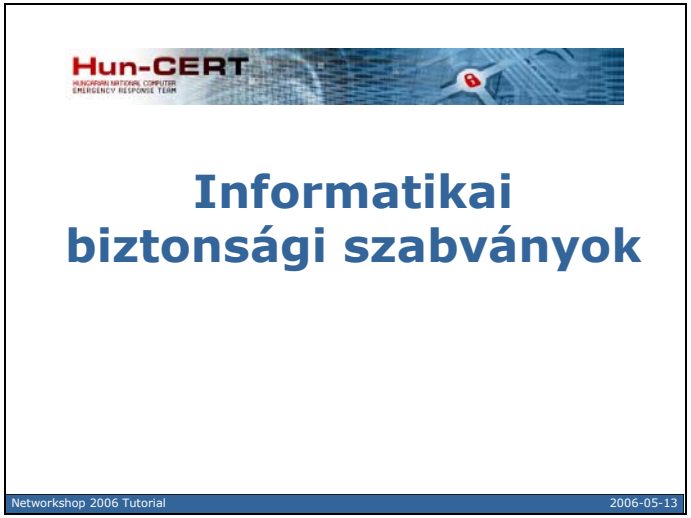
Forming an Incident Response Team

http://www.auscert.org.au/render.html?it=2252&cid=1938

48.


Hasznos linkek, referenciák
IETF Extended Incident Handling WG
http://www.ietf.org/html.charters/inch-charter.html
Clearing House for Incident Handling Tools (CHIHT)
http://chiht.dfn-cert.de/
SANS Institute
http://www.sans.org/
SecurityFocus
htto://www.securityfocus.com/incidents
ENISA – európai helyzetkép
http://www.enisa.eu.int/doc/pdf/deliverables/enisa_cert_inventory_v1.2_060210.pdf
Hálózati incidenskezelés – Tutorial - 48 - 2006 május

49.


Hun-CERT
Informatikai biztonsági szabványok
Networkshop 2006 Tutorial 2006-05-13

50.

Tartalom

- Információ/informatikai biztonság
- Szabványok, szintek szerinti osztályozásuk
- Az informatikai biztonság (IB) nemzetközi és hazai szabványosításának főszereplői
- Az információbiztonsági szabványok rendszere
- Néhány kiemelt szabvány ismertetése
  - Common Criteria , MIBÉTS
  - BS 7799 -> ISO 27000 , IBIK
  - COBIT
  - ITIL ->ISO20000

Hálózati incidenskezelés – Tutorial - 50 - 2006 május

A társadalom minden rétege – a kormányzati szektor, a gazdálkodó szervezetek és az egyének is – egyre fokozottabb mértékben **függ** az informatikai rendszerektől, új **kockázatok** jelennek meg, amelyeket **hatékonyan kezelnünk** kell.

Az embereknek az információs rendszerekhez vegyes érzelmekkel közelítenek: örülnek annak, hogy az információkhoz könnyen és gyorsan hozzájutnak (**az információhoz való jog**), ugyanakkor félnek, hogy a velük kapcsolatos, róluk szóló stb. bizalmas információk kikerülnek (**bizalom hiánya, tudatlanság**).

Az **informatikai biztonság** nemcsak, sőt elsősorban nem technológiai kérdés, hanem megközelítéséhez át kell alakítani a

- *technológiai feltételeket,*
- *környezeti feltételek,*
- *szervezeti kereteket.*

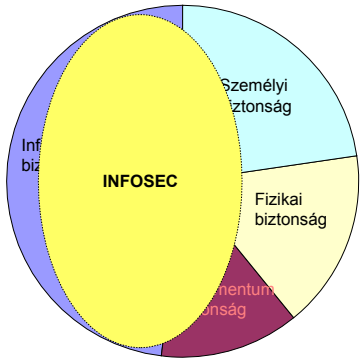
E feltételek átalakítása s**em vezet el a teljes biztonsághoz**, mivel olyan ma még nincs, csak valamennyire megközelíthető.

A következőkben

- a technológiai feltételekről csak érintőleges szólok, arról inkább az elkövetkező előadásokban lesz szó.
- környezeti feltételek alatt itt csak a s*zabványosítási tevékenységről* lesz szó, egyéb környezeti feltételek: *jog, emberi tényezők (tudatosság növelése)* itt nem kerül szóba.
- a szervezeti keretekből is egyetlen tényezőről, a számítógépes incidenskezelő csoportokról beszélünk.

51.

A biztonság elemei (NATO)



Hálózati incidenskezelés – Tutorial - 51 - 2006 május

A biztonság napjaink egyik leginkább előtérbe került problémája, a 2001. szept. 11-i események döntően befolyásolták ennek kezelését. A biztonsággal a hivatalos kormányzati, rendvédelmi, hazai és nemzetközi szervezetek (NATO) éppúgy foglalkoznak, mint az Internet felhasználók milliói. Éppen ezért a biztonság - sőt leszűkítve az informatikai biztonság - témakörére nagyon sok helyen, nagyon sokféle – néha egymásnak ellentmondó – meghatározásokat találunk.

Sokszor felhívják a figyelmünket arra, hogy **tegyünk különbséget az információ-biztonság és az informatikai biztonság között**, ezt most megtesszük. A NATO szabályai a biztonságnak öt eleme van: a személyi -, fizikai -, kommunikáció-, dokumentum -, iparbiztonság. Ez utóbbi nem tartozik a NATO titokvédelmi területei közé, csak az előző néggyel foglalkoznak.

(Az információ: olyan tények vagy elgondolások, amelyet különféle adatformában lehet reprezentálni.)

A személyi biztonság elve: „Szükséges, hogy megismerje!" „Csak, akire tartozik"

Fizikai biztonság: megvédeni a jogosulatlan hozzáféréstől az információkat (védelem az erőszakkal történő behatolás ellen; védelem a kialakított rend ellen tevékenykedők ellen)

Dokumentum biztonság területei: iratkezelési eljárások, dokumentumok minősítése, átvétele, továbbítása, megsemmisítése, betekintés szabályozása

Elektronikus információ (kommunikáció) biztonság: informatika, adatátvitel, rejtjelezés, kisugárzás.

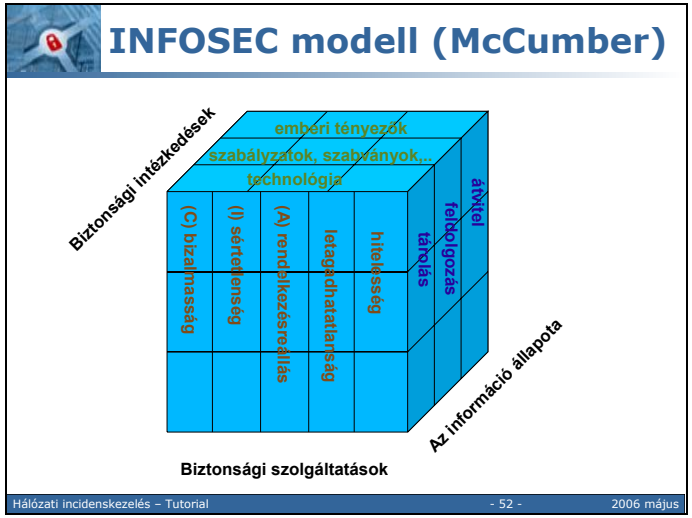
Az információbiztonság (information security) helyett gyakran használják az információ szavatolás/garancia (information assurance) kifejezést is.

Az informatikai rendszerek biztonsága (INFOSEC) = informatikai biztonság: az információs rendszerek védelme az információ jogosulatlan felhasználása vagy módosítása ellen, akár az információ tárolásáról, processzálásáról vagy átviteléről legyen szó, ide tartoznak

mindazok az intézkedések, amelyek a fenyegetettségek észleléséhez, dokumentálásához vagy elhárításához szükségesek.

(Azért megjegyzem, hogy pl. az Internet Security Glossary RFC2828 nem teszi meg a megkülönböztetést: „information security” = INFOSEC!!!)

52.



Az előző dia végén egy elég bonyolult definíciót mondtam az informatikai rendszerek biztonságáról, az 1991-ben elkészített McCumber -féle modell ezt szemléletessé teszi.

Az informatikai rendszerek biztonsága (INFOSEC) = informatikai biztonság(?): az információs rendszerek védelme az információ jogosulatlan felhasználásától vagy módosításától, akár az információ tárolásáról, feldolgozásáról vagy átviteléről legyen szó, valamint a védelem azért, hogy a jogos felhasználó a szolgáltatást elérhesse; és ide tartoznak mindazok az intézkedések, amelyek a fenyegetettségek észleléséhez, dokumentálásához vagy elhárításához szükségesek.

Information system security (INFOSEC): Protection of information system against unathorized access to or modification of information, whether in storage, processing or transit, and against the denial of service of authorized users, including those measures necessary to detect, document, and counter such a threats.

A McCumber -féle modell kezdetben a bűvös kockára hasonlított, ugyanis egy 3x3x3-as kocka volt. A tengelyeket értelmezve nem adok pontos definiciót, az megtalálható a NSTISSC 4009-ben.

Az első tengely a biztonsági szolgáltatások, ami kezdetben a „CIA” volt, azaz a megbízhatóság (titkosság), sértetlenség és elérhetőség. Ehhez jött később a letagadhatatlanság és a hitelesítés (hitelesség), ekkor már a kocka egy kicsit eltorzult.

Titkosság/bizalmasság: csak a jogosult személy, folyamat vagy eszköz juthat az erőforráshoz (információhoz)

Sértetlenség: erőforrás (információ/rendszer) az eredeti állapotnak megfelel és teljes; módosítás vagy törlés nem történt. (...Magába foglalja az információ pontosságát, lényegességét és teljességét – mindez adja ki a rendszer robosztusságát)

Elérhetőség: a jogosult felhasználó a megfelelő szolgáltatást, a megfelelő időben és helyen megkapja.

Letagadhatatlanság: hiteles információnk van egy adott cselekvéssel kapcsolatban (küldő a kézbesítés tényéről bizonyítékot kap, a fogadó pedig a küldő kilétéről biztosítva van).

Hitelesség: biztonsági intézkedés, ami arra szolgál, hogy az átvitel, az üzenet vagy a kezdeményező érvényességét igazolja, vagy egy olyan eszköz, ami egy adott személynek egy adott információhoz való hozzáférésének jogosultságát igazolja.(IP címek hamisításánál kezdtek erre felfigyelni)

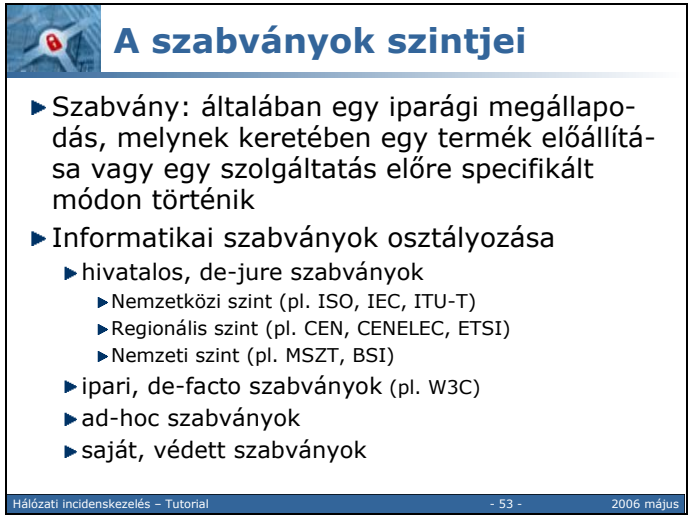
A második tengely: az információ állapota – tárolás, processzálás (feldolgozás) vagy átvitel. Az információ egyszerre kétféle állapotban is lehet. (pl. tárolás és átvitel)

A harmadik tengely: a biztonsági intézkedések, amely a technológiából,az üzemeltetésből (szabályzatok és eljárások/gyakorlat; ide tartoznak mindazok az intézkedések, amit pl. a rendszergazdák kényszerítenek a felhasználóikra) és az emberi tényezőkből áll. Ez utóbbi tkp „fekete doboz": betartják-e a szabályzatokat, mit csinálnak egy olyan helyzetben, ami nincs lefedve szabályzatokkal stb.

Negyedik dimenzió: idő – mindezt folyamatában kell tekintenünk. Az egyes elemek fontossága időben változhat, pl. egy projekt befejezésénél nagyobb szerepe lesz a tárolásnak, adatelérésnek, mint a letagadhatatlanságnak.

És nem véletlenül „kockaként" ábrázolják ezeket a dimenziókat, mert a modell elemei között kölcsönhatások vannak.

53.



Az előbbi kockát nézve a „felső rétegről" közelítem a modell, és abból is a középső sávból fogok részleteket ismertetni.

Szabvány:általában egy iparági megállapodást értünk alatta, melynek keretében egy termék előállítása vagy egy szolgáltatás üzemeltetése előre specifikált (szabványos) módon történik.

A szabványhoz olyan képzetek kapcsolódnak, mint időtállóság, minőség, tekintély, együttműködés, konszenzus stb.

Az informatikai szabványok négy szintjét szokták megkülönböztetni, ez az informatikai biztonsági szabványokra is igaz:

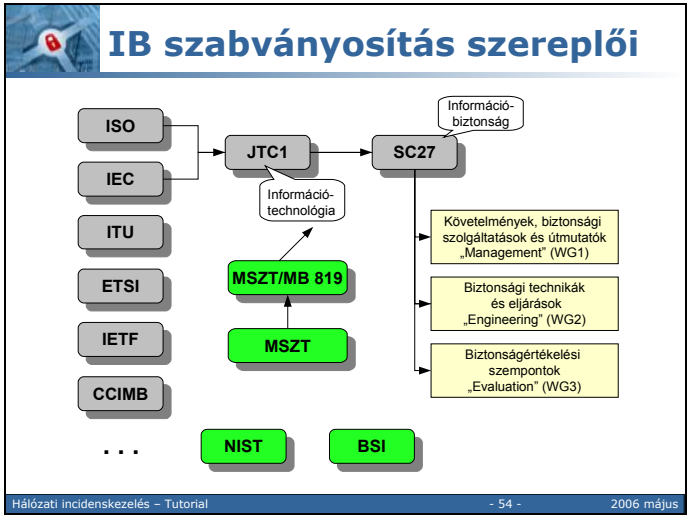
hivatalos (de-jure) szabványok: Idetartoznak azok a szabványok, melyeket a különböző **államok által törvényi szinten elismert,** szabványok megalkotására létrejött szervezetek adnak ki. A szabványügyi testületek három szinten helyezkednek, és az általuk kiadott szabványok is ezekre a szintekre érvényesek.

Ipari (de facto) szabványok: a legtöbb ilyen szabvány egy adott iparág konzorciumba tömörült érdekelt feleinek együttműködési törekvése kapcsán jött létre. Pl a W3C 350, informatikában érdekelt szervezet együttműködése.

Ad-hoc szabványok: habár egyik szabványügyi szervezet sem adta ki vagy hagyta jóvá, de lényegében szabvánnyá vált. A de-facto szabványok előképének lehet tekinteni.

Saját, védett szabványok – nem is igazi szabványok, általában egy domináns szoftverfejlesztő cég ad ki ilyet, a tulajdonjog a kibocsájtó kezében marad, licenszdíjat kérnek érte stb. (MS Windows)

54.



Az ábrán azok a szabványosítási szervezetek láthatók, amelyek az informatikai biztonság területén fontos szerepet játszanak.

Az ISO, a svájci székhelyű Nemzetközi Szabványosítási Intézet és az IEC, a Nemzetközi Elektrotechnikai Bizottság egy közös bizottságot (JTC1) hozott létre, melynek feladata az információtechnológia területén történő szabványosítás.

A JTC1-en belül különböző albizottságok működnek, a SC27-es az információtechnológiai biztonságért felelős („IT Security Techniques"). (SC7: rendszer és rendszerfejlesztés)

Három munkabizottsága működik, amelynek feladata magába foglalja

- az informatikai rendszerek biztonsági szolgáltatásai általános **követelményeinek** meghatározását,
- biztonságra vonatkozó **útmutatások** fejlesztését,
- támogató dokumentumok fejlesztését a **vezetés** számára,
- biztonsági **technikák** és mechanizmusok fejlesztését (kriptográfiai és nem kriptográfiaiit egyaránt)
- informatikai rendszerek, komponensek és termékek biztonsági **értékelésére** és tanúsítására vonatkozó szempontrendszer kialakítását

ITU (International Telecommunication Union) Nemzetközi Távközlési Egyesület - ENSZ égisze alatt működik

ETSI (European Telecommunications Standards Institute) Európai Távközlési Szabványosítási Intézet

NIST (National Institute of Standards and Technology) Amerikai Szabványügyi Testület

BSI (British Standards Institution) Brit Szabványügyi Testület

IETF (Internet Engineering Task Force) Internet szabványok (RFC-k)

CCIMB (CC Interpretation Management Board)

MSZT - Magyar Szabványügyi Testület. Az MSZT feladata: szabványosítás, tanúsítás (minőségirányítás ISO 9001:2000), oktatás, szabványkiadás, szabványforgalmazás, információszolgáltatás. A szabványosítás ún. Műszaki Bizottságok keretében működik. A 819-es Műszaki Bizottság felel az informatikáért. Tulajdonképpen ehhez a műszaki bizottsághoz kapcsolódik a ISO/IEC/JTC1 nemzetközi technikai bizottság..

A szabványosítási szervezetek természetesen egymással is tartják a kapcsolatot tartanak fent:

A JTC/SC27pl. az ITU-T SG7/Q20-val együtt közös szabványokat, vagy ún. „tükör"szövegű dokumentumokat adnak ki – erre példa : „Előírás kívül álló bizalmi felek (TTP) digitális aláírás alkalmazását támogató szolgáltatásaira"

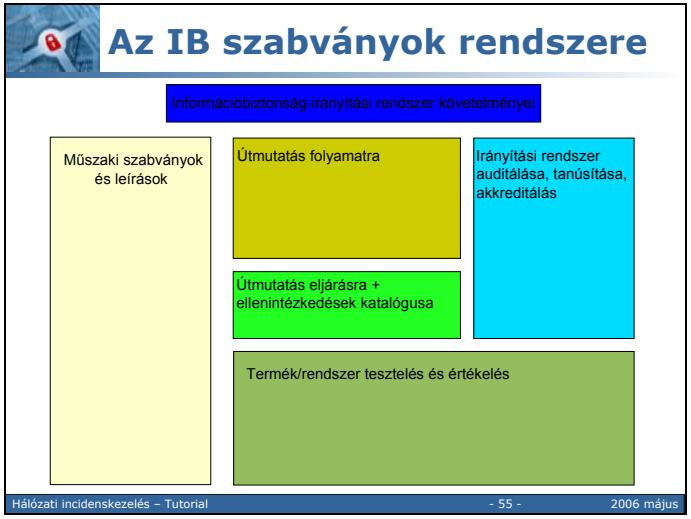
CCIMB – pl. az SC27 publikálta az „egységes szempontokat" IS 15408-ként.

Az ISO TC 68 („Bank és kapcsolódó pénzügyi szolgáltatás") és az SC27 kölcsönösen érdekelt az együttműködésben az informatikai biztonság terén (üzenelhitelesítés, védelmi profilok, biztonsági útmutatók stb.)

ISO TC 215 („Egészségügyi informatika", WG4 – biztonság)

ETSI TC SEC/ESI végezte pl. az elektronikus aláírás szabványosítását Európában (EESSI)

55.



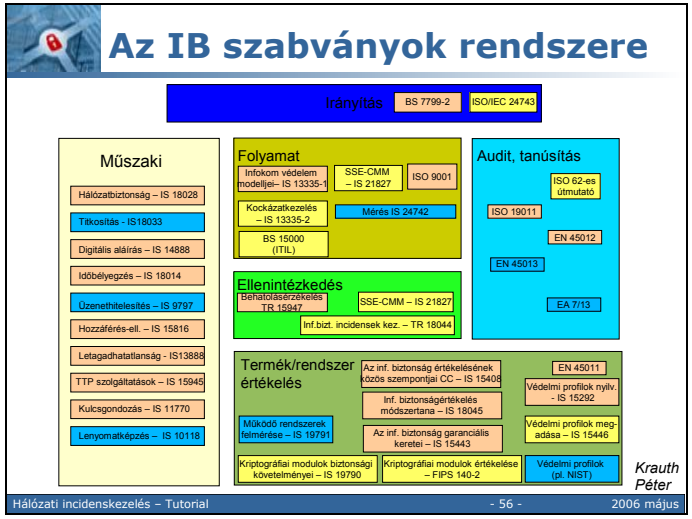
A fenti ábra az informatikai biztonsági (információvédelmi) szabványok téma szerinti csoportosítását mutatja be. (Ez és a köv. ábrát Krauth Pétertől, MSZT vettem át.)

Akkor nézzük a csoportosítást:

- a szabványosítás csúcsán az irányítási rendszer leírása van,
- jobb oldalon az irányítási rendszerek auditálása, tanúsítására vonatkozó szabványok láthatók,
- középen felül folyamatokra (üzemeltetés) vonatkozó szabványok helyezkednek el,
- alatta pedig a eljárások, védelmi módok katalógusa látható,
- külön csoportot képeznek a műszaki szabványok és leírások, ezek technikai jellegűek
- alul láthatók a termékek, rendszerek tesztelésére és értékelésére vonatkozó szabványok

Népesítsük be a fenti ábrát:

56.



57.

Magyar IB szabványok (1)

MSZ ISO/IEC 11770-1:2005	Informatika. Biztonságtechnika. Kulcsgondozás. 1. rész: Keretrendszer
MSZ ISO/IEC 11770-2:2005	Informatika. Biztonságtechnika. Kulcsgondozás. 2. rész: Szimmetrikus technikákat alkalmazó mechanizmusok
MSZ ISO/IEC 11770-3:2005	Informatika. Biztonságtechnika. Kulcsgondozás. 3. rész: Aszimmetrikus technikákat alkalmazó mechanizmusok
MSZ ISO/IEC 13335-1:2005	Informatika. Biztonságtechnika. Az informatikai és távközlési biztonság menedzselése. 1. rész: Az informatikai és távközlési biztonság menedzselésének fogalmai és modelljei
MSZ ISO/IEC TR 13335-3:2004	Informatika. Az informatikai biztonság menedzselésének irányelvei. 3. rész: Az informatikai biztonság menedzselésének technikái
MSZ ISO/IEC TR 13335-4:2004	Informatika. Az informatikai biztonság menedzselésének irányelvei. 4. rész: A biztonsági ellenintézkedések megválasztása
MSZ ISO/IEC TR 13335-5:2004	Informatika. Az informatikai biztonság menedzselésének irányelvei. 5. rész: A hálózatbiztonság menedzselési útmutatója
MSZ ISO 13491-1:2001	Bankügyek. Kriptográfiai eszközök biztonsága (kiskereskedelem). 1. rész: Elvek, követelmények és értékelési módszerek
MSZ ISO/IEC 13888-1:2005	Informatika. Biztonságtechnika. Letagadhatatlanság. 1. rész: Általános ismertetés
MSZ ISO/IEC 13888-2:2001	Információtechnika. Biztonságtechnika. Letagadhatatlanság. 2. rész: Szimmetrikus technikákon alapuló módszerek
MSZ ISO/IEC 13888-3:2001	Információtechnika. Biztonságtechnika. Letagadhatatlanság. 3. rész: Aszimmetrikus technikákon alapuló módszerek
MSZ ISO/IEC 14888-1:2001	Információtechnika. Biztonságtechnika. Digitális aláírások függelékkel. 1. rész: Általános ismertetés
MSZ ISO/IEC 14888-2:2001	Információtechnika. Biztonságtechnika. Digitális aláírások függelékkel. 2. rész: Azonosítás alapú módszerek
MSZ ISO/IEC 14888-3:2001	Információtechnika. Biztonságtechnika. Digitális aláírások függelékkel. 3. rész: Tanúsítvány alapú módszerek
MSZ ISO/IEC 15292:2005	Informatika. Biztonságtechnika. A védelmi profil regisztrációs eljárásai
MSZ ISO/IEC 15408-1:2002	Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 1. rész: Bevezetés és általános modell
MSZ ISO/IEC 15408-2:2003	Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 2. rész: A biztonság funkcionális követelményei
MSZ ISO/IEC 15408-3:2003	Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 3. rész: A biztonság garanciális követelményei
MSZ ISO 15668:2001	Bankügyek. Biztonságos fájlátvitel (kiskereskedelem)
MSZ ISO/IEC 15816:2005	Informatika. Biztonságtechnika. A hozzáférés-ellenőrzés biztonsági információobjektumai
MSZ ISO/IEC 15945:2002	Informatika. Biztonságtechnika. Ajánlás/nemzetközi szabvány bizalmi harmadik fél (TTP) digitális aláírások alkalmazását támogató szolgáltatásaira
MSZ ISO/IEC TR 15947:2004	Informatika. Biztonságtechnika. Az informatikai behatolás érzékelésének keretszabálya
MSZ ISO/IEC 17799:2002	Informatika. Az informatikai biztonság menedzselésének eljárásrendje
MSZ ISO/IEC 18014-1:2004	Informatika. Biztonságtechnika. Időbélyegzési szolgáltatások. 1. rész: Keretszabály
MSZ ISO/IEC 18014-2:2004	Informatika. Biztonságtechnika. Időbélyegzési szolgáltatások. 2. rész: Független adattokokat előállító mechanizmusok
MSZ ISO/IEC 18014-3:2005	Informatika. Biztonságtechnika. Időbélyegzési szolgáltatások. 3. rész: Összerendelt adattokokat előállító mechanizmusok
MSZ ISO/IEC 18028-4:2005	Informatika. Biztonságtechnika. IT-hálózatbiztonság. 4. rész: Biztonságos távoli hozzáférés

Az MSZT honlapjáról lekérdezhetőek a magyar szabványok (www.mszt.hu). A kérdezés történhet:

Szabványjelzet (hivatkozási szám) alapján vagy cím szerint

Besorolás szerint. A szabványok nemzetközi osztályozása (ICS – international classification if standards) háromszintű hierarchiát alkot.

- első szint a szakterület (ebből 40 van) „**35 Információtechnológia. Irodagépek**”
- -azon belül **„040 Karakterkészletek és információkódolás”**

Még egy megjegyzés: vannak angol nyelvű magyar szabványok is, pl. a kékkel megjelöltek.

A számozás utal az eredeti számozásra.

35.100.70 Alkalmazási réteg

35.240.15 Azonosítókártyák és a velük kapcsolatos készülékek

35.240.60 IT alkalmazása a szállításban, kereskedelemben

35.240.80 IT alkalmazása az egészségügyi technikában

35.240.80 IT alkalmazása az egészségügyi technikában

03.120.20 Terméktanúsítás és vállalattanúsítás. Megfelelőségértékelés

58.

Magyar IB szabványok (2)

MSZ ISO/IEC 9594-8:2004	Informatika. Nyílt rendszerek összekapcsolása. Névtár: A nyilvánoskulcs- és az attribútumtanúsítvány keretszabályai
MSZ ISO/IEC 7816-11:2005	Azonosító kártyák. Integrált áramkörös kártyák. 11. rész: Személyellenőrzés biometriai eljárásokkal
MSZ ISO 10202-1:2001	Pénzügyi tranzakciós kártyák. Integrált áramkörös kártyákat használó pénzügyi tranzakciós rendszerek biztonsági architektúrája. 1. rész: A kártya életciklusa
MSZ ISO 10202-2:2001	Pénzügyi tranzakciós kártyák. Integrált áramkörös kártyákat használó pénzügyi tranzakciós rendszerek biztonsági architektúrája. 2. rész: Tranzakciós eljárás
MSZ ISO 10202-3:2001	Pénzügyi tranzakciós kártyák. Integrált áramkörös kártyákat használó pénzügyi tranzakciós rendszerek biztonsági architektúrája. 3. rész: A titkosító kulcsok közötti kapcsolatok
MSZ ISO 10202-4:2001	Pénzügyi tranzakciós kártyák. Integrált áramkörös kártyákat használó pénzügyi tranzakciós rendszerek biztonsági architektúrája. 4. rész: Biztonságos alkalmazási modulok
MSZ ISO 10202-5:2001	Pénzügyi tranzakciós kártyák. Integrált áramkörös kártyákat használó pénzügyi tranzakciós rendszerek biztonsági architektúrája. 5. rész: Algoritmusok használata
MSZ ISO 10202-6:2001	Pénzügyi tranzakciós kártyák. Integrált áramkörös kártyákat használó pénzügyi tranzakciós rendszerek biztonsági architektúrája. 6. rész: A kártyabirtokos visszaigazolása
MSZ ISO 10202-7:2001	Pénzügyi tranzakciós kártyák. Integrált áramkörös kártyákat használó pénzügyi tranzakciós rendszerek biztonsági architektúrája. 7. rész: Kulcsgondozás
MSZ ISO 10202-8:2001	Pénzügyi tranzakciós kártyák. Integrált áramkörös kártyákat használó pénzügyi tranzakciós rendszerek biztonsági architektúrája. 8. rész: Alapelvek és áttekintés
MSZ ISO 9735-5:2000	Az igazgatási, kereskedelmi és közlekedési adatok elektronikus cseréje (EDIFACT). Alkalmazási szintű szintaktikai szabályok. (A szintaktika változatszáma: 4.) 5. rész: A kötegelt EDI biztonsági szabályai (hitelesség, sértetlenség és a származás letagadhatatlansága)
MSZ ISO 9735-6:2000	Az igazgatási, kereskedelmi és közlekedési adatok elektronikus cseréje (EDIFACT). Alkalmazási szintű szintaktikai szabályok. (A szintaktika változatszáma: 4.) 6. rész: A biztonságos hitelesítés és nyugtázás (AUTACK) üzenete
MSZ ISO 9735-7:2000	Az igazgatási, kereskedelmi és közlekedési adatok elektronikus cseréje (EDIFACT). Alkalmazási szintű szintaktikai szabályok. (A szintaktika változatszáma: 4.) 7. rész: A kötegelt EDI biztonsági szabályai (bizalmasság)
MSZ ISO 9735-8:1999	Az igazgatási, kereskedelmi és közlekedési adatok elektronikus cseréje (EDIFACT). Alkalmazási szintű szintaktikai szabályok. (A szintaktika változatszáma: 4.) 8. rész: Kísérő adatok az EDI-ben
MSZ ISO 9735-9:2000	Az igazgatási, kereskedelmi és közlekedési adatok elektronikus cseréje (EDIFACT). Alkalmazási szintű szintaktikai szabályok. (A szintaktika változatszáma: 4.) 9. rész: A biztonsági kulcs- és tanúsítványmenedzselés (KEYMAN) üzenete
MSZ EN 60950:2001	Információtechnikai berendezések biztonsága (IEC 60950:1999 + 2000. február helyesbítés, módosítva)
MSZ EN 60950-1:2001/A11:2004	Információtechnikai berendezések. Biztonság. 1. rész: Általános követelmények
MSZ EN 60950-1:2002	Információtechnikai berendezések. Biztonság. 1. rész: Általános követelmények (IEC 60950-1:2001, módosítva)
MSZ EN 60950-21:2003	Információtechnikai berendezések. Biztonság. 21. rész: Távoli energiabetáplálás (IEC 60950-21:2002)
MSZ EN 726-7:2000	Azonosítókártya-rendszerek. Távközlési integrált áramkörös kártyák és terminálok. 7. rész: Biztonsági modul

35.100.70 Alkalmazási réteg

59.

Magyar IB szabványok (3)

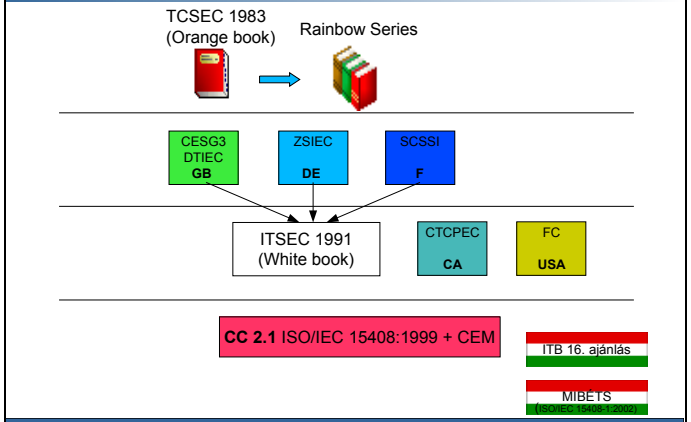
MSZ ENV 1257-1:2001	Azonosítókártya-rendszerek. A személyi azonosító szám kezelésének szabályai szektorok közötti környezetben. 1. rész: A PIN bemutatása
MSZ ENV 1257-2:2000	Azonosítókártya-rendszerek. A személyi azonosító szám kezelésének szabályai szektorok közötti környezetben. 2. rész: A PIN védelme
MSZ ENV 1257-3:2000	Azonosítókártya-rendszerek. A személyi azonosító szám kezelésének szabályai szektorok közötti környezetben. 3. rész: A PIN igazoló ellenőrzése
MSZ EN 1546-2:2000	Azonosítókártya-rendszerek. Szektorok közötti elektronikus pénztárca. 2. rész: Biztonsági architektúra
MSZ ENV 12924:2000	Orvosi informatika. Egészségügyi információs rendszerek biztonsági kategorizálása és védelme
MSZ ENV 13608-1:2000	Egészségügyi informatika. Az egészségügyi kommunikáció biztonsága. 1. rész: Fogalommeghatározások
MSZ ENV 13608-2:2000	Egészségügyi informatika. Az egészségügyi kommunikáció biztonsága. 2. rész: Biztonságos adatobjektumok
MSZ ENV 13608-3:2000	Egészségügyi informatika. Az egészségügyi kommunikáció biztonsága. 3. rész: Biztonságos adatátviteli csatornák
MSZ CR 13694:2001	Gyógyászati informatika. Biztonság és adatbiztonság vonatkozású szoftvertermőségi standardok az eü számára (SSQS)
MSZ ENV 13729:2001	Egészségügyi informatika. Biztonsági felhasználóazonosítás. Szigorú hitelesítést használó mikroprocesszoros kártyák
MSZ EN 14484:2004	Egészségügyi informatika. Az EU adatvédelmi irányelv hatálya alá tartozó személyes egészségügyi adatok nemzetközi adatátvitele. Magas szintű biztonságpolitika
MSZ EN 14485:2004	Egészségügyi informatika. Útmutató az EU adatvédelmi irányelvvel kapcsolatban a személyes egészségi adatok nemzetközi felhasználásokban való kezeléséhez
MSZ EN 61703:2002	A hibamentességi, a használhatósági, a karbantarthatósági és a karbantartás-ellátási fogalmak matematikai kifejezései (IEC 61703:2001)
MSZ EN 12251:2005	Gyógyászati informatika. Biztonságos felhasználóazonosítás az egészségügyben. A jelszavas feljogosítás kezelése és biztonsága
MSZ EN 45011:1999	Terméktanúsítási rendszereket működtető szervezetekre vonatkozó általános követelmények (ISO/IEC Guide 65:1996)
MSZ EN ISO 19011:2003	Útmutató minőségirányítási és/vagy környezetközpontú irányítási rendszerek auditjához (ISO 19011:2002)
MSZ EN 45012:2000	Minőségügyi rendszerek minősítését és tanúsítását/regisztrálását végző szervezetekre vonatkozó általános követelmények (ISO/IEC Guide 62:1996)
MSZE 17799-2:2004	Az információvédelem irányítási rendszerei. Előírás és használati útmutató
MSZE 15100-1:2005	Az informatikaszolgáltatás irányítása. 1. rész: Előírás a szolgáltatásirányításhoz
MSZE 15100-2:2005	Az informatikaszolgáltatás irányítása. 2. rész: Útmutató a szolgáltatásirányításhoz

Hálózati incidenskezelés – Tutorial - 59 - 2006 május

35.100.70 Alkalmazási réteg

60.

Termék/rendszer értékelési szabványok



Hálózati incidenskezelés – Tutorial - 60 - 2006 május

Az USA Védelmi Minisztériuma az 1980-as évek elején dolgozta ki a TCSEC-et (Trusted Computer System Evaluation Criteria), vagy közismertebb nevén az Orange Book-ot. Az ebben foglalt követelményrendszer az USA kormányzati és katonai szervezeteinél telepített **számítástechnikai rendszerek biztonsági szempontból történő** értékelésére szolgáltak. A narancs színű könyvet több kötet követte, amely az egyes részelemek biztonságának értékelésében nyújtott segítséget, ezek az ún. szivárvány kötetek. Ilyenek pl. Jelszókezelés – zöld könyv, naplózás - „tan" napbarna... Ezek mind a mai napig érvényesek, használatuk kötelező.

A TCSEC az informatikai rendszereket négy osztályba sorolja, amely a különböző erősségű védelmi szintek alapján értékelik a beépülő biztonsági szabályozás hatékonyságát. Jelenleg a D, C1,C2, B1,B2, B3, A1 osztályok léteznek, ahol a D a minimális, az A1 a legmagasabb szintű védelmet jelenti.

Az osztályozáshoz a minősítést négy területen kell elvégezni

Biztonsági stratégia (security policy)

Követhetőség (accountability)

Biztosítékok (assurance)

Dokumentálás (documentation)

Ezután több európai ország is fejlesztett saját kritériumrendszert, Nagy-Brittaniában (külön a kormányzat részére: CESG3, külön kereskedelmi célra DTIEC, Németországban ZSIEC, Franciaországban SCSSI)

1991-ben négy ország (a fenti három és Hollandia) dolgozta ki ITSEC 1.2-öt (Information Technology Security Evaluation Criteria), és ez az Európai Közösség közös értékelési rendszere lett. **AZ ITSEC és a TCSEC azonos módon** értelmezi a biztonsági osztályokat, de a TCSEC-kel összevetve finomít az értékelésen (pl. az TCSEC-kel szemben külön kell

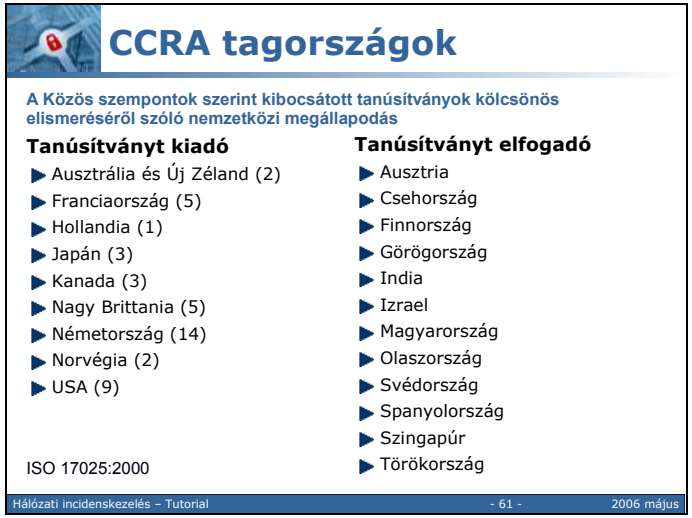
értékelni a veszélyeket elhárító intézkedéseket, és azok teljeskörűségét szolgáló garanciákat.)

Újabb kanadai és amerikai ajánlások után végre az ISO keretein belül kidolgozták a Common Criteria-t, a CC-t (Közös szempontrendszert) és a CEM-t (a közös értékelési módszertan), amely megpróbálta összhangba hozni a korábbi dokumentumok tartalmi és technikai vonatkozásait. 1996. ver.1; 1998 verzió 2; 2000 verzió 2.1. A 3.0-as verzió draft változata elkészült, nyilvános vitára és kísérleti kipróbálásra bocsájtották.

A CEM (Common Evaluation Methodology) a CC társdokumentuma. Célja, hogy leírja azokat a tevékenységeket, melyeket egy értékelő elvégez a CC szerinti értékelés folyamán.

A CC magyarországi honosításának első lépése 1997-ben történt, amikor a MEH támogatásával kiadták az ITB 16. sz. ajánlást (Címe: Common Criteria (CC), az informatikai termékek és rendszerek biztonsági értékelésének módszertana)

61.

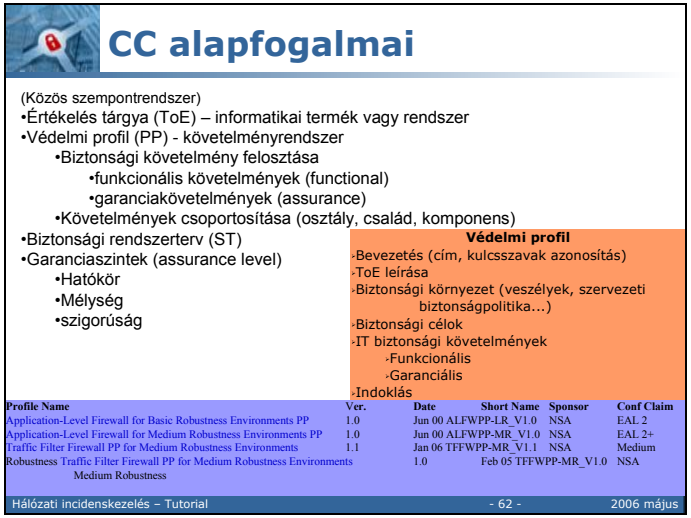


Magyarország 2003-ban csatlakozott a CCRA-hoz. A csatlakozás két lépcsőben valósul meg. Első lépcsőben (jobb oszlop) az országok vállalják, hogy elfogadják a kiállított tanúsítványokat, második lépcsőben pedig már maguk is kiállíthatnak ilyeneket.

Ahhoz, hogy átlépjünk a felsőbb csoportba, saját nemzeti sémát kell kidolgoznunk, működtetnünk, valamint ki kell alakítani a megfelelő bevizsgálási, auditálási folyamatokat. Ehhez pedig értékelő laboratóriumok/szervezetek és tanúsító szervezet felállítása szükséges.

A laboratóriumokat felállításuk után az ISO 17025:2000 szabványnak megfelelően auditáltatni kell. A baloldali oszlopban az egyes országokban található értékelő laboratóriumok számát jeleztük.

62.



http://www.commoncriteriaportal.org/

http://niap.nist.gov/cc-scheme/index.html

A CC informatikai termékek és rendszerek értékelésével foglalkozik.

Értékelés tárgya (target of evaluation): IT termék vagy rendszer

Védelmi profil (protection profile): előre megadott követelményelemekből egy adott feladatot lefedő, önmagában konzisztens követelményrendszer. Az adott feladat lehet pl. vírusírtóra, tűzfalra, operációs rendszerekre, biometriára, PKI-ra, adatbázisra stb. vonatkozó követelményrendszer.)

A védelmi profilokat a különböző alkalmazásokra felkészült szakemberek állítják össze – feladatspecifikus kockázatelemzés után. Természetesen egyre újabb PP-k jelennek meg. Jelenleg a NIST lapján kb 40 db PP látható, a másik (francia) honlapon kb 50. db.

A követelményeket két nagy csoportba osztják:

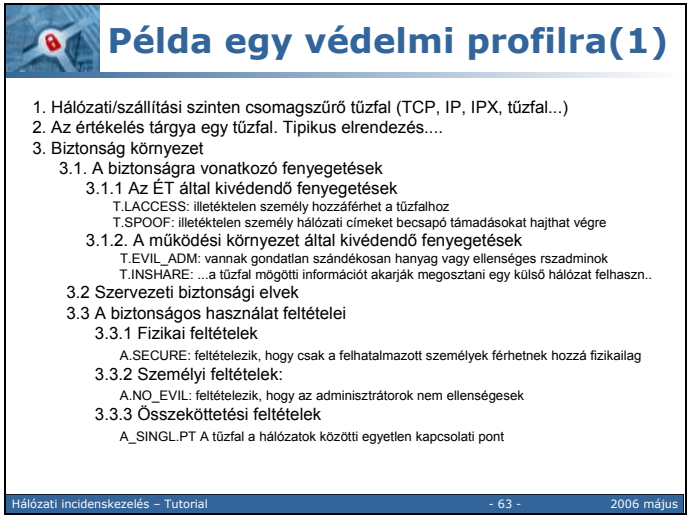
- funkcionális követelmények – az értékelés tárgyának a biztonság szempontjából lényeges funkcióira vonatkoznak
- garanciakövetelmények – a vizsgálatokkal szembeni követelések. A vizsgálatok garantálják,hogy az értékelés tárgya eleget tesz a funkcionális biztonsági követelményeknek, a megvalósítás megfelelő.

Mind a biztonsági, mind a garanciális követelményeket osztályozzák. A legfelső osztály a csoport, a csoport családokból áll, a család pedig komponensekből. A komponensek között hierarchia lehet.)

Garanciaszint: az értékelés tárgyának vizsgálatát milyen mélységben, milyen erőforrás-ráfordítással végezték

BRT – biztonsági rendszerterv/security target

63.



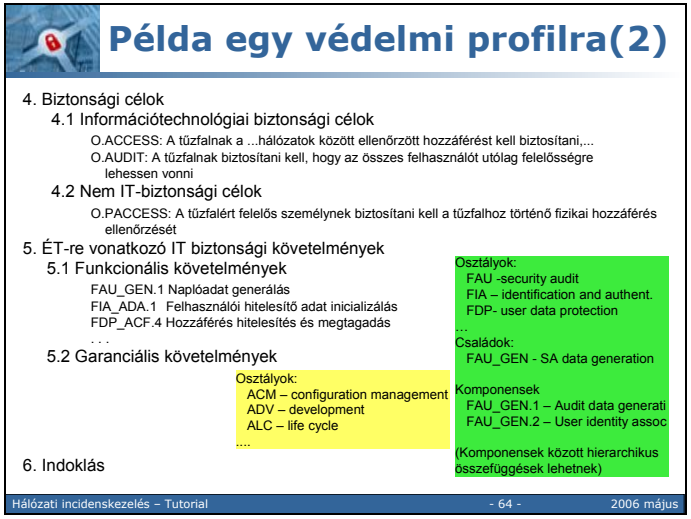
Bevezetés:

- védelmi profil azonosítás (címe, kulcsszavak), áttekintése

Az értékelés tárgya: tűzfal, tipikus elrendezésről egy ábrát közöl, mire jó a tűzfal (hálózati tartományok szétválasztására), a forgalom ellenőrzése hálózati/szállítási szinten történhet

Biztonsági környezet

64.



Funkcionális követelmények osztályainak száma: 10 osztály

FAO - security audit

FCO – communication

FCS – cryptographic support

FDP – user data protection

FIA – identification and authentication

FMT – security management

FPR – privacy

FPT – protection of TSF(ToE Security Function)

FRU – resource utilisation

FTA – ToE access

Garanciakövetelményekhez tartozó osztályok 7 osztály:

ACM – Configuration management

ADO – delivery and operation

ADV – development

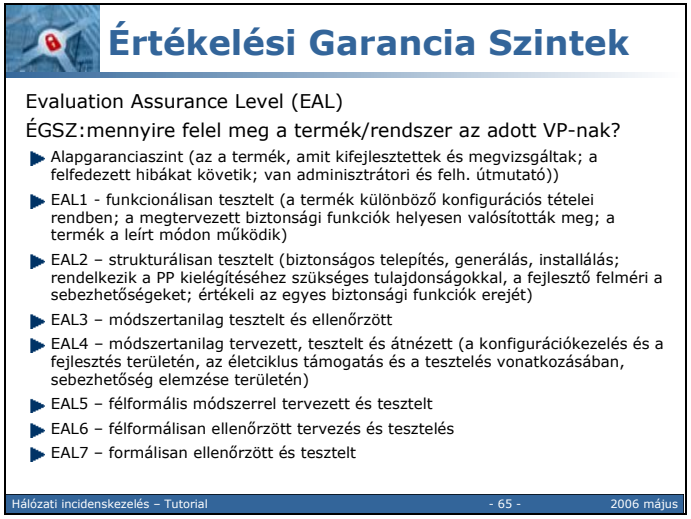
AGD – Guidance documents

ALC – life cycle support

ATE – tests

AVA -vulnerability assessment

65.



A védelmi profiloknál kétfajtakövetelményt állítottak fel, funkcionális és garanciakövetelményt. A CC szerint értékelt termék/rendszer két értékelést kap:

- funkcionálisan megfelel-e az adott Védelmi profil elvárásainak?
- mennyire biztos ez a megfelelés? (Hányas ÉGSZ-en volt biztosítva az értékelés?)

Egy felhasználó – ftlenül az értékelés szintjéről garanciát kap az alábbiakról:

- azt a terméket kapja, amit a gyártó kifejlesztett és az értékelő megvizsgált (tehát a szállítás során nem kompromittálódik)
- felfedezett hibákat nyomon követik, kijavítják
- a termékhez admin és felh. útmutatókat adnak, admin: installálás, biztonságos működtetés...)

ÉGSZ1:legnyilvánvalóbb hibák kimutatása min. ellenőrzési és értékelési költség mellett)

Az alapgaranciaszinten kívül az alábbi területeken ad többletgaranciát:

- -a fejlesztő nem keveri össze a termék különböző konfigurációs tételeit
- a fejlesztés során a megtervezett biztonsági funkciókat helyesen bontották le és valósították meg
- -a termék a leírt módon működik

ÉGSZ2: lényegesen magasabb garanciát biztosító szint, többletgaranciák:

- a termék biztonságos telepítéséhez, generálásához és indításához szükséges lépéseket az átadott dokumentációban leírta
- a biztonsági funkciókat helyesen valósították meg
- a fejlesztő felméri a termék létrehozása és működtetése során jelentkező sebezhetőségeket,

- a fejlesztő értékeli az egyes biztonsági funkciók erejét: alalp/közepes/erős

EAL4:tervszerűen tervezett, tesztelt és áttekintett – ez a a szint, ami gazdaságosan megvalósítható utólag egy már létező termékre. (A magasabb garanciaszintek csak úgy érhetők el, ha már a tervezést alárendelik a garanciaszintnek)

kb 150 értékelt terméka NIST oldalain, ebből 2 EAL5 és egy EAL7:

EAL5 XTS 400 op rsz.; multiple domain solution EAL5,7:Tenix Interactive Link Version 5.1 , Tenix Interactive Link Data Diode Device Version 2.1

66.

Példa az értékelt termékekre

Tűzfalak

Product Name / Manufacturer	Conformance Claim	PP	Valid. Date
CyberGuard Firewall/VPN v6.1.2			
CyberGuard Corporation	EAL 4 Augmented..	PP[1],PP[2]	Jun 05
CyberGuard Firewall/VPN v6.2.1			
CyberGuard Corporation	EAL 4 Augmented ...		Dec 05
Cryptek, Inc., DiamondTEK (DiamondCentral (NSC Application S/W version 2.4.0.5, NSD-Prime F/W version 2.4.0.3) and NSD (Dia			
Cryptek, Inc.	EAL 4		Dec 05
DiamondTEK			
Cryptek Secure Communications, LLC	EAL 4		Jun 02
Lucent Technologies Lucent VPN Firewall V7.0 (Patch 531)			
Lucent Technologies, Inc.	EAL 2		Oct 03
Lucent Technologies Lucent VPN Firewall (LVF) version 7.2 with patch 292			
Lucent Technologies, Inc.	EAL 4	PP[3]:	Jan 06
Marconi SA-400 Firewall			
Marconi Communications	EAL 2		Jul 04

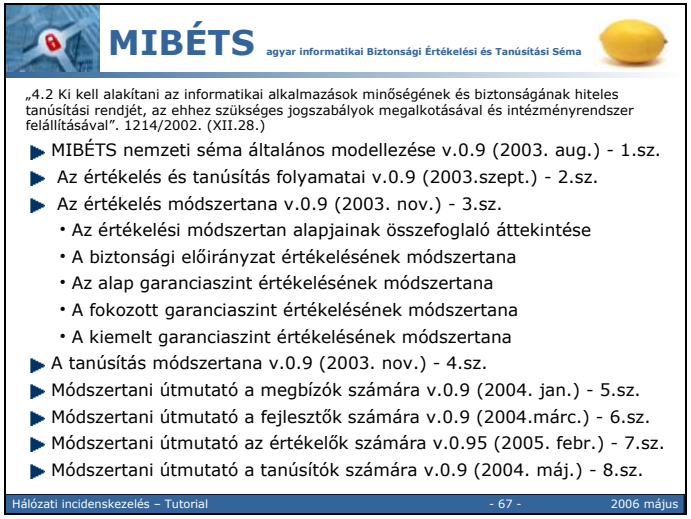
PP[1]: U.S. Government Application-Level Firewall Protection Profile for Low-Risk Environments
PP[2]: U. S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments
PP[3]: Traffic Filter Firewall Protection Profile for Low-Risk Environments, V1.1, Apr 1999

Hálózati incidenskezelés – Tutorial - 66 - 2006 május

A kiértékelés eredménye egy olyan dokumentum, amely kijelenti, hogy a termék/rendszer

- egy adott védelmi profilnak megfelel
- egy adott biztonsági cél követelményeinek megfelel
- -a megfelelés az 1-7 szint valamelyikén történik

67.



Visszatérve a CC + CEM-hez, két síkon zajlik a folyamat

A termékre vonatkozó szint– ez a CC – teljes egészében magyar szabvány (MSZ 15408)

azaz megfelel-e a termék azoknak a biztonsági tulajdonságoknak, amit ígér/állít magáról

Milyen a termék biztonsága, könnyen feltörhető-e

Elég biztonságos- a termék ahhoz, hogy egy adott környezetben használják

Az értékelés folyamata/gyakorlata - CEM

Az értékelés során helyes módszereket alkalmazunk-e?

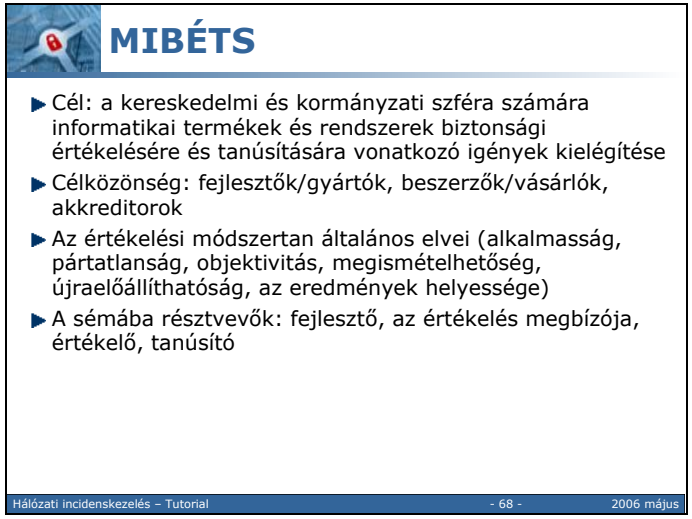
Elég biztonságos-e az értékelést végző labor?

A MITS készítéséről rendelkező 1024/2002 (XII.28.) sz. kormányhatározat többek között azt a feladatot tűzte ki célul: „4.2 Ki kell alakítani az informatikai alkalmazások minőségének és biztonságának hiteles tanúsítási rendjét, az ehhez szükséges jogszabályok megalkotásával és intézményrendszer felállításával”. 2003. óta előkészületben van az az IHM rendelettervezet, amely az értékelést végző szervezetek kijelölésnek szabályairól valamint magáról a tanúsításról szól. (Ez azóta is csak tervezet.)

A MIBÉTS dokumentumai fent láthatók.

A MIBÉTS az értékelés módszertanára a CEM (Közös Értékelési módszertan) egyszerűsített változatát dolgozta ki és fogadja el. Ez tulajdonképpen előkészítő anyag a teljes körű csatlakozáshoz.

68.



Célnál további feltételek is vannak: költség-hatékony és eredményes legyen az értékelés.

Célközönség:

fejlesztők/gyártók lehetőséget kapnak arra, hogy biztonsági állításokat fogalmazzanak meg

beszerzők/vásárlók: bizonyosságot szerezhetnek arról, hogy a felkínált termékek a biztonsági igényüket kielégítik

akkreditorok:meggyőződhetnek arról, hogy az őket érintő biztonsági fenyegetéseket kellően figyelembe veszi

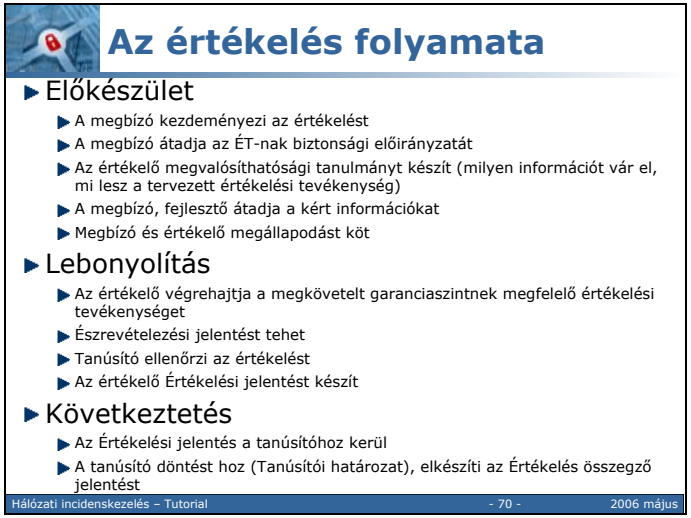
Módszertani elvek:

- alkalmasság: az alkalmazott értékelési tevékenységnek alkalmasnak kell lennie a megcélzott garanciaszint eléréséhez
- pártatlanság: elfogultságmentesség
- objektivitás szubjektív elemek vagy személyes vélemény csak min. mértékben
- megismételhetőség: ugyanazon termék ugyanazon értékelőkkel megismételve ugyanazt az eredményt adja
- újraelőállíthatóság: ugyanarra a termékre, ugyanazon követelmények mellett megismételt értékelésnek ugyanoda kell vezetnia
- az eredmények helyessége: az értékels eredményének teljesnek és szakmailag hibátlannak kell lennie

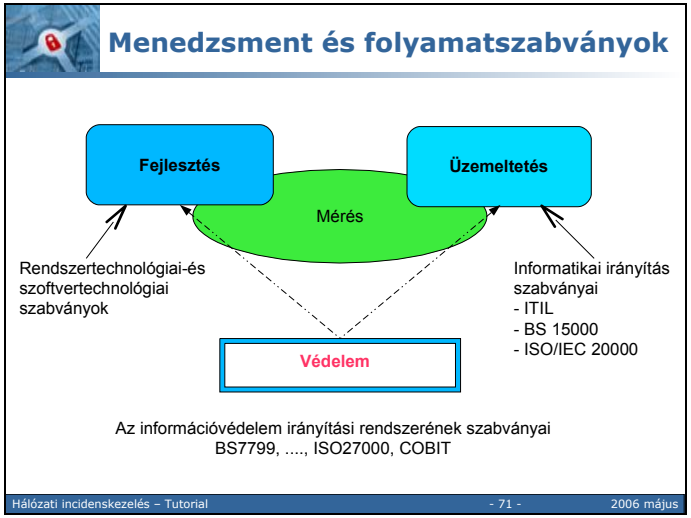
69.


Résztvevők közti kapcsolat, felelősség
- az értékelés támogatása
- az értékelésre átadandó bizonyítékok fejlesztése és kezelése
- szerződések létrehozása
- az értékelésre átadandó bizonyítékok biztosítása
fejlesztő
megbízó
értékelő
tanúsító
- bizonyítékok átvétele
-az értékelési tevékenység végrehajtása
- támogatás kérése, nyújtása
- a tanúsításra átadandó bizonyítékok biztosítása
- az értékelői vélemény indoklása
- az általános elveknek és előírásoknak való megfelelés
- az értékelés ellenőrzése
- a tanúsításra átadott bizonyítékok átvétele és megtekintése
- az értékelés megfelelő módjának biztosítása
- az értékelések támogatása előírások létrehozásával, a követelmények értelmezésével és iránymutatással
- az értékelői határozat jóváhagyása vagy elvetése
-a tanúsító szervezet számára a Tanúsító határozat dokumentálása és indoklása
Hálózati incidenskezelés – Tutorial - 69 - 2006 május

70.

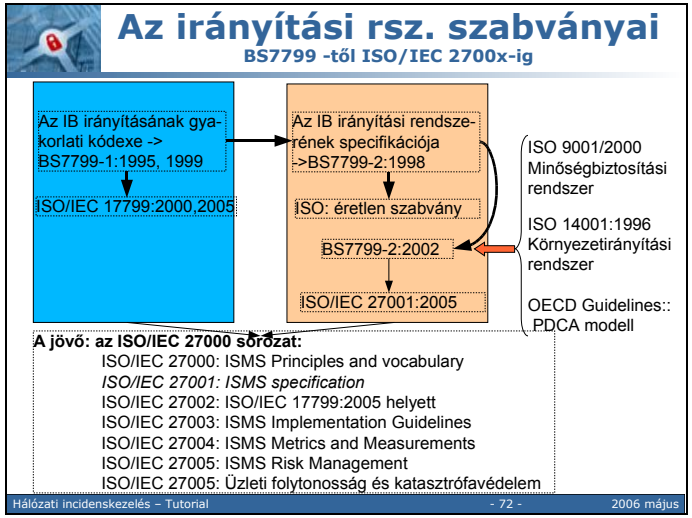

Az értékelés folyamata
Előkészület
A megbízó kezdeményezi az értékelést
A megbízó átadja az ÉT-nak biztonsági előirányzatát
Az értékelő megvalósíthatósági tanulmányt készít (milyen információt vár el, mi lesz a tervezett értékelési tevékenység)
A megbízó, fejlesztő átadja a kért információkat
Megbízó és értékelő megállapodást köt
Lebonyolítás
Az értékelő végrehajtja a megkövetelt garanciaszintnek megfelelő értékelési tevékenységet
Észrevételezési jelentést tehet
Tanúsító ellenőrzi az értékelést
Az értékelő Értékelési jelentést készít
Következtetés
Az Értékelési jelentés a tanúsítóhoz kerül
A tanúsító döntést hoz (Tanúsítói határozat), elkészíti az Értékelés összegző jelentést
Hálózati incidenskezelés – Tutorial - 70 - 2006 május

71.



Ez az ábra mutatja az menedzsment és folyamatszabványok fókuszterületeit. Egy informatikai rendszer vagy termék fejlesztése során tekintettel kell lenni a rendszer- és szoftvertechnológiai szabványokra. Az üzemeltetés során az informatikai irányítás szabványait kell figyelembe venni. A védelemre mind a fejlesztés, mind az üzemeltetés során gondolnunk kell, tehát az információvédelem irányítási rendszerének (azaz a menedzsmentnek) a szabványa így jön a képbe.

72.



Ez a szabvány nem az USA-ból, hanem Nagy-Brittaniából indult ki. 1987-ben az akkori Kereskedelmi és Ipari Minisztérium (Department of Commerce and Trade) megalapította a CCSC-t (Commercial Computer Security Center), kettős feladattal:

- a számítógépes termékek/rendszerek biztonsági értékelését oldja meg (ITSEC)
- segítse az embereket (a felhasználókat) a helyes biztonsági szabályzatok, gyakorlatok alkalmazásában.

Ennek eredményeképp 1989-ben elkészült a „**User Code of Practice”**, ami konzultációk és finomítások után 1995-ben brit szabvánnyá vált: „A code of practice for information security management” BS7799:1995. - Az információbiztonság irányításának gyakolati kódexe – lényegében a helyes biztonsági gyakorlatok átfogó katalógusa.

Az első rész 2000. decemberében kis módosításokkal ISO/IEC 17799:2000 néven szabvánnyá vált.

Azonban korán kiderült, hogy a szabvány nem ad arra választ, hogy az adott vezető melyik védelmi eszközt alkalmazza és melyiket ne. Ekkor fogalmazták meg a szabvány második részét, „Az információbiztonság irányításának specifikációja”,-t BS7799:2. A megfogalmazás során derült, hogy ez a rész sokkal fontosabb, mint az első. Mert a visszacsatolási hurkok bevezetésével a vezető figyeli és ellenőrzi a biztonsági rendszert, így minimalizálja a biztonsági kockázatot, és így sikerül a szervezeti, a vevői és jogi igényeknek megfelelni.

Ezután a BS7799:2-t jó néhány ISO szabvánnyal harmonizálták, és figyelembe vették az OECD Guidelines for the Security for the Security of Information Systems and Standards Plan-Do-Check-Act modelljét, és elkészült a 2002-es változat.

A jövő a 27000-es sorozat:

27001 -követelményrendszer

27002 – BS7799:1 új neve

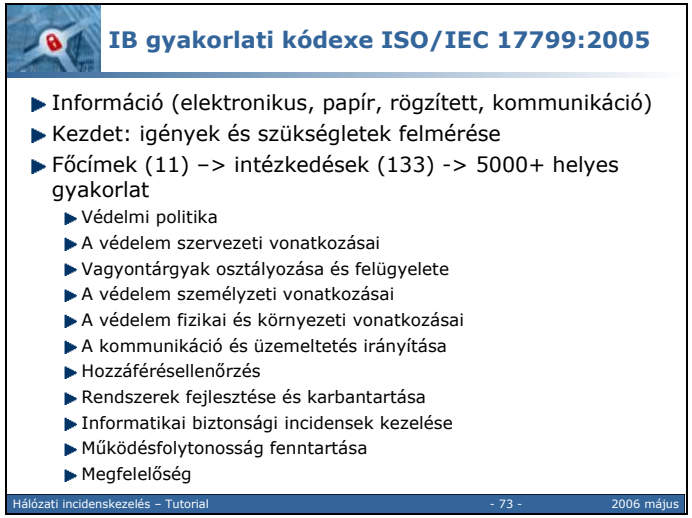
27003: Útmutató a 27001-hez

27004: ISM measurement and

27005: kockázatkezelés

MO: ISO 17799.2004 előszabvány

73.



A szabvány alapfogalma az **információ.** Az információt széles értelemben veszi:

- elektronikus fájl (szoftver fájl, adatfájl)
- papír alapú dokumentum (nyomtatott, kézzel írt, fényképek)
- rögzített (recording) dokumentumok: video és audio
- kommunikáció
  - beszélgetés (telefon-, mobil-, szemtől-szemben történő -)
  - üzenetek(email, fax, video, instant, fizikai)

Az információnak értéke van, tehát az **vagyontárgy**. A vagyon védeni kell, és védeni kell a vagyont tároló infrastruktúrát is. Védeni kell a fenyegetésről...

Az ISO 17799 szerint a védelem **intézkedések (control)** alkalmazásával valósítható meg. Az intézkedések lehetnek szabályzatok, eljárások, folyamatok és szervezési elemek.)

Az információ védelmére intézkedéseket kell kifejleszteni, telepíteni, figyelni (monitor), értékelni és javítani.

A szabvány szerint **induláskor az igényeket és szükségleteket** fel kell mérni:

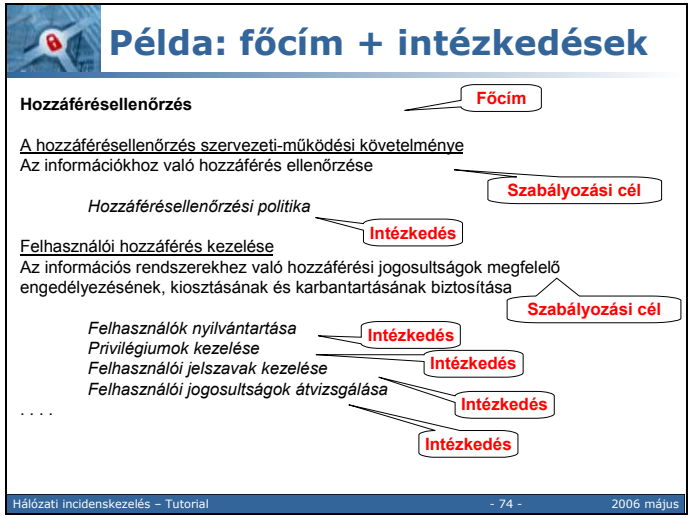
- kockázatelemzést kell végezni (fenyegetések, sebezhetőségek)
- jogi környezet átnézése (szabályzatok, szabályozások, előírások a szervezetben és a partnereknél)
- saját igények felmérése

A szabvány 11 főcím alatt 133 biztonsági intézkedést határoz meg, amelyek további intézkedéseket foglalnak magukban, így 5000 felett van a helyes gyakorlat kontrolljai és elemei

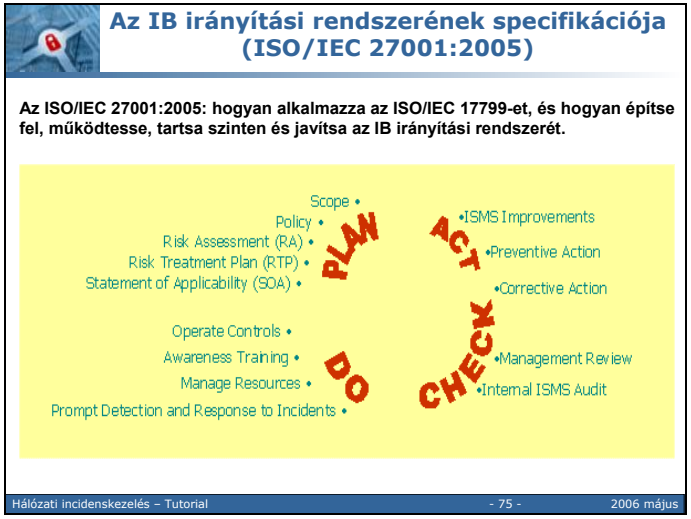
Minden intézkedés 4 részből áll:

- mi a szabályozási cél,
- hogy lehet az adott célt elérni (intézkedések - control)
- hogy lehet megvalósítani/implementálni a cél eléréséhez szükséges eszközöket
- útbaigazítás, magyarázat (note)

74.



75.



PDCA – ez az amit az OECD egyik ötletéből vettek át. A négy lépés (tervezés, megvalósítás, ellenőrzés, beavatkozás) állandó körforgásban van.

Tervezés:

Az első lépés az ISMS (IBIR) hatókörének meghatározása: az egész szervezet, egy részleg vagy csak egy szolgáltatás.

Irányvonal (policy): miért fontos az IB; van-e valamilyen speciális fenyegetettség; mit szeretne elérni a CIA (titkosság, sértetlenség, rendelkezésreállás) területén; mi az elfogadható kockázat; van-e valamilyen törvényi vagy egyéb korlátozás, amit be kell tartani;...

kockázatok felmérése: mit szeretne védeni; milyen kockázatok vannak; mi az kockázat, amit még elviselhetőnek ítél; mérje fel a kockázatokat a bekövetkezés valószínűsége és a kiváltott hatás függvényében,,,

Kockázatkezelési terv: egy adott kockázatot elfogad-e és ha bekövetkezik azonnal tudna arra válaszolni; egy másik kockázatot mindenáron el szeretne kerülni vagy harmadik félre hárítani (biztosítás)?...

Alkalmassági nyilatkozat: az ISO/IEC 17799 135 db intézkedésel melyeket szeretné alkalmazni, és melyeket nem.

Megvalósítás:

Hajtsa végre az intézkedéseket: szükség van eljárásokra, amelyek segítségével észleli az incidenseket és válaszol rájuk, képeznie kell az embereket, biztosítani kell a megfelelő infrastruktúrát stb.

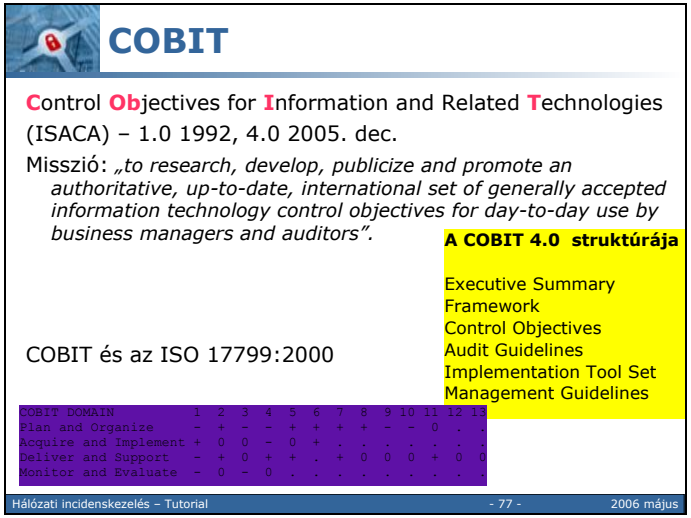
Ellenőrzés: az intézkedések megfelelően működnek és el is érik a céljukat

Beavatkozás: az ellenőrzés eredményeképp megteendő lépések: javító, megelőző akciók

76.

IBIV, IBIK státusza még bizonytalan.

77.



Az IB irányítási rendszerek közé tartozik, tudtommal még nem ISO szabvány.

A COBIT tulajdonképpen a helyes gyakorlatok gyűjteménye, amelyet az ISACA és az IT Governance Institute (ITGI) 1992-ben állított össze. A dokumentumot a **vezetők, auditorok és IT felhasználók számára készítették, általánosan elfogadott intézkedéseket, i**ndikátorokat, folyamatokat és helyes gyakorlatot tartalmaz. Célja, hogy az IT technológia használatából származó előnyöket maximálisan kihasználják a vállalatok/intézmények IT irányításánál és ellenőrzésénél.

Az első változat 1996-ban, a második 1998-ban, majd 2000-ben, a legújabb negyedik változat 2005. decemberében jelent meg. (Ez utóbbi már tartalmazza azokat a módosításokat, amelyeket az Enron botrány miatt tettek bele, és ami az hiíres Sarbanes-Oxley törvényhez vezetett (USA)).

A COBIT struktúrája:

- vezetői összefoglaló
- keretrendszer
- Kontroll célkitűzések
- implementációs eszköztár
- auditálási útmutató (Ingyenesen letölthető, kivéve ezt!!!)

A COBIT keretrendszere 34 informatikai folyamatot határoz meg, ehhez kapcsolódnak a (*215) részletes kontroll célkitűzést* tartalmaz 4 tárgykörben: Tervezés és Szervezés, Beszerzés és telepítés, Szolgáltatás és Támogatás valamint Monitorozás és Értékelés.

A kontroll: mindazon szabályok, eljárások, gyakorlati módszerek és szervezeti struktúrák, amelyeket arra a célra terveztek, hogy az üzleti célkitűzések megvalósítását elősegítsék, és a nemkívánatos eseményeket megelőzzék, felderítsék és korrigálják.

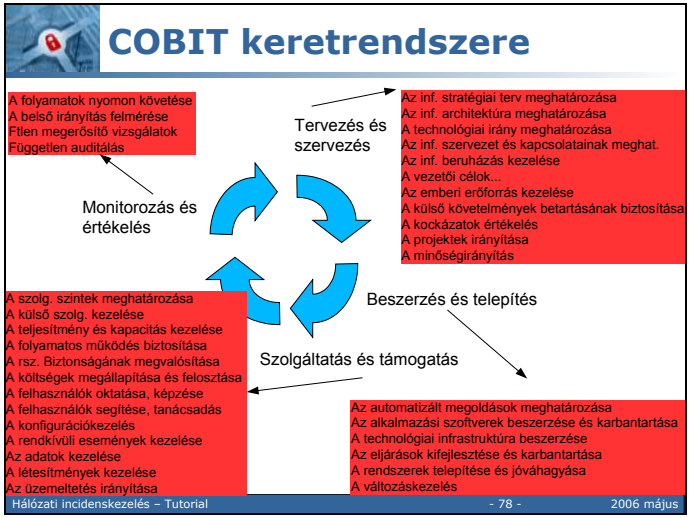
A COBIT az IT irányítás és vezetés nemzetközileg elfogadott keretrendszere. Az ISO17799:1 a helyes gyakorlatok kézikönyve, nem versenyeznek, hanem egymást

kiegészítik. A COBIT szélesebb területet fed le, az ISO17799 jobban fókuszál a biztonság területére.

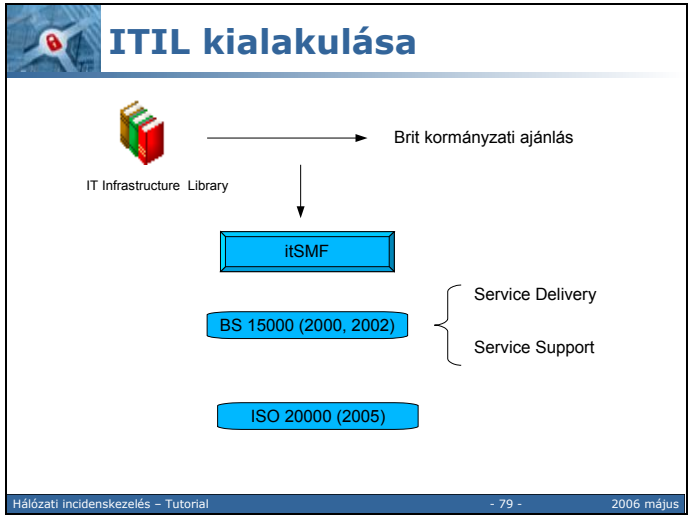
COBIT DOMAIN	1	2	3	4	5	6	7	8	9	10	11	12	13
Plan and Organize	–	+	–	–	+	+	+	+	–	–	0	.	.
Acquire and Implement	+	0	0	–	0	+	.	.	.	.	.	.	.
Deliver and Support	–	+	0	+	+	.	+	0	0	0	+	0	0
Monitor and Evaluate	–	0	–	0	.	.	.	.	.	.	.	.	.

+ jó illeszkedés; - nincs vagy kicsi illeszkedés, 0 részleges illeszkedés, . nincs

78.



79.



A 80-as évektől kezdve az informatikai rendszerek egyre mélyebben épültek be a vállalatok, intézmények életébe, és egyre inkább függő helyzetbe kerültek a vállalatok az informatikától. Az informatika üzemeltetése során felmerült problémára az angol CCTA (Central Computer and Telecommunicaton Agency) próbált választ adni avval, hogy összegyűjtötte és egységes formába öntötte a helyes gyakorlatot. Ez a dokumentum az ITIL: IT Infrastructure Library. Ebben a sorozatban mintegy 40 kötet látott napvilágot, és ez lett az alapja és névadója a kialakult módszertannak.

Ennek alapján megszületett a brit kormányzati ajánlás, amely a legfontosabb 10 témát tartalmazza, és ez az informatikai szolgáltatásirányítási és üzemeltetési módszertan „de facto” szabvánnyá vált.

Ezután Európa több országában is terjedt, helyi fórumok jöttek létre (a második éppen Hollandiában.) Végül megalakult az IT Service Management Forum (itSMF), amely segítette a ITIL terjedését, másrészt vigyázott arra, hogy egységes maradjon az ajánlás.

Mo.-on az MTA KFKI-ban és a MATÁV Informatikánál jelent meg először, majd a MEH ajánlások között jelent meg. (15. ajánlás)

A 2000-es évre ár nagyon sok nagyvállalat használta, pl. a Microsoft. Ebben az évben az ITIL brit szabvány lett BS 15000 számmal. A brit szabvány két kötetben jelent meg, az egyik a Szolgáltatásnyújtás, a másik a szolgáltatás támogatás.

2002-be a szabvány lényegesen megújult, majd 2005-ben javasolták, hogy gyorsított módszerrel ISO szabvány is legyen ISO 20000.

80.

ITIL „az informatika üzlet és az üzlet informatika”

- Informatikai szolgáltatásmenedzsment
- ~ célkitűzései:
  - Az informatika szolgáltatását hozzá kell rendelni a jelen és a jövő üzleti igényeihez és felhasználóihoz
  - Javítani kell a nyújtott információszolgáltatás minőségén
  - Csökkenteni kell a szolgáltatások hosszú távú költségét

Szolgáltatásbiztosítás	Szolgáltatástámogatás
→Szolgáltatási szint menedzsment	→Ügyfélszolgálat
→Rendelkezésreállás menedzsment	→Incidensmenedzsment
→Informatika-szolgáltatás folytonosság menedzsment	→Problémamenedzsment
→Kapacitásmenedzsment	→Változáskezelés
→Informatikaszolgáltatás pénzügyi irányítása	→Konfigurációkezelés
	→Kiadáskezelés

Hálózati incidenskezelés – Tutorial - 80 - 2006 május

Az informatikai szolgáltatásmendezsment egymással együttműködő folyamatok együttese, amelynekfeladata, hogy az ügyféllel megállapodott szolgáltatási szinteken biztosítsa az informatika szolgáltatás minőségét.

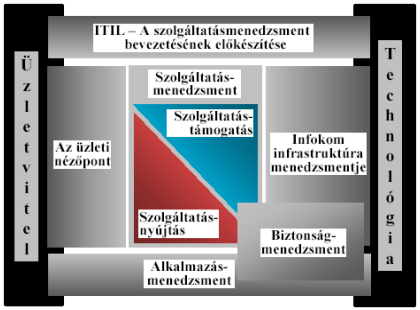
Az informatikai szolgáltatásmenedzsment a témaköröket két fő csoportba szervezte:

- szolgáltatásbiztosítás
- szolgáltatástámogatás

81.

ITIL dokumentációja

1.4. A kialakult dokumentáció



1. ábra: Az ITIL dokumentációs rendszere

Forrás: http://www.itsmf.hu

Hálózati incidenskezelés – Tutorial - 81 - 2006 május

Szolgáltatástámogatás

Szolgáltatásnyújtás

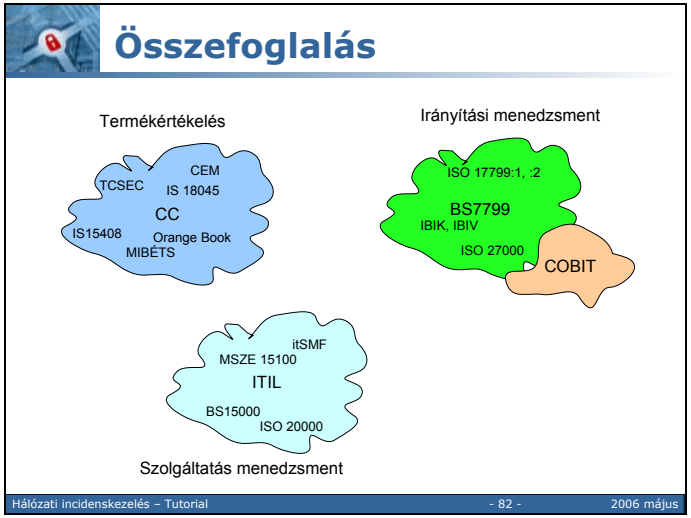
Az üzleti nézőpont: az üzletvezetést ismerteti meg az üzleti folyamatokat támogató informatikai és kommunikációs technológia összetevőivel, tervezésével és a bevált gyakorlatokkal.

Az infokommunikációs technológia menedzsmentje: aAz ICT infrastruktúra menedzsmentjének minden aspektusát tárgyalja: az üzleti követelmények meghatározását, a tenderezést, az infrastruktúra alkatrészeinek és az információszolgáltatás egyes elemeinek tesztelését, telepítését, üzembeállítását, karbantartását.

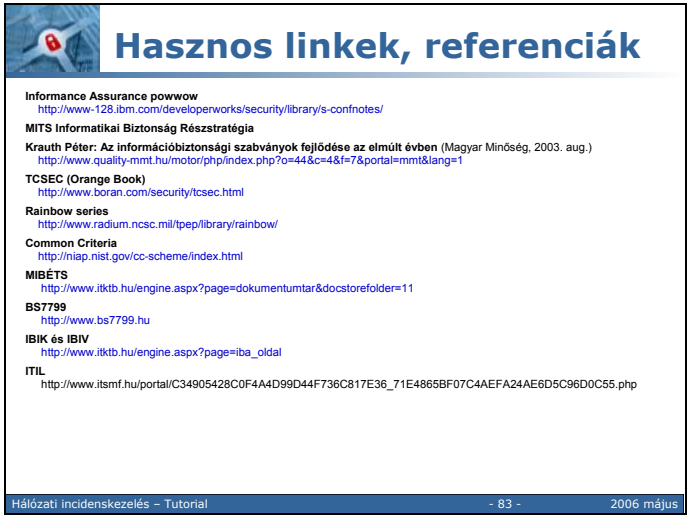
Alkalmazásmenedzsment: az ~tárgykörét dolgozza fel a kezdeti üzleti igényektől egészen a megszüntetésig.

Biztonságmenedzsment: különálló, de integrálódik a meglévő folyamatokba,

82.



83.



1. National Information Assur ance Glossary

Készítette: National Security Telecommunications and Information System Security Committee (NSTISSC, No. 4009) - http://www.cultural.com/web/security/infosec.glossary.html (1992. jún.)

2. Internet Security Glossary (RFC 2828)

http://www.ietf.org/rfc/rfc2828.txt

3. Informance Assurance powwow (indián ceremónia)

http://www-128.ibm.com/developerworks/security/library/s-confnotes/

MITS

http://www.bs7799.hu.

4. Krauth Péter: Az információbiztonsági szabványok fejlődése az elmúlt évben (Magyar Minőség, 2003. aug.)

http://www.quality-mmt.hu/motor/php/index.php?o=44&c=4&f=7&portal=mmt&lang=1
http://www.itktb.hu/engine.aspx?page=dokumentumtar&DocStoreFolder=13

5. TCSEC (Orange Book) http://www.boran.com/security/tcsec.html

6. Rainbow series http://www.radium.ncsc.mil/tpep/library/rainbow/

7. CC http://www.commoncriteriaportal.org

8. MIBÉTS: http://www.itktb.hu/engine.aspx?page=dokumentumtar&docstorefolder=11

9. IBIK és IBIV: http://www.itktb.hu/engine.aspx?page=iba_oldal

10. ITIL:

http://www.itsmf.hu/portal/C34905428C0F4A4D99D44F736C817E36_71E4865BF07C4AEFA24AE6D5C96D0C55.php1. NATO – a biztonság összetevői
http://www.mki.gov.hu/file/Biztonsagpolitikai_agazat.ppt

11. Az informatikai szabványokról általában

http://www.martin-charles.hu/forrasanyagok/szabvanyokrol.html

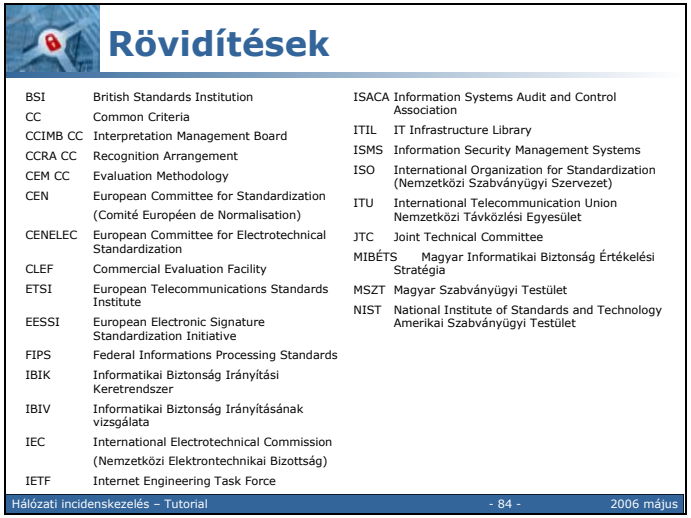
12. Common Criteria 3.0-as draft verzió készen

http://niap.nist.gov/cc-scheme/index.html

13. CCRA országok

http://www.commoncriteriaportal.org/public/developer/index.php?menu=8

84.

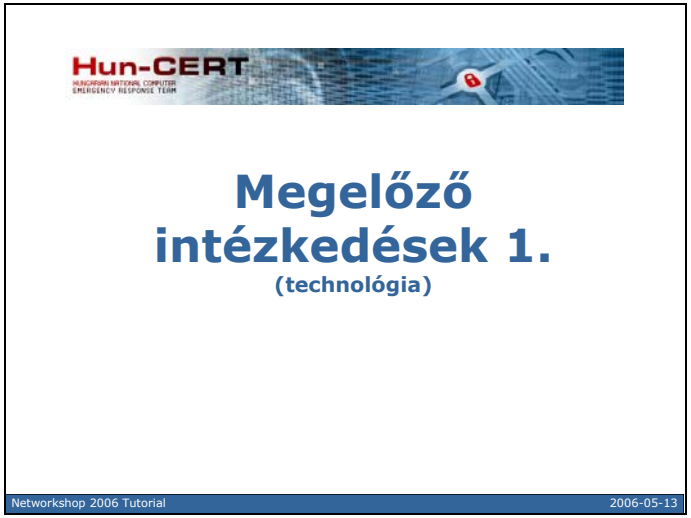


BSI	British Standards Institution
CC	Common Criteria
CCIMB	CC Interpretation Management Board
CCRA	CC Recognition Arrangement
CEM	CC Evaluation Methodology
CEN	European Committee for Standardization (rövidités: Comité Européen de Normalisation)
CENELEC	European Committee for Electrotechnical Standardization
CLEF	Commercial Evaluation Facility
ETSI	European Telecommunications Standards Institute (Európai Távközlési Szabványosítási Intézet)
EESSI	European Electronic Signature Standardization Initiative
FIPS	Federal Informations Processing Standards
IBIK	Informatikai Biztonság Irányítási Keretrendszer
IBIV	Informatikai Biztonság Irányításának vizsgálata
IEC	International Electrotechnical Commission (Nemzetközi Elektrontechnikai Bizottság)
IETF	Internet Engineering Task Force (RFC-k)
ISMS	Information Security Management Systems
ISO	International Organization for Standardization (Nemzetközi Szabványügyi Szervezet)
ITU	International Telecommunication Union Nemzetközi Távközlési Egyesület

(1947 óta az ENSZ távközlésre szakosodott szervezete. Feladata az egész hírközlési szektor munkájának összehangolása, koordinálása kezdve afejlesztlsektől, szabványoktól, egészen az egyes frekvenciák, műholdpályák kiosztásáig.)

JTC	Joint Technical Committee
MIBÉTS	Magyar Informatikai Biztonság Értékelési Stratégia
MSZT	Magyar Szabványügyi Testület
NIST	National Institute of Standards and Technology Amerikai Szabványügyi Testület

85.



86.

Tartalom

Bevezetés
Az internetes veszélyeztetettségről
Magyar és nemzetközi CSIRT-ek
Hálózatbiztonsági szabványok
▸Megelőző intézkedések
▸1. rész: Technológia
2. rész: Audit és management
Visszaható intézkedések

87.

Miről lesz szó?

- Biztonsági problémák előfordulásai
- Forgalomszűrés, tűzfalak
- Biztonsági kockázatok, támadások
  - Különböző hálózati rétegek
- Titkosítás és hitelesítés
  - Titkosítási módszerek és alkalmazásaik
- Jogosultságellenőrzés, hozzáférésvédelem
- AC-rendszerek áttekintő összehasonlítása
  - Elméleti
  - Gyakorlati

A biztonsági problémák előfordulási helyei, a különböző hálózati rétegek.

Fontos, hogy minden hibát a maga helyén kell kijavítani.

Vázlatos összefoglaló a különféle védekezési mechanizmusokról:

- megelőzés
- korlátozás
- kármentés

Titkosítások: szimmetrikus és nyilvános kulcsú

AC-rendszerek összehasonlítása: az elméleti elvek és az ismertebb implementációk

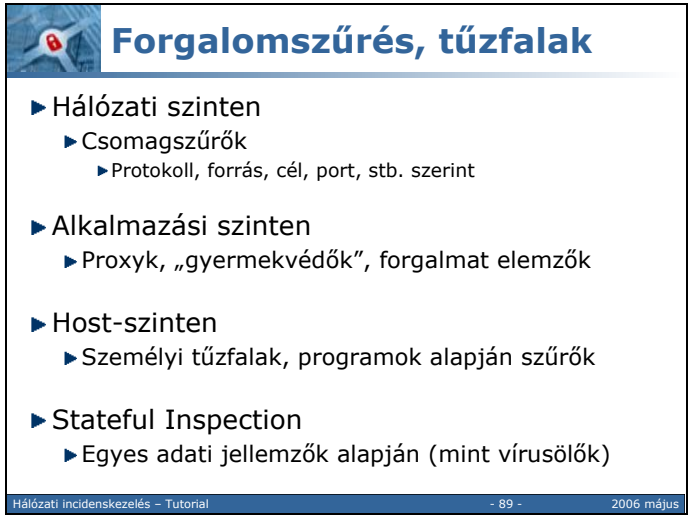
88.

Alulról fölfelé haladva a különböző rétegek:

1. Bitek továbbítása fizikai közegen (pl. Manchester-kódolás)
2. Az átküldött bitek hibátlan megérkezésének biztosítása (Ethernet-keretezés)
3. Routing, útvonal fölépítése pontról pontra
4. Két végpont kezelése
5. Session kezelése, szinkronizációk
6. Kódlapok konverziója
7. Alkalmazási protokollok

Beszámozva a rétegek alapfeladatai. Ezek kifejtése.

89.



Az alapvető tűzfaltípusok:

Csomagszűrő: pl. iptables, portokra és hostokra konfigurálható

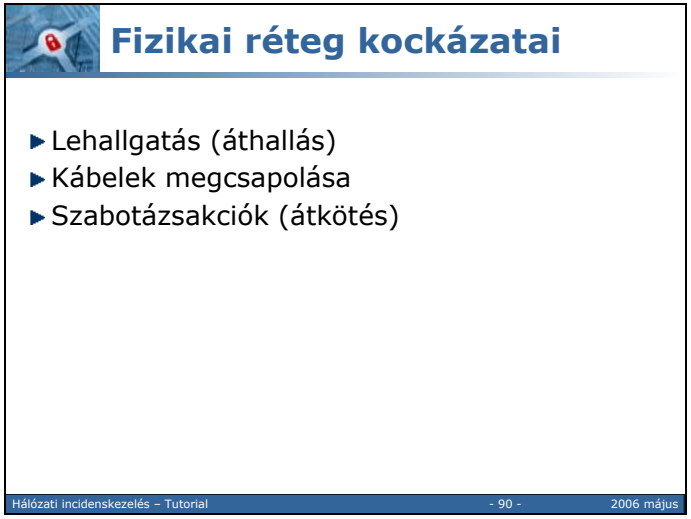
Application: pl. squid, tartalomelemzést végez

Személyi: programok hozzáférését engedi vagy nem engedi

Állapotgépes: jellemző minták, lenyomatok alapján keres (+connection tracking)

Bővebb kifejtése annak, hogy melyik hogyan működik.

90.



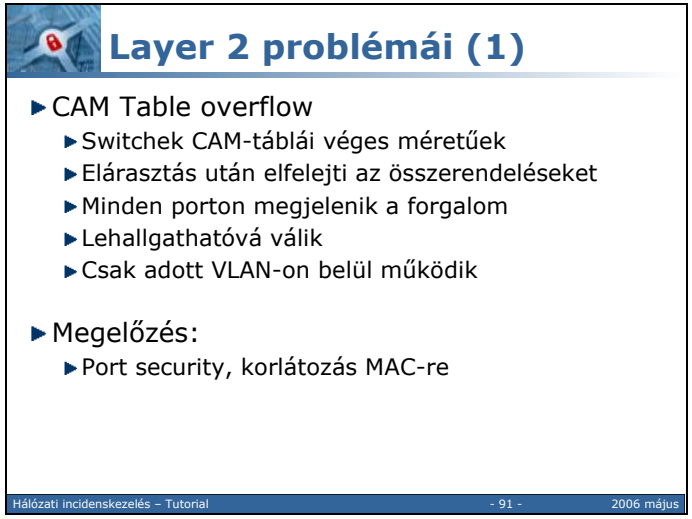
Rátérünk a különböző hálózati rétegekre.

Bevezető arról, hogy miért kell a támadásokat a saját rétegükben kezelni.

Rövid példa a monitor lehallgathatóságáról és a vámpírcsatlakozókról.

A szabotázsakciók, mint szélsőséges példa említése.

91.



Layer 2 rövid ismertetése (keretezés)

CAM-tábla lényegének ismertetése:

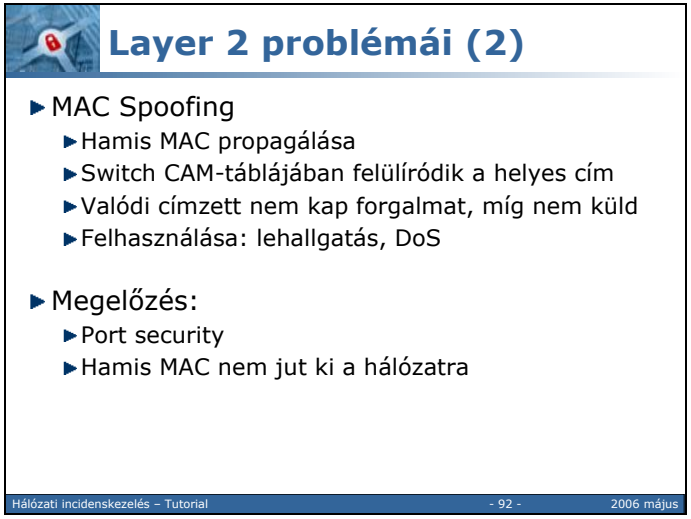
Ismert hostok helyét port szerint megjegyzi és a CAM-táblában tárolja

Hogyan is alakul ki a probléma: véges táblákat felülírják flooddal, így elfelejti a hozzárendeléseket

Bevezető a megelőzés módszereibe, rövid ismertető az említett technológiákról.

Port security: csak az adott MAC cím(ek)et engedi forgalmazni, így a hamisított forráscímmel küldött csomagok nem jutnak túl a switchen.

92.



Rövid bevezető az idtheft-es támadásokról: lehet IP-t vagy bármi mást spoof-olni.

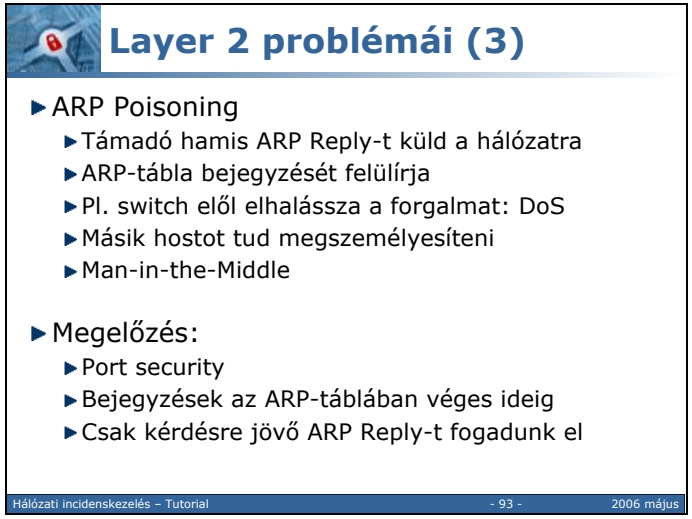
Általános ismertető a spoofing-ról: a forrást hamisítva másokat lehet megszemélyesíteni, ez sok támadás alapjául szolgál.

Switch forgalomirányítási módszerének rövid ismertetése: megjegyzi a switch, hogy melyik portján látta azt a MAC-címet, aminek a továbbítandó csomag szól. Így a csomagot ezen a portján adja ki.

Ezt hogyan használja ki a MAC Spoofing?

Úgy, hogy a hamis MAC-címmel mást megszemélyesítve valaki egy másik portjára küld csomagot a switchnek, mint ahol az eredeti tulajdonos tartózkodik. Innentől kezdve a switch azt fogja gondolni, hogy a hamisított csomagot feladó támadó a MAC-cím valódi tulajdonosa, így a továbbiakban erre a portra fogja továbbítani a neki szóló csomagokat, tévesen. Egészen addig így marad ez, amíg az eredeti tulajdonos egy újabb csomagot nem küld és ezzel vissza nem íratja a switchben a helyes portszámot.

93.



Switchekről most áttérünk a hostokra.

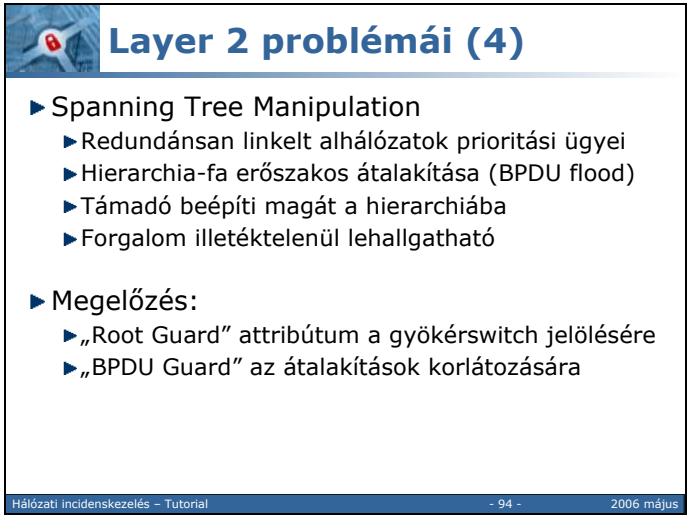
Mire is jó az ARP? Arra, hogy az interface szerepét játssza a layer2 és 3 között, összerendelést biztosítson MAC-cím és IP-cím között.

DoS-támadás rövid ismertetése: elárasztással vagy egyéb módszerrel a célpont szolgáltatási kapacitását kimeríteni, ezzel a szolgáltatást megbénítani.

Utalás a Man-in-the-Middle támadás későbbi részletezésére.

ARP-tábla kezelésének magyarázása: hostok a közelmúltban felbukkanó, ismert IP/MAC-összerendeléseket megjegyzik, hogy ne kelljen ARP kéréseket küldözgetniük a hálózaton fölöslegesen. Ezt a táblát lehet szándékosan, támadási céllal felülírni.

94.



Spanning Tree algoritmus rövid ismertetése

Switchek hierarchia-fáját elmagyarázni: a redundánsan kapcsolt switchek egy prioritási fába rendeződnek, hogy eldönthessék a forgalom útvonalát.

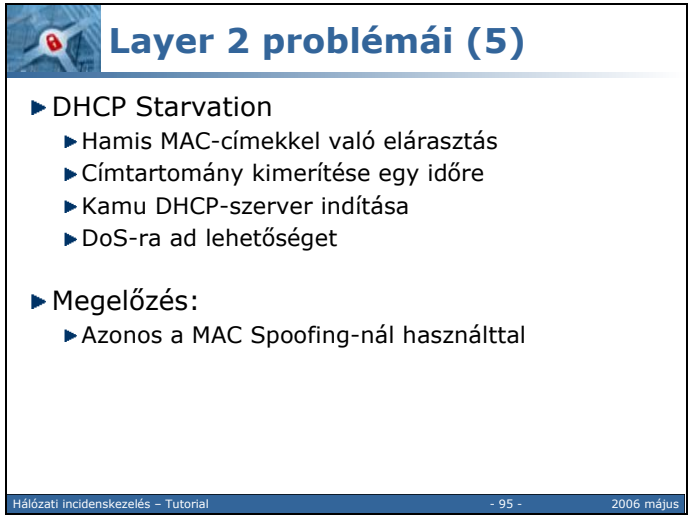
Miért van ezekre szükség? Local echo és üzenetpattogás megelőzésére, mert ha ez nem lenne, akkor minden switch minden vonalán adná-venné a forgalmat és megsokszorozódna a vonalon.

Támadó szerepe az, hogy erővel átalakítani próbálja a fát és ezzel saját maga felé irányítani olyan forgalmakat, amikhez eredetileg semmi köze sem lett volna.

Guard attribútumok ismertetése: Root Guard segítségével megmondhatjuk, hogy melyik switch legyen a gyökér a fában.

BPDU Guard pedig a portokra alkalmazható, ezzel lehet tiltani a BPDU-k elfogadását. Ha csak az uplink portokra engedjük, akkor a támadó gépek nem tudják a fát átalakítani.

95.

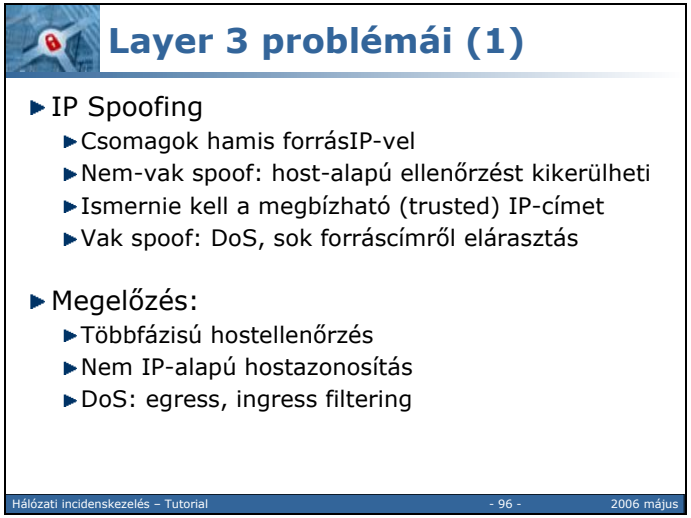


DHCP rövid ismertetése: Dynamic Host Control Protocol, dinamikus címkiosztás MAC-ekkel történő azonosítás alapján. IP-címet és a hozzá tartozó egyéb adminisztratív adatokat osztja ki a DHCP-szerver a kérést küldőknek.

Újabb idtheft-es támadás: MAC-ek hamisításával az összes kiosztható címet kiosztathatjuk a DHCP-szerverrel, ezzel egy időre leállíthatjuk a szolgáltatását. Ezalatt például kamu szervert indíthatunk és a további kéréseket ezzel kiszolgálva átverhetjük a hálózat gépeit.

DHCP->DoS magyarázása

96.



Áttérünk a hálózati rétegre.

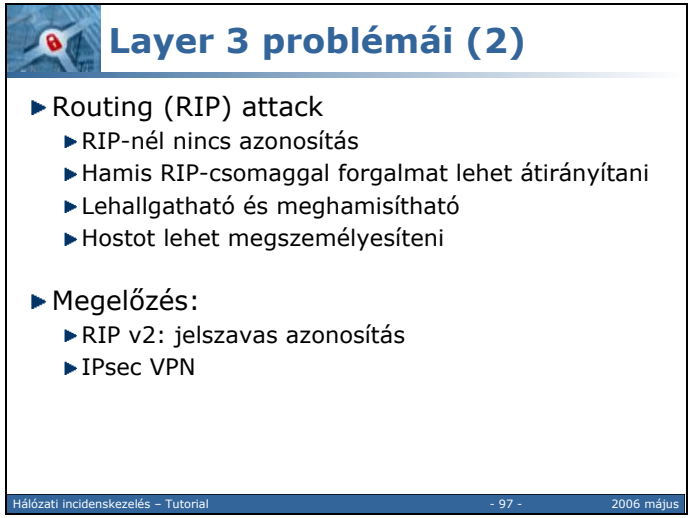
IP-címek ismertetgetése, úgyis mindenki tudja

Kétféle spoof van, vak és nem vak: a vak spoofnál ad hoc hamisítunk egy címet, tipikusan DoS-hoz, a nem vak spoofnál pedig egy általunk ismert gép nevében járunk el az ő IP-címével, hogy olyan szolgáltatáshoz jussunk hozzá, amihez egyébként nem lennénk jogosultak és a hozzáférés ellenőrzésére az IP-címet használja a szolgáltatást nyújtó.

Megelőzés módszerei, utalás előre (handshaking, authentication): visszaigazolásos handshake bevezetésével például ellenőrizni lehet, hogy valódi host van-e a forrásIP mögött. Más, nem IP-alapú azonosítással pedig a problémát teljes egészében meg lehet előzni.

Routerek egress/ingress filterezési technikáit ismertetni: egress filterezés a kimenő forgalmat elemzi és ha nem olyan forráscím szerepel benne, ami a belső hálózatban valóban létezik, akkor eldobja -> más hálózatok védelme; ingress filtering pedig bejövéskor elemzi a forgalmat és ha olyan forráscím szerepel benne, ami a bejövő hálózatban létezik, akkor eldobja -> belső hálózat védelme.

97.



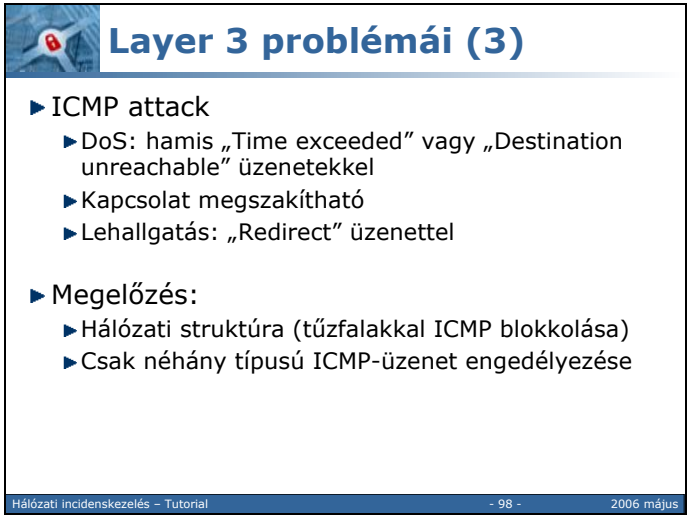
RIP ismertetése, mire való? A legrövidebb vagy legkisebb költségű utak megtalálására a hálózati topológiában.

Kiemelni, hogy nincs autentikáció RIP v1-ben: boldog-boldogtalan küldhet RIP-csomagokat, hogy ezzel átverje a routereket.

Újra idtheft, mint már korábban szerepelt.

Előreutalni VPN-re, meg a következő előadásra: vagy RIP v2-t kell használni, vagy VPN és titkosítás segítségével az azonosítást biztosítani.

98.



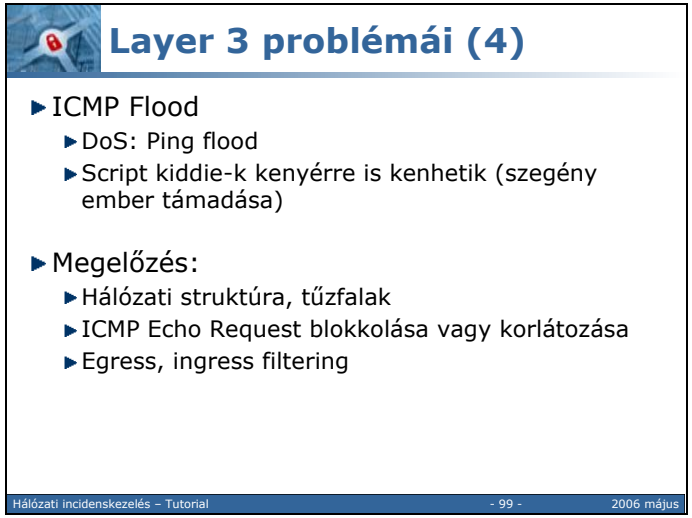
Ritkán használt ICMP üzenetekre figyelmet felhívni/

Time exceeded vagy Destination unreachable üzenetet küldve az egyik vagy mindkét kommunikáló félnek a kapcsolatot azonnal bontani lehet, mert a hostok úgy érzékelik, hogy a másik fél nem elérhető. Ez DoS-támadásra ad lehetőséget.

Redirect értelmét megmagyarázni: a gateway szokta küldeni azoknak a hostoknak a Redirect üzenetet, amelyek tévesen azt gondolják, hogy az általuk keresett címzett az alhálózaton kívül található, ezért a gateway-nek címeznek. Hamis Redirect üzenetekkel forgalmat lehet átirányítani és aztán illetéktelenül lehallgatni.

Struktúra: tűzfalakkal blokkolni a fölösleges ICMP üzeneteket, és csak a szükségeseket átengedni.

99.

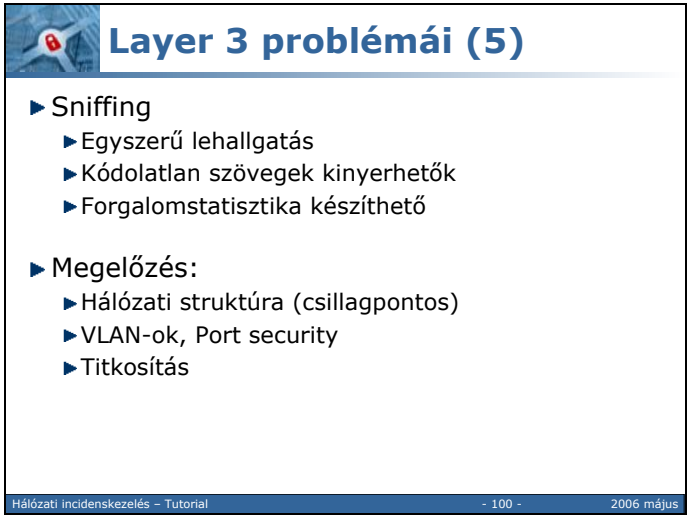


Egyszerű támadás, a jól ismert ICMP Echo Request csomagokkal elárasztani a tipikusan kis sávszélességű vonalon lógó célpontot. Nagy sávszélesség ellen nemigen van hatása. A keskeny vonal teljes elfoglalásával DoS-olható a célpont.

Gyakori próbálkozás, mert szaktudást és speciális segédprogramokat nemigen igényel.

ICMP Echo Request üzeneteket lehet például tűzfallal szűrni, valamint a korábban már említett egress ill. ingress filteringet használni.

100.



Lehallgatás, passzív támadás részletesebb kifejtése: a hálózaton közlekedő adatokhoz hozzáférve lehet a kódolatlan szövegek tartalmát kinyerni, illetőleg forgalomstatisztikát készíteni a megfigyelt forgalom jellemzői alapján.

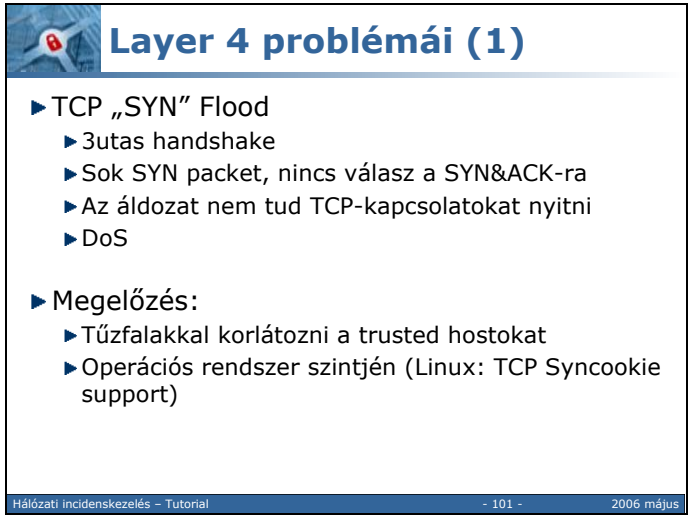
A szövegek kinyerése által okozott biztonsági kockázat triviális.

A forgalomelemzéssel arra következtethetünk, hogy a megfigyelt host vagy alhálózat milyen jellegű tevékenységeket végez és mekkora mennyiségben, ezzel sok információ szerezhető az ismeretlen célpontról.

Előreutalni VLAN-okra (következő előadás): forgalom lehallgathatóságának korlátozására.

Titkosítás: egyértelmű és legkézenfekvőbb módszer, mind a szövegek kinyerését, mint a minőségi és mennyiségi jellemzők alapján történő statisztikakészítést meg lehet vele előzni.

101.



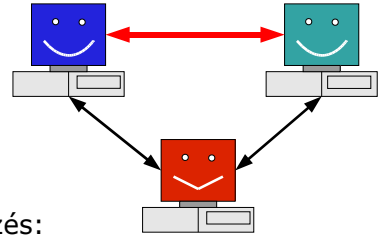
TCP handshake során 3 lépésben veszik fel egymással a kapcsolatot a kommunikáló felek. Az első lépés egy SYN csomag küldéséről szól a gyanútlan címzettnek, aki ekkor nyit egy csatornát és lefoglal hozzá egy erőforrást (TCP connection pool), majd visszaküld egy SYN&ACK-ot a feladónak. Ha a feladó nem válaszol a SYN&ACK-ra, akkor valamennyi idő (tipikusan 75 másodperc) után az erőforrás felszabadul.

Ha azonban a válasz helyett újabb SYN csomag érkezik, akkor úja csatorna nyílik és új erőforrás foglalódik. Ennek ismétlésével, valamint a SYN&ACK-ra történő válasz megtagadásával a véges TCP connection pool kimeríthető, ezután a célpont nem tud több TCP-kapcsolatot létesíteni addig, amit timeouttal föl nem szabadulnak a lefoglalt erőforrások.

102.

Layer 4 problémái (2)

- TCP Connection Hijacking
  - A tipikus Man-in-the-Middle attack
  - Rossz szinkron kihasználása kamu csomagokkal



- Megelőzés:
  - IP Spoofing megelőzésével

Hálózati incidenskezelés – Tutorial - 102 - 2006 május

Visszautalni a Man-in-the-Middle említésére (IP Spoofing): hamisított identitással mindkét fél számára eljátssza a támadó, hogy a valódi másik féllel beszélnek az áldozatok, miközben mindkettő számára a másikat megszemélyesíti. Teljes ellenőrzése alatt áll az adatforgalom: átengedheti, módosíthatja, meghamisíthatja, statisztikát készíthet.

TCP elcsúszott szinkronja során épülhet be a támadó, illetőleg handshaking közben.

Ha nem tud IP-címet hamisítani, akkor viszont esélye sincs: ezért IP Spoofing megelőzésével ez a támadás is megelőzhető.

103.

Layer 4 problémái (3)

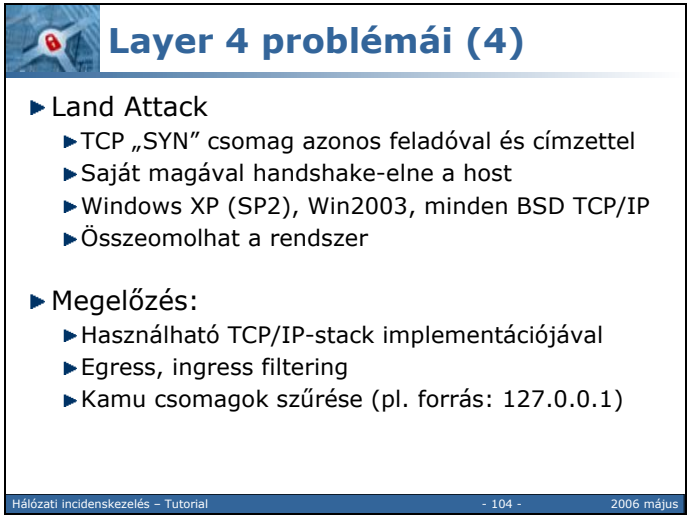
- UDP Flood
  - Véletlenszerű portokra csomagok
  - ICMP „destination unreachable” pattan vissza
  - DoS
- Megelőzés:
  - Tűzfallal a nem használt portokat védeni
  - ICMP echo üzeneteket tiltani

Hálózati incidenskezelés – Tutorial - 103 - 2006 május

Ha UDP-csomag érkezik egy portra, akkor a gép megnézi, hogy van-e ott szolgáltató. Ha nincs akkor visszaküld egy destination unreachable ICMP-csomagot.

Nagy mennyiségű UDP-csomag küldése esetén ezzel egyrészt a gép maga leterhelhető, másrészt a megduplázott hálózati forgalom miatt a vonala is eltömhető.

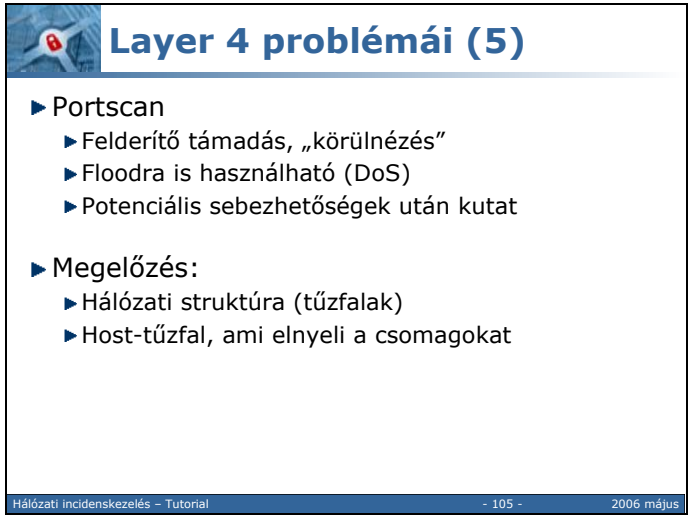
104.



Puttózni a rossz TCP/IP-stackeket: röhej, de nincs bennük ellenőrzés arra, hogy ne foglalkozzanak az azonos cél- és forráscímet tartalmazó csomagokkal, vagy azokkal, ahol a feladó 127.0.0.1-ként van jelezve. Ha egy ilyen csomagot kapnak, elkezdenek magukkal handshake-elni és összeomolhat az operációs rendszer.

Nagyon könnyen megelőzhető, tipikusan ingress filtering alkalmazásával.

105.



A portscan során a támadó megvizsgálja az ismeretlen célpontot, hogy szolgáltatások után kutasson rajta. Ha feltérképezte, hogy mik futnak a célponton, akkor utána célzott támadásokat indíthat ezek ellen.

Tűzfalakkal nagyon könnyen kivédhető.

106.

Layer 7 problémái (1)

- Végfelhasználói programok biztonsági zűrjei
  - Hálózaton közlekedő „plaintext” adatok
  - Régi protokollok: telnet, RSH, FTP
  - Ahány alkalmazás, annyi probléma: minden, ami autentikációt használ, veszélyes lehet
  - Hálózaton áthaladó érzékeny adatokra vigyázni
- Problémák áthidalása:
  - Hálózati forgalom titkosítása
  - Központosított, karbantartott autentikáció (LDAP, PAM)

Fölértünk a felhasználók szintjére.

A sok nyíltszöveges hálózati kommunikáció mind veszélyeket rejt magában, ld. Sniffing.

Az elavult telnet ilyen volt, ma már az SSH-t használják minden normális helyen (l. később).

De lehetne említeni sok példát, ami autentikációt használ, pl. Apache, samba, stb.

Két védekezési mód, ezeket mindjárt kifejtjük:

1. titkosítás
2. ellenőrzött autentikáció

107.

Layer 7 problémái (2)

- Hálózati forgalom titkosítása:
  - Telnet, RSH/RCP helyett SSH/SCP
  - FTP: túl elterjedt, nehéz róla leszokni – szorítsuk vissza és ne jelszavas, hanem host-alapú azonosítást használjunk inkább
  - Ha mégis jelszavas kell, akkor szeparált LAN-ban, VLAN-ban, minél kisebb nézőközönség előtt
  - Van SFTP is
  - HTTP: jelszavak, kényes adatok csak HTTPS-en
  - Példa: banki vagy egyéb személyes ügyintézés

A sokat emlegetett titkosítás.

Protokollok példaként citálása: HTTPS, meg úgy általában minden, ami SSL fölött van (l. később), SSH, VPN/IPSec, stb.

Példa a banki ügyintézésre, személyes adatokra való hivatkozást mindenki érti.

108.

Layer 7 problémái (3)

- Autentikáció:
  - Az áttekinthetőség érdekében központosítsunk
  - Használjunk bevett, bevált megoldásokat: LDAP, PAM, Kerberos
  - LDAP: felhasználói információk
  - PAM: alacsonyszintű autentikációs sémák integrációja magas szinten
  - Kerberos: szimmetrikus kulcsú titkosítást használó autentikációs protokoll

Második megelőzési forma. Emlegetni a bevált megoldásokat: LDAP, PAM, Kerberos.

Kicsit részletezve LDAP-ot: könyvtárstruktúra felhasználói adatok számára.

Pam: moduláris szerkezetű, wrapperként használható autentikációs sémagyűjtemény, amit számos program igénybe vesz.

Kerberos emlegetése és előreutalás a következő előadásra.

109.

Titkosítás

- Célok: nyilvánvalóak
- Felhasználás területei folyamatosan nőnek
- Sokféle módszer, elérhető számítási teljesítmény növekedésével sokan gyengévé váltak
- Ökölszabály: sohase gondoljuk azt, hogy a támadó nem ismeri a titkosítás módszerét
  - A kulcsra bízzuk magunkat, ne a módszerre
- Két titkosítási alaptípus:
  - Szimmetrikus kulcsú
  - Aszimmetrikus (általában nyilvános) kulcsú

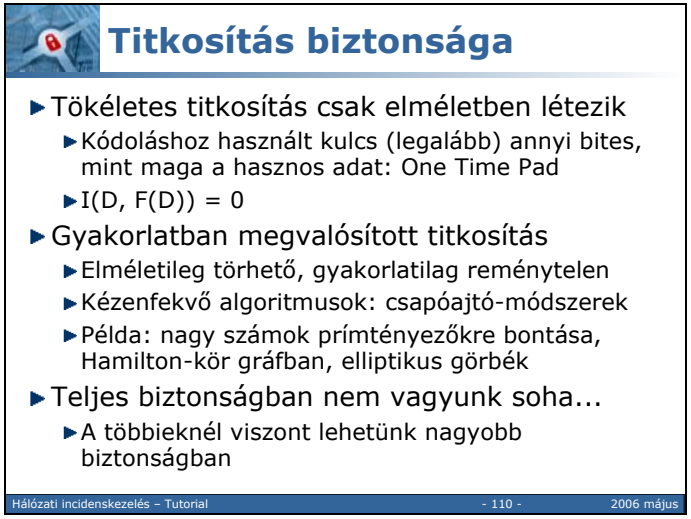
Titkosítás bővebb ismertetése jön.

Általános bevezető először, az alapvetések: katonai célból használták először, ma már meg sem lehet lenni nélküle. A módszerek mind arra alapoznak, hogy reménytelenül nagy teljesítményre lenne szükség a titkosítás feltöréséhez, nem arra, hogy a támadó nem tudja, hogy milyen módszert használunk.

Valós élet példáit hozni illusztrációnak.

Kiemelni, hogy alapvetően kétféle módszer van, ezeket mindjárt körüljárjuk.

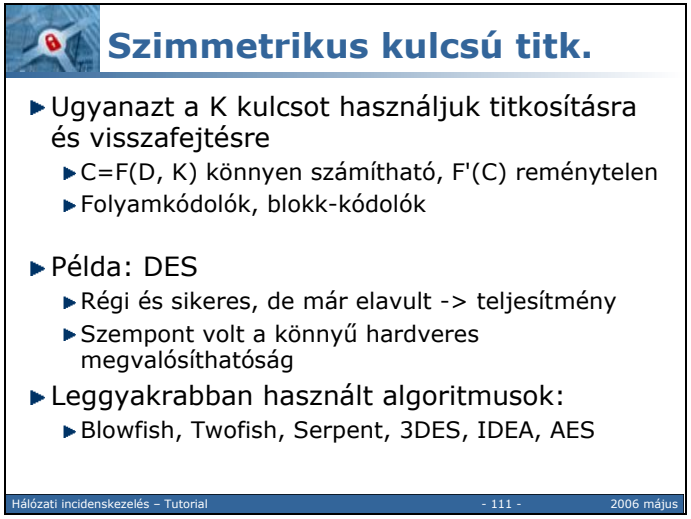
110.



Titkosítás általános jellemzői: Shannon-t felemlítve, One Time Pad-ot magyarázva: tökéletes titkosítás, legalább azonos kulcshossz, mint adatméret. Ez esetben semmi következtetést nem lehet levonni a titkosított szövegből az eredetire, azaz a kölcsönös információ nulla.

Gyakorlati módszerek elmélete: egyirányba könnyen, visszafelé igen nehezen számítható módszerek.

111.

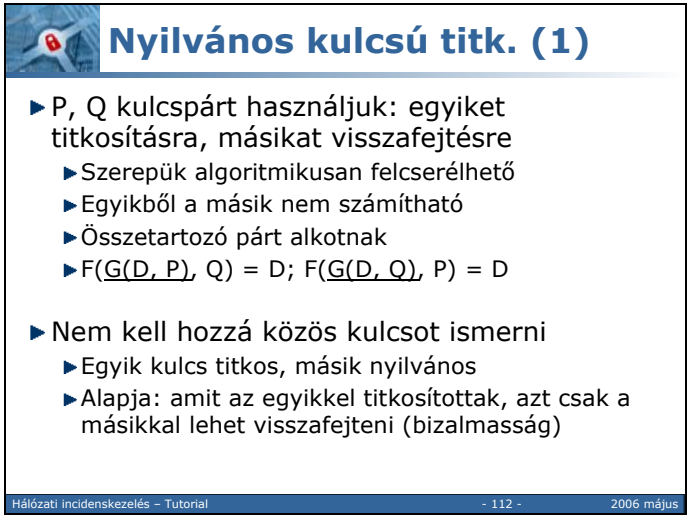


Első típusú módszer elmagyarázása: azonos kulcs oda-vissza. A kulcsot ismernie kell a címzettnek és a feladónak is. Sok problémát okoz, hogy mindkettő tudhasson a kulcsról, de úgy, hogy illetéktelenektől az rejtve maradjon. Lásd később: kulcskiosztás.

Stream cipher, block cipher, blokkok láncolása: kombinálva a módszereket, jelentősen javítani lehet a hatékonyságon.

Alsó sor példáinál kicsit elidőzni, pl. DES leváltására hirdetett pályázat.

112.



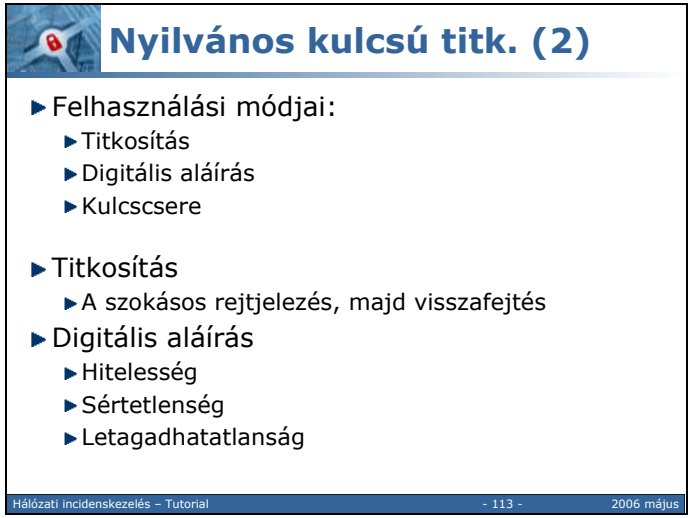
A két kulcspár viszonya részletesebben. Miért fontos, hogy nem számítható egyikből a másik? Hát azért, mert a módszer lényege, hogy az egyik kulcsot nyilvánosságra hozzuk. Ha ebből a másikat ki lehetne számítani, akkor teljesen értelmét vesztené az, hogy egyáltalán titkosítást használunk.

Hogyan kell kezelni? Úgy, hogy az egyik kulcsot propagáljuk, a másikat pedig szigorúan titokban tartjuk.

Formalizmus kicsit kifejtve azt mondja, hogy amit az egyik kulccsal elkódoltak, azt a másikkal vissza lehet fejteni, és viszont.

Három funkcióra utalni: bizalmasság, hitelesség letagadhatatlanság.

113.



Küröljárni a három felhasználási módot, melyik mire jó.

1. Titkosítás az egyik kulccsal visszafejtés a másikkal

2. Digitálisan aláírni dokumentumokat az egyik kulcs segítségével, így a másikkal ellenőrizhetővé válik az adat.

3. Kulcscserére lehet használni, mert a felek azonosítani tudják egymást. Nyilvános kulcsú módszerrel lehet titkosítani a szimmetrikus kulcsú algoritmusok kulcsait, ezzel biztonságossá téve a kulcskiosztást.

Kulcscserét főleg, miért van erre szükség, hol használják? (Kerberos)

114.

Nyilvános kulcsú titk. (3)

- Kulcscsere
  - Kulcs illetéktelen számára ismeretlen marad
  - Támadó nem tud kulcsot kényszeríteni a felekre
- Használt algoritmusok
  - RSA, DSS (DSA), Diffie-Hellmann
- Problémák:
  - Titkos kulcs nyilvánosságra kerülése aláássa az egész rendszert
  - Visszavonás propagálása megoldatlan (key revoke)

RSA emlegetése kapcsán visszautalni a bevett matematikai módszerekre (prímszorzat).

Részletezni, hogy miért megoldatlan a key revoke, előreutalni a PKI-ra (következő előadás): röviden azért, mert a kulcs kompromittálódásakor nincs módszer arra, hogy rövid idő alatt érvényteleníteni lehessen a kulcspárt, azaz a közkézen forgó nyilvános kulcsot ki lehessen vonni a forgalomból.

115.

Levelezés

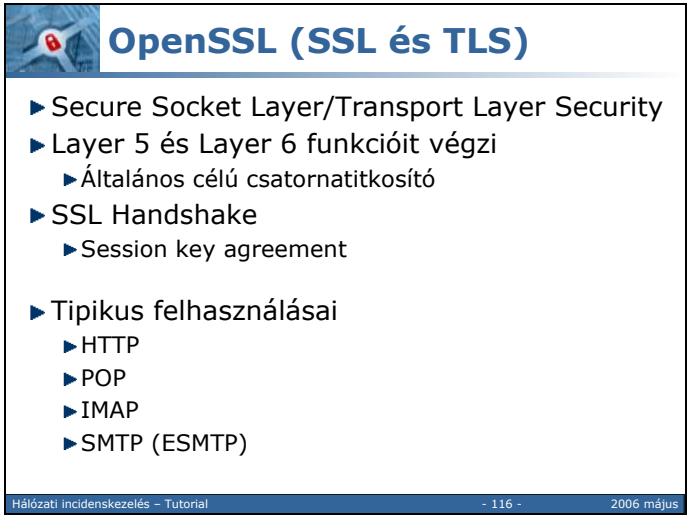
- S/MIME
  - RSA-t használ
  - Szabványba illeszkedik (X.500)
  - Központosított
- PGP (GnuPG/OpenPGP)
  - Phil Zimmermann maceratúrája
  - Aláírt kulcsok, bizalmi háló
  - Nyilvános kulcsszerverek

Jöjjenek a példák.

X.500 (megint csak előreutalni PKI-ra) hasznosságának emlegetése: illeszkedik a nyilvános kulcsú titkosítás infrastruktúrájába.

PGP és Zimmermann esete a szövetségi kormánnyal (per): a kormány azzal vádolta Zimmermannt, hogy megsérti a szabadalmi törvényt az algoritmus publikálásával, de valójában arról volt szó, hogy nem tudták visszafejteni (túl jó titkosítás volt) és ezért nem fértek hozzá az adatokhoz.

116.

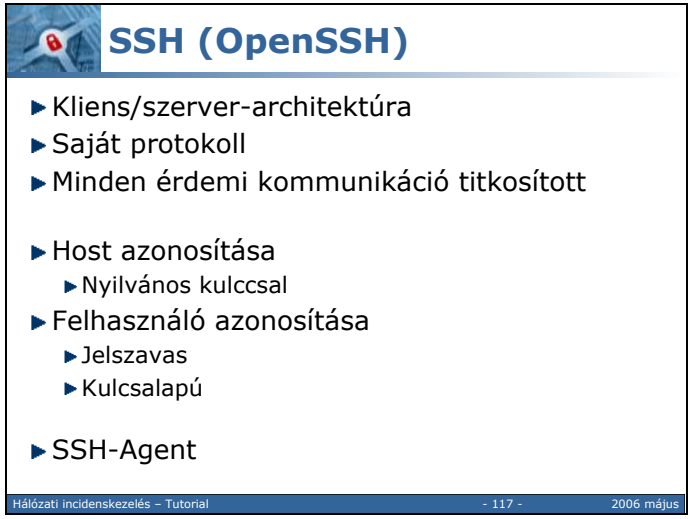


Ismertetni, hogy miért is tudja mindenki betéve, hogy mi az az SSL: wrapper a biztonságos kommunikációhoz és kliensazonosításhoz.

Handshake kapcsán konkrét példa a kulcscserére, megemlíteni, hogy a szimmetrikus kulcsú algoritmusoknak sokkal kisebb az erőforrásigényük.

A tipikus felhasználásokra példát hozni (mindre): banki tranzakciók, levelezések.

117.



Hostazonosítás és felhasználó-azonosítás.

Saját protokoll, saját port, minden titkosítva.

Hostot mindig a kulcsával (host key) azonosít, felhasználót lehet kétféleképpen: kulccsal és jelszóval.

Agent arra szolgál, hogy az azonosult felhasználónak ne kelljen mindig tornáznia, ha további hostokon is azonosítani akarja magát: agent megoldja helyette.

118.

SSH szolgáltatásai

- Sokféle titkosítási algoritmus
- Tömörítés
- Interaktív kapcsolat
- Távoli futtatás, csatornák átirányítása
- Port forwarding (SSH tunnel)
  - Távoli gép portjára kapcsolódás sajátról
  - Port nyitása távoli gépen saját gép felé
- X11 Forwarding
  - Adatcsatorna helyi X-szerver felé

Sorolni a titkosítási algoritmusokat, visszautalni az általános bevezető példáira.

Shell és távoli linuxos/unixos elérés feltétlen megemlítése.

Tunnelezés kapcsán személyes példa, ha belefér az időbe (férjen, színesíti az előadást).

X, mint grafikus felület számára nyújtott szolgáltatást, az X11 Forwardingot kiemelni, megjegyezni, hogy mennyire hasznos, meg azt is, hogy bezzeg ez is csak a unix/linux világában érhető el, mint szolgáltatás, a többiek mind ott lenn a porban.

119.

Hozzáférésvédelem (AC)

- Elméletben:
  - DAC: Discretionary Access Control
    - Tulajdonos szabja meg a hozzáférési jogokat
    - Technikák: ACL, RBAC
  - MAC: Mandatory Access Control
    - Rendszer szabja meg a hozzáférési jogokat
    - Technika: érzékenységi szint (címke)
  - RBAC: Role-Based Access Control
    - Szereplők tevékenységi csoportokba sorolva
    - Jogosultságok a csoportokhoz tartoznak
- Gyakorlatban:
  - RSBAC, GRSecurity, WinNT (Posix+) ACL

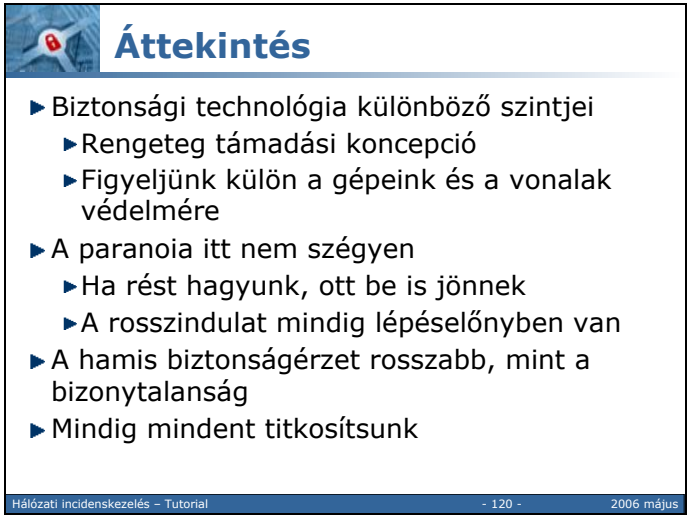
Rövidke ismertető mindegyik módszerről, példákkal illusztrálva, hogy tudják a valóságos operációs rendszerekhez kötni

Katonai példát felhozni MAC-re: például kártyák használata, illetékességi szintek. Amit mondjuk egy tábornok megtehet, azt nem teheti meg a közlegény, ezért a tábornoknak nagyobb jogokat biztosító kártyája lesz, így bemehet a fegyverraktárba, míg a közlegény csak az épület bejárati ajtaját nyithatja, hogy ne kelljen kint állnia az esőben.

RBAC pedig az adminisztratív megközelítés, különböző funkciók szerint csoportokba sorolt szereplők különböző dolgokhoz férnek hozzá.

Gyakorlati példákról mindről egy-egy mondatka.

120.

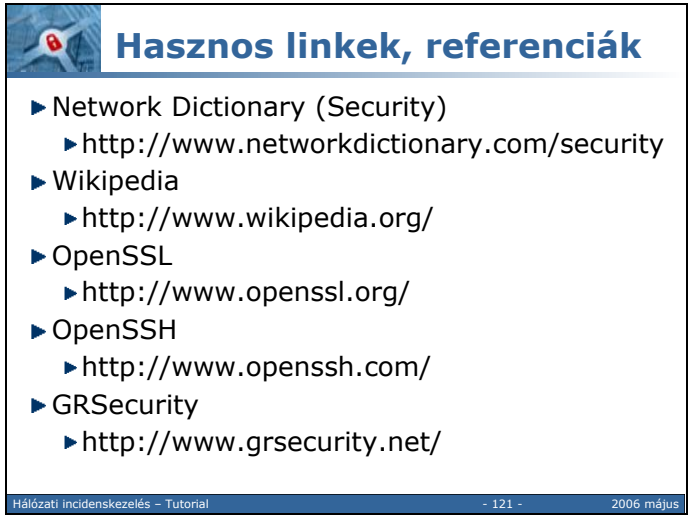


Összefoglalóan megismételni az ökölszabályokat a védekezésre és a titkosításra.

Mindig, mindenki csak minket akar bántani.

Hamis bzitonságérzet rossz voltának erős hangsúlyozása, előreutalás a következő utáni előadásra. Mindig mindent titkosítani kell, abból nem lehet baj.

121.



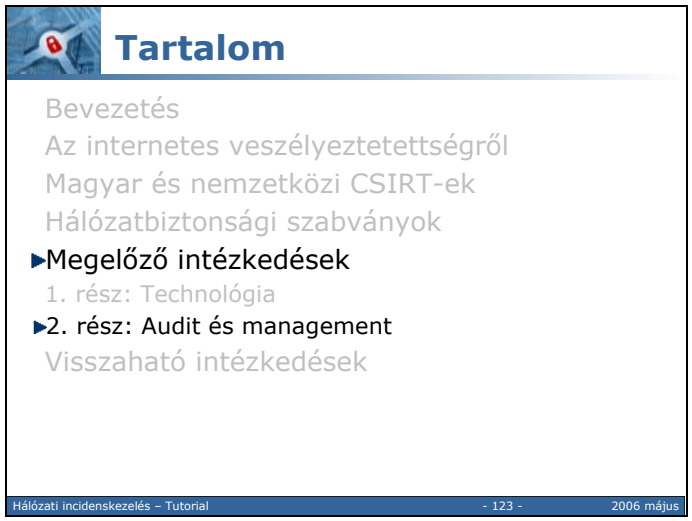
Linkekhez nem kell túl sok magyarázat, csak annyit említeni, hogy számtalant lehetett volna még felsorolni.

Kiemelni a netes irodalom gazdagságát

122.

A cél nem csak a konkrét tűzoltó technológiák bemutatása, hanem a probléma hosszú távú kezelésére is megoldásokat szeretnénk mutatni.

123.



124.

Miről lesz szó?

- Önmegtámadás, önellenőrzés
- Szoftverfrissítések, verziókövetés
- Elosztott biztonsági szolgáltatások
- Hálózati struktúra megfelelő kialakítása
  - Fizikai szint
  - Logikai szint

125.

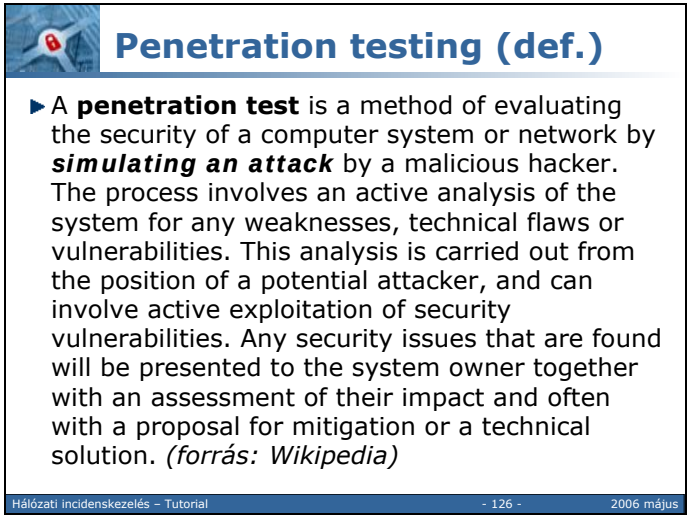
Penetration testing

- A probléma
  - A „biztonság” nem számszerűsíthető
  - Nem számszerűsíthető = nem mérhető
  - Nem mérhető = üzletileg nem indokolható
- Megoldás (?):
  - Önmegtámadás, önellenőrzés
  - Számszerűsíthetők:
    - Az elvégzett vizsgálatok
    - A felfedett biztonsági hiányosságok
  - A hatékonyság, pontosság kérdéses

A legtöbb támadási sorozat kézenfekvően a célzott rendszer sebezhetőségeinek feltérképezésével kezdődik. Ezek a vizsgálatok sok esetben nem konkrét gyengeségeket fedeznek fel, hanem a támadó számára hasonlóképp értékes szerkezeti információkkal szolgálhatnak.

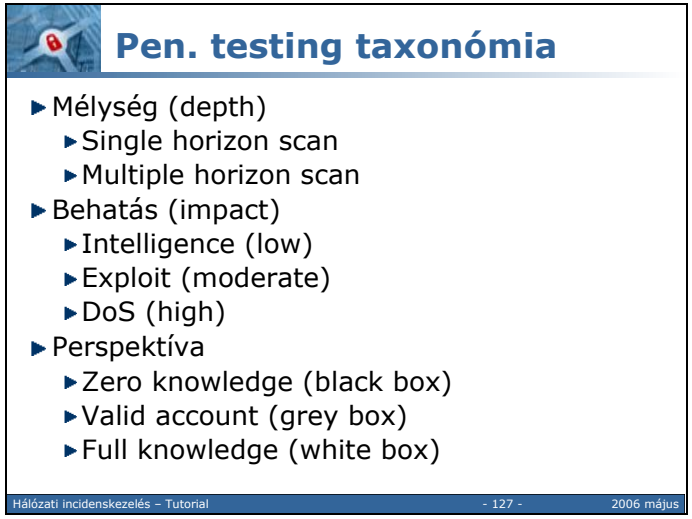
A támadó célszerűen először a célrendszer hálózatáról próbál bővebb információkat szerezni. Nem kevés esetben, például az automatikusan működő férgek vagy az esetlegesen kompromitált gépeken elhelyezett kémrobotok esetén a célhálózat akár az egész Internet is lehet.

126.



Egy ilyen szimulált támadás menete, és ennek megfelelően főbb eszközei megfelelnek egy valódi támadás jellemzőinek: első lépésben egy *host scannerrel* megkeresik azokat a számítógépeket (IP címeket), melyek a választott címtartományban elérhetőek, ezután az elérhető gépek által nyújtott szolgáltatások *port scannerrel* történő felderítésére van szükség, amit a szolgáltatások *security scannerrel* való ellenőrzése követ. Egyre gyakrabban előfordul, hogy a security scanner munkáját bizonyos helyzetekben a publikus információkeresés (például: web search) eszközeivel is megtámogatják, mivel bizonyos Internetes férgek és automaták hasonló módszerekkel kutatnak áldozatok után.

127.



Mélység

Az ellenőrzés mélysége nem a részletességre utal, hanem a feltételezett behatolás mélységére. A vizsgálni kívánt hálózat és rendszer a külvilág (Internet) felé általában csak egy korlátozott felületen, például egy tűzfalon keresztül nyújt szolgáltatásokat. A hálózat belülről is több részből, biztonsági zónából állhat, melyek önálló támadási területeket, szinteket jelölhetnek ki az ellenőrzés során. Mélység szempontjából az ellenőrzések két csoportját különböztetjük meg:

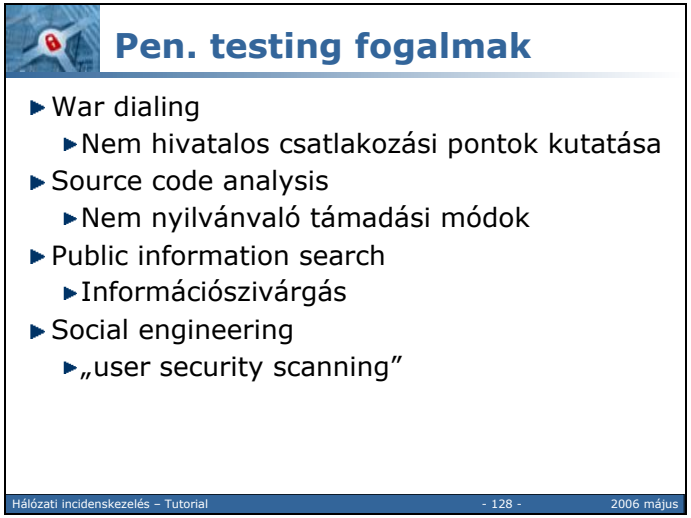
Behatás

A behatás (impact) a biztonsági ellenőrzés erőszakosságát határozza meg. Minél erőszakosabb egy támadás, annál több sebezhetőségre hívhatja fel a figyelmet, de annál több kárt is okozhat.

Perspektíva

Az ellenőrzés perspektívájának nevezzük a behatolást végző/megkísérlő ember vagy gép a hálózatra vonatkozó előzetes ismereteinek mélységét. Minél teljesebb ezen előzetes ismeretek köre, annál valószínűbb a behatolás sikeressége, vagyis a jogosulatlan információszerzés vagy károkozás.

128.



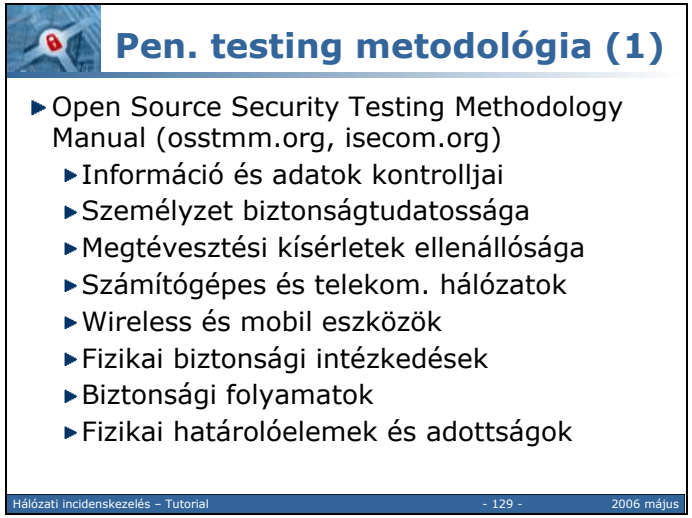
War dialing: célja egy hálózathoz való, a hálózat elsődleges védelmi peremeit (például a tűzfalat) megkerülő kapcsolódási lehetőségek felderítése. Általában az analóg telefonhálózat egyes mellékein a felhasználók által saját célokra üzemeltetett modemes elérésekre kell gondolni, melyeket a hálózatra való kapcsolódásra alkalmas gépek mellől elérhető telefonvonalak feltárcsázásával lehet legegyszerűbben felderíteni (innen az elnevezés).

Source code analysis: a kiszolgáló szoftverek forráskódjának analízise hálózati és általános biztonsági szempontokból, főként *buffer-túlcsordulás* hibák és egyéb hálózati viselkedési hiányosságok után kutatva.

Public information search: több esetben előfordul, hogy a védeni kívánt adatok egy része valamilyen módon nyilvánosan elérhető. Előfordulhat például, hogy egy távolról is elérhető webszerver egy cég dolgozóinak intranet szolgáltatást is nyújt, az intranet és internet felület pedig közös keresővel rendelkezik. Ilyenkor hiába elérhetetlenek kívülről az intranetes oldalak, a kereső jól formázott keresési feltételek alapján apró részletekben átszivárogtathatja az egész információt a külvilágba. Ilyen, és ehhez hasonló problémák alapján célszerű minden lehetséges információ megszerzésére próbákat tenni, hogy időben elzárhatóak legyenek az adatszivárgási csatornák.

Social engineering: sokszor nem is gondolnánk mekkora támadási felületet nyújthatnak egy hálózat jóhiszemű felhasználói, akik egy magát hálózati felügyelőnek vagy rendszergazdának kiadó személy telefonhívására vagy levelére hajlandók gépeikre ismeretlen eredetű programokat telepíteni, vagy jelszavakat és egyéb érzékeny információkat kiadni. A jóindulatú social engineering egyfajta “*user scanner*”-ként működve a felhasználók körében fellelhető ilyen jellegű biztonsági hiányosságokra próbál rátalálni.

129.

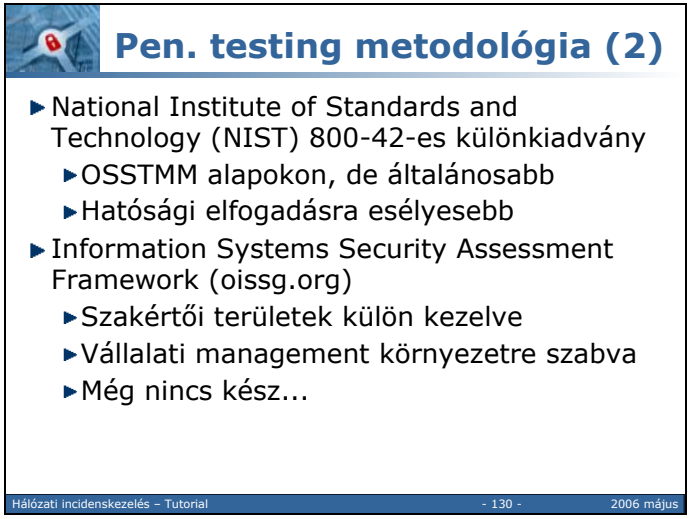


The Open Source Security Testing Methodology Manual (OSSTMM)is a peer-reviewed methodology for performing security tests and metrics. The OSSTMM test cases are divided into five channels which collectively test: information and data controls, personnel security awareness levels, fraud and social engineering control levels, computer and telecommunications networks, wireless devices, mobile devices, physical security access controls, security processes, and physical locations such as buildings, perimeters, and military bases.

The OSSTMM focuses on the technical details of exactly which items need to be tested, what to do before, during, and after a security test, and how to measure the results. OSSTMM is also known for its [Rules of Engagement] which define for both the tester and the client how the test needs to properly run starting from denying false advertising from testers to how the client can expect to receive the report. New tests for international best practices, laws, regulations, and ethical concerns are regularly added and updated.

The National Institute of Standards and Technology (NIST) discusses penetration testing in Special Publication 800-42, Guideline on Network Security Testing. NIST's methodology is less comprehensive than the OSSTMM however it is more likely to be accepted by regulatory agencies. For this reason NIST refers to the OSSTMM.

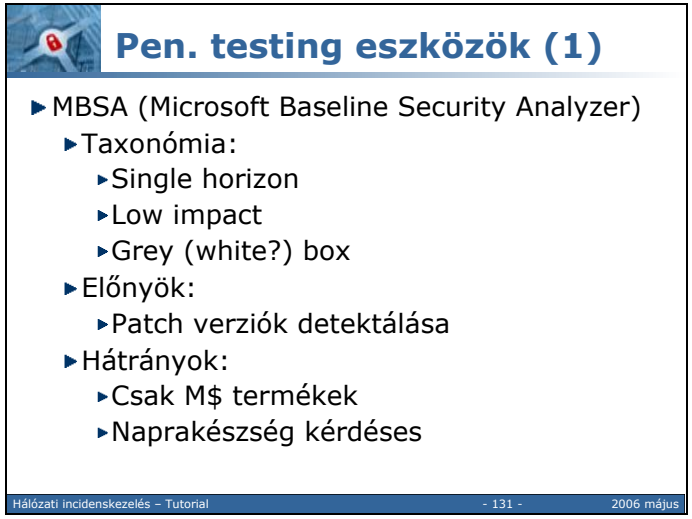
130.



There is a new Methodology known as the Information Systems Security Assessment Framework (ISSAF) by Open Information System Security Group

The Information System Security Assessment Framework (ISSAF) is a peer reviewed structured framework that categorizes information system security assessment into various domains & details specific evaluation or testing criteria for each of these domains. It aims to provide field inputs on security assessment that reflect real life scenarios. ISSAF should primarily be used to fulfill an organization's security assessment requirements and may additionally be used as a reference for meeting other information security needs. ISSAF includes the crucial facet of security processes and, their assessment and hardening to get a complete picture of the vulnerabilities that might exist. The ISSAF however is still in its infancy.

131.



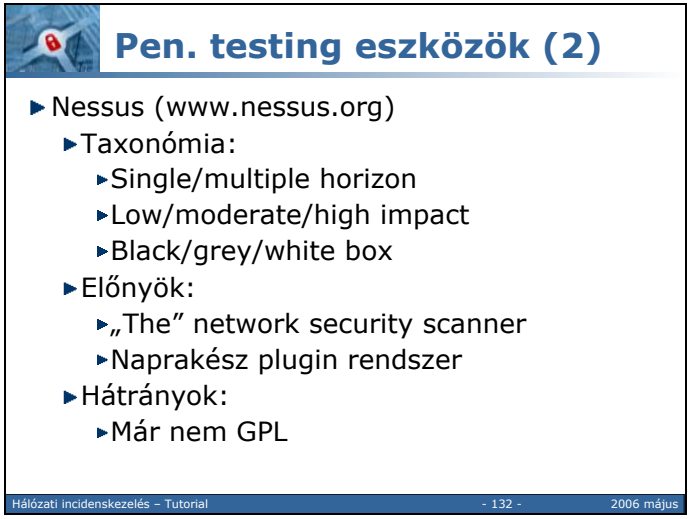
A host scanner működése a már említett ping programhoz hasonló, sőt sok esetben teljesen azonos: az ellenőrzést végző gép egy próbacsomagot küld a célgép hálózati címére, majd válaszra vár. A válasz elmaradása egyet jelent azzal, hogy a célgép nem érhető el. Már ez az információ is nagyon fontos lehet, hisz alkalmas a hálózat alapvető logikai felépítésének feltérképezésére, felfedi azokat a gépeket is, melyek nem feltétlen nyújtanak szándékosan publikált szolgáltatásokat, de elérhetőek.

A port scanner feladata a célgép egyenként 65535 TCP és UDP portja közül megkeresni azokat, amelyeket a gépen futó valamely alkalmazás nyitva tart. A működés alapvetően itt is a „kérés-válasz” módszerrel zajlik: az ellenőrző gép kapcsolatot próbál kezdeményezni a célgép adott portján keresztül, ha sikerrel jár, tudja, hogy a kérdéses port nyitva van, azaz a porton a célgép valamilyen szolgáltatást nyújt.

Ezután következik a legszerteágazóbb feladatot végrehajtó program, a security scanner, melynek tárházában a célgépen nyitva talált portokhoz tartozó szolgáltatások specializált ellenőrzésére alkalmas tesztek várnak kipróbálásra. Egy ilyen teszt két csoportba tartozhat:

A fenyegetettségi teszt csak a szolgáltatást végző kiszolgáló program létének, típusának, verziószámának megállapításából von le következtetést az ezekhez tartozó ismert hibák és támadási lehetőségek vonatkozásában.

132.

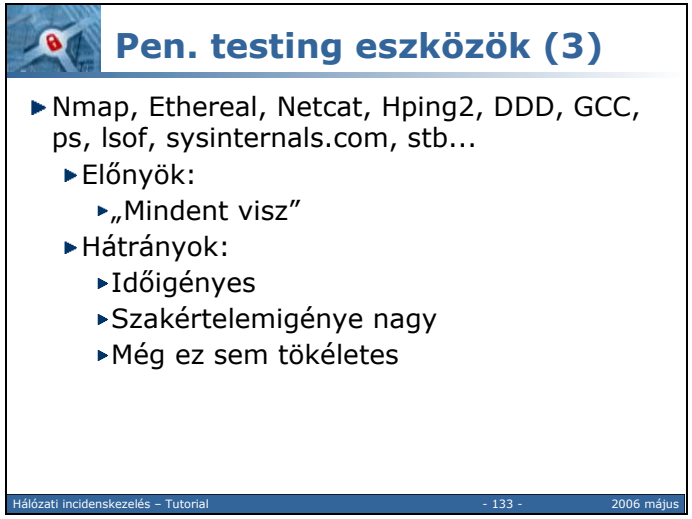


A behatolási teszt a rosszindulatú felhasználó viselkedésének szimulációjából, elérési jogosultságok ellenőrzéséből, sőt, esetleg károkozásra alkalmas szolgáltatás túlterhelési támadásból (denial of service attack, DoS), vagy a kiszolgáló szoftver puffer-túlcsordulásának előidézéséből is következtethet egy valódi támadás lehetséges eredményeire.

A figyelmet érdemes még felhívni arra, hogy az ellenőrzést végző és az ellenőrzött gép nem feltétlen különbözik egymástól, sőt léteznek olyan security scannerek, melyek nem is alkalmasak hálózati működésre. Ezek általában a helyi futtatásból származó helyzeti előny miatt fenyegetettségi tesztek végrehajtására különösen alkalmasak, viszont a behatolási tesztelés eredményeinek megbízhatóságát nagymértékben befolyásolhatja, ha egy gép saját magát teszi próbára.

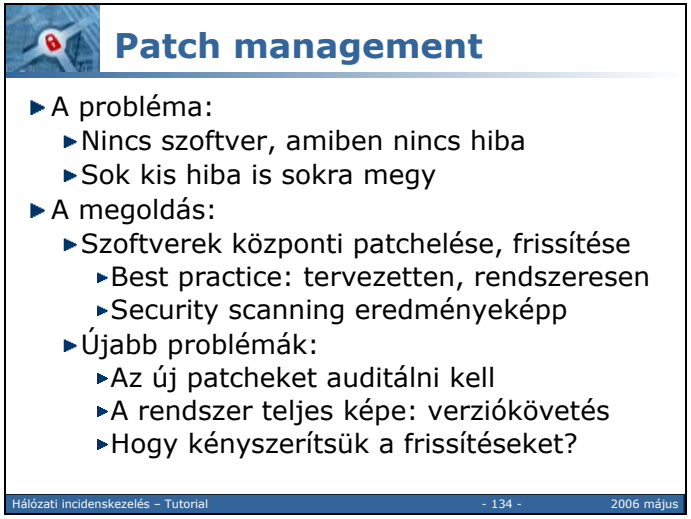
A hoszt, port és security scannerek által begyűjtött információkat, a tesztek eredményeit egy teljes alhálózat ellenőrzésekor általában összesített statisztika formájában érdemes megtekinteni, ezután nyílik lehetőség a kockázatok elemzésére és megfelelő kezelésére, vagyis a szükséges biztonsági frissítések, védelmi megoldások alkalmazására. Bizonyos idő elteltével érdemes lenne megismételni a teljes szimulált támadás alapú ellenőrzést, ez azonban sok erőforrást és időt vesz igénybe, ezért sok esetben előnyösebb úgynevezett „követő ellenőrzést” végezni, ahol csak az előző ellenőrzés óta nyilvánosságra került biztonsági rések vonatkozásában kell az egész alhálózatot újra áttekinteni.

133.



A hálózatbiztonsági pásztázások és ellenőrzések fejlődésére jellemző, hogy a támogató eszközök fejlődésével párhuzamosan nyílt csak lehetőség a teljes szimulált támadási folyamat automatikus elvégzésére, vagyis kezdetben csak a legegyszerűbb host scanner funkció volt bárki számára elérhető, majd később napvilágot láttak különböző port scanner eszközök, és csak az utóbbi években vált jellemzővé a nem ritkán üzleti forgalomban kapható security scannerek elterjedése. A publikus eszközök hiánya azonban nem jelentette soha az ellenőrzés megvalósíthatatlanságát, csupán jóval több szakértelmet igényelt a művelet végzőjétől. A mai napig nem megoldott, és a mesterséges intelligencia további fejlődéséig nem is lesz automatikusan megoldható, egy hálózat teljes körű biztonsági ellenőrzése.

134.



Frissítések által rejtett veszélyek fontosak!

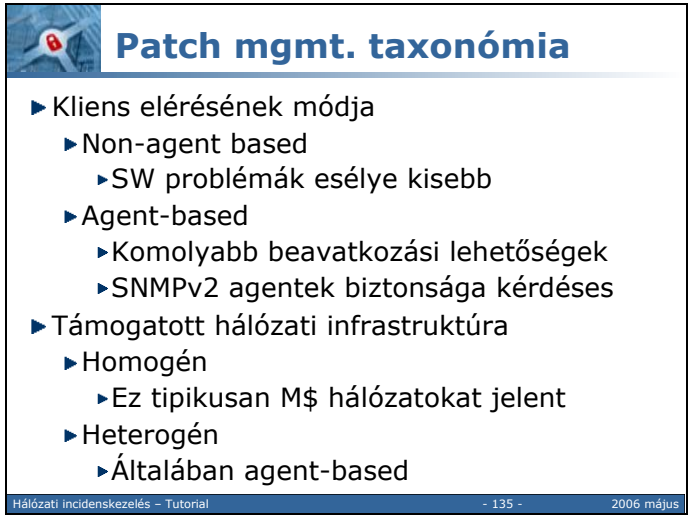
A hálózat védelmének fontos eszköze a felhasználói végpontok, a kiszolgálók és az aktív hálózati eszközök rendszeres szoftveres frissítése.

Az automatikus szoftveres frissítések kockázati tényezőinek ismeretében előfordulhat, hogy a frissítéseket célszerű egy mintagépen előzetesen kipróbálni.

A biztonsági frissítések hitelességének ellenőrzésére digitálisan aláírt frissítőcsomagok használata javasolható. Az aláírások ellenőrzése kézzel és automatikus eszközök segítségével, a frissítés telepítésének megkezdése előtt megtörténhet.

Fontos, de nem technológiai feladat a kritikus biztonsági hiányosságokról való időben való tájékozódás érdekében a biztonsági levelezőlisták, automatikus esetben ezek streaming news (RSS) forrásainak figyelése.

135.



Agent based: tipikusan Enterprise környezetben, tipikusan NMS-ek részeként.

136.

Patch mgmt. eszközök (1)

- „Nagy” NMS-ek idevágó funkciói (vízfejjel)
  - IBM Tivoli
  - CA Unicenter
  - HP OpenView
- GPL NMS megoldások (gyerekcipőben)
  - Nagios (nagios.org)
  - JFFNMS (jffnms.org)
- Egy újsütetű megoldás:
  - CiscoWorks (www.cisco.com)
    - IP routing felhasználása a kényszerítésre

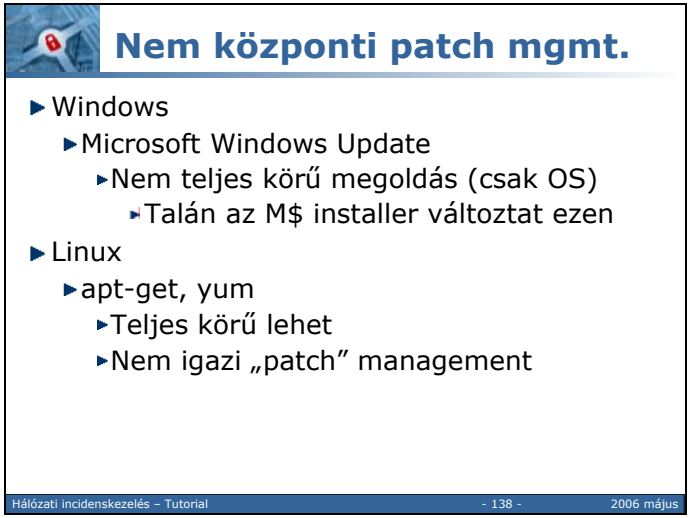
El lehet mondani, ogy a cisco megoldás azért nagyszerű, mert nem a kliensre bízza saját biztonságát...

137.

Patch mgmt. eszközök (2)

- Non-agent-based célszoftverek
  - Homogén
    - UpdateExpert (www.stbernard.com)
  - Heterogén
    - HFNetChkPro (www.shavlik.com)
- Agent-based célszoftverek
  - Homogén
    - M$ Systems Management Server
  - Heterogén
    - BigFix (www.bigfix.com)

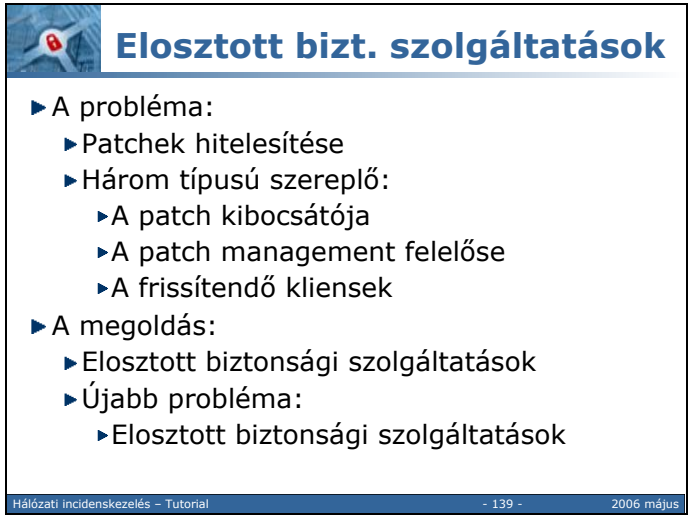
138.



Mi az a Windows Update?

A Microsoft egy webhelye, amely frissítéseket biztosít a Windows operációs rendszerekhez, illetve a Windows alapú hardvereszközökhöz. A frissítések megoldást nyújtanak az ismert problémákra, és elősegítik az ismert biztonsági fenyegetésekkel szembeni védelmet.

139.



Az LDAP, vagyis a Lightweight Directory Access Protocol egy objektum orientált, olvasásra és keresésre optimalizált, redundáns működésre is felkészített adatbázislekérdező nyelv. A központosított felhasználókezelés, vagyis az átfogó jogosultságkiosztás és hozzáférésvédelem elterjedt eszköze, használható kulcskiosztásra, authentikációra, authorizációra. A Microsoft Active Directory megoldásához hasonlít, azzal a különbséggel, hogy nem integrálja a Kerberost és inhomogén alkalmazási környezetben is működőképes.

140.

EBSZ - taxonómia

- Infrastruktúra
  - Centralizált („certification authority”)
  - Elosztott („web of trust”)
- Autentikáció módja
  - Nyilt kulcsú algoritmus („BLACK key”)
  - Osztott kulcsú algoritmus („RED key”)
- Alkalmazhatósági tartomány
  - Széleskörű, sok alkalmazási terület
  - Specializált, szűkebb alkalmazhatóság

A Certificate Authority, vagyis a hitelesítő hatóság, a nyilvános kulcs infrastruktúra gyökere, gyakorlatilag egy, a tanúsítványok kibocsátására és aláírására, használatos, erősen védett titkos kulcs, valamint a hozzá tartozó gyökértanúsítvány (root certificate) együttese alkotja. A CA kulcsának biztonsága az egész infrastruktúra kritikus pontja, kompromittálódása esetén az általa kibocsátott certificate-eket használó TLS és egyéb ügyfelek kommunikációja teljesen védtelenné válik a megszemélyesítéses támadások ellen, ezért célszerűen elzártan kell tárolni, és a tanúsítványok kibocsátásához egy erre a célra elkülönített, hálózati kapcsolattal nem rendelkező számítógépet ajánlatos használni.

141.

EBSZ – eszközök (1)

- X.509 authentication framework
  - Centralizált
    - - A CA a rendszer egyedüli kulcsa
    - + Tiszta, átlátható szerkezet
    - + CA anyagi felelősségvállalása (?)
    - - Tipikusan pénzbe kerül
  - Nyílt kulcsú
    - + Kulcsdisztribúció egyszerű (X.500)
  - Széleskörű alkalmazhatóság
    - SSL, S/MIME, stb...

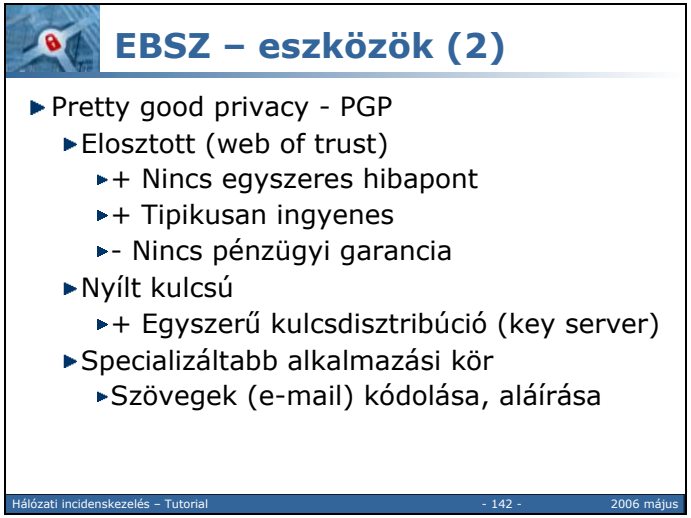
Biztonságos átviteli protokoll.

(Secure Socket Layer = biztonságos tartó réteg)

"RSA" eljárással titkosított biztonságos adatátviteli protokoll webszerverek és klienseik közötti kommunikációra.

Újabb webalapú levelezőrendszerek támogatják, a megcélzott távüzletek biztonságos lebonyolítása érdekében; az ilyen szerverek url címében (https://...) egy "s" betű jelzi a biztonságos adatátvitelt.

142.



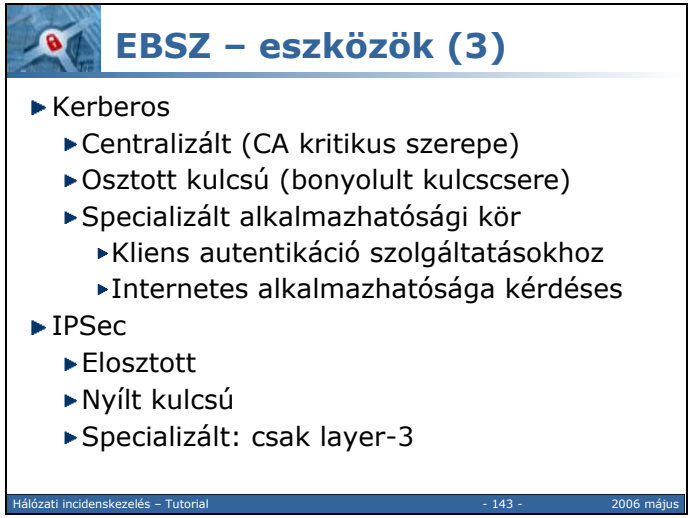
(Pretty Good Privacy = elég jó biztonság)

Az adatbiztonságot szolgáló, titkosító kulcsrendszer, mely az internet kommunikációnak egy alapvető feltételét hivatott szavatolni.

A PGP (Pretty Good Privacy) Phill R. Zimmermann egy RSA alapú, rejtjelezô programja. Több, mint egy tucat változatát két fô csoportra lehet osztani. Az RSAREF. függvényeivel fordított verziókat tilos az Egyesült Államok és Kanada területérôl kiadni vagy letölteni. Viszont nem tilos használni, ha már egyszer kikerültek - kivéve azokat az országokat, ahol az állam belsô törvényei tiltják vagy korlátozzák a titkosítást (például Franciaország, Oroszország, Irak, Irán, Kína) Az RSAREF freeware, az RSA Data Secutity Inc. szabadalma. Az USA-ban a PGP-nek csak az RSAREF-es verzióit szabad használni.

Az MPILIB is Phill R. Zimmermann munkája, de az MPILIB függvényeire épülô programokat az USA-ban tilos használni (!) Az MIPLIB-esek az ún. "nemzetközi" (i) verziók. Ezek hatékonyabbak (gyorsabbak), 100%-ig kompatibilisek a PGP 2.x (x =< 3) verzióival is, általában kevesebb hibát tartalmaznak, és többféle operációs rendszert támogatnak. Mivel Magyarországon minden verzió szabadon használható, célszerû az "international" változatokat elônyben részesíteni.

143.



IPV6-ban már több IPSEC funkciót is átvettek, pl IKE

Az Internet Key Exchange (IKE) protokoll közvetlenül az IPSec szabványhoz került kifejlesztésre, és, mint ahogy neve is sejteti, az Interneten zajló kommunikáció eseti titkosításához használható kulcsok megszerzését tenné lehetővé az IPSec projekt eredeti célkitűzésében szereplő eseti titkosított kapcsolatok kiépítéséhez.

144.

IT security management

- A probléma
  - „Security is a process, not a product” (B.S.)
- A megoldás
  - Módszertanok, szabványok alkalmazása
    - Erről volt már szó - Bea
  - Megfelelő fizikai struktúra
  - Megfelelő logikai struktúra
  - Megfelelő eszközök használata
  - Újabb probléma:
    - A biztonság a használhatatlanságig fokozható – kompromisszumok kellenek

A strukturálásnál elsődleges szempontként a fizikai adottságok és az elsődlegesen megoldandó feladatok játszanak szerepet. A hálózat az elsődlegesen fizikai elhelyezkedési alapokon kialakított munkacsoportokban (3), vagy ezeken praktikus okok miatt kívül eső (4, 7) munkaállomásokból, az ezek szoftveres működtetéséhez szükséges kiszolgálókból (9, 10), valamint a hálózati elérést biztosító aktív és passzív elemekből (2, 6, 8) áll.

145.

IT sec. - fizikai struktúra

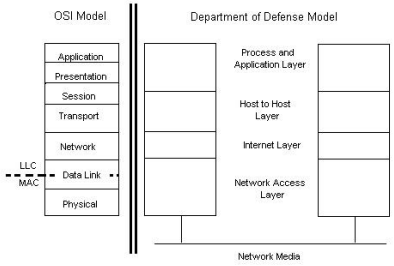
- A gyenge fizikai struktúra
  - Egyszerű lehetőséget ad SW behatolásra
    - (keylogger, usb diszk, reboot, stb...)
  - Hajlamosabb a meghibásodásra
    - (DoS érzékenyebb lehet)
  - Nem IT szempontból is veszélyes
  - Logikailag is meghatároz egyes tényezőket
- Alapvető probléma az organikus fejlődés
  - Gondoljunk a jövőre is vásárláskor
  - Tervezett bővítés, legyen policy

Nem IT szempont: tűzvédelem

146.

IT sec. - logikai struktúra

- Alapja a helyes fizikai struktúra
- ISO OSI (DoD) bottom-up tervezés



Hálózati incidenskezelés – Tutorial - 146 - 2006 május

A komponensek logikailag csak a funkcionális szempontoknak felelnek meg, azaz:

Az „1” jelölésű LAN egy Ethernet szegmenst alkot, az összes szereplő valós publikus IP címmel rendelkezik, vagyis minden kiszolgáló és munkaállomás minden kiszolgálót és munkaállomást teljes felületen elérhet. A hálózat a „2” jelölésű elérési pontokon biztosít elérést a külvilág (WAN) számára. A „3” jelölésű helyi (LAN kapcsolat) munkaállomások, a „4” jelölésű otthoni (WAN és pont-pont elérés) munkaállomások és a „7” jelölésű mobil (WLAN) számítógépek egyenlő jogú felhasználói a hálózati szolgáltatásoknak.

Az „5” jelölésű helyi használatú szerverek szintén a hálózat egész területéről elérhetőek, bár csak lokálisan, az adott munkacsoport kiszolgálását végzik. A „8” jelölésű router nem végez címfordítást és tűzfalszerű funkciókkal sem rendelkezik, hisz ezek egyike sem szükséges a hálózat üzemeltetéséhez. A hálózati kiszolgáló funkciókat a „9” jelölésű, a munkaállomásokkal, munkacsoportokkal fizikailag azonos hálózatra kötött gépek végzik, esetlegesen együttműködve a „10” jelölésű, az Internet más részén elhelyezkedő kiszolgálókkal.

147.

IT sec. - network access (1)

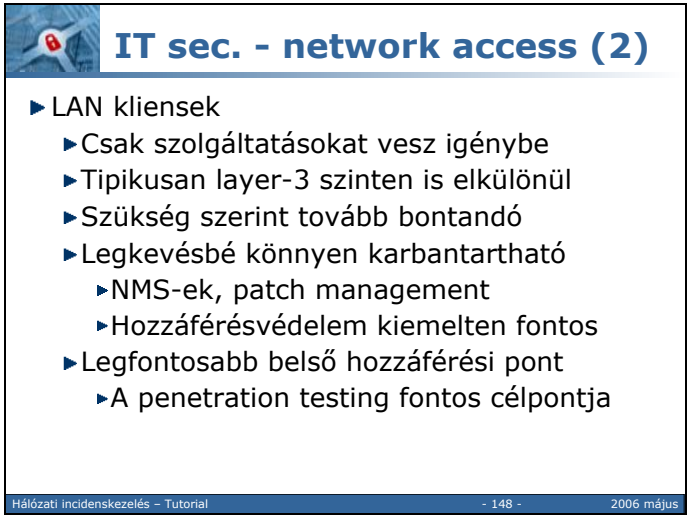
- ISO OSI layer-1 (phy.) és layer-2 (data link)
- Hozzáférésvédelem
  - Ethernetnél pl. MAC korlátozás
  - Csatlakozási pontok fizikai védelme
- Hálózati szintű elkülönítés, VLAN technológia
  - Funkcionális szempontok szerint
    - LAN (Local Area Network) kliensek
    - LAN kiszolgálók
    - DMZ (DeMilitarized Zone)
    - VPN (Virtual Private Network)

Hálózati incidenskezelés – Tutorial - 147 - 2006 május

A demilitarizált zóna, röviden DMZ azokat a gépeket („9“) tartalmazza, melyek szolgáltatásait egyaránt igénybe veszik az Interneten és a helyi hálózaton elhelyezkedő gépek is. A DMZ gépei legfőképp abban különböznek a hálózat többi zónájától, hogy az Internet irányába közvetlen kiszolgáló tevékenységet végeznek.

A DMZ védelmét a „14“ jelölésű tűzfal látja el, mely, az ábra egyszerűsítése végett – ahogy az ábrán látható többi tűzfal is – router szerepet is vállal. A DMZ hálózat klasszikusan publikus, statikus IP című gépeket tartalmaz, de a „14“ jelölésű tűzfal port átirányító szolgáltatásai esetén akár privát címek hozzárendelése is lehetséges. Ez a tűzfal a zóna funkcióinak megfelelően mindkét irányban végez forgalomtovábbítást.

148.



A LAN az eredeti hálózat fizikai munkacsoportjait, vagyis a hálózat java részét kitevő kliens szerepű munkaállomásokat („1“) tartalmazza. Ellentétben az eredeti fizikai elhelyezkedésen alapuló elkülönítéstől, az új megoldás a hálózatot logikailag, a munkacsoportok alapján csoportosítva layer 2 szinten szeparált virtuális LAN-okra bontja.

A LAN védelmét a „13“ jelölésű központi tűzfal látja el, a LAN gépeinek korlátozott elérést biztosítva a többi főbb csoportban található számítógépek szolgáltatásaihoz. A LAN és virtuális felbontásai privát IP címtartományokat foglalnak el, mivel ezek a számítógépek csak kliens szerepű felhasználói a rendszernek. A tűzfal csak a LAN gépei által kezdeményezett forgalom továbbítását végzi a LAN irányába, ez megoldható a hálózati címfordítást alkalmazó NAT technológia alkalmazásával is.

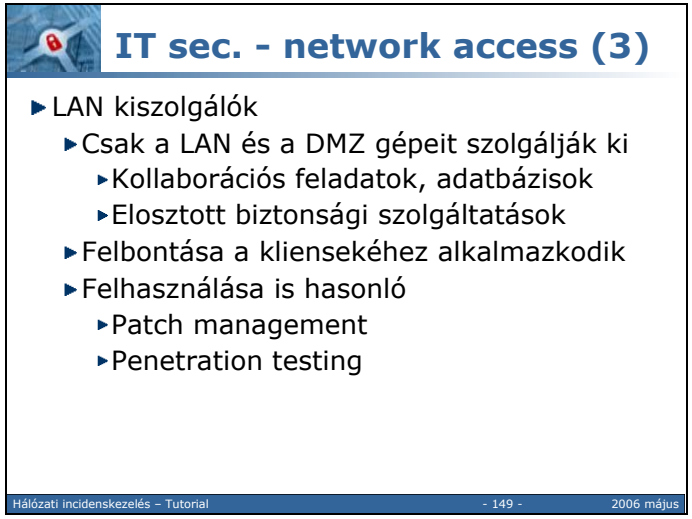
A LAN esetében dinamikus címkiosztás (DHCP) is célszerűvé válhat. Ilyen esetben, mivel a DHCP protokoll alapvetően nem route-olható, problémát jelenthet a kiszolgáló („16“) VLAN-okhoz viszonyított elhelyezése. A problémára több megoldás adható:

Minden VLAN-ba külön DHCP kiszolgálót kell telepíteni. Ennek csak akkor van értelme, ha az aktív hálózati eszközök („6“) támogatják a címkiosztást. Ez nem ritkán így van.

Egy DHCP kiszolgálót kell telepíteni, de a kiszolgálónak támogatnia kell a VLAN protokollt, így megoldható, hogy fizikailag egy gép több VLAN-t is ellásson dinamikus címekkel.

Az előző megoldáshoz hasonlóan egy kiszolgálót kell telepíteni, azonban a VLAN-ok kiszolgálása megoldható az aktív hálózati eszköz („6“) DHCP-proxy szolgáltatás támogatásának segítségével.

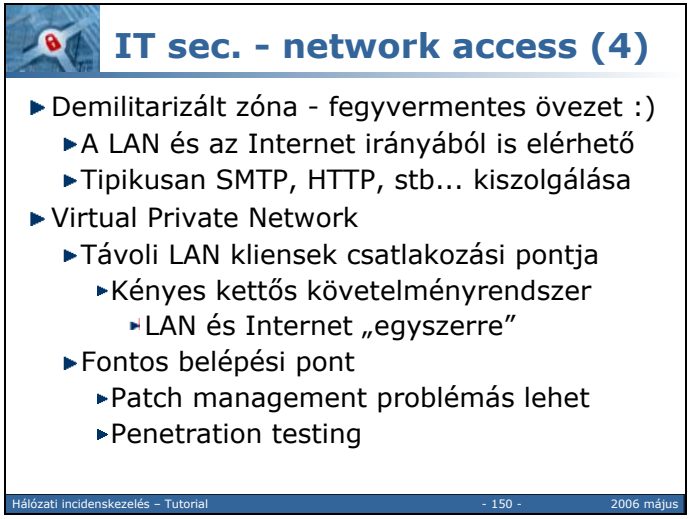
149.



A SERVICE zóna a DMZ privát megfelelője. Itt találhatók azok a nem kliens szerepű gépek, melyek szolgáltatásokat nyújtanak a DMZ és a LAN számítógépei számára. Ilyen szerep juthat egy intranetes groupware („3“), egy általános, a ., funkcionális ábrán egy vagy több logikai munkacsoport kiszolgálását végző általános szerepű szerver („5“) és általában minden adatbázis-kiszolgáló („4“).

A SERVICE zóna védelmét a „13“ jelölésű tűzfal látja el, a DMZ és LAN zónák számítógépeinek korlátozott elérést biztosítva a zóna szolgáltatásaihoz. A SERVICE zóna számítógépei a belső elérhetőség biztosítása érdekében célszerűen statikus privát IP címmel rendelkeznek, az Internetet a LAN gépeihez hasonlóan csak kliens szerepben érhetik el.

150.



Külön zónaként szerepel a LAN-on fizikailag kívül, de logikailag belül elhelyezkedő, a LAN-hoz hasonló szolgáltatásokat igénybe venni kívánó, úgynevezett „szatellit“ munkaállomásokat kiszolgáló VPN zóna. A VPN biztonsági problémáiról a . fejezetben bővebb információ található.

A VPN zóna az általánosan elterjedt három külső csatlakozási pont felől a következőképpen érhető el az otthoni („4“) és mobil („7“) szatellit munkaállomások számára:

Az internet kapcsolattal rendelkező szatellitek, a hálózat egyéb internetes forgalmával együtt, a „14“ jelölésű tűzfalon keresztül juthatnak el a „11“ jelölésű VPN szerverhez.

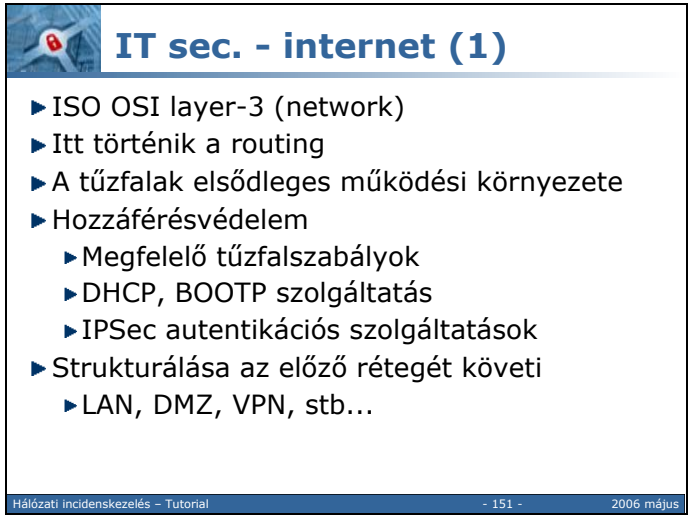
A telefonos behívók a „2“ jelzésű modemen keresztül a „12“ jelölésű, elkülönített terminálszerverrel veszik fel a kapcsolatot, ahonnan a „15“ jelölésű tűzfalon keresztül juthatnak el a VPN szerverhez.

A „7“ jelölésű mobil munkaállomások egy WLAN elérési ponton keresztül szintén a „15“ jelzésű tűzfalhoz kerülnek, melyen keresztül a VPN szerverhez csatlakozhatnak.

Mint látható, a szatellit gépek egymástól és a hálózat többi részétől layer 2 szinten elkülönítve, tűzfalas szűrés után juthatnak el az azonosítást és hitelesítést végrehajtó, valamint a biztonságos csatornát közvetlenül kiépítő központi VPN szerverhez. Az így authentikált forgalom a „13“ jelzésű tűzfal szigorú szűrőszabályain keresztül logikailag a LAN egy VLAN-jából származó forgalomként kezelhető a továbbiakban, de a szolgáltatásokat az útba eső tűzfalak segítségével célszerű minimálisra korlátozni.

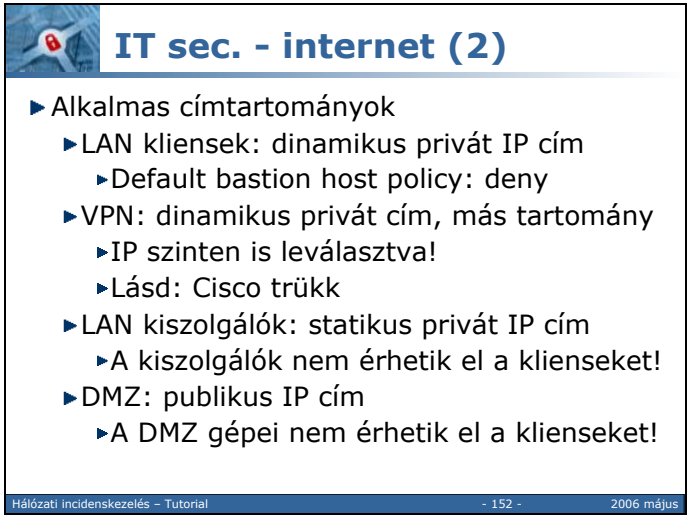
A szatellit gépek biztonságos kezelésére, mivel ezek a gépek a védeni kívánt hálózat számára ellenőrizhetetlen adatforgalmat is folytathatnak, nincsen teljes értékű megoldás, csak abban az esetben ha teljesen a hálózatkezelő felügyelete alá vonhatók, ám erre a gyakorlatban kevés lehetőség adódik.

151.



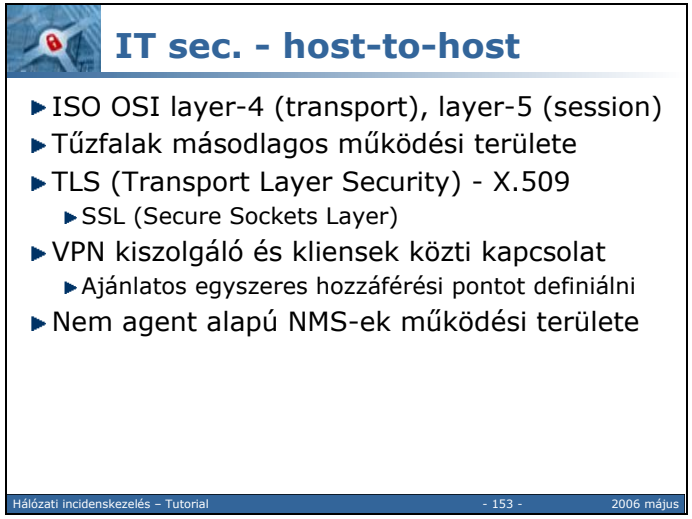
Az ábrán látható struktúra fizikai szempontból összevonásokra ad lehetőséget, a „6“, „13“, „14“, „15“ jelölésű aktív hálózati eszközök akár egyetlen VLAN kompatibilis routing switch-ben is helyet kaphatnak, fontos azonban, hogy az apró szaggatott vonallal elkülönített hálózatok (DMZ, LAN és részei, SERVICE, VPN és részei) fizikailag, vagy virtuálisan is különböző (Ethernet) szegmensekre essenek. Az ábrán vázolt logikai struktúra a . fejezetben említett fizikai központosítást is könnyebbé téve az eszközök behatolás elleni védelmét is.

152.



A routing trükk az, hogy a peccseletlen klienset a peccsszerverrel egy vlanba zárják, és minden http requestet hozzá irányítanak.

153.



Főként egyszerűbb, de a magyarországi Internet elterjedésének kezdeti korszakában kiépített hálózatokra jellemző lehet a csak kliens jellegű felhasználási mód mellett a publikus internetes elérhetőség. Ilyen esetben gyakorlatilag a kliensek számára semmi szükség a publikus IP címek megtartására, vagyis az egész hálózat, egy ToReS IP címtranszformációs tűzfal mögé elhelyezve, az ábrán „NAT” jelöléssel ellátott alhálózatnak megfelelő pozícióba tolható. Ezzel a megoldással részben kiválthatóak a kliensekre telepített alkalmazástűzfalak, hiszen a hálózat kívülről indított kapcsolatfelvételek ellen védetté válik, a NAT hálózat privát IP címei nem elérhetők az Internet irányából.

154.

IT sec. - alkalmazások

- ISO OSI layer-6 (present.), layer-7 (app.)
- Agent alapú NMS-ek működési területe
- Elosztott biztonsági szolgáltatások
  - X.500, PGP, Kerberos
- Penetration testing
- Patch management
- Lan alkalmazások telepítésének korlátozása
- Layer-7 szintű (proxy) tűzfalak

Fontos megjegyezni, hogy sok tűzfal eldobja az ICMP echo-request és echo-reply üzeneteket, ezért nem vonhatóak le feltétlen következtetések egy ping próba eredményéből, szükség lehet további ellenőrzésekre. Ennek legegyszerűbb módja az lehet, hogyha a host scannert teljesen kihagyjuk a pásztázási műveletből, és egyenesen a port scannert irányítjuk a letapogatni kívánt címtartományba, a ping módszer által eldöntendő kérdést úgy fogalmazzuk át, hogy egy hoszt akkor érhető el, ha a port scanner talált rajta nyitott, vagy zárt portot, és akkor nem érhető el, ha semmilyen választ sem sikerült kapni. A módszer hátránya természetesen a nagy időigényben rejlik: a ping program egy üzenetváltással eldönthette az elérhetőséget, míg a port scanner technikával nagyságrendekkel több üzenetre is szükség lehet.

155.

Összefoglalás

- A megelőzés alapjai:
  - Legyen világos és átlátható
    - Fizikai, logikai struktúra, management
  - Tudjuk, hogy mink van
    - Penetration testing, NMS-ek
  - Tartsuk karban
    - Patch management
  - Kövessük a biztonsági szempontokat
  - Kössünk tudatos kompromisszumokat
    - A biztonság használhatatlanságig fokozható, ugyanígy a management is

156.

Hasznos linkek, referenciák

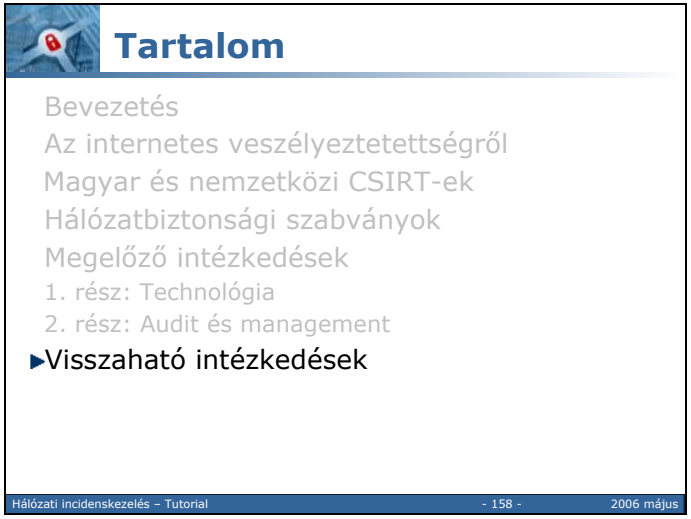
- Önmegtámadás, önellenőrzés
- Szoftverfrissítések, verziókövetés
- Elosztott biztonsági szolgáltatások
- Hálózati struktúra megfelelő kialakítása
  - Fizikai szint
  - Logikai szint

157.

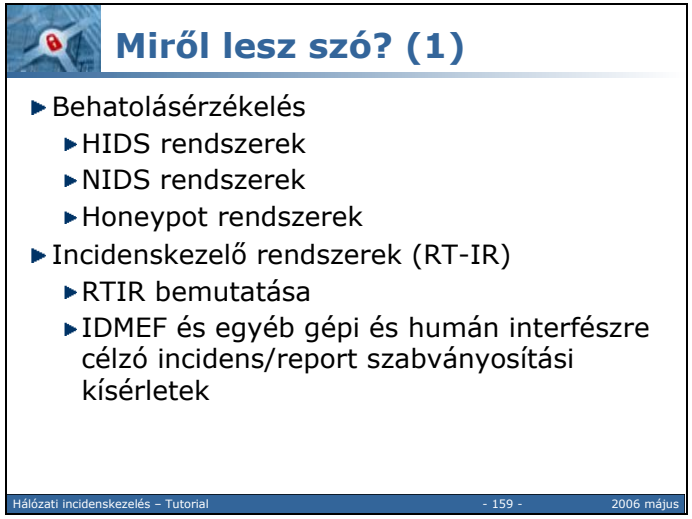
Hun-CERT
HUNGARIAN NATIONAL COMPUTER EMERGENCY RESPONSE TEAM

Visszaható intézkedések

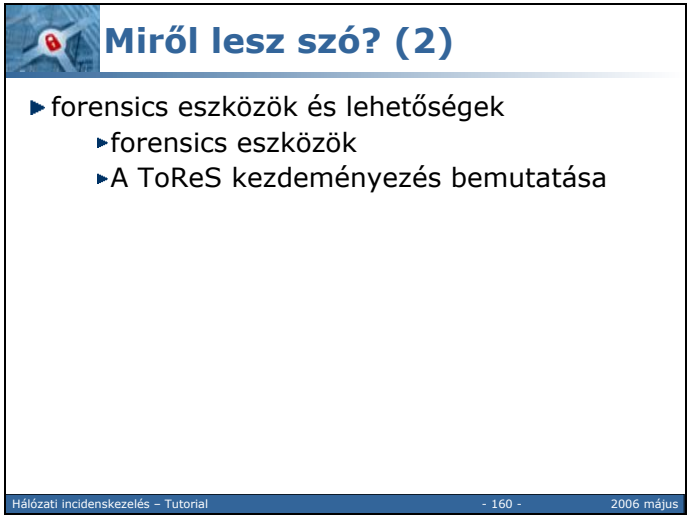
158.


Tartalom
Bevezetés
Az internetes veszélyeztetettségről
Magyar és nemzetközi CSIRT-ek
Hálózatbiztonsági szabványok
Megelőző intézkedések
1. rész: Technológia
2. rész: Audit és management
Visszaható intézkedések
Hálózati incidenskezelés – Tutorial - 158 - 2006 május

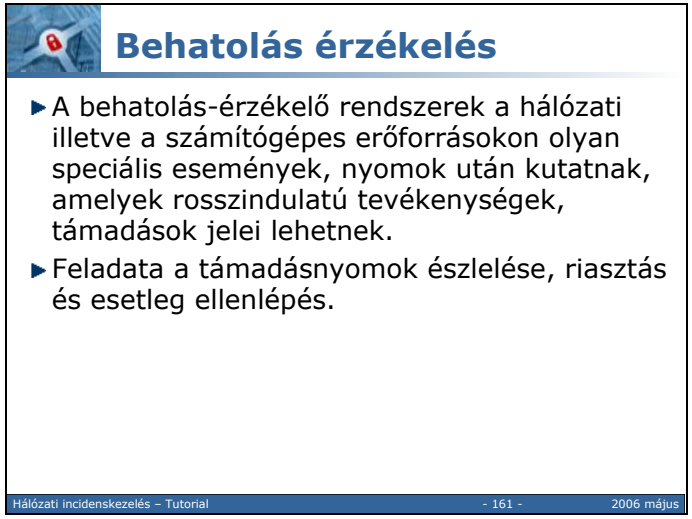
159.


Miről lesz szó? (1)
Behatolásérzékelés
HIDS rendszerek
NIDS rendszerek
Honeypot rendszerek
Incidenskezelő rendszerek (RT-IR)
RTIR bemutatása
IDMEF és egyéb gépi és humán interfészre célzó incidens/report szabványosítási kísérletek
Hálózati incidenskezelés – Tutorial - 159 - 2006 május

160.


Miről lesz szó? (2)
forensics eszközök és lehetőségek
forensics eszközök
A ToReS kezdeményezés bemutatása
Hálózati incidenskezelés – Tutorial - 160 - 2006 május

161.


Behatolás érzékelés
A behatolás-érzékelő rendszerek a hálózati illetve a számítógépes erőforrásokon olyan speciális események, nyomok után kutatnak, amelyek rosszindulatú tevékenységek, támadások jelei lehetnek.
Feladata a támadásnyomok észlelése, riasztás és esetleg ellenlépés.
Hálózati incidenskezelés – Tutorial - 161 - 2006 május

162.

Történelmi áttekintés

- Történelem
  - 1980 - James P. Anderson tanulmánya: számítógépek biztonsági vizsgálatának és felügyeletének javítás; automatikus behatolás-érzékelés
  - 1984 - 1986 IDES (Intrusion Detection Expert System)
  - Az IDES után a fejlesztések sora indult meg, az USA kormánya támogatta az ilyen irányú kutatásokat. Jelentősebb projektek voltak: Discovery, Haystack, MIDAS (Multics Intrusion Detection and Alerting System), NADIR (Network Audit Director and Intrusion Reporter). Ez utóbbi rendszert Los Alamos 9000 felhasználós hálózatára telepítették. Bár jobbára offline működött, a behatolások érzékelésére statisztikai módszereket és nyomfelismerést (signature) használt.

A behatolás-érzékelés majdnem egyidős a számítógépek megjelenésével Kezdetben a adminisztrátorok monitorozták a felhasználók tevékenységét, észrevehették pl. ha egy szabadságon lévő munkatárs nevében bejelentkeztek stb. Ebben az időben szokás volt a bejelentkezési logfájlok kinyomtatása és utólagos elemzése. Egy esetleges incidens esetén kevés remény volt a támadó azonnali azonosítására.

1980-ban James P. Anderson tanulmányában azt elemezte, hogy lehetne a

számítógépek biztonsági vizsgálatát és felügyeletét javítani. Az automatikus behatolás-érzékelés gondolatát is neki tulajdonítják, amelyet egy másik cikkében írt le.

1984 és 1986 között Dorothy Denning és Peter Neumann fejlesztette ki az első valósidejű IDS-t, az IDES-t (Intrusion Detection Expert System). Az IDES tulajdonképpen egy szabályalapú szakértői rendszer volt, amit a rosszindulatú, veszélyes tevékenység érzékelésére tanítottak. A következő generációja a NIDES lett, amit még ma is használnak. Az IDES után a fejlesztések sora indult meg, az USA kormánya támogatta az ilyen irányú kutatásokat. Jelentősebb projektek voltak: Discovery, Haystack, MIDAS (Multics Intrusion Detection and Alerting System), NADIR (Network Audit Director and Intrusion Reporter). Ez utóbbi rendszert Los Alamos 9000 felhasználós hálózatára telepítették. Bár jobbára offline működött, a behatolások érzékelésére statisztikai módszereket és nyomfelismerést (signature) használt.

163.

IDSek osztályozása (1)

- Beavatkozási pont szerint
  - *HIDS* - Hoszt-alapú IDS-eket magára a védendő hosztra telepítik, adatforrása a gépen lévő logfájlok, naplófájlok és megadott biztonsági szabályok. A hoszt alapú rendszerek nemcsak az operációs rendszer elleni behatolás--védelemre, hanem az alkalmazások védelmére is szolgál.
  - *NIDS* - Hálózat-alapú IDS-ek adatforrása a hálózaton áthaladó csomagok, ezeket elemzi.
  - *Stack-alapú* IDS-ek a rendszerek figyelik, ahogy a protokollelemek haladnak a különböző OSI szintek között felfelé, és még mielőtt az operációs rendszer vagy az alkalmazás megkapná, az IDS elemzésre magához vonja.

Az IDSeket alapvetően két kategóriába sorolhatjuk attól függően, hogy hol helyezkednek el az infrastruktúrában. Egyrészt telepíthetünk behatolás érzékelőt a rendszerben használt hostokra. Itt tudunk védekezni mint az operációs rendszert, mind a hoston futó szolgáltatásokat, alkalmazásokat ért támadások ellen.

Telepíthető IDS a hálózat kritikus pontjaira is. Ezeken a pontokon az áthaladó hálózati forgalom megfigyelésével és ezek elemzésével vonhatunk le következtetéseket az esetleges behatolásokra nézve.

Újabban szokás megkülönböztetni egy harmadik típust is, az úgynevezett stack alapú rendszert. Ez esetben arról van szó, hogy míg a NIDSek userspaceben futó programok, addig a stack alapú rendszerek beépülnek az operenciás rendszer hálózatot kezelő részébe, és már ott képesek az adatok elérésére. Tehát tulajdonképpen ez nem egy külön kategória, inkább a hálózat alapú IDSek következő evolúciós lépése.

164.

IDSek osztályozása (2)

- Alkalmazott technológia szerint
  - *Rendellenességet észlelő modell* (anomaly-based, behavior-based, policy-based): az ilyen IDS-t először megtanítják arra, hogy az adott hálózaton, gépen melyek a normális események. A normálistól eltérő viselkedést észleli a rendszer, támadásnak veszi és riaszt.
  - *Visszaélést érzékelő modell* (misuse detection, knowledge-based): az ilyen modell esetében a különféle támadásokról és sebezhetőségekről szóló információt tárolják, és ha rendszer egy olyan adatot észlel, ami a tárolt információkkal egybeesik, támadásnak jelzi azt.

Hálózati incidenskezelés – Tutorial - 164 - 2006 május

Alkalmazott technológia szerint alapvetően két módszer különböztethető meg. Az első kategóriába azok a rendszerek tartoznak, amelyek rendellenességet észlelnek. Ezek az IDSek úgy működnek, hogy a működésük elején „megtanulják" azt, hogy az adott környezetben mi tekinthető normális működésnek, és az ettől való eltérésekre riaszt.

A másik kategória a visszaélést érzékelő modell. Ezek egy olyan adatbázisból dolgoznak, amely ismert behatolási módszerekre vonatkozó információkat tartalmaz. A rendszer ezek nyomát keresi.

A második rendszer előnye, hogy kevesebb fals pozitív eredményt ad, hátránya viszont, hogy ismeretlen módszerrel elkövetett behatolások érzékelésére alkalmatlan.

165.

IDSek osztályozása (3)

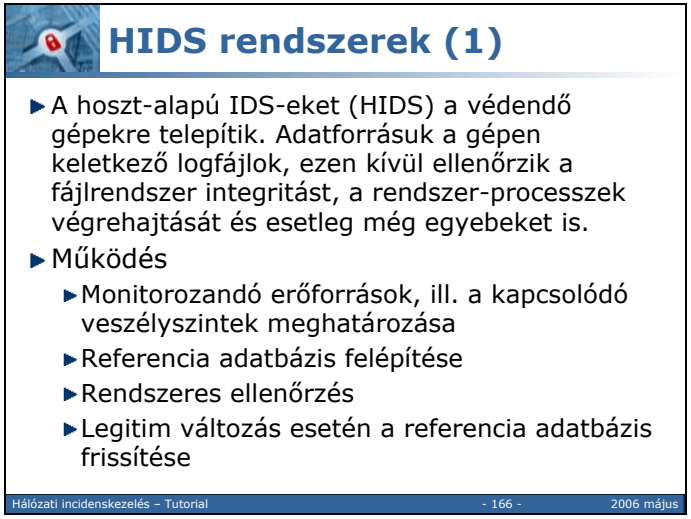
- Utólagos reakció szerint
  - *Passzív rendszer*: a passzív rendszer érzékeli a behatolási kísérletet, feljegyzi az erre vonatkozó adatokat, riaszt.
  - *A reagáló rendszer* (reactive): a fentieken kívül még további automatikus védekező tevékenységet is végez.

Hálózati incidenskezelés – Tutorial - 165 - 2006 május

Utólagos reakció szerint ismerünk passzív rendszereket, amelyek működése csak a riasztásig terjed, vagyis csak felismer, naplóz és jelez, ill. reagáló rendszereket, amelyek megpróbálnak valamilyen automatikus válaszlépést is eszközölni a behatolás ellen.

Ez utóbbi sajnos jelenleg még gyerekcipőben jár, aminek oka egyrészt a hamis riasztások igen nagy száma, másrészt az ilyen automatizmusok kihasználhatósága. (Példaként hozhatók egy fontos host nevében elkövetett támadás hatásai egy ilyen automatára).

166.



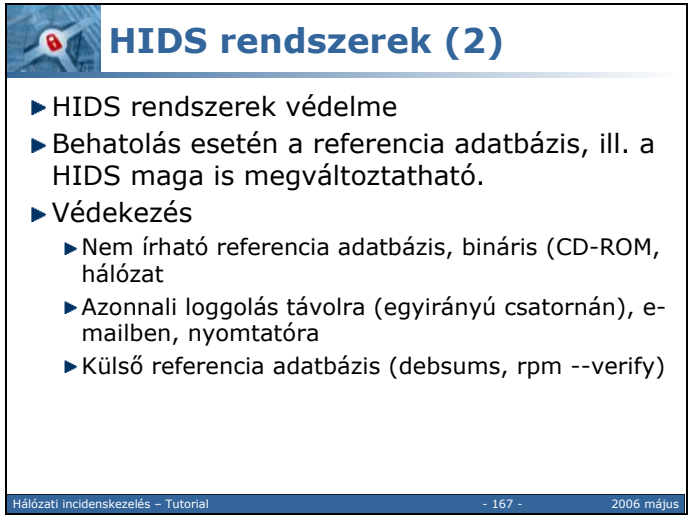
A host alapú rendszereket a hálózat számítógépeire telepítik. Információforrásaik a rendszeren található fileok, a naplózott adatok és a futó alkalmazásokra vonatkozott adatok.

A host alapú IDSek telepítése előtt meg kell határozni a megfigyelni kívánt erőforrásokat, ill. az ezekhez kapcsolódó veszélyszinteket. Ezekből aztán fel kell építeni egy olyan referencia adatbázist, amely a normális állapot jellemzőit tartalmazza.

A működés során az aktuális állapot kerül összehasonlításra a referencia adatbázissal, és a különbségek alapján történik meg a figyelmeztetés.

Természetesen ha egy eseményről kiderül, hogy az mégis legitim volt, akkor a változásokat be kell vezetni az adatbázisba.

167.



HIDS rendszereknél tekintettel kell lenni arra, hogy a host kompromittálódása esetén az IDShez is hozzáfér a támadó, így lehetősége van nyomai elleplezésére. Ez ellen többféleképpen lehet védekezni:

Nem írható helyen tárolt referencia adatbázissal: cd-rom, csak olvasható hálózati meghajtó, stb. Természetesen az adatbázis gyakori változásánál ez kényelmetlenséget okozhat.

Azonnali naplózás egyirányú (vagyis csak egyszer írható) csatornán, pl. e-mail, nyomtató.

Bizonyos esetekben, pl. Linux disztribúcióknál rendelkezésre áll független referencia adatbázis.

168.

HIDS rendszerek (3)

- Előnyök
  - Monitorozható a felhasználók tevékenysége, a fájlokon végzett műveletek.
  - Lehetővé teszi a rendszerkomponensek figyelését, mint pl. Windows esetén a Registry vagy fontos DLL-ek monitorozása.
  - A kódolás használata a NIDS-et egyes támadásokkal szemben érzéketlenné teheti, a HIDS-et pedig nem.
  - A HIDS futatásához nem használnak külön hardvert, így olcsóbb lehet a NIDS-nél.
  - Megállapítható egy támadás sikeressége, ill. részletesebb információk szerezhetők róla.

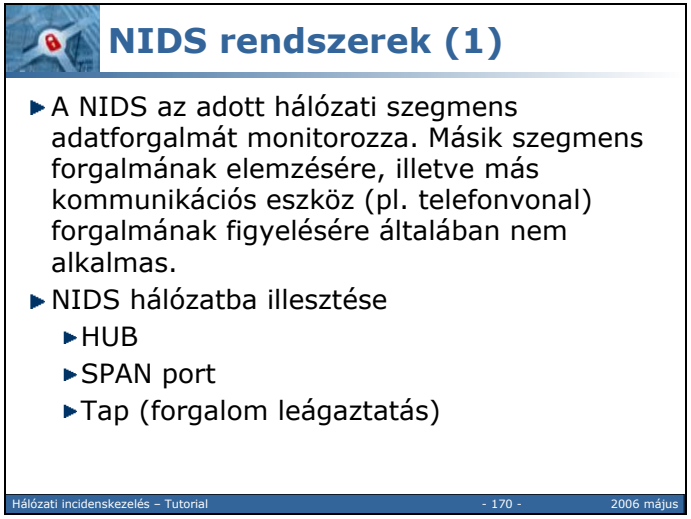
169.

Tripwire

- Kritikussági típusok
  - SEC_CRIT – fájlok, amelyek soha nem változhatnak
  - SEC_BIN – fájlok, amelyeknek nem kellene változniuk
  - SEC_CONFIG – ritkán változó, de gyakran olvasott konfigurációs fileok
  - SEC_LOG – Folyamatosan növekvő, de sosem tulajdonost változtató fájlok
  - SEC_INVARIANT – könyvtárak, melyeknek sosem változik a tulajdonosuk, vagy a jogosultságaik

A fenti felsorolás a Tripwire nevű HIDS osztályozási rendszerét mutatja be. Természetesen lehetőség van ezeknek a megváltoztatására, ill. újak létrehozására.

170.



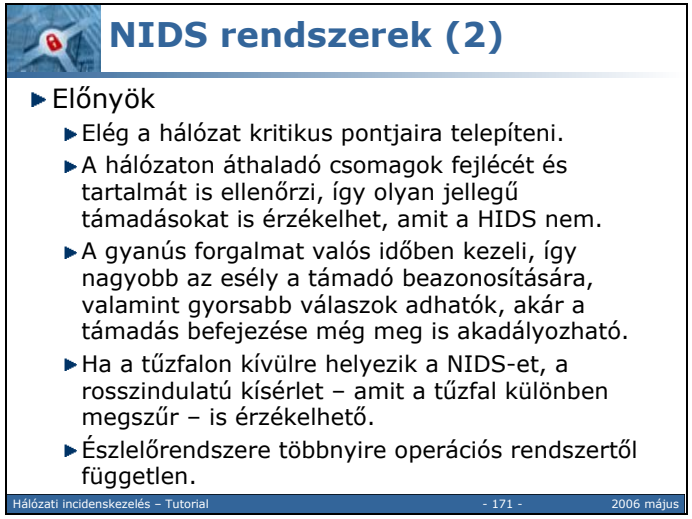
A hálózati IDSek (NIDS) egy adott hálózati szegmens forgalmát figyelik, és ebben keresnek behatolásra utaló nyomokat.

Mivel jelenleg a tipikus számítógép hálózatok mikroszegmentáltak (switcheltek), ezért meg kell oldani, hogy a NIDShez a hálózat teljes forgalma eljusson. Erre háromféle módszer adódik:

A csatlakozási pont és a hálózat közé egy HUB segítségével beköthető a NIDS. Ezen megoldás azonban teljesítmény- és megbízhatóságbeli problémákat jelenthet.

Komolyabb switchek képesek bizonyos portjaikra a teljes forgalmat kivezetni (span port), ill lehetőség van a direkt forgalomágaztatásra készített eszközök (un. tap-ek) használatára.

171.



172.

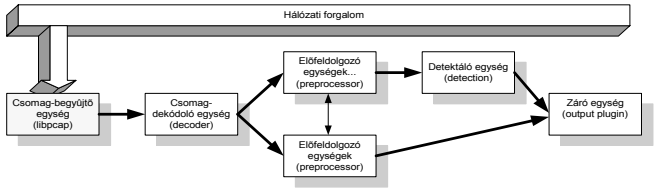
NIDS technikák

- Mintaillesztés
- Állapotfüggő mintaillesztés
- Heurisztikán alapuló elemzés (statisztikai becslések)
- Rendellenességen alapuló elemzés
  - Profil alapú
  - Protokoll alapú
  - Trend elemzés
  - Statisztikai rendellenesség
- Protokoll-dekódoló elemzés

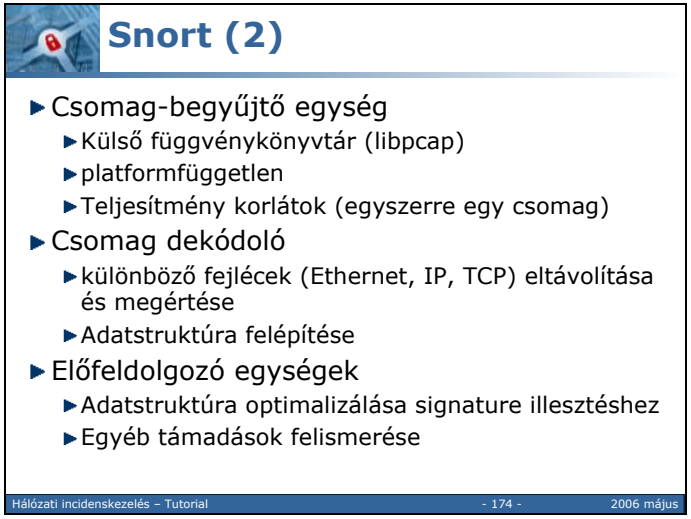
173.

Snort (1)

- Felépítés
  - csomag-begyűjtő egység (packet capturing)
  - csomag dekódoló (packet decoder)
  - előfeldolgozó egységek (preprocessor)
  - detektáló egység (detection engine)
  - záró egységek (output plugins)



174.

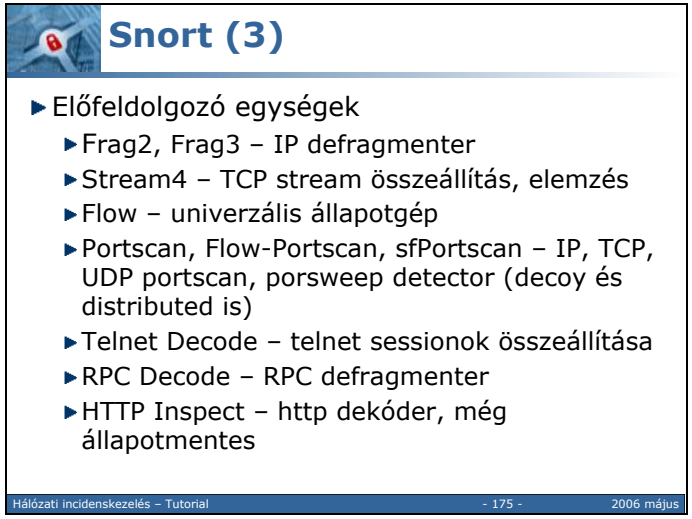


A Csomag-begyűjtő egység feladata a csomagok begyűjtése az az operációs rendszertől. A Snort a libpcapet használja, ami sok platformon elérhető, hátránya, hogy párhuzamos feldolgozásra még alkalmatlan.

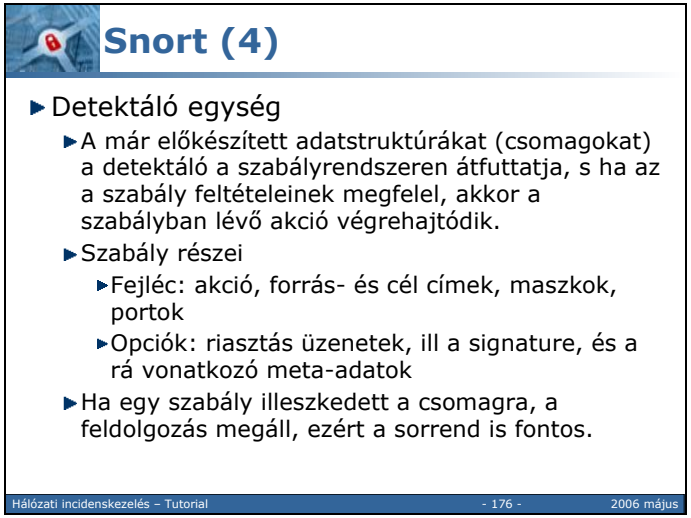
A dekódoló egység feladata a csomagok fejléceinek eltávolítása, ill. a későbbiekben használható adatstruktúra felépítése.

Az előfeldolgozó egységek adatstruktúra optimalizációt végeznek a mintaillesztéshez, ill. bizonyos általános támadási formák felismerése is itt történik meg.

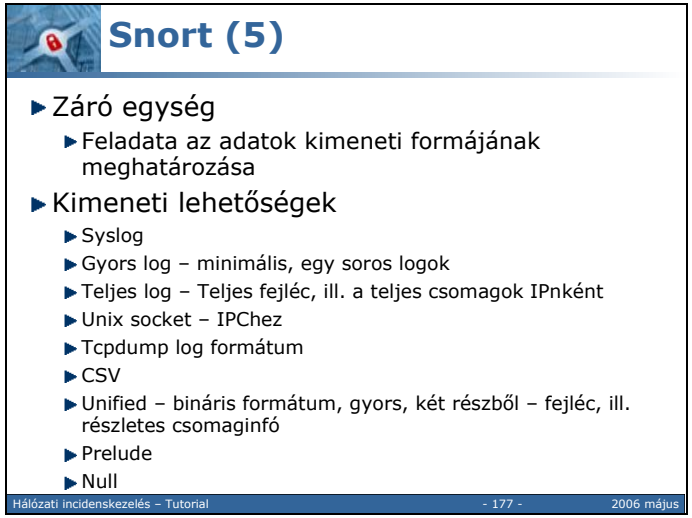
175.



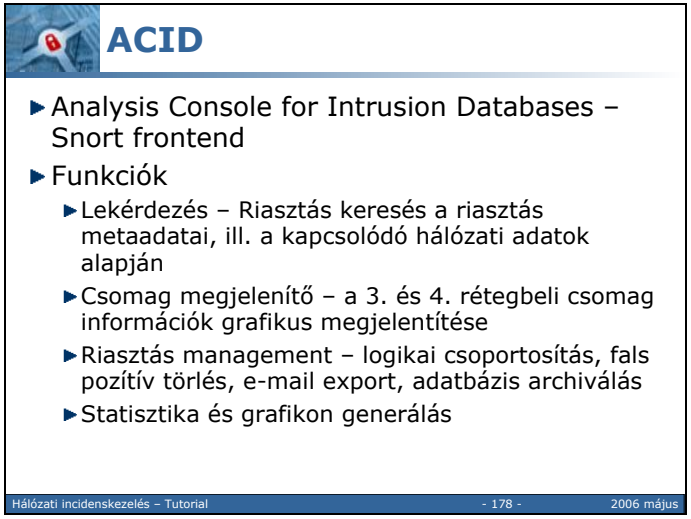
176.


Snort (4)
Detektáló egység
A már előkészített adatstruktúrákat (csomagokat) a detektáló a szabályrendszeren átfuttatja, s ha az a szabály feltételeinek megfelel, akkor a szabályban lévő akció végrehajtódik.
Szabály részei
Fejléc: akció, forrás- és cél címek, maszkok, portok
Opciók: riasztás üzenetek, ill a signature, és a rá vonatkozó meta-adatok
Ha egy szabály illeszkedett a csomagra, a feldolgozás megáll, ezért a sorrend is fontos.
Hálózati incidenskezelés – Tutorial - 176 - 2006 május

177.


Snort (5)
Záró egység
Feladata az adatok kimeneti formájának meghatározása
Kimeneti lehetőségek
Syslog
Gyors log – minimális, egy soros logok
Teljes log – Teljes fejléc, ill. a teljes csomagok IPnként
Unix socket – IPChez
Tcpdump log formátum
CSV
Unified – bináris formátum, gyors, két részből – fejléc, ill. részletes csomaginfó
Prelude
Null
Hálózati incidenskezelés – Tutorial - 177 - 2006 május

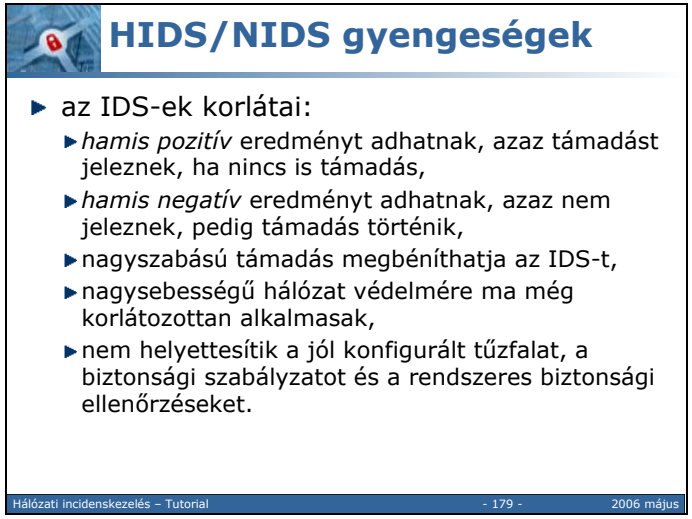
178.



A Snort rengeteg információt naplóz, aminek áttekintése nehézkes. Ebben nyújt segítséget az Analysis Console for Intrusion Databases. Az ACID egy webfelületű frontend a snort által naplózott adatok áttekintéséhez.

Képes különböző szempontok szerinti lekérdezésekre, riasztás-management funkciókkal rendelkezik (logikai csoportosítás, archiválás, stb.), statisztikákat készít, ill. képes grafikusan megjeleníteni az adatbázisban található csomagokra vonatkozó 3. és 4. rétegbelii információkat.

179.



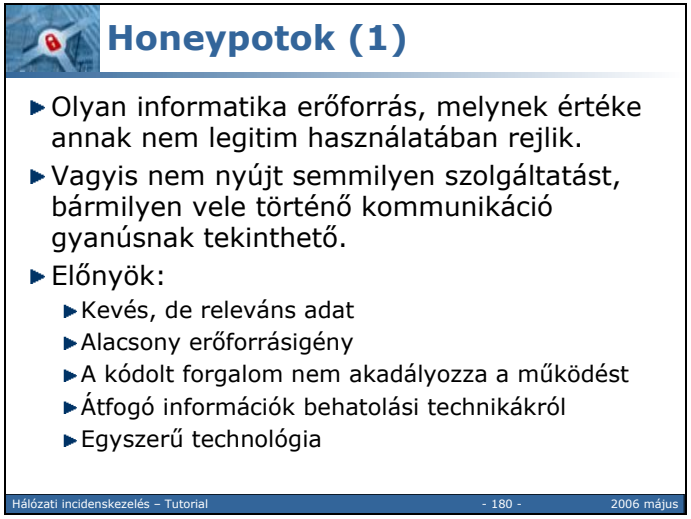
A HIDS/NIDS rendszerek használata – minden egyéb intézkedéshez hasonlóan – bizonyos kockázatokkal jár, amelyekkel számolni kell.

Egyrészt fals pozitív eredményeket adhatnak. Ez akkor jelent problémát, ha ezekből túl sok van, egyrészt mert eltereli a figyelmet az igazi támadásokról, másrészt mert komoly erőforrás és időveszteség ezeknek a feldolgozása, ill. reaktív rendszerek esetén vezethet hibás intézkedéshez.

Fals negatívok is keletkeznek, vagyis bizonyos problémákat nem vesz a rendszer észre. (Pl. a visszaélést felismerő rendszerek működési modelljükből adódóan nem alkalmasak ismeretlen módszerrel történő behatolások detektálására.) Fontos, hogy ne alakuljon ki hamis biztonságérzet a felhasználóban, és tudatosítsa, az IDS rendszerek használata önmagában nem megoldás.

A nagy számítási teljesítmény miatt bizonyos NIDSek kiemelten érzékenyek a DOS típusú támadásokra.

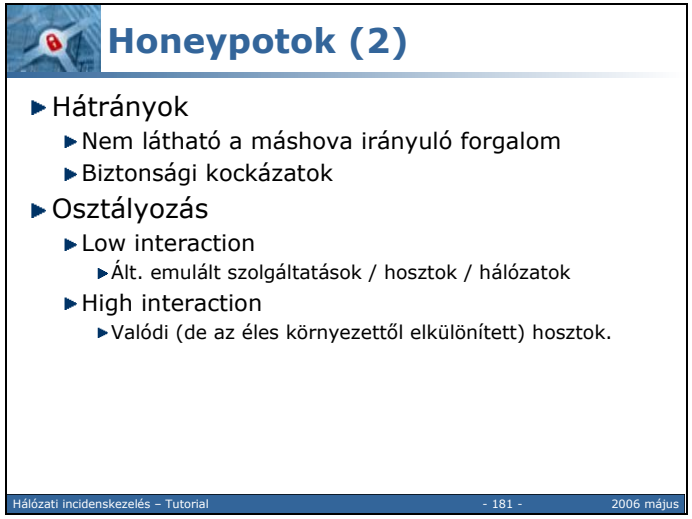
180.



A honeypot rendszerek olyan rendszerek, amelyek „csaliként” vannak kihelyezve, nincsenek valós funkcióik, szolgáltatásaik, ezért a rendszerhez történő összes hozzáférés elve gyanús.

Ezen technika előnye, hogy kevés, de releváns adatot szolgáltat, a HIDSekhez képest lényegesen alacsonyabb erőforrásigényekkel rendelkezik, nem jelent problémát a kódolt csatornák használata.

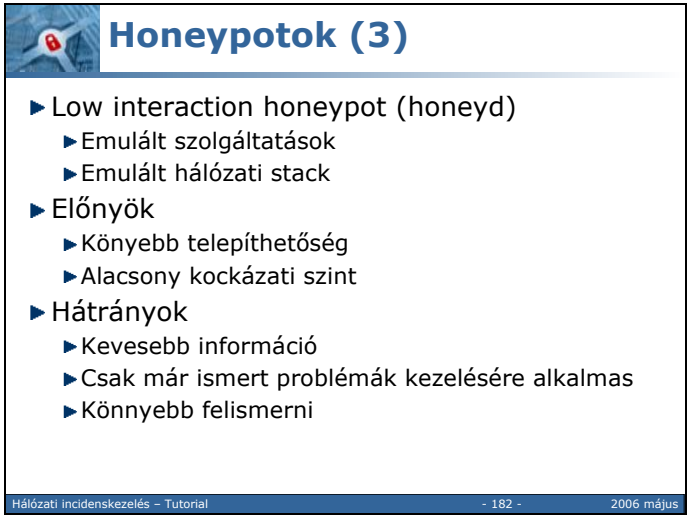
181.



A honeypot rendszereknek természetesen hátulütői is vannak: egyrészt csak az a forgalom jelenik meg rajtuk, aminek ők voltak a címzettjei, vagyis önmagában nem alkalmas teljes körű behatolás detektálásra, ill. (az esetenként szándékosan rosszul védett) hamis rendszerek beépítése a hálózatba biztonsági kockázatot jelent.

A honeypotokat két csoportba szokás sorolni: low ill. high interaction rendszerek.

182.

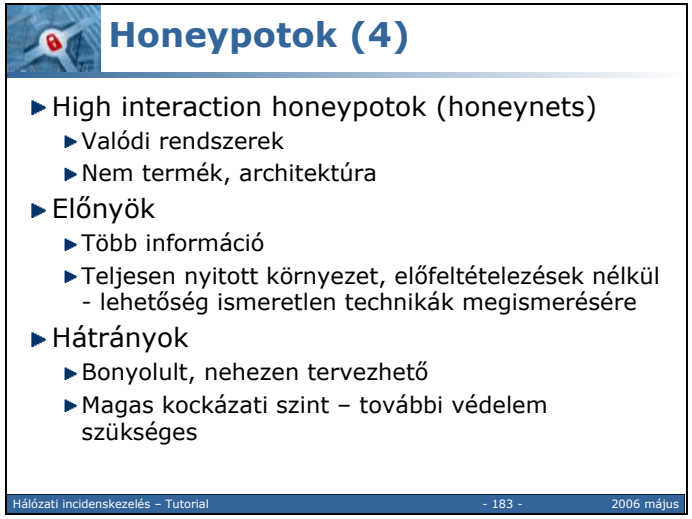


A low interaction rendszerek ált. szolgáltatásokat, számítógépeket, hálózatokat emuláló programok. Az egyik legismertebb ilyen a honeyd nevű szoftver, ami a fentieken felül képes különböző operációs rendszerek hálózati stackjának emulálására (az nmap adatbázisa alapján), vagyis képes elrejteni, a host operációs rendszer identitását.

Ezen rendszerek előnye, hogy vannak kész megoldások, amelyek viszonylag könnyen beállíthatóak, ill. mivel emulációról van szó, lényegesen alacsonyabb a kockázati szint.

Hátrányuk, hogy kevesebb információhoz jutunk, csak ismert problémákat tud kezelni (hiszen az emulációt csak már ismert esetre lehet írni), ill. az emuláció felismerése könnyebb, mintha valódi rendszereket használnánk.

183.

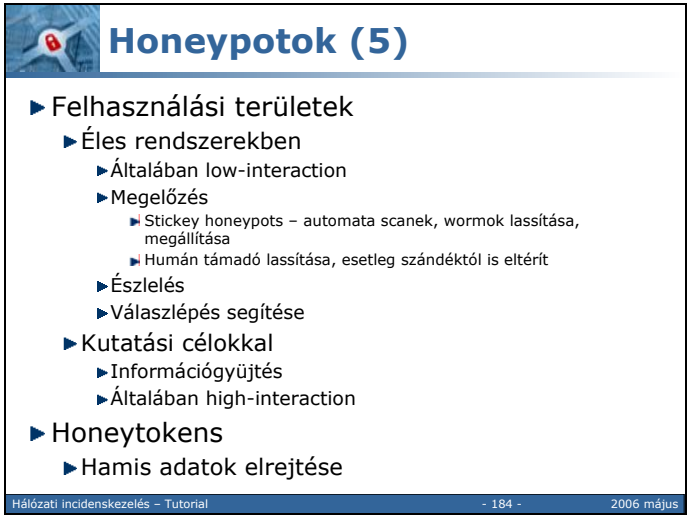


A high interaction rendszereknél nincsenek kész termékek. Itt arról van szó, hogy valódi számítógépekre telepítünk valódi szoftvereket, amelyek igazából nyújtanak szolgáltatások, és esetleg igazi hálózatokba vannak rendezve, de egyéb célra ezeket nem használjuk. Ilyen hálózatok összefogása pl. a honeynet projekt.

Ennek előnye, hogy lényegesen több ismeretet lehet begyűjteni, ill. mivel egy ilyen rendszer teljesen nyitott, mindenféle előfeltételezéstől mentes, lehetőséget nyújt az eddig ismeretlen támadási módszerek megismerésére.

Hátránya egyrészt, hogy komoly hozzáértést igényel, ilyen rendszerek építése egyáltalán nem triviális, és meglehetősen költséges, igazából csak kutatási célokra használható. Továbbá tekintve, hogy itt valódi rendszerektől van szó, a biztonsági kockázatok meglehetősen magasak.

184.



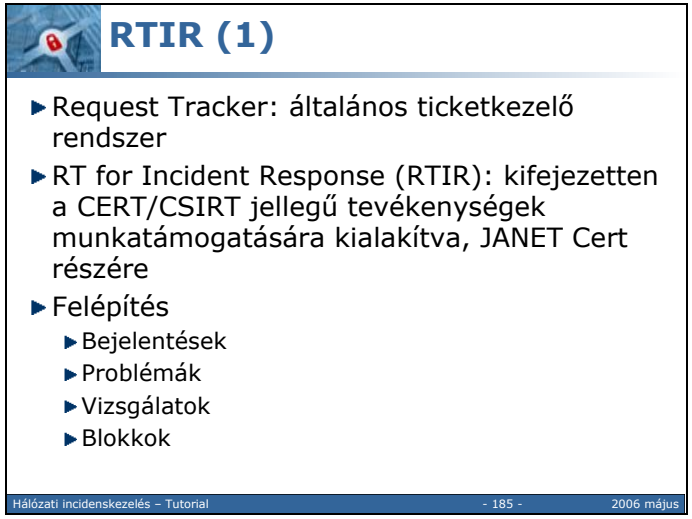
A honeypot rendszerek főbb felhasználási területei a következők:

Éles rendszerekben észlelésre, megelőzésre lehet őket használni, különböző trükkökkel az automaták működését jelentősen le lehet vele lassítani, ill. plusz adatokkal szolgáltathat az esetleges válaszlépések megtételéhez. Ilyen célokra általában low intercation rendszereket használunk.

Kutatásra is remekül használható, jó módszer a friss támadások felismerésére.

A gondolat egy másik igen érdekes lehetséges felhasználási területe a honeytokenek bevezetése. Ezek hamis adatok éles rendszerben való elhelyezését jelentik (pl. híres emberek szerepeltetése adatbázisokban), amivel valamilyen szinten szűrhető az egyébként megbízhatónak tartott felhasználók esetleges rosszindulatú tevékenységének felismerése.

185.



A következőkben röviden megismerkedünk Az RTIR nevű ticketing rendszerrel, amelyet kifejezetten az CSIRT jellegű tevékenységekkel kapcsolatos feladatok megkönnyítésére fejlesztettek.

Az RTIR egy web alapú rendszer, amiben a nyitott jegyek (ticketek) négy csoportba sorolhatóak: A bejelentések a nyers beérkező adatokat tartalmazzák, a problémák a valós megállapított problémákat (amikről több bejelentés is érkezhetett), a vizsgálatok a problémák kapcsán esetlegesen felmerült külső kommunikációk (pl. szolgáltatókkal) nyilvántartására szolgál, a blokkok pedig a saját hálózat üzemeltetéssel folytatott kommunikációra való.

Természetesen a rendszer tud minden olyan alapfunkciót, amely egy ticketing rendszertől elvárható, mint jegyek közötti relációk, keresések, szűrések, stb.

186.

RTIR (2)

Az ábra egy jegy életútját követi nyomon a rendszerben.

Miután a bejelentés beérkezik a rendszerbe (és átesik az esetleges előzetes automata vizsgálatokon, pl. spam és vírusszűrés) bekerül a bejelentések közé. Itt el kell dönteni, hogy kezelendő kérdésről van-e szó, és ha igen, akkor ismert problémához kapcsolódik-e?

Probléma esetén meg kell tenni az esetlegesen szükséges lépéseket a saját hálózatunkban, ill. le kell folytatni a külső felekkel történő kommunikácitót, ha erre szükség van a probléma elhárításához.

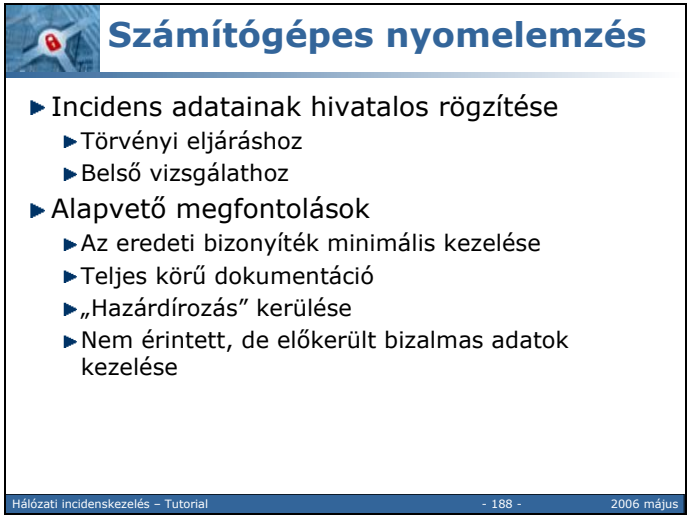
Végül a jegyet le kell zárni..

187.

RTIR (3)

- További szolgáltatások
  - Csoportos értesítések létrehozása, akár whois alapján is
  - Integrált hálózati lekérdező eszközök (traceroute, whois)
  - Vélhetően kapcsolódó jegyek keresése
  - Testreszabható automatikus események (scrips)
  - Automatikus statisztikák

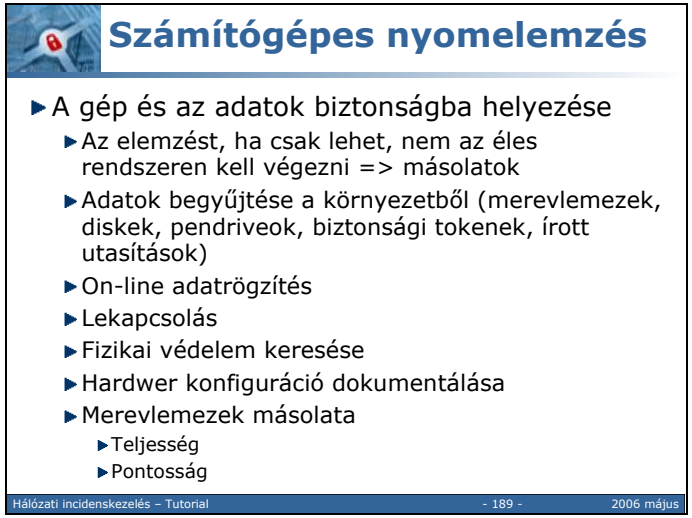
188.



A következőkben azt tekintjük át, hogy milyen alapvető elvárásoknak kell megfelelni, ha egy incidenssel kapcsolatban nyomrögzítésre van szükség, akár belső vizsgálathoz, akár jogi eljáráshoz.

A mai magyar jogi gyakorlatban sajnos nincs egyértelműen rendezve a digitális bizonyítékok kezelésének módja, az ilyen döntések igazságügyi szakértői vélemények alapján meglehetősen eseti jelleggel történnek. Ezért nagyon fontos a munka pontos dokumentálása.

189.



190.

ToReS

- Több száz, szabadon felhasználható, rendszerezett program előzetes telepítést nem igénylő futtatásának lehetősége
- Egyszerű, részben automatikus hálózati konfiguráció a kezdő felhasználók munkájának megkönnyítése érdekében
- Számos szolgáltatás futtatását biztosító kiszolgáló alkalmazások
- Hálózati biztonság fokozására figyelemmel előzetesen beállított konfigurációs állományok
- Utólagos adatmentést, bizonyíték-gyűjtést támogató segédprogramok
- A bővítés, frissítés, módosítás lehetősége nyitott

191.

Hasznos linkek, referenciák

- http://www.snort.org
- http://www.cert.hu/szabaly/
- http://sysinternals.com

192.

Kapcsolatfelvétel

- MTA – SZTAKI, Hálózatbiztonsági osztály
  - 1518 Budapest, Pf. 63
  - 1111 Budapest, Lágymányosi utca 11.
  - Tel: (1) 279-6222
  - http://nsd.sztaki.hu
- Hun-CERT
  - http://www.cert.hu

- btoth@sztaki.hu (Tóth Beatrix)
- becz@sztaki.hu (Becz Tamás)
- don@sztaki.hu (Pásztor Szilárd)
- mcree@sztaki.hu (Rigó Ernő)
- tiszai@sztaki.hu (Tiszai Tamás, ov.)

193.

Hun-CERT
HUNGARIAN NATIONAL COMPUTER EMERGENCY RESPONSE TEAM

Köszönjük a figyelmet!