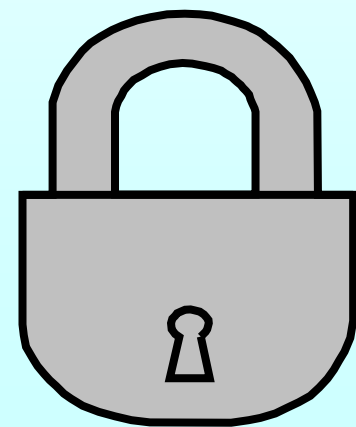


Adat és információvédelem

Dr. Beinschróth József
CISA



Informatikai biztonság



Technológia?

Kevin Mitnick, a legendás hekker, a Keselyű: „...nem hisz a technikában. Az adatvédelmi rendszerek egyre fejlettebbek, és ha az információhoz való hozzáférésről van szó, az igazán üdvöztető módszer a social engineering, vagyis az emberi tudatlanság, hiszékenység és segítőkészség kihasználása...ő például annak idején rettenetesen kíváncsi volt a Motorola legújabb szoftverének forráskódjára. Mit tett tehát? Felhívta a Motorolát, és elkérte a hipertitkos forráskódot. Nem ment nagyon egyszerűen, többekkel is beszélnie kellett, de végül egy segítőkész titkárnő összetömörítette neki a fájlokat, és feleltépezte egy nyilvános szerverre.

És ez még mind semmi: a Keselyű és barátai hajdanán előszeretettel turkáltak a számítástechnikai cégek szemeteszsákjaiban - Mitnick szerint a kis zsákokra érdemes hajtani, mert a nagyobbak a véceből származnak - és belső használatra szánt telefonkönyvekhez meg jelszavakhoz jutottak hozzá a kukabúvárkodás révén. A szemét: aranybánya, állítja a Keselyű, aki szerint az ilyesmi azért lehetséges, mert "lyukak vannak az emberi tűzfalon". Ráadásul az ember már csak olyan, hogy hisz saját sebezhetetlenségében. Ezért nem kapcsolja be a biztonsági övet, ezért dohányzik, és ezért dobja ki a szeméttbe a jelszót. Nem szabadna, állítja a Keselyű, és hozzáteszi: a social engineering százszázalékosan hatékony, a támadónak alig jelent kockázatot, ráadásul - a technikai védelmi eszközökkel szemben - teljesen platformfüggetlen.

Hogyan védekezhetünk a social engineering ellen? Minden cég fogalmazza meg biztonsági alapelveit, figyelmeztet a Keselyű, osztályozza az adatokat titkosságuk alapján, végezzen behatolási teszteket, okítsa az alkalmazottakat és készítse fel őket arra, hogyan reagáljanak éles helyzetekben - például ha egy Keselyű a jelszavukat követeli telefonon...” (www.index.hu - 2005.02.02.)



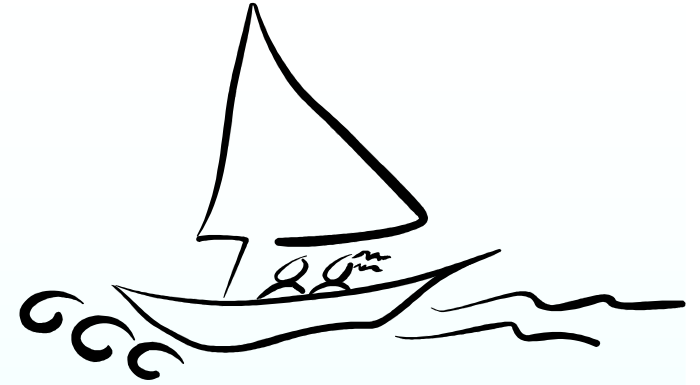
Tematika – miről szól a tárgy?

- Alapfogalmak, az IT biztonság problematikái
 - Problémák, következmények
 - Biztonság, informatikai biztonság
 - Technológia
 - Informatikai kockázatok
 - Adatbiztonság, adatvédelem, titokvédelem
- Nemzetközi és hazai ajánlások
- Az IT rendszerek fenyegetettsége
 - Fenyegetettség, veszélyérzet, hamis biztonsági tudat
 - Biztonsági környezet
 - Veszélyforrások (szervezeti, humán, természeti, fizikai, logikai, életciklus, elemekhez kapcsolódó)
 - Kárkövetkezmények

- Az IT rendszerek védelme
 - Védelmi módszerek (szervezeti, humán, természeti, fizikai, logikai, élelciklus)
 - A védelem erőssége
- Az IT biztonság tervezése
 - Védelmi igények, helyzetfeltárás, biztonsági cél
 - Fenyegetettség elemzés
 - Kockázatelemzés
 - Kockázat menedzselés (normál üzemeltetés, krízishelyzet, katasztrófa helyzet)
- BCP, DRP
- A biztonság ellenőrzése: biztonsági audit

Alapfogalmak, az IT biztonság problematikái

- Problémák
- Következmények
- Fogalmak
- Technológia
- Ajánlások



“ I cannot imagine any condition which could cause this ship to flounder. I cannot conceive of any vital disaster happening to this vessel.”

E.J. Smith, Captain of the Titanic, 1912

Problémák

- Informatikai robbanás (hardver-szoftver technológia, Internet, hatalmas adatbázisok, e-business...)
- A gazdálkodó szervezetek informatikától való függősége megnőtt
- Az informatikai kockázat üzleti kockázattá vált
- A megfelelő technológia alkalmazása és a szabályozás nem feltétlenül követte a kockázat növekedését

- A biztonsági tudatosság nem megfelelő, hamis biztonsági tudat, a kellő szakértelem hiánya, hanyag kezelés

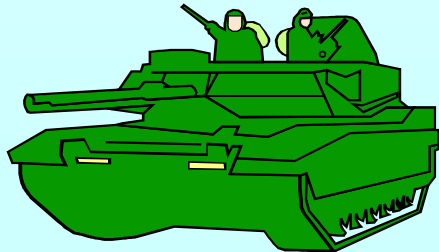
- Felügyelet nélkül hagyott gépek
- Nem megfelelő jelszóhasználat
- Hordozható gépeken értékes adatok
- Megfelelő mentések hiánya
- Bizalmas információt tartalmazó gépet szerviznek, kölcsön adnak
- ...



- **Visszaélések**

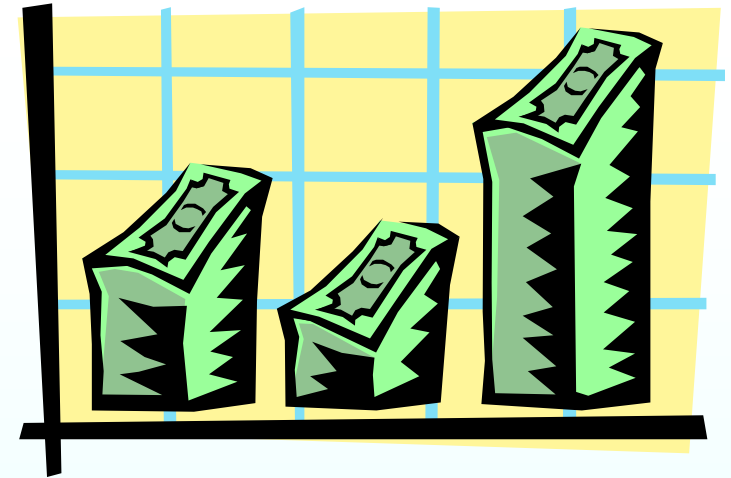
- Információ gyűjtés
 - Ajánlatok adatainak eladása
 - Fizetési lista illetéktelen olvasása
- Adatmódosítás
 - Fizetés növelés
 - Banki átutalás módosítás
- Más névben történő manipuláció
 - Levélküldés, rendelésfeladás más névben
 - Továbbjelentkezés más névben

- **Informatikai hadviselés, fehérgalléros bűnözés, terrorizmus**



Következmények

- Veszteségek több területen
 - a szolgáltatásokban
 - a működésben
 - a megbízhatóságban
 - a hírnévben
 - az üzleti eredményben
- Költségek merülnek fel
 - A prevenció olcsóbb és kalkulálható



Költségek?

- Biztonság-költség összefüggés
 - Nagyobb biztonság-nagyobb költség
 - Nemlineáris összefüggés
 - Létezhet optimum: kielégítő biztonság elfogadható költségek mellett – átfogó vizsgálat, szakértői közreműködés szükséges
- Játékelméleti megközelítés
 - Az IT rendszert üzemeltetőnek csak veszteségei lehetnek, így célja ezek minimalizálása lehet

Fogalmak

- Biztonság:
 - Kedvező állapot, megváltozása nem kizárható, de kis valószínűségű – Üzleti követelmény!
 - A biztonság dinamikus állapot (folyamat) !
 - A biztonság nem teremthető meg pusztán áru és szolgáltatás megvásárlásával, hanem minden esetben a szervezet életébe beépülő folyamatnak kell lennie.

Fogalmak

A biztonság összetevői

Gazdasági biztonság

A gazdasági szervezet működéséhez szükséges, az üzleti követelményeknek megfelelő gazdasági feltételek, folyamatos biztosítása

Üzembiztonság

Az intézmény technikai biztonsági feltételeinek biztosítása

Vagyonbiztonság

Az intézmény technikai biztonsági feltételeinek biztosítása

Informatikai biztonság

Az informatikai erőforrások bizalmassága, sértetlensége, rendelkezésre állása minimálisan fenyegetett, azaz a kedvező állapot megváltozásának valószínűsége igen kicsi

Fogalmak

Bizalmasság

Korlátozott kevesek számára megismerhető

Sértetlenség

Az eredeti állapotnak megfelel, teljes

Rendelkezésre állás

Az eredeti rendeltetésnek megfelelő szolgáltatások nyújtása, meghatározott helyen és időben, megfelelő performanciával

(Hitelesség Működőképesség)

Fogalmak

Védelem

- Tevékenység (tevékenység sorozat), amely a fenntartásra irányul, a védelem egy olyan tevékenység, illetve olyan tevékenységek sorozata, amely arra irányul, hogy megteremtse, folyamatosan szinten tartsa és fejlessze azt a dinamikus állapotot, amit biztonságnak neveznek
- A védelemre vonatkozó követelmények: zárt (minden fenyegetésre), teljeskörű (minden rendszerelemre) , folytonos (időben), kockázatokkal arányos

Informatikai védelem

- olyan védelem, amelyben tárgy az információ ill. az adat
- alapvetően két feladat megoldására koncentrál:
 - az információ elvesztésének (megsemmisülésének) megakadályozása;
 - az információ illetéktelen kézbe kerülésének megakadályozása

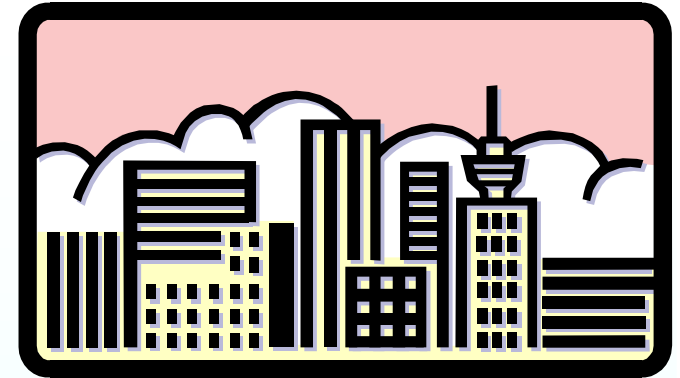
Információ védelem

- Tárgya nemcsak az elektronikusan tárolt információ, hanem az összes többi is (pl. papíralapú, tudás stb.)

Technológia: az informatikai rendszer

- Az informatikai rendszer főbb elemei:
 - A környezeti infrastruktúra elemei
 - Hardver elemek
 - Adathordozók
 - Dokumentumok
 - Szoftver elemek
 - Adatok
 - A rendszerekkel kapcsolatba kerülő személyek (humán faktor).
 - Hálózatok (kommunikáció)

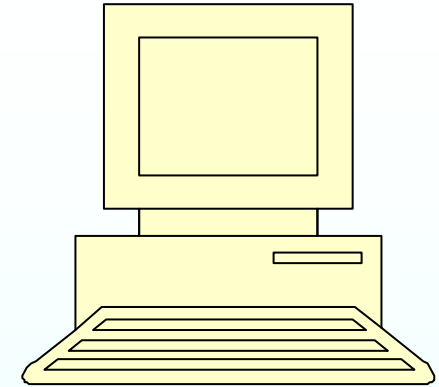
A környezeti infrastruktúra



- Terület (épület, objektum)
- A rendszer elemeinek elhelyezésére szolgáló helyiségek (irodák, szerver szobák...)
- Átviteli vezetékek az épületben és az épületen kívüli területeken egyaránt (kábelrendezők...)
- Áramellátás (szünetmentes, megerősített...)
- Klimatizálás
- Víz, csatorna, szellőzés
- Telefon
- Belépés-ellenőrző eszközök
- Tűzvédelmi berendezések
- Betörésvédelmi berendezések

Hardver elemek

- Felhasználói terminálok
- Felhasználói (desktop gépek)
- Hordozható számítógépek
- Beviteli és kiviteli eszközök
- Cserélhető tároló eszközök
- Speciális biztonsági berendezések (token, chipkártya, ujjlenyomat leolvasó...)
- Rendszerkonzolok
- Központi hardver (szerver, mainframe gépek)
- (Adathordozók)



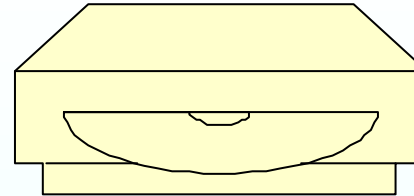
Adathordozók

– Adatok jellege

- Biztonsági másolatok
- Munka másolatok
- Archív adatokat tartalmazó adathordozók
- Új és újrafelhasznált adathordozók

– Eszközök

- Mágnesszag/kazetta
- Magneto-optikai diszk
- Floppy
- Cdrom, DVD
- Pen drive
- Hard disk



Dokumentumok

- Kezelési, felhasználási utasítások (hardver,szoftver)
- Üzemeltetési előírások
- Nyilvántartások
- Jegyzőkönyvek
- Munkaköri leírások
- Működési folyamat leírások
- Szabályzatok
- Egyéb dokumentációk



Szoftverek

- Rendszerszoftverek (operációs rendszer)
- Alkalmazások
- Javítóprogramok
- Egyéb szoftverek

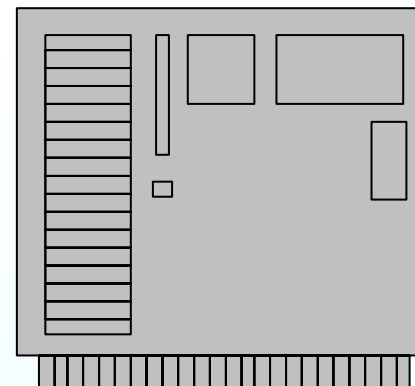


Személyek

- Felhasználók
- Üzemeltetők
- Fejlesztők
- Őrző és felügyelő személyzet
- Segédszemélyzet
- Külső munkatársak
- Hackerek ...



Adatok



- Adatok a bevitel folyamatában
- Adatok a feldolgozás folyamatában (központi egységben, alkalmazói programmal)
- Tárolt adatok (tartósan vagy csak a feldolgozás idejében)
- Adatok a kivitel folyamatában
- Mentett adatok
- Archivált adatok

Hálózatok (kommunikáció)

- Kábelezés
- Hálózati aktív elemek
- Modemek
- Infrared
- Bluetooth
- Wireless LAN
- VPN
- Kriptográfia

Informatikai kockázatok

- A rendelkezésre állás sérül
Adatok, szolgáltatások nem, vagy csak korlátozottan elérhetők
- A bizalmasság sérül
Illetéktelen hozzáférés: kémkedés, kíváncsiság stb.
- A sértetlenség sérül
Nem valós adatok jelennek meg, ugyanakkor azt hisszük, hogy valósak



Az informatikai biztonság összetevői:

- Fizikai biztonság
 - Hozzáférések
 - Rendelkezésre állás
- Logikai biztonság
 - Hozzáférések
 - Rendelkezésre állás
- Szervezési biztonság
 - Szervezet és működés szabályozása
 - Humán biztonság
 - Titokvédelem
 - Szerződések harmadik felekkel
- Életciklushoz kapcsolódó biztonsági kérdések

Adatvédelem - adatbiztonság

- Adat

Tények, elképzelések, utasítások emberi vagy technikai eszközökkel történő formalizált ábrázolása ismertetés, feldolgozás ill. távközlés céljára (nemcsak a rögzített információ, hanem az emberi beszéd is)

- Adatvédelem = Titokvédelem

Jogi kérdés: (MIT?)

A hatályos jogszabályok és egyéb előírások alapján meghatározott, a titoktartás körébe tartozó adatok (államtitok, banktitok, üzleti titok stb.) védelme

- Adatbiztonság = Informatikai biztonság

–Műszaki, szervezési kérdés: (HOGYAN?)



Adatvédelem

- Jogsabályok

- 1992. évi LXIII. törvény: A személyes adatok védelméről, a közérdekű adatok nyilvánosságáról (Adatvédelmi törvény)
- 1995. évi LXV. törvény: Az államtitokról és szolgálati titokról
- 1996. évi XII. törvény: A pénzintézetekről és a pénzintézeti tevékenységről szóló, többször módosított 1991. évi LXIX. törvény módosításáról
- 1998. évi VI. törvény: Az egyének védelméről a személyes adatok gépi feldolgozása során, Strassbourgbán 1981. január 28. napján kelt Egyezmény kihirdetéséről
- 2000. évi IV. törvény: Az információ biztonságáról szóló, Brüsszelben, 1997. március 6-án kelt NATO Megállapodás megerősítéséről és kihirdetéséről
- ...

Nemzetközi és hazai ajánlások

- TCSEC
- ITSEC
- CC
- ISO17799
- MEH ITB ajánlásai
- COBIT
- ITIL
- MABISZ



Nemzetközi és hazai ajánlások

- TCSEC (DoD Department of Defence)
Trusted Computer System Evaluation Criteria
Biztonságos Számítógéprendszerek Értékelési
Kritériumai
Orange Book of DoD: 1985
- ITSEC (Európa)
Information Technology Security Evaluation Criteria
Információtechnológia Biztonsági Értékelési Kritériumok
White Book (ITSEC 1.2) Európai Közösség: 1991

- CC (Common Criteria)
 - Common Criteria for Information Technology Security for Evaluation (CCITSE)
 - (CC 2.1 = ISO/IEC 15408) 1998
- BS7799 1. része
 - British Standard – Brit Szabványügyi Hivatal
 - (ISO/IEC 17799) 2000
 - Szempontrendszer tartalmaz
- BS 7799 2. része
 - Tanúsításhoz szükséges követelményrendszer
 - Az A melléklete tartalmazza az 1. részben felsorolt követelményrendszert
 - Definiálja a bevezetés és működtetés folyamatát (PDCA ciklus stb.)
 - (Nem ISO szabvány)

- MEH ITB 8. sz. ajánlás - Informatikai biztonsági módszertani kézikönyv
 - Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság: 1994 (www.itb.hu web site)
- MEH ITB 12. sz. ajánlás – Informatikai rendszerek biztonsági követelményei
 - Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság: 1996 (www.itb.hu web site)
- MEH ITB 16. sz. ajánlás – CC, az informatikai termékek és rendszerek biztonsági értékelésének módszertana
 - Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság: 1998 (www.itb.hu web site)
 - A CC 1.0 változatának hazai feldolgozása
- COBIT (Control Objectives for IT and Related Systems)
 - ISACA (www.isaca.com, www.isaca.hu)
 - Nemcsak security, hanem elsősorban üzemeltetési kérdések

- ITIL (Information Technology Infrastructure Library)
 - OGC (Office of Government Commerce)
 - Könyvsorozat: Az informatikaszolgáltatás-irányítás gyakorlatát írja le
 - Nem rendszerekben, hanem folyamatokban gondolkodik
 - www.itsmf.hu weblap
- ITIL-re épülő gyártófüggő megoldások
 - Microsoft: MOF (Microsoft Office Framework)
 - HP: ITSM (IT Service Management)
 - IBM: IT Service Processes
- MABISZ ajánlás
 - Nem közvetlenül az IT biztonságot tárgyalja, korlátozottan használható
 - (Kockázatathárítás esetén)

Jellemzők:

- TCSEC, ITSEC, CC:
 - Az ITSEC a TCSEC filozófiáját követi
 - IT rendszerek **logikai védelme**
 - Funkcionális és minősítési követelmények
 - Nem tárgyalják az adminisztratív, szervezeti, személyi és fizikai kérdéseket–**nem teljes körűek**
 - Elsősorban az IT termékek **gyártóit** támogatják és nem az üzemeltetőket, a termékre koncentrálnak, a termékre vonatkozó követelményrendszert állítanak fel. Az üzemeltetőknek ez a gyakorlatban kevés.
 - CC: A követelmények árnyaltabbak, lehetőség van kifejezetten biztonsági termékek (pl. tűzfal) alaposabb biztonsági minősítésére.
 - Példák:
 - A Microsoft Windows NT Workstation Version 4.0 ill. Windows NT Server Version 4.0 operációs rendszerek a TCSEC C2 biztonsági csoportba lettek besorolva 1999-ben
 - Sun Solaris 2.6 operációs rendszer az ITSEC E3 biztonsági csoportba lett besorolva 1999-ben
 - A Cisco Secure PIX Firewall a CC EAL4 biztonsági osztályba lett besorolva 2001-ben

- BS7799 1. része – MSZ ISO/IEC17799
 - Új szemlélet: Nemcsak a logikai védelemmel foglalkozik, minden rendszerelemet tárgyal, **teljeskörű** követelményrendszert tartalmaz.
 - Kifejezetten a felhasználókat, az üzemeltetőket támogatja.
 - Felhasználásával egy konkrét, üzemelő rendszer minősíthető
 - Információvédelmi kézikönyv
 - De facto standard az EU-ban
 - Az informatikai biztonság átfogó vizsgálata
 - A multinacionális cégek általánosan használják
 - Vannak magyar cégek is akik eszerint minősítenek

- MEH ITB 12. sz. ajánlás
 - Logikai védelmi kérdésekben az ITSEC-et adaptálja
 - Részletes követelmények az adminisztratív, szervezeti, személyi, fizikai védelmi területekre
 - Harmonizációja szükséges lenne az ISO17799-cel!

TCSEC

- Biztonsági osztályok
 - D csoport: minimális védelem (érdemtelen pl. MDOS)
 - C csoport: szelektív és ellenőrzött védelem
 - B csoport: kötelező és ellenőrzött védelem
 - A csoport: bizonyított védelem (jelenleg gyakorlatilag nem valósítható meg – nincs megfelelő op. rendszer)

- A C csoport osztályai
 - C1: Korlátozott védelem
 - DAC (Discretionary Access Control): Az objektumoknak tulajdonosai vannak, a tulajdonosok és privilegizált felhasználók az objektumokat mások számára megoszthatják
 - ID (Identification): Azonosítható és ellenőrizhető felhasználók (nevek, jelszavak)
 - A termék jól dokumentált legyen (tartalom+forma)
 - C2: Ellenőrzött védelem
 - A C1 osztály követelményei
 - Audit: biztonsági események naplózása
 - Object reuse: Az objektumok nem újrahasznosíthatóak

- A B csoport osztályai (teszt: független szakértők)
 - B1: Címkézett védelem
 - C2 osztály követelményei
 - MAC (Mandatory Access Control): Az objektumoknak és szubjektumoknak címkéi vannak, a hozzáférés az objektuménál gyengébb címkével nem lehetséges
 - B2: Struktúrált védelem
 - B1 osztály követelményei
 - Trusted Path (biztonságos kommunikációs csatorna a távoli felhasználó és a számítógép között)
 - Device Label (eszközként meghatározott, hogy milyen érzékeny adatok tárolhatók rajta)
 - Structured Protection (A rendszer jól definiált formális modell alapján épül fel)

- B3: Biztonsági tartományok
 - B2 osztály követelményei
 - A biztonsággal kapcsolatos kódok áttekinthetők jól elválaszthatók az op. rendszer egyéb részeitől
 - Biztonsági adminisztrátor alkalmazása

MSZ ISO/IEC17799

- Informatikai biztonsági politika
 - A felsővezetés elkötelezettségének kinyilvánítása az informatikai biztonság kialakításához
 - Az informatikai biztonsági politika minimum tartalma
 - A dokumentum rendszeres felülvizsgálatának és kiértékelésének biztosítása (milyen gyakorisággal)

- Biztonsági szabályzat - az informatikai biztonsági politika minimum tartalma
 - Az informatikai biztonság pontos meghatározása, tárgya, keretei, a biztonság fontossága
 - A felsővezetés elkötelezettségének kinyilvánítása az informatikai biztonsági célok eléréséhez, az irányelvek betartásának és betartatásának teljes körű felsővezetői támogatása
 - A vállalat számára legfontosabb biztonsági elvek, szabványok és követelmények meghatározása
 - Általános és speciális információvédelmi felelősségi körök meghatározása

- Szervezetbiztonság

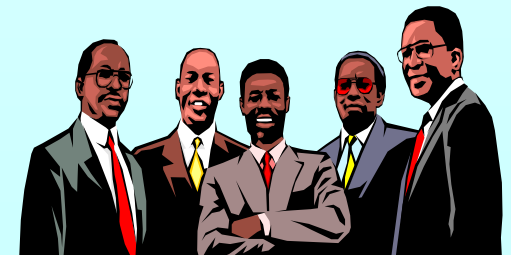
- Informatikai biztonsági infrastruktúra létrehozása az informatikai biztonság irányítására: (Vezetői fórum, a szervezet működtetése, koordináció kialakítása, szerepkörök, felelősségek meghatározása, szervezeti együttműködés, tanácsadás, független felülvizsgálat létrehozása)
- Harmadik féllel kötött szerződések informatikai biztonsági követelményei (titoktartási nyilatkozat, garanciák stb.)
- Az outsourcing (vállalkozásba adás) biztonsági szempontjai (a szerződésnek külön kell foglalkoznia a biztonsággal)



- Az informatikai vagyonelemek biztonsági szempontból történő osztályozása
 - A felelősségek meghatározása az informatikai vagyon védelmére, az adatgazdák kijelölése, a szervezet adatvagyonának (adatbázisok, alkalmazások, rendszerszoftverek, dokumentációk stb.) felmérése, nyilvántartásba vétele, felelősök névjegyzékének felvétele
 - Információ osztályozási alapelvek és kategóriák, adatok biztonsági osztályozása (nyilvános, belső, bizalmas, szigorúan bizalmas stb.)
 - Az információ minősítése, címkézése, kezelése

- Humán erőforrás védelem

- Munkaköri leírások biztonsági előírásai (biztonsági szerepkörök meghatározása, átvilágítás, a dolgozói titoktartás, alkalmazási feltételek: végzettség, tapasztalat, referenciák)
- Felhasználói oktatás (informatikai biztonsági oktatás és training)
- Biztonsági események és üzemzavarok kezelése (biztonsági események, veszélyek jelentése, rögzítése, a tapasztalatok feldolgozása, fegyelmi eljárások)



- Fizikai és környezeti biztonság
 - Védett és nem védett területek meghatározása (beléptetés rendje, a beléptetés fizikai eszközei, a munkavégzés szabályainak rögzítése, a védelmi rendszerek: beléptető, monitoring és riasztórendszerek kialakítása)
 - Az informatikai eszközök védelme (elhelyezés, szünetmentes energiaellátás, a kábelezés biztonsága, karbantartási szabályok, védelem üzemi területen kívül, hordozható gépek biztonsága, berendezés újrafelhasználás biztonsága)
 - Általános védelmi előírások (védekezés a jogtalan eltulajdonítás ellen: üres íróasztal politika, üres képernyő politika, eszköz kiszállítás szabályozása)

- A kommunikáció és az üzemeltetés menedzselése
 - Üzemeltetési eljárások és felelősségek (dokumentálás, változások követése, fejlesztői és üzemeltetői környezet elkülönülése, fejlesztői és üzemeltetői munkakörök szétválasztása, üzemeltetés külső helyszínen)
 - Rendszerek tervezése és átvétele (üzemeltetés kapacitásának tervezése)
 - Vírusvédelem
 - Rendszerháztartási feladatok (biztonsági másolatok, operátori és rendszernaplók készítése)
 - A hálózat védelme
 - Adathordozók kezelésének biztonsága
 - Információ és szoftvercsere

- Hozzáférés-ellenőrzés

- A hozzáféréseket meghatározó üzleti követelmények (mindenkinek csak annyi jogosultsága lehet, amennyi a munkája végzéséhez szükséges)
- A felhasználói hozzáférések kezelése
- A felhasználó felelősségek (jelszóhasználati szabályok, felügyelet nélkül hagyott eszközök)
- Hálózati hozzáférés ellenőrzés
- Hozzáférési jogosultságok az op. rendszerhez
- Az alkalmazások hozzáférési szabályozása
- Hozzáférések és a rendszerhasználat ellenőrzése
- Hordozható eszközök és távmunka

- Rendszerfejlesztés és karbantartás
 - Rendszerek biztonsági követelményei (analízis és specifikációk)
 - Az alkalmazási rendszerek biztonsága (beviteli és feldolgozási kontrollok, kimeneti hitelesítés)
 - Kriptográfiai kontrollok (rejtjelezés, digitális aláírás, letagadhatatlanság, kulcsok védelme)
 - Rendszerállományok biztonsági követelményei
 - Rendszer fejlesztések és karbantartások biztonsága

EXTRA EDITION AMERICA UNDER ATTACK

Newsweek®

THE INTERNATIONAL NEW

**9:03 A.M.
TUESDAY,
SEPT. 11, 2001**

**Hijacked United Airlines
Flight 175 explodes into
the World Trade Center**

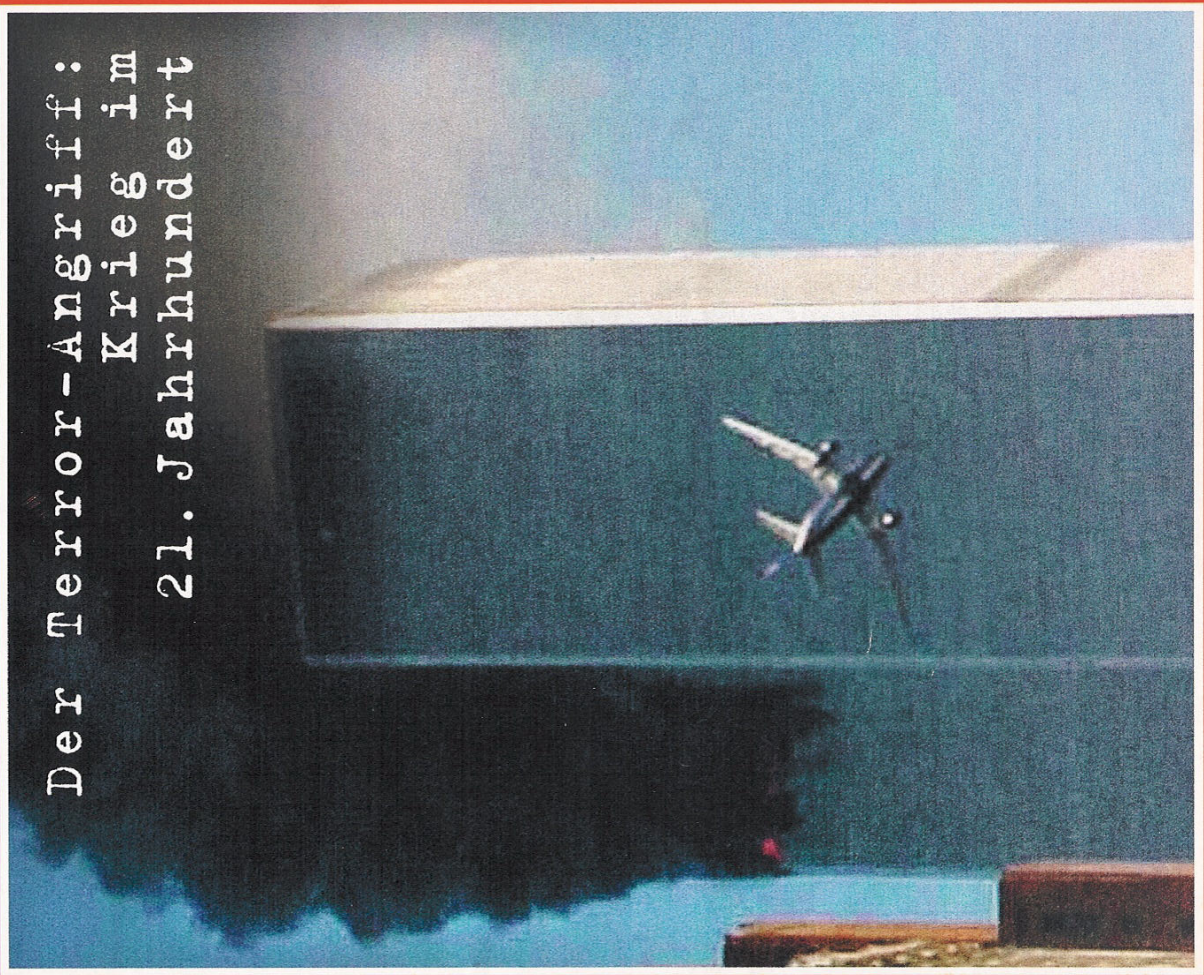
DESPERATE

Nr. 38/15.9.01 - 5,50 DM



4 390700 705500 38

Der Terror-Angriff: Krieg im 21. Jahrhundert

[illegible]

www.spiegel.de



- Üzletmenet folytonosság
 - Az üzletmenet folytonosság fenntartásának szempontjai
 - Az üzletmenet folytonosság és üzleti hatáselemzés
 - Üzletmenet folytonossági tervek (BCP, DRP) készítése és bevezetése
 - Üzletmenet folytonossági tervek tesztelése, értékelése
 - Üzletmenet folytonossági tervek karbantartása, felülvizsgálata, oktatása, tárolása, tesztelése

- **Megfelelőség**

- A jogi követelményeknek és szabványoknak való megfelelés (az alkalmazható jogszabályok meghatározása, a szellemi tulajdon védelme, az adatvédelem és a személyes adatok védelme, kriptográfiai szabályok betartása, jogkövetkezményű bizonyítékok rögzítése)
- Az információvédelmi politika és a technikai megfelelés felülvizsgálata
- Rendszerauditok működése, védelme

MEH ITB 12. sz. ajánlás

- Biztonsági osztályokat határoz meg lehetséges kárérték alapján
 - Alap
 - Fokozott
 - Kiemelt
- Két konkrét kategória
 - Információ védelem: IV-A, IV-F, IV-K
 - Megbízható működés: MM-A, MM-F, MM-K
 - Mindegyik biztonsági osztályhoz részletes követelményrendszer tartozik (infrastruktúra, hardver, szoftver, adathordozók, dokumentáció, adatok, kommunikáció, személyek tekintetében)

- Kárértékek

- (közvetlen kár – Ft, helyreállítás – embernap, bizalomvesztés, negatív sajtókampány, társadalmi/politikai hatás, személyi sérülések száma, adatok bizalmassága/hitelessége sérül)
- "0": jelentéktelen kár
- "1": csekély kár
- "2": közepes kár
- "3": nagy kár
- "4": kiemelkedően nagy kár
- "4+": katasztrofális kár

- Besorolások kárérték szerint
 - Alap biztonsági osztály: max. „2”
 - Fokozott biztonsági osztály: max. „3”
 - Kiemelt biztonsági osztály: max. „4+” (4 és 4+)
- Besorolások a konkrét kategóriákra a kárértékekből következően

A besoroláshoz nem kell forintban megadott kárérték!
Egyszerűbb, ha rendszerekben ill. rendszertípusokban gondolkodunk és ez alapján definiáljuk az egyes osztályokat.

- **IV Alapbiztonsági (IV-A) osztály:**
Személyes adatok, üzleti titkok, pénzügyi adatok, illetve az intézmény belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.
- **IV Fokozott biztonsági (IV-F) osztály:**
A szolgálati titok, valamint a nem minősített adatok közül a különleges személyes adatok, nagy tömegű személyes adatok, banktitkok, közepes értékű üzleti titkok feldolgozására, tárolására is alkalmas rendszer biztonsági osztálya.

- IV Kiemelt biztonsági (**IV-K**) osztály:
Az államtitok, a katonai szolgálati titok, valamint a nem minősített adatok közül a nagy tömegű különleges személyes adatok és nagy értékű üzleti titkok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.

- Megbízható működés:

	Rendelke- zésre állás	Max. kiesési idő egy hónapban	Max. kiesési idő egy alkalomra
MM-A	95,5%	23,8 óra	-
MM-F	99,5%	2,6 óra	30 perc
MM-K	99,95%	16 perc	1 perc

COBIT (Control Objectives for Information and Related Technology)

- ISACA - COBIT
 - ISACA (Information Systems Audit and Control Association) – konferenciák, oktatás, CISA
 - Információ rendszerek átvilágítási/auditálási szempontjai – nemcsak biztonsági audit
 - Az IT szabványok, módszerek, élenjáró gyakorlatok egységes rendszerbe foglalt **módszertani eszköze**

- Alapelv: Az információtechnológiát az **üzleti célok** elérése érdekében alkalmazzuk, ennek során az IT erőforrások **IT folyamatokat** hajtanak végre, ezek eredményei hozzájárulnak az üzleti folyamatok eléréséhez. Közben **veszélyforrások** keletkeznek, ezek különböző kockázatokat jelentenek. **Kontrollok** alkalmazásával ezek elfogadható szintre csökkenthetők.
- Kontroll kialakítási irányelveket dolgoztak ki
 - Preventív
 - Detektív
 - Korrektív

- Négy főterület (az informatikai életciklus négy szakasza)
 - Tervezés és szervezet
 - Beszerzés és bevezetés
 - Informatikai szolgáltatás és támogatás
 - Felügyelet



- Informatikai szolgáltatás és támogatás
 - Szolgáltatási szintek meghatározása
 - Külső szolgáltatások kezelése
 - Teljesítmény és kapacitás kezelése
 - Folyamatos működés biztosítása
 - Rendszer biztonságának biztosítása
 - Költségek megállapítása és felosztása
 - Felhasználók képzése
 - Informatikai felhasználók segítése
 - Konfiguráció kezelése
 - Problémák és rendkívüli események kezelése
 - Adatok kezelése
 - Létesítmény kezelése
 - Üzemeltetés irányítása

ITIL (IT Infrastructure Library)

- De facto szabvány az IT szolgáltatás-irányítás területén
 - Az IT szolgáltatásirányításra vonatkozó, heterogén környezetben értelmezett, nyilvános, gyártófüggetlen keretrendszer
 - Konzisztens, integrált megközelítést és terminológiát nyújt
 - Szolgáltatásirányítási folyamatokat és eljárásokat definiál az IT szolgáltatás jó minőségű és költség-optimalis biztosítására és támogatására
 - Mindezekkel a szervezet üzleti folyamatainak eredményes működését teszi lehetővé

- Folyamatokat kezel, két fő folyamat-csoport létezik
 - Szolgáltatásbiztosítás (Service Delivery)
 - Szolgáltatásszint biztosítás (SLM)
 - Rendelkezésre állás biztosítás (AM)
 - Informatikaszolgáltatás-folytonosságbiztosítás (ITSCM)
 - Kapacitásbiztosítás (CM)
 - Informatikaszolgáltatás pénzügyi irányítása (FM)
 - Szolgáltatástámogatás (Service Support)
 - Ügyfélszolgálat (Szervezeti egység: Service Desk)
 - Incidenskezelés (Incident Management)
 - Problémakezelés (Problem Management)
 - Változáskezelés (Change Management)
 - Konfigurációkezelés (Configuration Management)
 - Kiadáskezelés (Release Management)

MABISZ AJÁNLÁS

- Védelmi intézkedés a biztosítás is (kockázathárítás)
- Kizárólag a fizikai biztonsággal foglalkozik
- A Biztosítók akkor kötnek biztosítást meghatározott értékekre, ha az általuk előírt védelmi intézkedések megtörténtek.
- Állami Biztosításfelügyelet jóváhagyásával: „Betöréseslopás, Rablás Biztosítási szabályzat” (elterjedt elnevezés: MABISZ Ajánlás)
- A magánszférában és az üzleti szférában egyaránt használják.

- Négyféle vagyoncsoport
 - 1.:Ékszer, értékpapír, kp. stb
 - 2.:Műérték, nemes szőrme, antik bútor stb.
 - 3.:Lakás és iroda-felszerelés
 - 4.:Telephelyek, komplett létesítmények, raktártelepek, kereskedelmi elosztóhelyek
- Hétféle védelmi osztály = színvonal (minden vagyoncsoportban)
 - Az egyes osztályokhoz meghatározták a maximális biztosítói kockázatviselés határértékét és a védelmi előírásokat

- Példa: 4. Vagyoncsoport követelményei
 - A osztály (legerősebb)
 - A védett terület jól körülhatárolt, a kerítés nehezen küzdhető le
 - Biztosított a folyamatos megfigyelés
 - Egymástól látó és hallótávolságra elhelyezett őrk
 - Épületen kívül kutyás járőrök, az őrk között folyamatos információcsere
 - Speciális mechanikai-fizikai védelemmel ellátott nyílászárók, biztonsági zárok
 - Kritikus pontokon (pl. páncélszekrények) jelzőrendszer
 - Közvetlen összeköttetés a rendőrséggel vagy más fegyveres szolgálattal

- Probléma: Csak az információt tartalmazó értékrendszerre vonatkozik magára az információra nem.
- Az információ értékének meghatározása nem egyszerű, általában az újraelőállítás költségét veszik alapul.
- Ezen az alapon még biztosítás is köthető:
Adatvesztési biztosítás
 - Mentésre olyan feltételek, hogy betartása esetén az adatvesztés valószínűsége igen kicsi

Az IT rendszerek fenyegetettsége

- Fogalmak, kiinduló gondolatok
- Veszélyforrások
 - Fizikai veszélyforrások
 - Logikai veszélyforrások
 - Szervezet és működési kérdésekhez kapcsolódó veszélyforrások
 - Életciklushoz kapcsolódó veszélyforrások
 - Az IT rendszer elemeihez kapcsolódó veszélyforrások

Fogalmak, kiinduló gondolatok

- Az IT rendszer folyamatos, és rendeltetésszerű működése, a kedvező állapot fenntartása üzleti érdek
- A biztonság sérülhet, az erőforrásokat támadás fenyegeti
- Támadás:
 - Egy veszélyforrásból kiinduló, az erőforrások **bizalmassága, sértetlensége** ill. **rendelkezésre állása** ellen irányuló folyamat
- Veszélyforrás:
 - Bekövetkezésekor az IT rendszerben nem kívánt állapot jön létre, az IT rendszer biztonsága sérül.

- Sebezhetőség – érzékenység (Hol lehetséges támadás, melyek a leginkább jellemző gyenge pontok?)
 - Az **eszközök** elpusztítás (rendelkezésre állás) és módosítás (sértetlenség), ill. egyes eszközök (rejtjelező eszköz) felfedés (bizalmasság) érzékenyek
 - A **hálózati kapcsolatok** behatolás ill. felfedés (bizalmasság) érzékenyek
 - A **platformok, rendszer szoftverek** megkerülés (bizalmasság) érzékenyek
 - Az **adatok, alkalmazások** felfedés (bizalmasság) ill. módosítás (sértetlenség) érzékenyek
 - Az **emberek** felfedés (bizalmasság) érzékenyek

- Fenyegetés: egy személy, dolog, esemény, ötlet, amely a támadás lehetőségét képezi az erőforrás(ok)ra. Jellemzői:
 - A veszélyforrás, amely pl. szervezési vagy technikai
 - A támadás módja, amely aktív vagy passzív
 - A támadás célja – irányulhat a bizalmasság sértetlenség, rendelkezésre állás ellen
 - A kárkövetkezmény, amely vonatkozhat egy vagy több erőforrásra
- Fenyegetettség: Olyan állapot, amelyben az erőforrások bizalmassága, sértetlensége, rendelkezésre állása sérülhet.

- Veszélyérzet – a veszélyérzet hiánya
 - A fenyegetettség fel nem ismerése
 - A menedzserek költségtakarékossági igénye
 - A védelem folyamatos korszerűsítésének elmaradása
 - Nem publikált biztonsági események
 - A védelmi intézkedések nem megfelelő betartása
 - A biztonsági tudatosság hiánya



- A veszélyforrások a biztonsági környezetben értelmezettek
 - Jogszabályok, belső szabályok, elvárások, szokások, szakértelem, tudás által alkotott környezet
- Lehetséges veszélyforrások:
 - Fizikai veszélyforrások
 - Logikai veszélyforrások
 - Szervezeti és működési kérdésekhez kapcsolódó veszélyforrások
 - Életciklushoz kapcsolódó veszélyforrások
 - Az IT rendszer elemeihez kapcsolódó veszélyforrások
- Veszélyforrások okozta kárkövetkezmények
 - Átfogó
 - Részleges

Fizikai veszélyforrások

- A földrajzi környezetből származó természeti veszélyforrások
 - Földrengés, földcsuszamlás, árvíz, vízbetörés, szélvihar, szélsőséges időjárás, villámcsapás (nemcsak tűz, hanem áramkörök meghibásodása is!) tűzhányó kitörés stb.
 - Valószínűségük többnyire becsülhető
 - A károkozás többnyire igen nagy, saját eszközeinkkel nem tudunk védekezni ellenük.



Fizikai veszélyforrások

- A földrajzi környezetből származó technikai veszélyforrások
 - Hatásuk a természeti veszélyforrásokhoz hasonló, saját eszközeinkkel nem tudunk védekezni ellenük
 - A szomszédos szervezetnél robbanás, tűz, veszélyes gázképződés
 - Közlekedési katasztrófa
 - Kommunális ellátással kapcsolatos katasztrófa (gázömlés, nagyfesz.vezeték szakadás, víznyomócső törés)
 - Informatikai, távközlési, erősáramú becsatlakozás kiesése

Fizikai veszélyforrások

- Jogosulatlan hozzáférés
 - Aktív hozzáférés
 - Illetéktelen belépés, mozgás az objektumon belül
 - Nem megfelelő beléptető rendszer ill. a beléptető rendszer megkerülése, kijátszása
 - Elrejtőzés az objektumban várva az inaktív időszakot
 - Erőszakos behatolás - betörés
 - Többnyire materiális érték eltulajdonításáért, általában éjjel
 - Munkahely őrizetlenül hagyása
 - Irodák nyitva hagyása, aktív számítógépek magára hagyása stb.
 - Hordozható gépek nem kerülnek elzárásra

Fizikai veszélyforrások

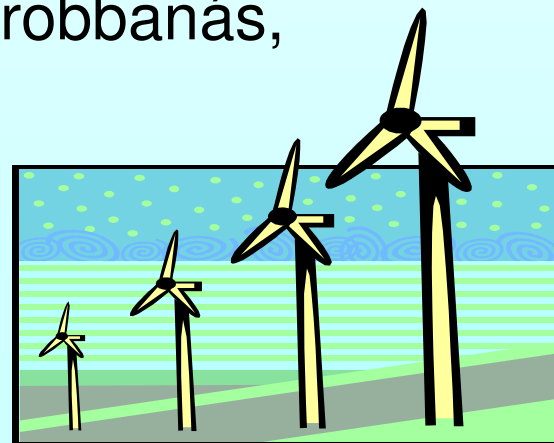
- Passzív hozzáférés
 - Akusztikus hozzáférés
 - Telefonba épített lehallgató, mikrofonpuska, lézerpuska stb.
 - Elektromágneses hozzáférés
 - Lehallgatás (képernyő, keyboard, soros port stb.)
 - Wifi lehallgatása
 - Zavarás – sugárzott és vezetett zavaró jelek
 - » Nagyfeszültségű rendszerek, nagyfeszültségű energiahálózat
 - » Rádiófrekvenciás jelek

Fizikai veszélyforrások

- A fizikai rendelkezésre állás megszakadása
 - Nem megbízható eszközök
 - Az eszközök rendelkezésre állása 95,5-99,5%
 - Nem megfelelő légállapot
 - Klíma: hő és páratartalom
 - Duplikálás, áramszünet utáni újraindulás, tűz esetén kikapcsolás
 - Tűz
 - Leggyakoribb és legveszélyesebb
 - Villám, hibás szigetelés, rossz kontaktus, zárlat, dohányzás, nyílt láng, gyúlékony anyagok tárolása, robbanás, szándékosság, terrorizmus, bomba-merénylet
 - Nem megfelelő tűzmegeelőzés és oltás

Fizikai veszélyforrások

- Természeti és ipari katasztrófa
 - Nagy hatású természeti csapások, emberek elvesztése
 - Bombariadó: a tevékenység hosszú időre kiesik
 - A munkahely megközelíthetetlensége (pl.: hóesés, tömegbaleset)
 - Munkavégzés kiesése (pl.: ételmérgezés, járvány)
 - Földrengés, árvíz, villámcsapás, robbanás, vegyi/nukleáris szennyezés



Fizikai veszélyforrások

- Az energiaellátás és távközlés zavarai
 - Szolgáltatások külső gazdasági szervezetektől (elektromos energia, telefon, adatátvitel, víz, szennyvíz, szemétszállítás, gázszolgáltatás, hőszolgáltatás)
- Hiányos, hibás, nem létező dokumentáció
 - Hiányos változáskövetés
 - Nem megfelelő dokumentáltság

Logikai veszélyforrások

- Jogosulatlan logikai hozzáférés
 - Belépés ellenőrzés
 - Gyenge jelszó használati szabályrendszer
 - A felhasználók hozzáférési jogosultságai nem megfelelően szabályozottak
 - Nem megfelelő naplózás
 - Kriptográfiai támadások
 - Gyenge pont: a kulcs
 - Az elterjedt algoritmusok garantálják a visszafejthetetlenséget
 - Passzív: lehallgatás
 - Aktív: lehallgatás + megváltoztatva továbbítás

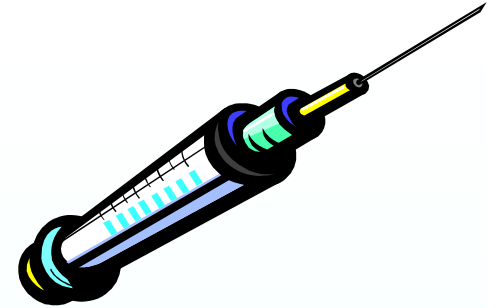
Logikai veszélyforrások

- A logikai rendelkezésre állás megszakadása
(A folyamatos működés megszakadása)
 - Alternatív helyszínek hiánya
 - A mentések hiánya, hibás, hiányzó ill. nem megfelelő mentési eljárások
 - Az erőforrások kisajátíthatók, használatuk nincs korlátozva
 - Nem elégséges a rendelkezésre álló kapacitás
- Rosszindulatú szoftverek – programozott kártevők – (vírusok)
 - Vírusok
 - Más programokhoz hozzáépül, önmagát reprodukálja
 - Trójai faló – trójai program
 - Ismert programnak álcázott (rosszindulatú) szoftver
 - Önmagát nem reprodukálja

Logikai veszélyforrások

- Programférgek
 - Önálló, önmagukban is futásképes programok
 - Túlterhelést okoz, lebénítja a gépet ill. a hálózatot
 - Tipikusan levélmellékletként terjed
- Logikai bomba
 - Bizonyos feltételek bekövetkezésekor elinduló programok
 - Többnyire a szoftverfejlesztők terjesztik
- Hátsó ajtó – csapóajtó – kiskapu – csapda
 - Szoftverfejlesztéskor segédeszköz – gyorsabb belépés, nyomkövetés
- Baktériumok – nyulak
 - Önmagukról készítenek másolatot
 - Erőforrások lekötése

Logikai veszélyforrások



- Phishing (adathalászat)
 - a felhasználó olyan emailt kap, amely úgy néz ki, mintha egy legálisan működő intézménytől - leggyakrabban internetes áruházról, banktól, aukciós oldaltól - érkezett volna. A felhasználót ezzel csalják az eredetihez hasonlító, de hamis internetes oldalra, ahol aztán valamilyen indokkal személyes adatai, például bankkártyaszáma, pin-kódja vagy jelszavai megadására kérik fel.
- Betárcsázó programok
 - A magánszférában jellemzőek
- Vírusvédelmi hiányosságok
 - Vírusvédelmi szabályok hiánya – nem megfelelő gyakorlat
 - A folyamatos frissítések hiányoznak

Logikai veszélyforrások

- Integrált információ rendszer hiánya – szigetek – sziget megoldások
 - Nem biztosítható az egyenszilárdság elve
- Logikai rombolás
 - Elektromágneses támadás (vezetékes, sugárzásos)
- Nem megfelelő, hiányos szoftver dokumentáció
 - Hibás, használhatatlan dokumentáció
 - Nem megfelelő követés

Logikai veszélyforrások

– Hálózati veszélyforrások

- Illetéktelen rácsatlakozás, hozzáférések, forgalmi analízis
- Jogosulatlan módosítások – program, adat
- Rombolás – vírusok, törlés...
- A működés megakadályozása, korlátozása - attack
- Betárcsázás – modemcsatlakozás
- Internet csatlakozás

Szervezeti és működési kérdésekhez kapcsolódó veszélyforrások

- A biztonsági szervezet hiánya, gyengeségei
 - Általánosan jellemző
 - Nincs integrált biztonsági szervezet
 - A vagyon és adatbiztonság egymástól függetlenül működik ill. a funkciók összekeverednek
 - Az adatvédelem és adatbiztonság szétválasztásának hiánya
 - Biztonsági ellenőrzések hiánya
 - Biztonsági szervezetek (tűzvédelmi, polgári védelmi hiánya, gyengesége
 - Biztonsággal kapcsolatos dokumentumok hiánya: Biztonsági Stratégia, Biztonsági Politika, Biztonsági átvilágítás, Katasztrófaterv, IBSZ

Szervezeti és működési kérdésekhez kapcsolódó veszélyforrások

- Szabályozások hiányosságai
- Szabályok be nem tartása
- A munkakörök és szakmai kompetencia nem teljesen függ össze
- A munkaköri leírás és a tényleges tevékenység nem egyezik meg
- Seggregation of duties
- Nem megfelelő oktatás



Szervezeti és működési kérdésekhez kapcsolódó veszélyforrások

- Titokvédelmi hiányosságok, gyengeségek
 - Nincsenek osztályozva titokvédelmi szempontból az **adatok, alkalmazások, eszközök, helyiségek** (Ha nincs meghatározva, hogy **MIT** kell védeni, nem lehet megmondani, hogy **HOGYAN**)
 - A titokvédelmi munkatárs elhelyezkedése a szervezeti hierarchiában nem megfelelő (nem az elsőszámú vezető közvetlen alárendeltje)
- Iratkezelési hiányosságok
 - Nincs szabályozva az elektronikus íratok **kezelése, előállítása, megsemmisítése, archiválása** (szemben a hagyományos papír alapú íratok kezelésével)
 - Nincs megfelelő jogi szabályozás – jelenleg



Szervezeti és működési kérdésekhez kapcsolódó veszélyforrások

- Harmadik féllel kötött szerződések gyengeségei
 - A szerződések nem tartalmazznak biztonsági garanciákat (fejlesztők, szállítók, karbantartók, üzemeltetők...)
 - Outsourcing, SLA kockázatok
 - A megbízó hatáskörén kívül eső biztonsági környezet
 - A biztonsági követelmények érvényesítése, a számon kérhetőség biztosíthatósága
 - A cég területén „idegen szakemberek”, hozzáférnek a rendszerhez. A biztonsági szabályzatok betartatása problematikus.
 - Korlátozott felelősségvállalás – az üzleti tevékenység megszakadására vonatkozóan a harmadik fél nem vállal garanciát -- vis maior

Szervezeti és működési kérdésekhez kapcsolódó veszélyforrások

- A humán erőforrásokat fenyegető veszélyforrások
 - A humán erőforrások bizalmassága (személyes adatok, feladatkörök stb.), sértetlensége (sérülés), rendelkezésre állása (sérülés, betegség, haláleset, túsztevényt, aztrájk stb.) sérülhet



Szervezeti és működési kérdésekhez kapcsolódó veszélyforrások

- IDG felmérés 2004:

Követhetetlen felhasználók - A dolgozók csaknem fele (46 százalék) ismeri el, hogy mások is hozzáférnek a laptopjukhoz mikor a munkahelyen kívül tartózkodnak, minden ötödiknek (22 százalék) pedig fogalma sincs arról, hogy tulajdonképpen ki és mire használja noteszgépét.

Veszélyes letöltések - Az alkalmazottak 86 százaléka ismerte el, hogy a munkahelyen kívül a munkához nem kapcsolódó szoftvereket is le szokott tölteni a céges laptopra.

Törvénsértés - Csupán tízből egy alkalmazott törődik azzal, hogy cégét megbüntethetik a szerzői jogok megsértéséért az illegális zene- vagy filmletöltések miatt - míg 15 százalék tart attól, hogy őt magát vonják felelősségre.

Kapcsolt letöltések - 74 százalék ismeri el, hogy nem mindig olvassa el a letöltésre vonatkozó feltételeket és szabályokat, nem csoda hát, hogy a felhasználók 15 százaléka fedezett fel PC-jén olyan szoftvereket, amelyeket nem is akart letölteni.

A felelősség terhe? - Meglepő módon, annak ellenére, hogy a felhasználók 42 százaléka elismeri a fájlcserélő hálózatok használatát, a felnőtteknek szóló illetve a hacker oldalak látogatását, 35 százalékuk úgy érzi, hogy a vállalat számítástechnikai osztálya felelős a laptop állapotáért, noha azt a dolgozó otthon is használja.

Szervezeti és működési kérdésekhez kapcsolódó veszélyforrások



- A humán erőforrások képezte veszélyforrások
 - Nem megbízható, nem lojális munkaerő alkalmazása (erkölcsi bizonyítvány?, előző munkahely?, életvitel, pénzügyi zavar stb.)
 - Nem megfelelően képzett, nem elegendő gyakorlattal rendelkező munkatárs alkalmazása
 - Távozó dolgozók hozzáférései megmaradnak (belépő kártya, account, kulcs), a munkatársak nem kapnak értesítést a távozás tényéről.
 - A biztonsági tudatosság hiánya

Veszélyforrások az IT rendszer életciklusában

- Fejlesztés/beszerzés
 - A fejlesztési cél nem tartalmaz biztonsági követelményeket
 - Nincs elkülönült fejlesztő rendszer (személyzet is!)
 - A szállító nem ad megfelelő biztonsági garanciákat
 - Elterjedt, szabványos szoftverek beszerzése
- Átadás/átvétel
 - A biztonsági követelményrendszer ellenőrzése hiányzik
 - Speciális hozzáférések (programozók spec. jogosultságai), hátsó ajtók megmaradnak

Veszélyforrások az IT rendszer életciklusában

- Üzemeltetés
 - A biztonságkritikus munkakörök nincsenek szétválasztva
 - Fejlesztések folynak az éles rendszeren
 - A biztonsági események feltárása, értékelése nem történik meg
 - Outsourcing igénybevétele
 - Szabályozások hiányoznak
- Selejtezés
 - Nincs jól szabályozott selejtezési rend (hardver
 - szoftver - dokumentáció)

Az IT rendszerek védelme

„NEM VÁLLALOK KÖZÖSSÉGET
AZZAL A KÖNNYELMŰ REMÉNNYEL,
HOGY VALAMI VÉLETLEN MAJD MEGMENT
BENNÜNKET.”

(CLAUSEWITZ)

- Védelmi módszerek
- Technikai védelmi módszerek
 - Fizikai hozzáférés-védelem
 - Fizikai rendelkezésre állás
 - Logikai hozzáférés védelem
 - Logikai rendelkezésre állás
 - Hálózatok védelme
 - Védelem az IT rendszer életciklusa során
- Szervezet és működésszabályozás
- A védelem erőssége

A védelmi módszerek a biztonsági környezetben

- A bekövetkezési valószínűség csökkentése
 - A nemkívánatos események, a támadás valószínűsége csökken
 - A sikeres támadás esélye csökken
- A károkövetkezmények csökkentése
 - Maradó kockázat
 - Katasztrófa terv
 - Biztosítás

Technikai védelmi módszerek

- Fizikai hozzáférés-védelem
- Fizikai rendelkezésre állás
- Logikai hozzáférés védelem
- Logikai rendelkezésre állás
- Hálózatok védelme
- Védelem az IT rendszer életciklusa során

Fizikai hozzáférés védelem

- Objektum védelem
 - Objektum helyének megválasztása
 - Épület automatika, épület informatikai rendszer
 - Integrált biztonság felügyelet rendszer
 - Belépés és mozgás ellenőrzés, tűzvédelmi, gázvédelmi, stb. rendszer
 - Komplex vagyonvédelem
 - Mechanikai, élőerős, elektronikus jelzőrendszerek
- Belépés és mozgás ellenőrzés
 - Élőerő
 - Beléptető rendszer
 - Zártláncú TV
 - Őrjárat ellenőrző rendszer

- Behatolás védelem
 - Mechanikai védelem
 - Elektronikus jelzőrendszer
 - Élőerő
- Kisugárzás elleni védelem
 - Akusztikus lehallgatás védelem
 - Elektromágneses kisugárzás védelem
- Üres íróasztal politika
- Irat/hulladékmegsemmisítés

Fizikai rendelkezésre állás

- Eszköz redundancia
 - Jó minőségű eszközök és/vagy tartalék
- Klimatizálás
 - 500-700W/m² elszállítás
 - Páratartalom: 40-60%
 - Ha emberek is: 21-23 C
 - Duplikálás, automatikus újraindulás
- Szünetmentes áramellátás
 - Több irányú betáplálás egymástól fizikailag távol
 - Aggregátor
 - UPS

- Tűzvédelem

- Országos szervezet
- Gazdálkodó szervezetek és intézmények feladata
- Sok jogszabály foglalkozik vele
- Védekezés
 - Megelőző tűzvédelem: szabályok, szakhatósági tevékenység
 - Mentő tűzvédelem: Tűzoltási, kárelhárítási tevékenység
 - Felderítő tűzvédelem: Utólagos tűzvizsgálat

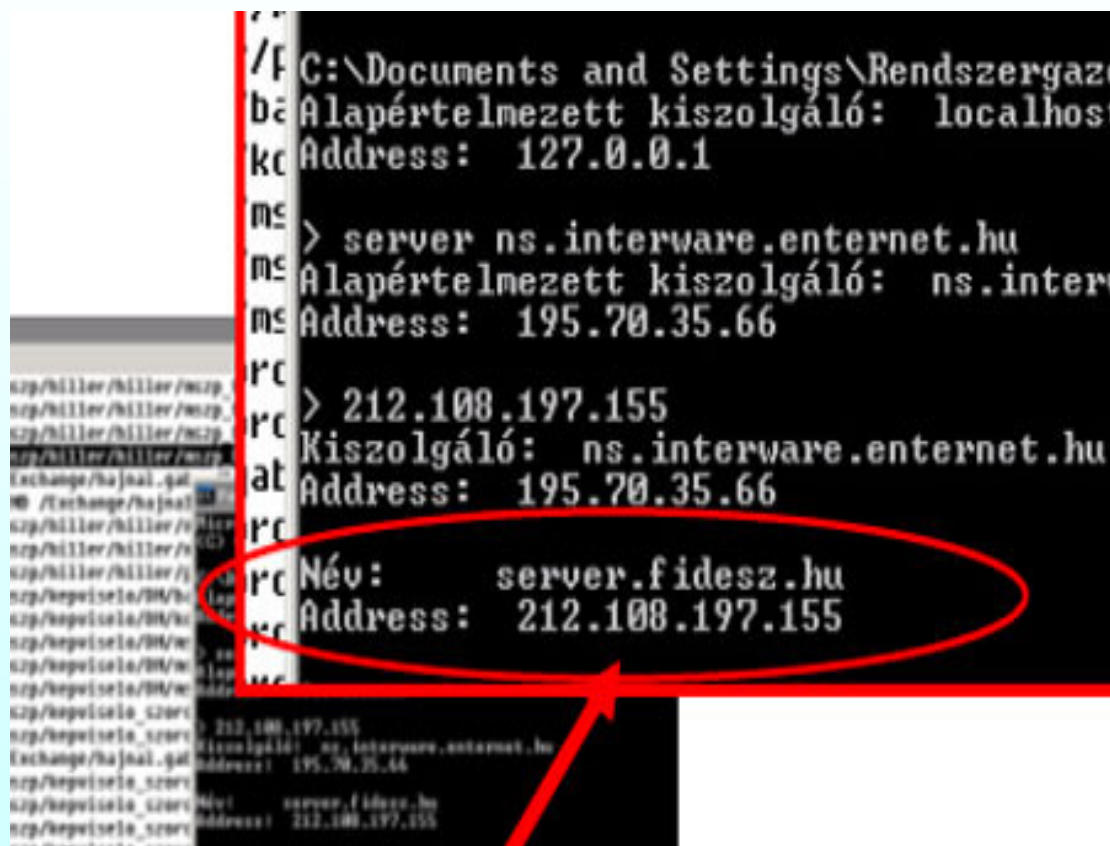
- Létesítmények: tűzveszélyességi osztályokba soroltak
 - A, B, C, D, E
- Tűzveszélyességi osztályonként előírások
 - Milyen rendszer, milyen védekezés, milyen ellenőrzés szükséges
- Tűzvédemi Utasítás, Tűzriadó Terv szükséges
- Polgári védelem
 - Törvény: Fegyveres konfliktus, természeti katasztrófa stb. esetén történő védekezés
 - Minden időben rendelkezésre áll

Logikai hozzáférés védelem

- Jelszavas hozzáférés védelem
 - A belépni szándékozónak meg kell győznie a rendszert, hogy ő azonos azzal, akinek mondja magát
 - Név+jelszó (többször használatos jelszó – **mit tudsz**, egyszer használatos jelszó – **mi van a birtokodban**, biometria jelszó – **ki vagy**) = account
 - Az account és az objektumok között relációk = hozzáférési jogosultságok ill. jogok léteznek.
 - (olvasás, írás, végrehajtás, törlés stb.)
 - Többszintű hozzáférés védelem: pl. az alkalmazás eléréséhez újabb azonosítás szükséges.
 - Jelszó használati szabályok: írott/íratlan
 - Probléma: egy felhasználónak túl sok jelszót kell ismernie, ezért rögzíti őket.

Logikai hozzáférés védelem

A Fidesz internet szerkesztősége beismerte, hogy "nyilvános fórumokon" szerzett felhasználónévvel (mszp) és jelszóval (pirosvirág) "meglátogatta" az oldalt. Az MSZP anyagainak elkészítésével megbízott Relatív Kft. - a párt kampánykiadványait tároló - ftp-szerverére a letöltési naplóban rögzített adatok szerint a server.fidesz.hu gépről léptek be, és onnan töltötték le a gyártás-előkészítésre elhelyezett anyagokat. (www.index.hu 2006.02.14.)



```
C:\Documents and Settings\Rendszergaz...> ipconfig /all
Álapértelmezett kiszolgáló: localhost
Kiszolgáló Address: 127.0.0.1

ms> server ns.interware.enternet.hu
ms> Álapértelmezett kiszolgáló: ns.interware.enternet.hu
ms> Address: 195.70.35.66

rc> 212.108.197.155
rc> Kiszolgáló: ns.interware.enternet.hu
rc> Address: 195.70.35.66

rc> Név: server.fidesz.hu
rc> Address: 212.108.197.155
```


- Rejtjelezés, kriptográfia
 - Az adatokat titkosítva tároljuk vagy továbbítjuk
 - Primitív titkosítás: egyszerű karakterhelyettesítés
 - One time pad: a kulcs azonos hosszúságú véletlen sorozat – nem megfejthető, de használhatatlan.
 - Kategóriái:
 - Szimmetrikus rejtjelezés
 - Aszimmetrikus rejtjelezés
 - Digitális aláírás
 - PKI

Szimmetrikus rejtjelezés

- Titkos kulcs
 - Bonyolult matematika, a kulcs titkos, a kulcs ismeretében mind a kódolás, mind a visszafejtés viszonylag egyszerű, kulcs hiányában a visszafejtés nagyon nehéz. (a kódolási algoritmus publikus: bitek felcserélése és bitminták más bitmintákkal való helyettesítése.) – LUCIFER, DES, Triple DES, DESX, GDES, RDES, IDEA.
 - Probléma : a kulcs, ill. az abszolút biztonságos csatornán történő továbbítása.

Aszimmetrikus kriptográfia

- Nyilvános kulcsok
 - Minden résztvevő két kulccsal rendelkezik, egy publikus (nyilvános) és egy privát (titkos) kulccsal, a két kulcs között bonyolult matematikai összefüggés van.
 - Minden résztvevő ismeri minden résztvevő publikus kulcsát.
 - A privát kulcsát minden résztvevő titokban tartja és senkinek nem küldi el.
 - Egy egy résztvevő publikus és privát kulcsa között összefüggés van: a publikus kulccsal kódolt üzenet a privát kulccsal fejthető vissza. A publikus kulcs ismeretében sem a privát kulcs, sem a kódolt üzenetből a kódolatlan nem állítható vissza gyakorlatilag.

- RSA, RC1-9,PGP
- Hosszabb kulccsal nő a biztonság.
- Hosszú üzenetek továbbítása problematikus (lassú algoritmusok).
- A szimmetrikus kulcsok továbbításához viszont praktikusán használható eljárás.

Digitális aláírás

- Igazolja, hogy az üzenet a feladótól és nem mástól származik, ill., hogy az üzenetet nem változtatták meg illetéktelenül.
- Fő összetevője a hash – kivonat – digitális újlenyomat, egy bitsorozat, amelyet ismert algoritmussal az üzenetből készítünk.
- A feladó és a címzett ugyanazt a hash algoritmust használja
- A hash-t rejtjelezzük és továbbítjuk
- A hash-t a címzett is előállítja és összeveti a kapottal

PKI (Public Key Infrastructure)

- A gyakorlatban használt hitelesítő, tanúsító rendszer
- Szimmetrikus, aszimmetrikus titkosítás, digitális aláírás, kulcsgondozás (a kulcs valóban azé, akit mondanak, kulcskiosztás stb.)
- Használatához regisztráció szükséges

- **Tűzfal, VPN, DMZ**

- Gépek és szoftverek együtt
- A hálózat kapcsolódik más, olyan hálózatokhoz, amelyekre nem érvényesíthető a biztonságpolitika.
- A csatlakozási pontokon ellenőrizzük, naplózzuk a forgalmat: tűzfal (firewall).
- Forgalomszűrő tűzfal (network ill. transzport layer szint):
 - Packet Filter: csomagokat továbbít vagy eldob
 - Vizsgálat csomagonként: feladó ill. címzett címe, be/ki stb.
- Alkalmazás szintű tűzfal (alkalmazási réteg)
 - Proxy szerver: minden engedélyezett protokollhoz tartozik egy proxy
 - Nem szűr, hanem közvetít, kívülről nem látható a hálózat
- DMZ (Demilitarized Zone)
- VPN (Virtual private Network)

Logikai rendelkezésre állás

- A folyamatos működés biztosítása
 - Mentések, visszaállítások
 - Hibatűrő rendszerek
 - Védekezés a rosszindulatú szoftverek ellen
- Védekezés logikai rombolás ellen

Mentések, visszaállítások

- Jól definiált mentési eljárás
 - Mit?
 - Milyen gyakran?
 - Inkrementális/teljes mentés?
 - Mikor?
 - Mire?
 - Hány példányban?
 - Mennyi ideig?

Hibatűrő rendszerek – spec. háttér típusok

- A rendelkezésre állás nő, a bizalmasság, sértetlenség fenyegetettsége esetleg fokozódik
- Csoportosítás:
 - Hideg
 - Meleg
 - Forró
 - Katasztrófa tűrő
- Üres helyiség + infrastruktúra
- Nem minden rendszer
- Minden rendszer
- Minden rendszer (seb. ablak=0)
- Más csoportosítás
 - Lokális (ugyanazon épület, környezet, 500m is lokális)
 - Távoli (több km)

-További csoportosítás

– Adat redundáns rendszerek

- RAID (1-10, 53) – (tükrözés, duplikálás stb.)

– Rendszer redundáns rendszerek

- Passzív redundáns rendszerek

- A rendszer nem vesz részt az eredeti feladat végrehajtásában
- Off line (külön oda kell vinni az adatbázist – mennyi idő?)
- Visszaállítás bázisú (pl. ¼ óránként automatikusan átkerül oda az adatbázis – kimaradhat ¼ óra)
- Hátrányok: Az installálás, konfigurálás nehézkes, adat és teljesítményvesztés, működés megszakadás lehetséges.
Reaktív megközelítés

- Aktív redundáns rendszerek
 - Az eredetivel azonos műveletet hajt végre egyidejűleg
 - Automatikus ellenőrzések, hiba esetén automatikus átkapcsolás (elterjedt: cluster technika – distant cluster)
 - Nincs szükség újraindításra, adatbázis visszaállításra
 - Hibatűrés – hibatűrő rendszerek
 - Folyamatos rendelkezésre állást biztosítanak

Védekezés a rosszindulatú szoftverek ellen

- Vírusdetektálás

- A vírus detektálható a rendszerbe való bekerülés előtt, a működés megkezdése előtt és működés közben.
- Antivírus programok (SymantecNAV, McAfee, F-PROT, stb):
 - Fertőzés megelőző (rezidens program a memóriában)
 - Fertőzés feltáró/azonosító (jelzi a fertőzés tényét esetleg eltávolítja a vírust)

- Az antivírus szoftverek fajtái
 - Szekvenciakereső rendszerek (adott vírusra jellemző „szignatúrákat” keresünk)
 - Változásdetektorok (rendellenes változások keresése)
 - Ellenőrző összegek számítása és követése
 - Heurisztikus rendszerek (vírusokra jellemző műveletek keresése és minősítése – milyen sok van? – ismeretlen vírust is detektál, de csak véges valószínűséggel)
 - Memóriarezidens ellenőrző programok (illegális memóriakezelés, diszk művelet van-e)
 - Viselkedésblokkolók (vírusra jellemző akciók blokkoltak – pl. magának a levelező kliensnek attachementként történő elküldése vagy, hogy a levelező kliens igen sok példányban fut egy gépen)
 - Immunizáló programok
 - Egyedi killerek

- Hardveres védelem
 - Vírusvédelmi kártyák - régi
 - Állandó vírusfigyelés, gyanú esetén figyelmeztető üzenet
- Vírusfertőzésre utaló jelek
 - Program méretváltozások
 - Lassúbb betöltődés
 - Dátumváltozások
 - Kapacitások csökkenése (memória, diszk)
 - Szokatlan hibaüzenetek
 - Ismeretlen file-ok megjelenése – pl. szokatlan kiterjesztések
 - Indokolatlan billentyűleütési zaj
 - Folyamatos diszk aktivitás/elérhetetlenség
 - Szokatlan képek a képernyőn

- Védelmi intézkedések

- Megelőző intézkedések

- Beszerzés: eredeti, jogtiszta szoftver biztos forrásból
 - Floppy drive nélküli rendszerek – pen drive?
 - Írásvédett lemezek használata
 - Tesztrendszer kialakítás
 - A biztonsági tudatosság fokozása - spam!
 - Ellenőrzés a határfelületeknél
 - A védelem kiterjesztése az egész rendszerre
 - Ellenőrzés minden adathordozóról történő adatbevitel esetén
 - Fertőzést megelőző szoftver alkalmazás
 - Adathordozóról történő adatbevitel korlátozása
 - Számonkérhetőségek biztosítása
 - Naplózások, a napló kiértékelése, intézkedések

- Feltárás, vírus eltávolítás
 - Antivírus szoftver alkalmazása
- Elszigetelés
 - A fertőzés kiterjedésének meghatározása
 - A fertőzött állományok elkülönítése
- Visszaállítás
 - Mentés, biztonsági másolat készítése
 - Törlések
 - Visszaállítás mentésből

Védekezés logikai rombolás ellen

- A vezetett jelek és tápellátások szűrése
- Elektromágneses árnyékolás
- Védekezés sztatikus feltöltődés ellen
- Megfelelő földelési hálózatok kialakítása
- Villámvédelem

Hálózatok védelme

- ISO – OSI 7498-2 (X800)
- (Triviális módszer: izolált működtetés)
- Tűzfalak, határfelületi védelmek alkalmazása
- Titkosított adattovábbítás: kriptográfia
- Nem titkosított jelszótovábbítást használó alkalmazások kizárása (telnet, ftp) – megoldás: ssh
- Szükségtelen hálózati szolgáltatások inaktiválása
- Szükségtelen szállítási protokollok inaktiválása (pl. IPX/SPX)
- Rendszeres ellenőrzések, diagnosztikai programok

- Op. rendszer és alkalmazások security hole-jainak kezelése
- Levelezési szabályok (filtering rules), tartalomszűrés
- Penetration teszt, Intruder Detection System (IDS)
- Hordozható gépek: irodán kívüli használat: hálózati adatok leolvashatók, vírus jöhet be
- Illegális szoftvertelepítések megakadályozása
- Felhasználói oktatások
- Naplózások

– Fizikai hozzáférés védelem

- Vezetékek csőben, zárt elosztók
- Szerverek, hálózati aktív eszközök, rendezők: zárt, kizárólag erre a célra szolgáló helyiségben
- Nem használt csatlakozók inaktiválása

– Redundanciák, hibatűrő hálózat

– Modemes kapcsolat

- Titkos, a vállalati számmezőben nem szereplő szám a hívószám
- A hívószám ellenőrzése
- Visszahívás megadott számra
- Titkosított jelszó átvitel: PAP, SAP; egyszer használatos jelszó
- Betárcsázási lehetőség csak meghatározott időszakban
- Inaktív időszakban a modem leválasztása
- Naplózások

Védelem az információ rendszer életciklusa során

- Fejlesztés/beszerzés
 - Védelmi intézkedések szükségesek mind a fejlesztés tárgyát képező rendszerben, mind a fejlesztési környezetben
 - Az intézkedések egyaránt szükségesek kész eszköz vásárlása és fejlesztési megbízás esetén
 - A biztonsági követelményeket szerződésben kell rögzíteni.
 - A fejlesztési célnak tartalmaznia kell a beépítendő védelmi intézkedéseket
 - A fejlesztés alatt meg kell tervezni az átadás/átvétel menetét és a konkrét implementációt

- A fejlesztési környezetet az éles rendszertől minden szempontból (humán, fizikai, logikai) le kell választani
- A fejlesztési környezetben a biztonsági követelményeket érvényesíteni kell
- A fejlesztésnek minőségbiztosítás mellett kell folynia
- A fejlesztést korszerű fejlesztési módszertan alapján kell véghezvinni
- **Átadás/átvétel**
 - Bizonyítani szükséges, hogy a fejlesztési folyamatra és környezetre teljesültek a biztonsági követelmények

- Szállítói nyilatkozatok
 - Fenyegetés mentességi nyilatkozat (az eszköz nem tartalmaz olyan elemet, amely fenyegeti a megbízó biztonságát)
 - Jogtisztasági nyilatkozat
- A szállítás biztonsági ellenőrzése szükséges
- A forráskód tárolásáról történő megegyezés (pl. közjegyző)
- A beépített védelmi intézkedések ellenőrzése
- Az előírt formai és tartalmi követelményeknek megfelelő dokumentációk átvétele
- A fejlesztők speciális jogosultságainak visszavonása
- A fejlesztés és üzemeltetés el kell, hogy különüljön!!

• Üzemeltetés

- Szabályozott change management (jóváhagyás, végrehajtás menete, szerepek, dokumentálás, a felhasználók értesítése, oktatása, naplózás)
- A hardver karbantartások, konfiguráció módosítások, szoftver követések szabályozottak és nem sérthetik a biztonsági követelményeket
- A hardver karbantartások, konfiguráció módosítások, szoftver követések végrehajtói korlátozott hozzáférési jogosultságokkal rendelkezhetnek
- Távoli üzemeltetési célú hozzáférések csak szigorú hozzáférés ellenőrzés és naplózás mellett engedhetők meg.
- A biztonsági eseményeket naplózni, a naplót értékelni kell. A biztonsági események újbóli előfordulását megakadályozó ellenintézkedések megtétele szükséges

- Selejtezés

- Szabályozott selejtezési eljárások (jóváhagyás, végrehajtás menete, szerepek, dokumentálás, naplózás)
- Adathordozók megsemmisítése:
 - Égetés
 - Zúzás
- A megsemmisítés tételes ellenőrzése szükséges

Szervezet és működésszabályozás

- A biztonsági szervezet és működés
 - A biztonságért a szervezet első számú vezetője felelős
 - Az informatikai biztonság és a vagyonbiztonság nem elkülönült egység
 - Az informatikai biztonság nem az informatikai szervezet alegysége
 - A biztonsági vezető és az adatvédelmi (titokvédelmi) felügyelő az első számú vezető közvetlen alárendeltje
 - A biztonsági szervezet feladatai
 - A védelmi intézkedések meghatározása, betartatása
 - A biztonsági események kezelése
 - Követés. naprakészség biztosítása

- Titokvédelem

- Az adatokat, alkalmazásokat, eszközöket és helyiségeket osztályozni, minősíteni kell
- Az osztályozás alapja a titokvédelemről, az üzleti titokról, a személyes adatokról, a banktitokról szóló jogszabályok és saját üzleti érdek
- Az **adatvédelmi osztályok**: titkos (pl. államtitok, üzleti titok), bizalmas (pl. szolgálati titok, személyes adatok) belső használatra, nyilvános -- (alkalmazások és eszközök is)
- Az **alkalmazások védelmi osztályozása**: milyen osztályba tartozó adatokat kezel (a legerősebb)
- Az **eszközök** védelmi osztályozása: biztonságkritikusságuk alapján, ugyanazon osztályok
- A **helyiségek** védelmi osztályozása funkcióik alapján: zárt, kiemelten ellenőrzött, ellenőrzött, nyilvános

- Iratkezelés
 - Iratkezelési Utasítás szükséges (elektronikus iratok előállítására, feldolgozására, továbbítására, megsemmisítésére is kitér)
 - Kiindulás: az adatok titokvédelmi osztályozása
 - Kritikus rész: áttérés elektronikusról papíralapúra és viszont
 - Papír alapú outputok előállítása
 - A minősítést fel kell tüntetni a papíralapú iraton
- Biztonsági alrendszer tervezés
 - Átvilágítási jelentés
 - Biztonsági Politika
 - Katasztrófa Terv
 - Biztonsági Szabályzat

- Humán védelmi módszerek
 - Megbízhatóság biztosítása (a munkaviszony teljes időtartamára)
 - Munkaviszony létesítésekor (Felvételi Policy)
 - Háttér ellenőrzés, referenciák bekérése, erkölcsi bizonyítvány, folyamatban levő bűnügyi eljárás ellenőrzése
 - Titoktartási nyilatkozat (a munkaviszony megszűntetése utáni időszakra is)
 - Nyilatkozat a biztonsági követelmények ismeretéről
 - Érdeklődési nyilatkozat (nincs olyan érdekeltsége, amely nem teszi lehetővé a tervezett munkakör betöltését)
 - Szakmai és emberi kompetencia vizsgálat

– Munkaviszony alatt

- Védelmi intézkedések a megbízhatóság fenntartása érdekében
- Teljesítménykövetés
- Karrier menedzsment – lojalitás, kötődés
- Szakmai kompetencia és feladatok közötti konzisztencia biztosítása
- Képzések
- Munkaköri leírások naprakészsége
- Egymást kizáró biztonságkritikus munkakörök figyelembe vétele
 - Adatvédelmi és adatbiztonsági
 - Adatbiztonsági és bármely informatikai
 - Informatikai fejlesztési és üzemeltetési
 - Üzemeltetési és adatellenőrzési
 - Üzemeltetési és karbantartási
 - Üzemeltetési és felhasználói

– Szerepkörök

- Tulajdonos
- Felhasználó
- Biztonsági adminisztrátor
- Üzemeltető
 - Operátor
 - Rendszergazda
 - Karbantartó
 - Rendszer szoftveres
 - Alkalmazói szoftveres
 - Adat ellenőr
- Fejlesztő
 - Hardver fejlesztő
 - Szoftver fejlesztő

– Munkaviszony megszüntetésekor

- Jogosultságok, accountok visszavonása (felmondási idő: legalább korlátozás)
- Megszüntetési interjú: (nyilatkozat a vállalati dokumentumok és adathordozók visszaszolgáltatásáról, kilépés utáni titoktartásról)
- Vállalati tulajdon visszavonása (beléptető kártya, kulcsok is)
- Törlés a fizetési listáról
- A munkatársak értesítése a kilépés tényéről

– (A humán erőforrásokat fenyegető veszélyforrások elleni védelem: nem IT biztonság, hanem a vagyonvédelem tárgya)

- Szerződés harmadik féllel
 - Garanciák szükségesek
 - Megfelelő védelmi intézkedésekre a biztonsági környezetben
 - Megfelelő védelmi intézkedések a feladat végrehajtása során
 - Megfelelő védelmi intézkedések a végtermékben
 - Outsourcing fejlesztési megbízás:
 - A fejlesztési környezetre vonatkozó biztonsági követelmények
 - A megbízó ellenőrzési jogosultságának elismerése
 - A fejlesztés tárgyára vonatkozó biztonsági követelmények
 - Fenyegetettség mentességi nyilatkozat az átadás/átvételkor

- Outsourcing üzemeltetési megbízás:
 - A biztonsági környezetre vonatkozó követelmények (humán, fizikai, logikai leválasztás)
 - A megbízó ellenőrzési jogosultságának elismerése
 - Megfelelő erősségű humán, fizikai és logikai védelmi intézkedések megtétele
- Outsourcing karbantartási, rendszerkövetési megbízás
 - A szolgáltató alárendelése a megbízó Biztonsági Politikájának
 - A szolgáltató jogosultságainak korlátozása, rögzítése
 - Ellenőrzési lehetőség biztosítása

– Munkaerőbérlet

- A munkaerő alárendelése a megbízó Biztonsági Politikájának, nyilatkozat ennek elfogadásáról
- Számokérési, szankcionálási lehetőség biztosítása

– Kockázat áthárítás: Biztosítások

A védelem erőssége

- Egyenszilárdságú védelem
 - A támadás sikeressége a védelem leggyengébb pontján a legvalószínűbb
 - Optimális megoldás: a védelem minden ponton azonos szintű, azonos ellenálló képességű legyen
 - Példa: a védelmi intézkedések meg nem kerülhetőségének biztosítása – az egyenszilárdság elvének alkalmazása
 - Ellenálló képesség: kifejezi, hogy a biztonsági alrendszer milyen támadási potenciálú lehetséges támadásokat képes visszaverni
 - Támadási potenciál: a sikeres támadás esélye

- Az ellenálló képesség kategóriái
 - Nem ellenálló
 - Nyilvánvalóan ellenálló
 - Mérsékelten ellenálló
 - Magasan ellenálló
- Az ellenálló képesség meghatározása
 - Kiindulás: az egyes veszélyforrásokhoz tartozó kockázatelemzés

A meghatározás lépései:

1. A lehetséges veszélyforrásokat osztályokba ill. csoportokba soroljuk

- Szervezési kockázati osztály
 - Szabályozás
 - Humán politika
 - Szerződések
- Technikai kockázati osztály
 - Fizikai hozzáférés védelem
 - Fizikai rendelkezésre állás
 - Logikai hozzáférés védelem
 - Logikai rendelkezésre állás
 - Hálózat
 - Életciklus

1. Az egyes osztályok ill. csoportok minősítését a benne előforduló legnagyobb kockázati értéket jelentő veszélyforrás határozza meg
2. Nagyobb kockázathoz gyengébb minősítés tartozik

Kockázat	Ellenálló képesség
XL (Extra Large)	Nyilvánvalóan ellenálló
L (Large)	Nyilvánvalóan ellenálló
M (Medium)	Mérsékelten ellenálló
S (Small)	Magasan ellenálló
VS (Very Small)	Magasan ellenálló

- A védelmi intézkedések kiválasztása
 - A gyakorlatban az ellenálló képesség követelményként jelentkezik
 - Az elvárt ellenálló képesség meghatározása a top management feladata
 - A vállalat tevékenysége
 - Adatok bizalmassága
 - Támadási potenciál
 - Erőforrások
 - Stb.
 - A gyakorlatban az ellenálló képesség meghatározása után születik döntés arról, hogy az elfogadható vagy növelése szükséges

- A védelmi intézkedések erőssége
 - A védelmi intézkedések erősségének meghatározásához az egyenszilárdság elvét figyelembe kell venni
 - A védelmi intézkedések erősségét ajánlások alapján lehet meghatározni
 - Nincs egységes szerkezetű, egyetlen figyelembe vehető ajánlás.
 - Mindenre nincsenek ajánlások

- Elterjedt tévhitek
 - A jelszó biztonságos
 - Az íratlan szabályok be nem tartása a fő probléma
 - Korlátozott hosszúság – próbálkozások lehetségesek
 - Kódolatlan átvitel a hálózaton – lehallgathatóság
 - Jelszó elfogó programok – képernyő, billentyűzet naplózás
 - A rejtjelezés mindent megold
 - Mi van, ha a rejtjeles üzenet nem érkezik meg, vagy, ha többször is megérkezik
 - A rejtjelezés a hitelesítést nem oldja meg
 - A rejtjelfejtés nem az összes kulcs kipróbálását jelenti
 - A vállalat dolgozói lojálisak, elkötelezettek

Az IT biztonság szervezése

- Alapelvek
- A biztonságsszervezési folyamat
 - Helyzetfeltárás
 - Veszélyforrás analízis
 - Kockázatmentzés
 - Biztonsági cél
 - Biztonsági követelmények
 - Védelmi intézkedések
- BCP, DRP

Alapelvek:

- Rendszer és folyamatszempléletű tervezés
- Egyenszilárdság elvének betartása
- Top-down megközelítés

Helyzetfeltárás

- A gyengeségek és kockázatok feltárása (a kockázatelemzés előkészítése)
 - Jogszábaályi feltételek
 - Üzleti elvárások
 - Szervezet és működés
 - Humán politika
 - Informatikai erőforrások
 - (Már megtett intézkedések)
- Módszer (szemlék, bejárások, interjúk, dokumentum tanulmányozások)
- Eredmény: Helyzetfeltárási jelentés

Veszélyforrás analízis

- A gyengeségek meghatározása a helyzetfeltárás alapján
 - Tényleges fenyegetést jelentenek-e?
 - Vannak-e megfelelő védelmi intézkedések és ezek összhangban vannak-e Biztonsági politikával?
 - A védelmi intézkedések gyakorlata összhangban van-e az előírásokkal?
 - (Korábbi audit következményei)
- A veszélyforrások csoportosítása:
 - Részleges
 - Átfogó
- (Javaslat azonnali intézkedésekre)
- Eredmény: Biztonsági átvilágítási jelentés (a Helyzetfeltárási jelentéssel együtt)

Kockázat elemzés

- Alapelvek:
 - A veszélyforrás analízisre épül: A veszélyforrás pontos megnevezése, bekövetkezési valószínűsége, a várható (számszerűsített) kárkövetkezmény
 - A valószínűség statisztikai módszerrel történő kiszámításához egy hosszabb idősor adataira van szükség, amely a biztonsági események tekintetében gyakran nem áll rendelkezésre. Ezért a bekövetkezési valószínűség meghatározása közvetett módon történik.
 - Exakt módszerekkel meghatározni igen nehéz, kénytelenek vagyunk becsülni
 - A becsléshez segítség:
 - Relatív gyakoriság (100 évente egyszer – 1%)
 - Hasonló felhasználása (hasonló cég, hasonló épület, másik város, másik ország stb.)
 - Egyebek pl. szolgáltatók szerződése

Kockázat elemzés

- Változatok:
 - Kvantitatív kockázatelemzés
 - Erőforrásigényes
 - Hosszabb távon térül meg
 - Modellekben gondolkodik
 - Függvényeket (igen sok változó) használ (nem feltétlenül publikusak)
 - Számszerű adatokat szolgáltat
 - Az eredmények megbízhatóságára vonatkozóan is számadatokat szolgáltat
 - Kvalitatív kockázatelemzés
 - Szinteket, skálákat használ, nem számszerű adatokat

- Kockázatok kezelése - lehetőségek
 - T (Terminate) – Megszüntetés
 - R (Reduce) – Csökkentés
 - A (Accept) – Elfogadás
 - P (Pass) - Átadás, áthárítás - biztosítás

- Mértéke, bekövetkezési valószínűsége lehet (P):
 - Igen kicsi - Very Small (VS)
 - Kicsi - Small (S)
 - Közepes - Medium (M)
 - Nagy - Large (L)
 - Igen nagy - Extra Large (XL)
- A becslést segíti a **támadási potenciál** elemzése (leginkább humán fenyegető tényezők esetén használható)

- Támadási potenciál
 - A sikeres támadás esélye
 - Függ:
 - A védelem erősségétől
 - A támadási cél értékétől
 - A sikeres támadáshoz szükséges szakértelemtől (laikus, profi – ismeri a rendszert, szakértő – spec. eszközöket is használ)
 - A sikeres támadáshoz szükséges erőforrásoktól (eszköz és idő)

- A támadási potenciál annál nagyobb, minél
 - Nagyobb a támadási cél értéke
 - Nagyobb a támadó szükséges szakértelme
 - Gyengébb a védelem
 - Kifinomultabb a sikeres támadáshoz szükséges eszköz
 - Kisebb a támadás végrehajtásához szükséges idő

- A támadási potenciál lehetséges értékei
 - Kicsi
 - Közepes
 - Nagy
 - Gyakorlat feletti
- Összefüggés: Minél kisebb, a támadási potenciál, annál nagyobb a bekövetkezési valószínűség (Szakértő támadó, spec. eszközzel, rövid idő alatt: ennek kicsi a valószínűsége)

Támadási potenciál	Beköv. valószínűség
Gyakorlat feletti	VS
Nagy	S
Közepes	M
Kicsi	L

- Lehetséges kárkövetkezmény, sebezhetőség (V)
 - Globális (G)
 - Részleges (R)
- Kockázat:
 - A bekövetkezési valószínűség (P) és a sebezhetőség (V) egybevetéséből adódik

	R	G
VS	VS	S
S	S	S,M
M	M	M,L
L	L	L,XL
XL	XL	XL

- Gyakorlat: Cobit 3 (Control Objectives for Information and Related Technology, 2000)
 - A bekövetkezési valószínűség (P) lehet:
 - Nagyon kicsi (PVS – Very small)
 - Kicsi (PS – Small)
 - Közepes (PA – Medium)
 - Nagy (PL – Large)
 - Nagyon nagy (PVL – Very large)
 - A hatás, kár lehet:
 - Elhanyagolható (VS – Very small)
 - Kicsi (S – Small)
 - Közepes (M – Medium)
 - Jelentős (L – Large)
 - Katasztrófális (VL – Very large)

– A kockázat (R) lehet:

- Elhanyagolható (RVS – Very small)
- Kicsi (RS – Small)
- Közepes (RM – Medium)
- Nagy (RL – Large)
- Nagyon nagy (RVL – Very large)

– Az összevetés

P \ Hatás, kár	VS	S	M	L	VL
PVS	RVS	RVS	RS	RM	RL
PS	RVS	RS	RM	RM	RL
PM	RVS	RS	RM	RL	RL
PL	RS	RM	RL	RL	RVL
PVL	RS	RM	RL	RVL	RVL

- A kockázatelemzés lépései:
 - Az egyes veszélyforrások értelmezése, minősítése
 - Vállalt kockázati szint meghatározása
 - Döntés a szükséges védelmi intézkedésekről

- Az egyes veszélyforrások minősítése
 - A veszélyforrásokra egyenként meghatározzuk a következőket (táblázatokat töltünk ki)
 - Vm-xx A veszélyforrás neve
 - Vm: a veszélyforrás kódja, ahol „m” a típusát jelöli (SZ-szervezési, F-fizikai, L-logikai, H-hálózati, É-életciklus veszélyforrás)
 - Xx: azonosító szám
 - A veszélyforrás neve: A veszélyforrás rövid megnevezése
 - Szakmai magyarázat:
 - A veszélyforrás rövid szakmai magyarázata, amely leírja, hogyan veszélyeztet a biztonságot, és ha a veszélyforrás képezte fenyegetés realizálódik akkor, milyen hatása van.
 - bekövetkezése esetén mekkora a becsült hatása a vizsgált cégre

– Miért léphet fel:

- A helyzetfeltárás során szerzett információkkal alátámasztjuk, hogy a vizsgált cégnél mi okozza a veszélyforrás létezését.

– Mit fenyeget:

- Bizalmasság (**C**onfidentiality), Sértetlenség (**I**ntegrity) és a Rendelkezésre állás (**A**vailability) közül.

– Valószínűség:

- A veszélyforrás becsült bekövetkezési valószínűsége.

– Hatás, kár:

- A veszélyforrás által jelentett fenyegetés

– Kockázat:

- A bekövetkezés valószínűség és a hatás összevetéséből határozzuk meg a veszélyforrás kockázatát.

Példák:

VF-08 A szerver szobába illetéktelenek is be tudnak jutni.

Szakmai magyarázat	A hierarchikus beléptető rendszer alkalmazásának lényege, hogy adott zárt térrészre csak olyanok tudjanak belépni akiknek a munkája ezt szükségessé teszi. Ezért fontos olyan mértékű területi szeparálást biztosítani, amely ezt az elvet támogatja. Ha illetéktelenek tudnak a védett berendezésekhez férni, megnő a veszélye annak, hogy az információ biztonsági kritériumok sérülnek.
Miért léphet fel	Az XXXX szervereit tartalmazó térrészbe a szerverek üzemeltetéséhez szükségesnél több személy tud belépni. Ennek oka elsősorban az, hogy a térrészben nemcsak az XXXX szerverei lettek elhelyezve, hanem más szervezetek berendezései is.
Mit fenyeget	C, I, A
Valószínűség	PS (Kicsi)
Hatás, kár	M (Közepes)
Kockázat	RM (Közepes)

VF-12 Nincsenek automatikus tűzérzékelők telepítve a szerverereket tartalmazó szobákban, ezért nincs megelőző tűzriasztás

Szakmai magyarázat	<p>A szerver berendezések folyamatosan üzemelnek. Személyzet a berendezéseket tartalmazó szobákban csak ritkán van jelen. Az esetleg előforduló tűz a kezdeti szakaszában felismerhető elektronikus érzékelők használatával.</p> <p>A laza villamos kötéseknel kialakuló átmeneti ellenállás felmelegíti a környezetet, a szigeteléseket. Kezdetben szemmel nem látható füst szivárgás történik, amit az érzékeny ionizációs füstérzékelők már detektálnak. A riasztó jelzés lehetővé teszi, hogy időben védekezzünk, a komolyabb károkozást megelőzően.</p>
Miért léphet fel	Az XXXX YYYY-i telephelyén a szerver szobákban nincs telepítve ionizációs füstérzékelő.
Mit fenyeget	I, A
Valószínűség	PM (Közepes)
Hatás, kár	L (Nagy)
Kockázat	RL (Nagy)

VSZ-11 Az üzemeltetői munkakörök meghatározásánál nem veszik figyelembe az egymást kizáró munkakörök (segregation of duties) feltételeit

Szakmai magyarázat	A nem kellőképpen szétválasztott munkakörök azt eredményezhetik, hogy egy személy saját magát ellenőrzi, ill. képes a saját hibáira, esetleg visszaéléseire utaló bizonyítékokat eltüntetni.
Miért léphet fel	Az üzemeltetési feladatokat kis számú munkaerő látja el, munkaköri leírásaik alapján feladataik gyakorlatilag azonosak. Az ügyeleti rendszer miatt az ügyeles üzemeltetőnek mindent el kell tudnia érni.
Mit fenyeget	C, I, A
Valószínűség	PS (Kicsi)
Hatás, kár	M (Közepes)
Kockázat	RM (Közepes)

- A vállalt kockázati szint meghatározása
 - Meghatározzuk, hogy mekkora kockázatot vállalunk fel (pl. RM)
- Döntés a szükséges védelmi intézkedésekről
 - Az eredmény alapján a menedzsment dönthet a védelmi intézkedésekről
 - Ismert a maradó kockázat
 - Egyenszilárdság elve!

- Biztonsági cél:
 - Az informatikai erőforrások folyamatos és rendeltetésszerű használata
 - Ezt a top management kell, hogy deklarálja, ezzel kinyilvánítja az elkötelezettségét.
- Biztonsági követelmények
 - Biztonsági cél + a kockázatelemzés eredményei
 - A különböző kategóriákban általános követelmények meghatározása
 - Szervezési
 - Technikai
 - ...

- Részleges védelmi intézkedések specifikálása
 - Biztonsági Politikában megfogalmazva
 - Felhasználhatók a tervezéshez, beszerzéshez, de nem konkrét termék specifikációja

BCP, DRP

- Fogalmak: BCP, DRP
- Felkészülési/készenléti szakasz
- Katasztrófa helyzet kezelése
- A katasztrófa kezelés dokumentumai
- A visszaállítási folyamat
- A helyreállítási folyamat
- Tesztelés, karbantartás, tárolás
- Oktatás
- Költségek
- Szükséghelyzeti tervek

BCP (Business Continuity Plan)

DRP (Disaster Recovery Plan)

- A BCP (BPC) - Üzletmenet folytonosság terv
 - Az üzleti folyamatokra, a szolgáltatásokra koncentrál
 - Megfogalmazza a folytonosság érdekében szükséges **preventív intézkedéseket**
- DRP – Katasztrófa terv
 - Válasz a **katasztrófa helyzetekre** – (DRP) katasztrófa terv
 - Üzletmenet folytonossági terv a kritikus üzleti folyamatokra, technikai katasztrófaterv a folyamatok által igényelt lényeges távközlési, informatikai és logisztikai szolgáltatásokra vonatkozik
 - **Sebezhetőségi ablak:** Meddig vagyunk képesek elviselni egy-egy folyamat kiesését?

Szakaszok

- Felkészülési/készenléti szakasz
- Katasztrófa helyzet
 - Visszaállítás
 - Helyreállítás

A felkészülési/készenléti szakasz

- Megfelelő szabályzatok és utasítások megléte és betartása, ellenőrzések
- (Ki? Mikor? Mit? – szabályzatok, Valóban? – auditok)
 - Biztonsági szabályzat
 - Dokumentálási rend
 - Tesztelések
 - Mentési rend
 - Naplózási rend
 - Vírusvédelmi szabályzat
 - Rendszerspecifikus üzemeltetési utasítások
 - Stb.

- **Katasztrófa terv készítés ill. karbantartás**
 - A küldetéskritikus üzleti folyamatok felmérése
 - a folyamat neve, a kritikusság oka és mértéke, a kiszolgált ügyfelek, belső felhasználók, az érintett objektumok, a folyamathoz szükséges fő informatikai alkalmazások és távközlési szolgáltatások, a normál üzemmenetért felelős személyek, illetve minimális üzletmenet követelményei (jogszabályokban rögzített, vagy szerződésekben vállalt szint).
 - Kockázatelemzés
 - A veszélyforrás pontos megnevezése, bekövetkezési valószínűsége, a várható számszerűsített kárkövetkezmény

– Üzleti hatáselemzés

- Olyan kárelemek vizsgálata, amelyek hatásai nagyon nehezen számszerűsíthetők (például imidzsvesztés az ügyfelek körében, negatív reklám, a biztonság fokának csökkenése, befektetői megítélés romlása).

– Védelmi stratégiák kidolgozása – magas szintű elképzelés

- Cél a legkritikusabb veszélyforrások kockázatának csökkentése a veszélyforrás bekövetkezési valószínűségének csökkentésével vagy a veszteségek minimalizálásával.
- A stratégia-alternatívák megfogalmazása során az egyes lehetőségeket erőforrásigény, megvalósítási időtartam, maradványkockázat, ügyfelekre gyakorolt hatás, valamint hosszú és rövid távú hatás szempontjából értékelni szükséges.

– Döntés a védekezés szükségességéről – felelős vezető

- Védekezés/vállalható kockázat

– Implementáció – konkrét tervek

- Szervezési, beszerzési, üzembe helyezési, szerződéskötési, programfejlesztési és egyéb feladatok
- A stratégiát elfogadó felsőszintű döntés után, kiindulópont az elfogadott stratégia ill. az abban megadott **erőforrásigény** és az implementációhoz szükséges **időtartam**
- Az implementációhoz szükséges összes feladat felsorolása és minden egyes feladat kapcsán a **felelős**, a szükséges **erőforrás** és **határidő** megadása
- Fontos szempontok: Beszerzések tervezése, és a területek közti együttműködés

- Általános vészhelyzeti intézkedések (válaszok krízishelyzetekre)
 - Katasztrófa esetén elsődleges az alkalmazottak és a vagyontárgyak védelme
 - Előre kidolgozott intézkedési tervekre van szükség
 - Tüzriadó terv
 - Szükséghelyzeti terv villamos energia, távközlés kiesés esetére
 - Szükséghelyzeti terv vírusfertőzés/hacker támadás esetére
 - Szükséghelyzeti terv természeti katasztrófa/extrém időjárás esetére

- Szükséghelyzeti terv az épület/telephely megközelíthetlenségének esetére (extrém időjárás, nagy kiterjedésű baleset stb.)
- Szükséghelyzeti terv illetéktelen személy behatolásának esetére (erőszakos cselekmény, túszejtés stb.)
- Szükséghelyzeti terv robbantással történő fenyegetésre
- Szükséghelyzeti terv jelentős személyi sérülések esetére
- Szükséghelyzeti terv vízbetörés esetére
- Egyéb

A katasztrófa helyzet kezelése

A katasztrófa kezelő szervezet felépítése:



- Vezetői team

- A team feladata és felelőssége **stratégiai döntések** hozása olyan fontos vészhelyzetekben, amikor az eset az egész cég működésére kihatással lehet, vagy testületi intézkedést kell kezdeményezni. A létrejövő vészhelyzetekben a vezetői teamnek az adott helyszínen kell tájékozódni, és részt venni a visszaállítási munkában.
- A találkozó helyeket meg kell nevezni. Mivel érheti az adott objektumot/vállalatot olyan kár, hogy az értekezlet ott nem tartható meg, ezért alternatív helyszín is szükséges, lehetőleg a közelben.
- Tagjai:
 - Biztonsági igazgató
 -igazgató
 -

- Kríziskezelő team

- A vezetői team-el tartja a kapcsolatot, ugyanakkor közvetlen segítséget kell adnia katasztrófa menedzsernek
- A kármegállapító team értékelése alapján kezdeményezni a katasztrófa helyzet kinyilvánítását
- Kríziskezelő központ felállítása (a helyszínen ill.a közelben)
- Minden szükséges intézkedés dokumentálása a kezdetektől a befejezésig
- A szükséges személyek kinevezése
- Kapcsolattartás a beszállítókkal (tárgyalások, szerződések)

- Intézkedés a szükséges anyagi eszközökről
- Intézkedik a források elkülönítéséről a visszaállítási periódusban
- Pénzügyi és politikai döntést hoz.
- Tagjai:
 - ... ig. helyettes
 - Szervezeti egység vezetők

- **Katasztrófa manager**
 - A legfőbb operatív irányítója a visszaállítási és helyreállítási folyamatnak.
 - Kapcsolatot tart a kárfelmérő, a technikai szükséghelyzeti és infrastruktúra visszaállító teamekkel és koordinálja munkájukat.
 - Ellátja a szükséges adminisztráció koordinálását
 - A különböző technikai szükséghelyzeti team rajta keresztül tesz jelentést a krízis kezelő team számára
 - Felelős az érvényben lévő katasztrófa terv karbantartásáért, teszteléséért és begyakoroltatásáért
 - Ellentmondások feloldása
 - Szervezeti egység vezető

- Kárfelmérő team(ek)

- Részletesen meghatározza a kár kiterjedését a helyszínen, és az erőforrásokon belül is.
- Megvizsgálja milyen a komolysága és az időtartama az üzleti folyamat megszakadásának
- Megfelelő lebonyolítást ajánl a visszaállítási akcióra a krízis kezelő team számára.
- Célszerű, hogy a kárfelmérő csoportoknak kinevezett operatív vezetője is legyen a kárfelmérő teamen belül
 - szolgáltatási kárfelmérő vezető
 - személyi kárfelmérő vezető
 - hardver kárfelmérő vezető
 - szoftver kárfelmérő vezető
 - távközlési kárfelmérő vezető

- Technikai visszaállító teamek
 - A szükséges technológiák helyreállítása a kárt szenvedett területen, felhasználva a háttér (back up) erőforrásokat az akció tervek szerint (háttér berendezések, mentések, és egyéb erőforrások)
 - Azonosítja és megszerzi a pótlólagos erőforrásokat, szükség szerint a kritikus üzleti folyamat helyreállításához
 - Előkészít egy ütemtervet a technikai személyzet felállítására minden technikai funkció támogatására
 - Korszerűsíti a technikai visszaállítási tevékenység folyamatát a krízis kezelő team ütemterve szerint

- Koordinálja a technológiával kapcsolatban álló feladatokat a visszaállított helyszínről az új vagy helyreállított állandó helyszínre történő visszatéréshez
- Biztosítja az alkalmazások sikeres helyreállítását, gondoskodik a távközlési infrastruktúra (telefon stb.) működéséről a háttér helyszínen
- Teamek: hardver szoftver távközlési

- Infrastruktúra visszaállító team
 - A visszaállítása nem alaptevékenységet szolgáló szolgáltatás és erőforrások vonatkozásában a háttér helyszínen. (az irodák ellátása, a terület, a bútorok, az irodai eszközök, a vízszolgáltatás, a villamos energia, a légkondicionálás és a fizikai behatolás és tűzvédelem biztosítása, stb.)
 - Logisztikai támogatással látja el a különböző technikai visszaállító teameket a visszaállítási munkák alatt
 - Intézkedik a személyzet számára szükséges szolgáltatásokról a szolgálati út kihagyásával (pl. üzenet feladás és szállítás, adminisztratív támogatás az átmeneti visszaállítási helyszínen, biztonsági rendszerek biztosítása, stb.)
 - Gondoskodik az irodák berendezéséről és ellátásáról (pl. írószerszámok, papír, asztalok, székek, másoló, stb.)

A katasztrófa kezelés dokumentumai

- A folyamatos aktualizálás nagyon fontos!
- Beosztások/pozíciók és személyek megfeleltetése
- Elérhetőségek (telefonkönyv több elérhe-tőségi lehetőséggel)
 - A katasztrófa szervezet tagjai
 - A visszaállításban résztvevő **operatív munkatársak** (pl. szerverek rendszergazdái, speciális ismeretekkel rendelkező szakértők)
 - A visszaállításban résztvevő **üzleti partnerek/hatóságok** (mentők, tűzoltóság, rendőrség, polgári védelem, karbantartók, gyorsfutár szolgálat stb.)

- Értesítési utasítások
 - értesítési sorrend/lánc
 - Időzítés (Kit mikor?)
 - az értesítés tartalma
 - teendők
 - követendő hierarchia
 - helyszín
 - stb.)
- Helyszín/alternatív helyszín

- **Akcióterv:**

- A katasztrófa helyzet deklarálásának és a terv életbeléptetésének és végrehajtásának folyamata
 - Esemény meghatározása, elsődleges kárfelmérés
 - Katasztrófa helyzet deklarálása
 - Értesítések (felsővezetés, teamek, szakértők, sajtó?...) ...

- **Visszaállítási időmátrix**

- Az egyes üzleti folyamatok és erőforrások vonatkozásában megadott elfogadható maximális kieső időtartam megadása

- **Szükséghelyzeti tervek**

A visszaállítási folyamat

- Cél: a folyamatok újraindítása
 - Definiálni szükséges a visszaállítási folyamatokat, amelyek segítségével a szolgáltatás, a folyamatok a **lehető legrövidebb időn belül** visszaállnak egy előre definiált minimális szolgáltatási szinten. (Lehetséges, hogy nem az eredeti jellemzőkkel.)
 - Részletes tervek a visszaállításra. Az **eljárások, a résztvevő szakértő csoportok és a szükséges erőforrások** meghatározása.

– Lehetséges megoldások:

- Alternatív erőforrások, alternatív helyszínen, alternatív személyzettel (meleg, hideg tartalék, duplikálás, reciprok megállapodások stb.)

– Beszállítói kapcsolatok

- Tartalmazza az erőforrás beszállítói listát és azon cégeket, akik a berendezések sürgős pótlására aláírt szerződéssel vállalkoztak.
- Beszállítói szerződések

A helyreállítási folyamat

- Visszatérés normál üzemeltetésre
 - Definiálni szükséges a helyreállítási folyamatokat, amelyek segítségével **az eredeti szolgáltatás, az eredeti folyamatok az eredeti jellemzőkkel** helyreállnak.
 - Részletes tervek a helyreállítás menetére.
 - Az eljárások, a résztvevő szakértő csoportok és a szükséges erőforrások meghatározása.
 - Infrastruktúra helyreállítási kapcsolatok
 - Beszállítói kapcsolatok (IT)
 - A kárt szenvedett infrastruktúra helyreállításában potenciálisan résztvevő további (építészeti, szakipari, hatósági, stb.) kapcsolatok
 - Szerződések

Tesztelés, karbantartás, tárolás

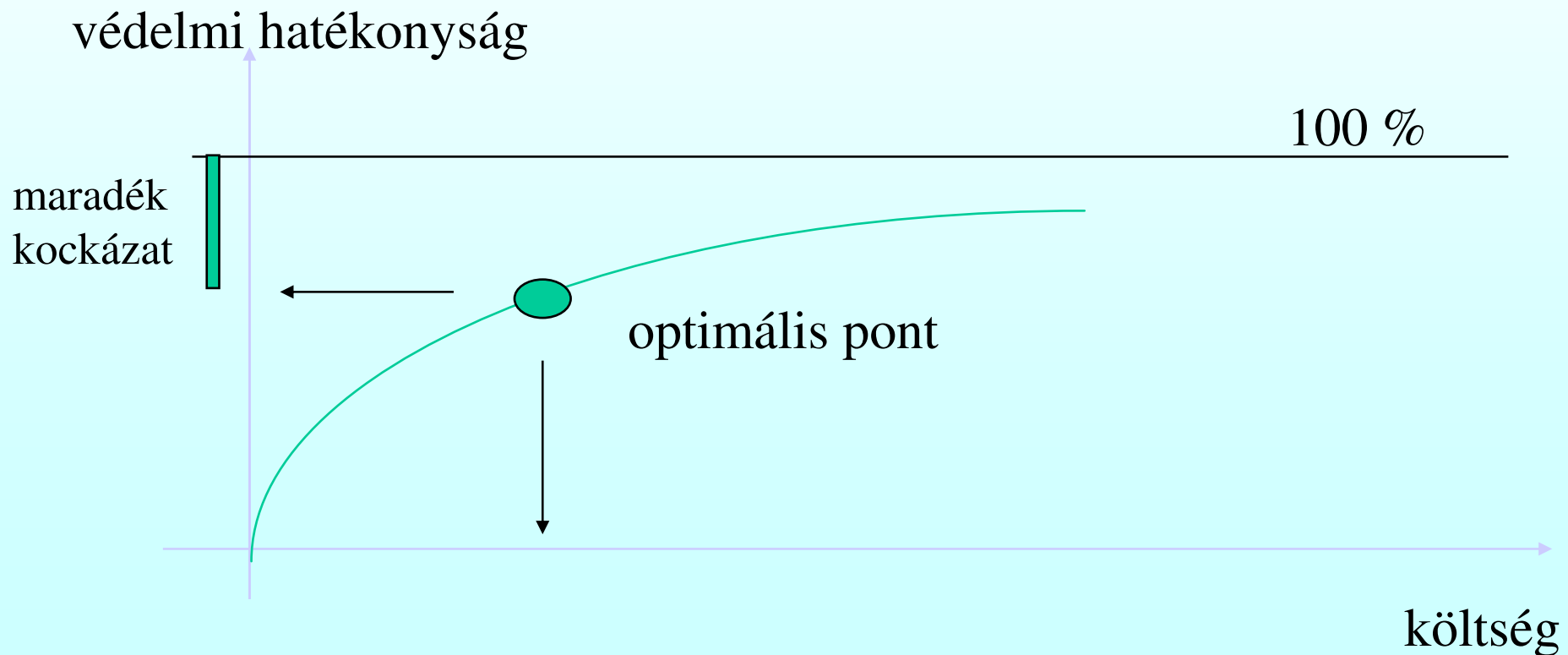
- A a tesztelés módja (éles?, szimulációs vagy szóbeli)
- Előre definiált eredmények
- A teszteléshez szükséges eszközök, erőforrások és személyzet. Menetrend.
- Jegyzőkönyv és kiértékelése, esetleges javítások
- Teljes körű karbantartás (új küldetéskritikus folyamat esetén)
- Részleges karbantartás (erőforrások rendelkezésre állása, módosulása, naprakészség)
- Tárolás: Alternatív, de könnyen elérhető helyszínen, csak az utolsó (érvényes) változat létezzen

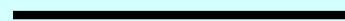
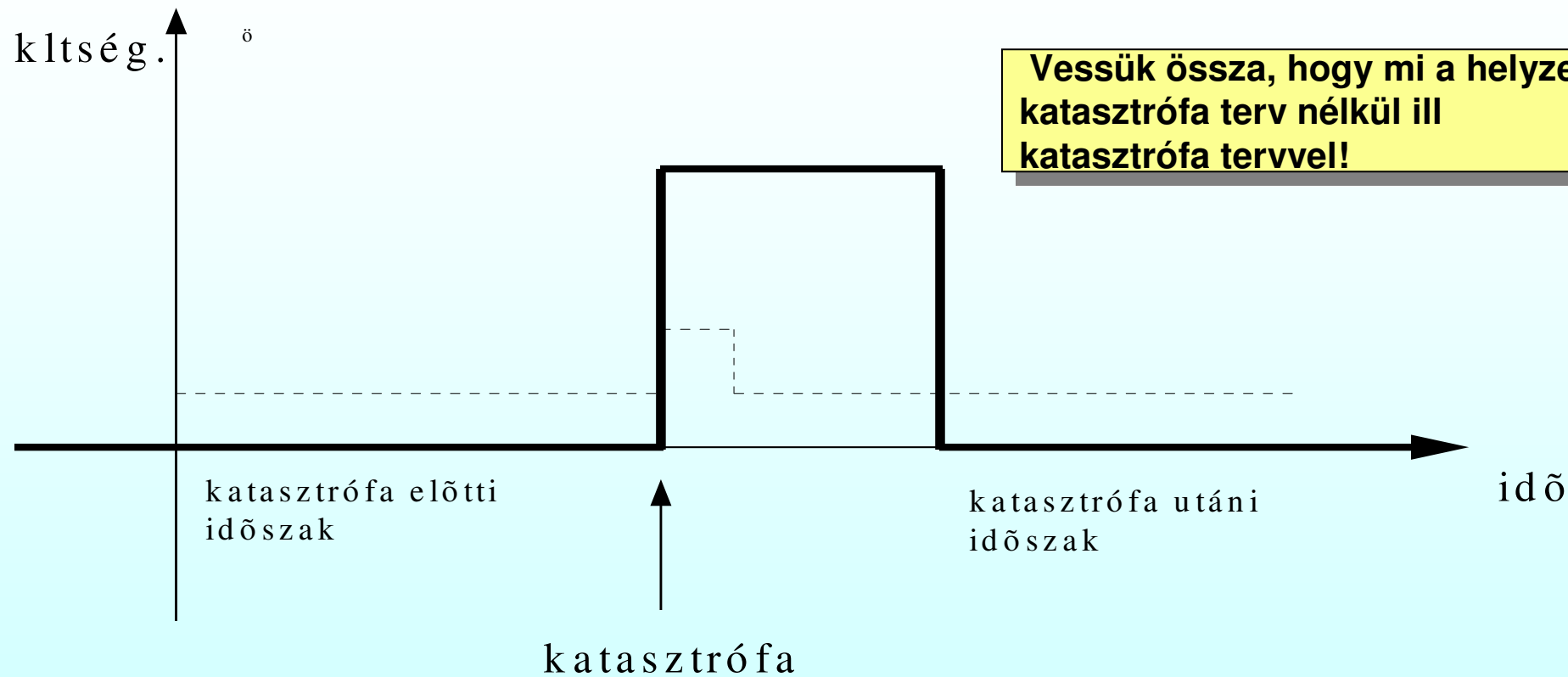
Oktatás

- Ismertető és gyakorlati rész
- Általános, biztonsági tudatot növelő oktatás
- A **konkrét tervek** oktatása a **felelősök számára** (az érintett munkatársaknak pontosan tudniuk kell, hogy mi a szerepük a katasztrófát követő munkában, milyen felelősséggel és hatáskörrel rendelkeznek (ez eltérhet a normál munka során betöltött szerepektől), és konkrét feladataikat végre is tudják hajtani
- Az oktatásra gyakoriságának meghatározása (Gyakorlat: **legalább évente** – a tesztelésekkel összhangban)

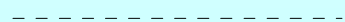
Költségek

- A védelmi hatékonyság és a költségek összefüggnek





költségek alakulása katasztrófa terv nélkül



költségek alakulása katasztrófa tervvel

Szükséghelyzeti tervek (példák)

- Tűzriadó terv
 - Az alkalmazottak feladatai: Minden alkalmazottnak **tudomásul kell vennie** a tüzesetet, és ajánlatos a következőket tenni
 - Tűzriadót előidézni (pl. betörni a kézi riasztó üvegét)
 - Értesíteni a biztonsági/portaszolgálatot
 - Ha szükséges a személyzetet a veszélyeztetett területről elküldeni (pl. robbanás veszély)
 - Ha lehetséges meg kell próbálni a kis kiterjedésű tüzet eloltani
 - Követni kell a tűzvédelmi megbízott és az épület biztonsági személyzetének utasításait.
 - Lehetőség szerint támogatni kell a sérült vagy hátrányos helyzetű személyeket

- A biztonsági személyzet feladatai
 - Értesíteni a tűzoltóságot a 105-ös telefonszámon, és szükség szerint a mentőket a 104-es telefonszámon
 - Megbízottat küldeni az épület elé, akik a tűzoltókat és a mentőket fogadják
 - Értesíteni a katasztrófa menedzsert

- Terv illetéktelen behatolás esetére
 - Az alkalmazottak feladatai
 - A jogrendben kisebb biztonsági ügynek ítélt esetben a gyanús vagy részeg személyt ki kell kérdezni a portaszolgálatnál
 - Értesíteni kell a biztonsági személyzetet
 - Ne próbálkozzunk erőt alkalmazni vagy vitát kezdeményezni a jogosulatlan személy eltávolítása érdekében
 - A biztonsági személyzet feladata
 - Megpróbálni eltávolítani a jogosulatlan személyt a területről
 - Értesíteni kell a munkahelyi vezetőt ill. a katasztrófa managert
 - Szükség esetén értesíteni a rendőrséget

- Terv robbantással történő fenyegetés esetére
 - Az alkalmazottak feladatai
 - Ha telefonon keresztül ismeretlen személy azzal fenyeget, hogy bombát helyezett el, fel kell jegyezni a fenyegetés pontos idejét, és meg kell próbálni kikérdezni a következők felől:
 - A fenyegetés indítéka
 - A robbanás időpontja
 - A robbanó eszköz fajtája (leírását)
 - A robbanó eszköz pontos helye az épületen belül
 - Az információt bizalmasan kell kezelni.
 - Értesíteni a biztonsági szolgálatot.
 - Követni kell a rendőrség utasításait
 - A közvetlen környezetben szemrevételezéssel meg kell vizsgálni van-e idegen vagy szokatlan tárgy.
 - A biztonsági személyzet feladata
 - Értesíteni kell a rendőrséget, a munkahelyi vezetőt ill. a katasztrófa managert

- Terv orvosi beavatkozásra
 - Az alkalmazottak feladatai
 - Értesíteni a biztonsági szolgálatot
 - Minél több ismeretet szerezni a sérülésről vagy betegségről
 - Melegre és kényelembe kell helyezni a sérült/beteg személyeket
 - Szakképzett elsősegélyt nyújtó személyért küldeni
 - Nyugodtnak kell lenni, és a beteg(ek)kel kell maradni
 - A biztonsági személyzet feladata
 - Értesíteni kell a mentőket
 - Értesíteni kell a katasztrófa menedzsert (abban az esetben, ha tömeges sérülés vagy betegség történik)

- Terv vízbetörés esetére
 - Az alkalmazottak feladatai:
 - Ha víz folyik a padlón, vagy csöpög a mennyezetről vagy a fali locsolóból (tűzoltóvíz, stb.) minden alkalmazottnak a következőt célszerű tenni:
 - Ha szükséges ki kell kapcsolni az elektromos berendezéseket
 - Értesíteni az üzemeltető csoportot
 - Nem szabad bekapcsolni az elektromos berendezéseket akkor sem, ha vízbetörés megállt.
 - Az üzemeltető személyzet (infrastruktúra visszaállító team) feladata:
 - Felmérni a helyzetet
 - Ellenőrizni a kritikus helyiségeket és szerver szobákat
 - Villamos kapcsolókat lekapcsolni szükség szerint
 - Értesíteni a katasztrófa menedzsert

- Terv villamos energia kiesésre
 - Az alkalmazottak feladatai
 - Értesíteni a biztonsági szolgálatot
 - Lekapcsolni a hordozható (egyedi) klíma berendezéseket (ha használatban volt) és minden szükségtelen berendezést, mint a monitorok, nyomtatók, fax készülékek, és a használaton kívüli asztali számítógépek
 - Ki kell támasztani minden ajtót a szerver szobákban, és kihasználni minden lehetséges szellőző nyílást, segítve ezzel a szobák hűtését a légkondicionálás megszűnte idejére
 - Kérésre segédkezni kell a rendszer adminisztrátor személynek a rá bízott szerver lekapcsolásában

– A villamos energia ellátást biztosító személy(ek) feladata a következő

- Ellenőrzi az UPS-eket és meghatározza az akkumulátorok működési idejét addig amíg a szobák teljes villamos teljesítménye megmarad
- Megpróbálja meghatározni a kiesési időt és becsült időt az energia ellátás helyreállításához
- Értesíti az Szolgáltató helyi részlegét
- Megtudja a szerelők várható érkezési idejét
- Riasztja a megfelelő osztályt és értesíti őket, lehet hogy szükséges lehet egy diesel aggregátor beállítása
- Ha az energia kiesés becsült ideje hosszabb mint amit a helyi UPS pótolni tud, riasztani kell a megfelelő osztályt, hogy üzembe kell helyezni a diesel aggregátort
- értesíteni kell a katasztrófa menedzsert

IT audit

- Az audit (ellenőrzés) fogalma
- Az audit célja
- Az audit lépései
- Az audit tárgya
- Az audit típusai
- Az auditor
- Az ellenőrzési terv
- Az audit végrehajtása
- A záró dokumentum
- Problémák

Az audit fogalma

- Audit
 - Az audit valamely szervezet, intézmény vagy személy munkájának **vizsgálata**, a mennyiségi és minőségi mutatók adatainak a normatívákkal való egybevetése, abból a célból, hogy ezáltal megítélhető legyen, eleget tesz-e bizonyos követelményeknek.
 - **Összehasonlítás**, a megismert tényeknek valamilyen követelményekhez, normákhoz való hasonlítása, mérése.
 - Az ellenőrzés a hatékony működést segíti elő a **tények okainak keresésével**.
 - **Lehetővé teszi** a hiányok pótlását, a hibák kijavítását, az eredmények megerősítését, a jó módszerek alkalmazásának elterjesztését.
 - Az ellenőrzési tevékenység nem egyszerűen egy esemény, hanem egy dinamikus **folyamat**, amely nem elégszik meg a tények feltárásával, hanem egy-egy fázisa azok elemzésével, értékelésével, a tapasztalatok megfogalmazásával, javaslatok kidolgozásával zárul.

Az audit célja

- Mit várunk el egy audittól:
 - Az eredményekből következtetéseket vonjunk le, bizonyosságot szerezzünk.
 - (A konkrét célt az ellenőrzést kezdeményező által képviselt érdekek nagymértékben meghatározzák.)
 - Kezdeményezők lehetnek
 - Tulajdonos
 - Vezetőség
 - Felügyeleti szervek
 - Könyvvizsgáló
 - Hitelezők
 - Vásárlók
 - Potenciális felvásárlók

Az IT audit lépései

- Megfelelőség vizsgálata
 - A védelmi intézkedések megfelelnek-e a hatályos jogszabályoknak?
 - Titokvédelemmel kapcsolatos törvények
 - (Pénzügyintézetekkel kapcsolatos jogszabályok)
 - Tűzvédelemmel kapcsolatos jogszabályok
 - Fizikai biztonsággal kapcsolatos feltételek (pl. MABISZ)
 - Belső szabályozások
- A megvalósulás ellenőrzése
 - A védelmi intézkedések a gyakorlatban megvalósulnak-e – az eltérések feltárása.
- A védelmi gyengeségek rögzítése
- Javaslat a gyengeségek kiküszöbölésére vonatkozó intézkedésekre

Az audit tárgya

- A vizsgálat elrendelésére jogosult határozza meg!
 - A teljes biztonsági alrendszer
 - A teljes biztonsági alrendszer része
 - Szervezési
 - Fizikai hozzáférés védelem
 - Logikai hozzáférés védelem
 - A fizikai rendelkezésre állás
 - A logikai rendelkezése állás
 - A Katasztrófa tervben megadott védelmi intézkedések
 - A biztonsági dokumentumokban megadott védelmi intézkedések megvalósulása
 - A biztonsági dokumentumok karbantartása
 - A biztonsági dokumentumok oktatása
 - Egy védelmi intézkedésre irányuló célvizsgálat

Az audit típusai

- Belső ellenőrzés (internal audit)
 - Illeszkedik a vállalat belső ellenőrzéséhez ill. működéséhez
 - A vállalat saját munkatársai hajtják végre
 - Jellemzői:
 - Helyismeret
 - Éves munkaprogram
 - Néhány rendszer részletes vizsgálata
 - A módszertan és képzettség egyénfüggő
 - Jelentés: az igazgatóságnak vagy felügyelő bizottságnak

- Külső ellenőrzés (external audit)
 - Spec. probléma esetén (EMC, rejtjelezés stb.)
 - Belső erőforrás hiányában
 - Valószínűsíti függetlenséget
 - Időszakonként (pl. 3 év) indokolt
 - Jellemzői:
 - Összehasonlító ismeret
 - Projekt munkaprogram
 - Átfogó és rendszerspecifikus vizsgálatok
 - Módszertan és képzettség előírható
 - Jelentés: általában a vezetőségnek

Internal/external audit

	Előny	Hátrány
Internal	Helyismeret Alacsonyabb költségek Folyamatosság	Helyismeret !!!! Függetlenség??? Harmadik fél nem fogadja el
External	Függetlenség Harmadik fél elfogadja Spec. szakértelem rendelkezésre áll	Magasabb költségek Folyamatosság hiánya

Az auditor

- Az auditorra vonatkozó követelmények
 - Függetlenség
 - Megfelelő szakmai kompetencia
 - Rögzített feladat, szerep, felelősség
 - A vizsgálat idejére fizikai és logikai hozzáférési jogosultságok

Az ellenőrzési terv

- Évente új terv, kétevente a teljes biztonsági alrendszer ellenőrzése szükséges
- Az ellenőrzési terv fajtái
 - Megelőző – rendszeres ellenőrzés
 - Feltáró – biztonsági esemény után
 - Javító – ismert védelmi gyengeség megszüntetésére
- Az ellenőrzési terv feladatai
 - Folyamatos – pl. naplók kiértéklése
 - Terv szerinti - megelőző jelleg
 - Célvizsgálat – feltáró és/vagy javító jelleg

Az audit végrehajtása

- **Fázisok**

- 1. Felkészülés

- Az ellenőrzés tárgya
 - Ellenőrzési lista (pl. jelszó rendszer, hozzáférési jogosultságok, tatalmi hitelesség védelem stb.)
 - Az ellenőrzés végrehajtói (belső/külső munkatársak)
 - Interjú alanyok listája
 - A tanulmányozandó dokumentumok listája
 - A szemlék listája
 - A tervezett tesztek listája

2. A helyzetfeltárás (az 1. szerint)

- Kockázatok felmérése és elemzése
- Kontrollok felmérése és elemzése
- Kockázatok kontrollokkal való lefedettségének elemzése
- Maradványkockázatok meghatározása, elemzése

3. A követelmények és a gyakorlat összehasonlítása

- A gyakorlat megfelel-e a követelményeknek?

4. Javaslat szükséges teendőkre

5. Jelentés összeállítása

A záró dokumentum

A záró dokumentum (jelentés) tartalma

- Az ellenőrzés tárgya
- Az ellenőrzés módszere
- Az ellenőrzés végrehajtói
- Az ellenőrzés megállapításai
 - A feltárt gyengeségek
 - A vizsgált terület minősítése (pl. nincs gyengeség, gyengeségek tapasztalhatók a megfelelés/megvalósulás vonatkozásában)
 - A vizsgálat gyengeségei (a módszer problémái, az ellenőrzést akadályozó tények)
- Javasolt intézkedések

Problémák

- Az audit visszahat a rendszerre (zavart, gondot okozhat)
- Az audit hibás eredményt adhat (sérült, hibás auditáló eszközök stb.)
- Elkerülés
 - Megfelelő tervezés
 - Auditor hozzáférése: csak olvasás, ezen túli hozzáférés csak másolaton (a másolatok az audit után megsemmisítendőek!)
 - Az audit eszközök sértetlensége problematikus! (Elkülönített tárolás ill. kiegészítő védelem szükséges)
 - Minden körülmény és eljárás dokumentálandó