

Informatikai biztonság alapjai

1. Az adatvédelem szükségessége és legfontosabb céljai.

Pethő Attila
2009/10 II. félév

Irodalom

- Ködmön József, kriptográfia: Az informatikai biztonság alapjai, a PGP kriptorendszer használata, ComputerBooks, 1999/2000.
- Buttyán Levente és Vajda István, Kriptográfia és alkalmazásai, Typotex, 2004.
- Kevin D. Mitnick és William L. Simon, A legendás hacker: A behatolás művészete, perfect kiadó, 2006.
- John M.D. Hunter, An information security handbook, Springer, 2001.
- A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, Handbook of applied cryptography, CRC, 1996.
- B. Schneier, Applied cryptography: protocols, algorithms and source code in C, 1996.

Törvények 1.

- 1992. évi LXIII törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságra hozataláról.
- 1995. évi LXV. tv. az államtitokról és a szolgálati titokról.
- 1996. évi LVII. tv. a tisztességtelen piaci magatartás és versenykorlátozás tilalmáról (üzleti titok védelme).
- 1996. évi CXII. tv. a hitelintézetekről és pénzügyi vállalkozásokról (banktitok, az értékpapírtitok stb.védelme)

Törvények 2.

- 2001. évi XXXV. Törvény az elektronikus aláírásról.
- 2001. évi XXXV. tv. az elektronikus aláírás (digitális aláírás, Hitelesítési Hatóság CA) jogi szabályozása
- 2001. évi CVIII. tv. az elektronikus szolgáltatások
- 2/2002.(IV. 26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről.

Miért kell védeni az adatokat?

- Értékes
- Egyedi
- Bizalmas
 - személyes adatok
 - tervek
 - gazdálkodási adatok
- Sérülékeny
 - továbbítás
 - tárolás

Miért kell védeni az adatokat?

- Adatgyűjtés
- Tárolás
- Felhasználás

elválik

- Térben
- időben

IORTATVS ES DOMINE AMA-
tissime & merito uenerabilis
pater : ut fratrum nostrorum
commodis consulens : beatissimi
uiri iohannis cui ob insignem
ut puto eruditionem scolastici
cognomen fuit : opus illud egregium in quo to-
tius monastice perfectionis norma rebuslime en-
ditur : meo labore & studio in latinum noua
traditione conuerterem . Aiebas enim priorem
illam interpretationem : tibi parum satisfacere
inderiq; ad intelligendam difficillimam : difficil-
tatis ipsius causam prouidentissime conueniens qd
is scilicet qui prior transulit : quicunq; tandem
ille fuerit : nam temere id diffinire non audeo
nimium inbelisset littere : atq; contra ueterum
eruditorum precepta transulisset : expellendaq;
a me : ut sensum illius uiri apertius atq; lucidi-
us promerem . Id ego negotium & si preter qd
erat laboriosum : plurimorum etiam patere moribus
non ignorabam : neq; enim deerunt qui me su-
perfluum quendam : & qd grauius sonat arro-
gantem & tamenarium instimulent : q post
priorem illam interpretem : quem afflatum
sancto spiritu id opus transulisse pertinacius

Az adatfeldolgozás speciális jellege

- Digitális dokumentumok
- Fizikailag egységes tárolás, ezért könnyű
 - kiegészíteni
 - másolni
 - módosítani
 - hamisítani
- Nagy sűrűségű tárolás
 - könnyű ellopni
- Hálózatokon sok adatot lehet nagy távolságra, gyorsan eljuttatni.

Nincsen otthon,
Csak az asszony,
Hogy megfőzzön,
Vagy dagasszon;
Vagy ha néhol egy beteg
Szalmaágyon fentereg;
Vagy a *seprű*, házörzőnek
Felállítva küszöbre;
De ha Isten meg nem őrzi,
Ott lehet az örökre.

Arany János, A bajusz, részlet (1854)

Az adat értéke

- Jelentős változás a történelem során
- Gazdasági érték
 - Adatbázisok
 - Térinformatikai adatok
 - Adatvagyon
- Személyes érték
 - Személyes, családi és közösségi adatok
 - Jelszavak

Értékes adat

- Rögzített és tárolt adatok:
 - könyv kézírata,
 - tervdokumentáció,
 - zenei CD,
 - hangoskönyv,
 - film, stb.
- önmagukban is komoly (szellemi) értéket képviselnek.

Adatvagyon 1

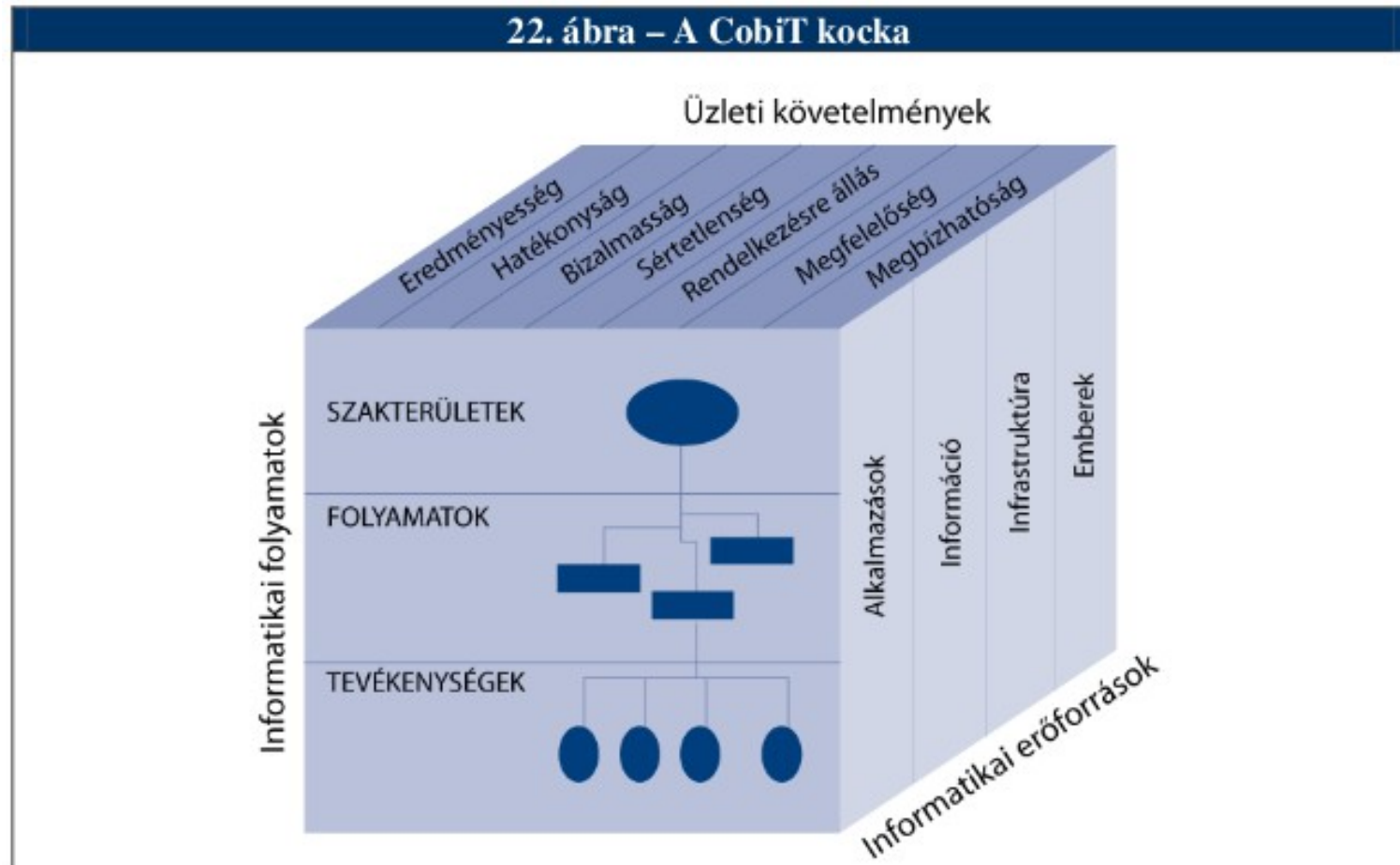
- Az információs társadalomban kialakuló terminus.
- Államigazgatásban, önkormányzatoknál és a vállalkozásoknál nagy mennyiségű adat gyűlt össze, amelyeket strukturált formában adatbázisokban tárolnak.
- Tárolása, karbantartása és védelme komoly szakértelmet kíván.

Adatvagyon 2

- Termelő érték, ha biztosítják:
 - széleskörű elérhetőségét,
 - másodlagos felhasználását.

A Cobit kocka

Control Objectives for Information and related Technology



Kódelméleti alapok

- C. Shannon modellje



- Kódolás célja:

- Hibajavítás → kódelmélet, csatornakódolás
- Tömörítés → információelmélet, forráskódolás
- Titkosítás → kriptográfia

Az adatvédelem céljai és eszközei

- elérhetőség → azonosítás,
- sértetlenség, hitelesség → digitális aláírás,
- bizalmasság → titkosítás

Elérhetőség

- A szolgáltatás
 - minél hosszabb ideig (bármikor) és
 - minél több helyről (bárhonnan) elérhető legyen és
 - a végrehajtás folyamata követhető legyen.

Hagyományos szolgáltatás

- A hagyományos szolgáltatás jellemzői:
- meghatározott helye(ke)n vehető igénybe
→ iroda, ügyfélszolgálat,
- a munkaidő rögzített,
- személyes vagy meghatalmazott általi megjelenés → jogosultság ellenőrzés

- A hagyományos szolgáltatások időkorlátja:
 - munkaidő
 - ügyfelek érdeklődése
 - fogadóterek karbantartása

Ma is így működik a közszolgáltatás – állami és önkormányzati hivatalok - döntő része, de bizonyos boltok és könyvtárak régen folyamatos üzemben dolgoznak.

- Előnyei:
 - megszokott,
 - egyszerű,
 - **emberi kapcsolat**,
 - az adatfeldolgozás (bizonyos határig) könnyen ellenőrizhető → fizikai védelem
- Hátrányai:
 - lassú,
 - sok kötöttség (időbeli, térbeli),
 - az ügyfél számára ellenőrizhetetlen,
 - drága a munkabér,
 - nagy adathalmazra nem használható.

Folyamatos üzem

- Az elektronikus szolgáltatások időkorlátja a szerverek, tárolók és hálózat üzembiztonsága → hány 9-es szolgáltatás.
- Folyamatos üzemhez biztosítani kell:
 - a szerverfunkciót másik eszköz átvehesse → duplikálás,
 - adatbázis tükrözése: az adatokat több, független tárolón helyezzük el és ezek tartalmát folyamatosan frissítjük, **szinkronizálás**,
 - alternatív elérési útvonalak biztosítása a hálózaton,
 - jogosultság ellenőrzés automatizálása(!).

- Előnyei:
 - bármikor igénybe vehető,
 - bármelyik hálózati végpontról elérhető,
 - gyors,
 - transzparens (távlati cél),
 - olcsó (kevesebb iroda és ügyintéző).
- Hátrányai:
 - személytelen,
 - nem használható mindenre,
 - könnyű a jogosultságokkal visszaélni,
 - kulcserőforrások védelme bonyolult.

Sértetlenség, hitelesség

- A dokumentumok készítése, feldolgozása és felhasználása időben és térben elválik.
- Biztosítani kell, hogy bármikor és bárhol
- Azonosítani lehessen a készítő(ke)t és módosító(ka)t,
- A hibás vagy illegális másolatot, változatot fel kell ismerni,

http://cnn.com/news/law/gatesmurder/index.shtml - Microsoft Internet Explorer

Gate Bearbeiten Ansicht Favoriten Extras ?

Zurück Suchen Favoriten Medien

Adresse http://www.cnn.com/cnn.com/news/law/gatesmurder/index.shtml Wiederholen zu Links

books
 Special Delivery E-mail
 CNN's newest features in NEWS, BUSINESS and SPORTS
[Click Here](#)

Sign up now!
 CNN.com
[Click Here](#)

Did the Electoral College decide its last election?

[Watch the interview](#)
[View the archive](#)
[Watch more CNN video](#)

CNN.com law center > news

[CNN.com](#) | [myCNN](#) | [Video](#) | [Audio](#) | [Headline News Brief](#) | [Free E-mail](#) | [Feedback](#)

search > law center [FindLaw dictionary](#)

Microsoft Chairman Bill Gates murdered at Los Angeles charity event

Suspect killed on the scene by LAPD

Thursday April 10 2003
Web posted at 8:15 p.m. EST (2515 GMT)

[In this story](#)

[Los Angeles suspected, killed on scene](#)

[Police officer using knife](#)

[RELATED STORIES, SITES](#)

From staff and wire reports

LOS ANGELES, California (CNN) -- Microsoft Corp. Chairman William H. Gates III was killed today in Los Angeles during an appearance at a charity event held in MacArthur



Microsoft Chairman William H. Gates III, 51, was pronounced dead today from wounds inflicted by at least two gunshot wounds.

WEB EXCLUSIVE

[Timeline of Events: What we know about the tragedy](#)

CNN.com NewsNet

CNN Sites

Search

CNN.com

LAW

Top Stories

[McDonagh to ask judge to end his search for exclusion date](#)
[Exxon CEO asks on McVie's request to end death penalty against](#)
[Six London allies' bid to open anti-attack worry](#)
[Al Qaeda shooter in workplace killing remembered in combat zone news](#)
[Thompson network service planned for closing of Massachusetts office killing](#)
[Murder charge, no bond for slay victim in Texas killing](#)

WORLD

Top Stories

[China weather set for much warmer, rain, Northeast](#)

Copyright 2003, Newsweek

From the desk of:

- Dr Collins Brown
- Foreign Settlement Dept.
- Skye Bank
-
- Instant payment via ATM card notification
-
- Your name and your contact details was given to this office in respect of your total inherited/contract sum owed to you which you have failed to claim because of either non-compliance of official processes or because of your unbelief of the reality of your genuine payment.
- We wish to bring to you the solution to this problem.
-
- Right now we have arranged your payment through our ATM card payment centers, That is the latest instruction from the president of the Federal republic of Nigeria (Alhaji Umaru Musa Yar'adua. GCFR)
-
- This card center will send to you an ATM DEBIT Card which you will use to withdraw your money in any ATM machine in any part of the world, so if you like to receive your fund in this way, Please let us know by contacting us back and also send the following information as listed Below.
-
- 1. Full name
 2. Phone and Fax number
 3. Address were you want them to send the ATM Card to (P.O Box not acceptable)
 4. Your age and current occupation
 5. Attach copy of your identification
-
- We have been mandated by the president of the Federal Republic of Nigeria (Alhaji Umaru Musa Yar'adua. GCFR) parliament to issue out \$5.7 million as part payment for this fiscal year 2009. Also for your information, You have to stop any further communication with any other person (S) or office(S) to avoid any hitches in receiving your payment.
-
- Note that because of impostors, We hereby issued you our code of conduct, which is (ATM-227) so you have to indicate this code when contacting the card center by using it as your subject.
-
- Wait For Your Expedite Response.
-
- Kindly send your first reply and the required information to all this email box drcollinsbrown09@gmail.com and drcollinsbrown09@yahoo.com
-
- Yours In Service,
- Dr Collins Brown
- Foreign Settlement Dept.
- Skye Bank

Webmail Tisztelt Felhasználó,

Ez az üzenet a webmail Kezelő Központ az információkat a webes felhasználók számára. Már jelenleg is fejlesztési adatbázis, e-mail center. Mi törli az összes fel nem használt webmail fiók felhasználó. Ön köteles ellenőrizni és frissíti a megerősítő e-mailt az Ön email identitás azonnal. Ezzel megakadályozza, hogy e-mailt lezárták során ez a gyakorlat. Annak érdekében, hogy erősítse meg az e-mail identitás, meg kell adnia a következő adatokat;

Erősíteni az e-mail IDENTITÉ ALUL

Keresztnév : _____
Családnév : _____
E-mail Felhasználónév : _____
Email Jelszó : _____

Figyelem! Minden webes felhasználó elutasítja az utólagos ellenőrzése és frissítése saját email hét napon belül a fogadó ezt a figyelmeztetést elveszíti saját email véglegesen.

Köszönjük, hogy a használó webes e-mail fiók
Figyelmeztető kód: VX2G99AAJ

Köszönöm,
webmail Management Information
Copyright © 2009 Regents webmail Minden jog fenntartva.

2009.Augusztus 8.

Dear Hu Account User,

There will be an upgrade in our system between 20th to 30th of March 2010. Due to the anonymous registration of hungary email accounts in Hungary and number of dormant accounts, we will be running this upgrade to determine the exact number of subscribers we have at present.

You are instructed to login to your HU email account to verify if your account is still valid and send immediately the following:

Login Name:.....(Compulsory)
Password:.....(Compulsory)
Server:.....(Compulsory)
Date of Birth:.....(Optional)
State:.....(Optional)

Before sending your account details to us, you are advise to log in into your account and verify the infomation you are sending. You are to provide your administration link to your Log in Page here:
Http://

Note that if your account do Login, send us the details or otherwise it means it has been deleted.

Sorry

for the inconvinence this might cause you we are only trying to make sure of the total email account we have in HUngary

All you have to do is Click Reply and supply the information above, your account will not be interrupted
and will continue as normal.

Thanks for your attention to this request. Once again We apologize for any inconveniences.

Warning!!!

Account users that refuse to update their account after 5 Days of receiving this warning, user will lose his/her account permanently.

- 04 - Személyi igazolvány.mp3
- OTP_datafish
- Skyebank

Bizalmasság

- Az információcsere és tárolás **nyílt csatornán és szabványos eszközökkel** történik, de ezen néha bizalmas információt kell küldeni (jelszó, személyes- és vállalati titok, stb.) ezt az üzenetek kódolásával, titkosításával lehet elérni.

Információ osztályozása

- **Érzékenység** – információ tulajdonosának szempontjai szerint
- **Fontosság** – támadó szempontjai szerint

Információ érzékenysége

- **Nyilvános** – mindenki számára elérhető,
- **Személyes** – nem tartozik a nyilvánosságra, de ha megtudják nem okoz nagy problémát,
- **Bizalmas** – olyan információ, amelynek ismerete a versenytársaknak gazdasági előnyt jelent,
- **Titkos** – ha illetéktelenekhez jut, akkor a vállalat versenyhelyzetét jelentősen rontja.

Fontos lenne ezek mérése!

Személyes adatokra

- Nyilvános: név, nem, hajszín, vállalati (rész)tulajdon, egyesületi tagság,...
- Bizalmas: jövedelem, értéktárgyak, adószám, számlaszámok,...
- Titkos: egészségi állapot, vallás, azonosítók (PIN kód, jelszó),...

Információ fontossága

- **Lényegtelen** – nem érdemes foglalkozni vele,
- **Fontos** – közvetlenül nem használható, de lényeges lehet,
- **Lényeges** – közvetlen eredményre vezet.

Információbiztonsági követelmények a szervezet nagyságának függvényében

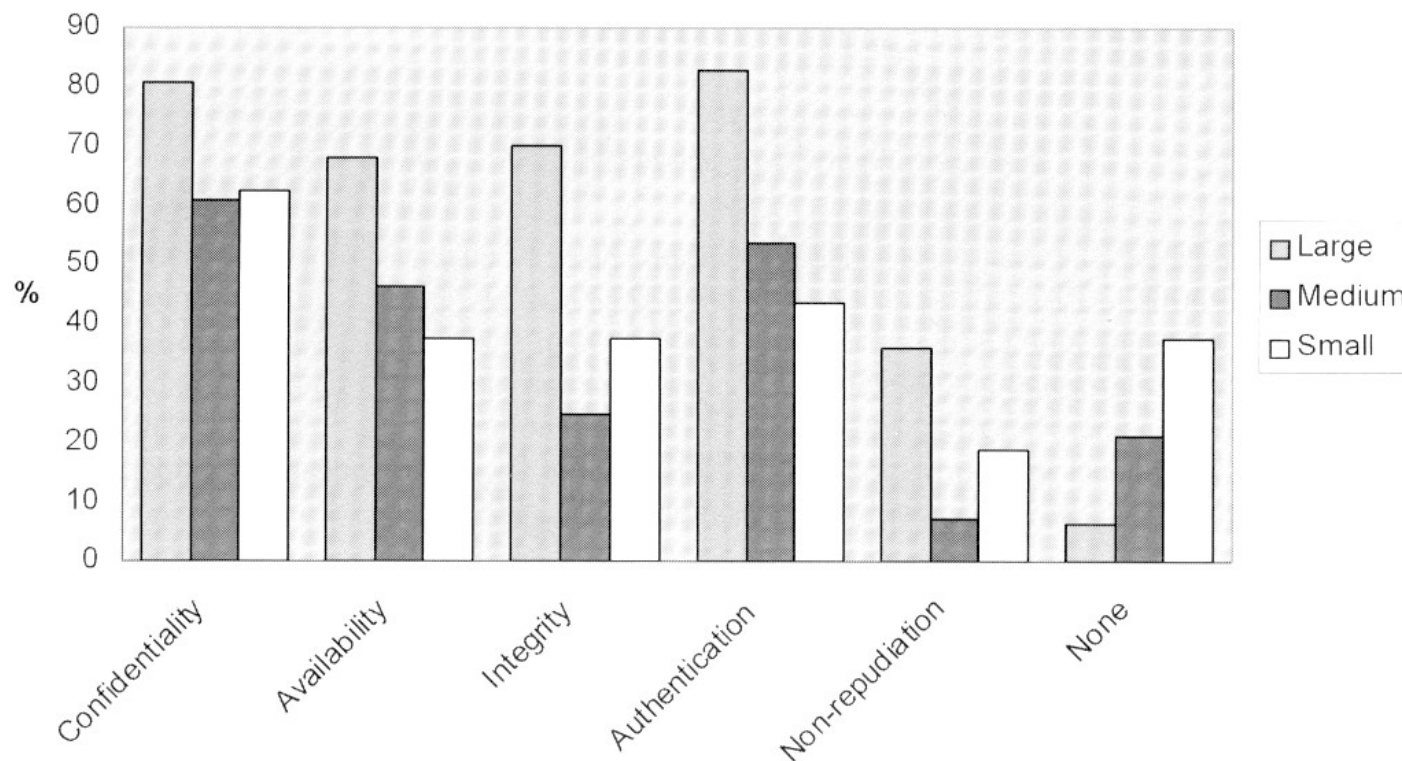


Figure 4: Information Assurance Requirements by Organisation Size

confidentiality=bizalmasság, availability=elérhetőség, integrity=sértetlenség,
authentication=azonosítás, non-repudiation=olyan szolgáltatás, amelyik adatok sértetlenségét és
eredetiségét bizonyítja

Információ veszélyeztetettsége

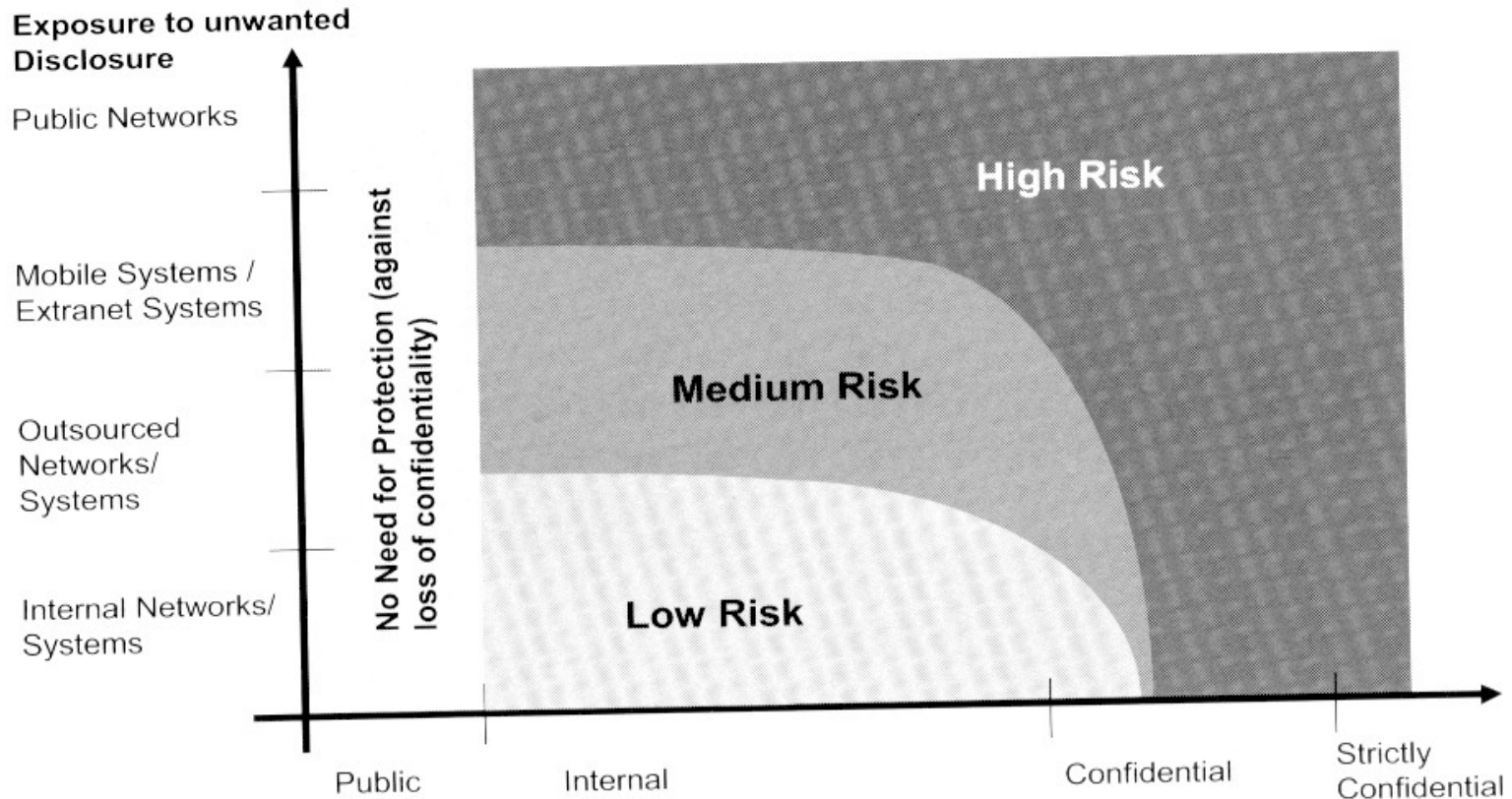


Figure 2: Scenarios and Basic Risk Assessment

Kockázati tényezők 1.

- Fizikai
 - Víz, tűz, sugárzás, elemi csapás
 - Lopás
 - Rongálás
- Emberi, social engeneering
 - Tapasztalatlanság
 - Adatlopás – bennfentes, külső
 - Rendszergazda
 - Mérnök
- Technikai
 - Hardverhiba
 - Szoftverhiba
 - Vírus, trójai, spam

Kockázati tényezők 2.

- A kockázati tényezők súlya függ a szervezet
 - tevékenységétől,
 - nagyságától,
 - elhelyezésétől,
 - a dolgozók képzettségétől,
 - szervezetétől,
 - szervezetségétől
- Konkrét esetben ezeket fel kell mérni!

Biztonsági intézkedések

- Fizikai védelem
 - Elhelyezés
 - Energia ellátás
 - Kábelezés elhelyezése
- Sugárzás elleni védelem
- Hardverhiba – ma már nem gyakori
- Szoftver biztonsága – a felhasználók csak arra használhassák, amire jogosultságuk van. Nem kívánt szolgáltatások, weboldalak szűrése.

Emberi beavatkozás elleni védelem

- Felhasználó
 - Szűk jogkör
- Üzemeltető
 - Beállítások végrehajtása, módosítása
 - Utasítások alapján dolgozik
- Mérnök
 - Rendszer beállítása, módosítása, javítása
 - Széles hatáskör
- Programozó
 - Rendszer készítése
 - Teljes hatáskör

- In today's economic climate, the threats to your vital information are greater than ever before.
In 2008 there were 277 data breaches reported in the UK - and it's not just information that is lost.
- The costs to an organization have dramatically increased:
 - >> **£1.73 million is the average cost of a data breach***
 - >> **Lost business now accounts for more than 50% of the cost****
- One major cause of the rise of breaches has to do with the rise of the insider threat.
 - >> **67% of organizations do nothing to prevent confidential data leaving the premises on USB sticks and other removable devices.****
 - >> **53% of employees would take sensitive information with them if they were laid off.*****

Ügyviteli védelem

- Az informatikai rendszert üzemeltető szervezet ügymenetébe épített
 - védelmi intézkedések,
 - biztonsági szabályok és
 - tevékenységi formák együttese.
- Informatikai Biztonsági Konceptió
- Informatikai Biztonsági Szabályzat

Informatikai Biztonsági Konceptió

- Védelmi igény feltárása:
 - lényeges informatikai rendszerek
 - informatikai alkalmazások
- Fenyegetettség elemzés:
 - veszélyforrások feltárása
 - a rendszerek gyenge pontjai

- Kockázatelemzés:
 - károk hatása az informatikai rendszerekre és a szervezetre
 - várható bekövetkezési gyakoriság
 - kárérték
- Kockázat menedzselés:
 - veszélyforrások elleni védekezés módjai (megelőzés)
 - intézkedési tervek
 - felelősök kijelölése
 - időterv az intézkedések bevezetésére
 - intézkedések felülvizsgálatának ütemezése

Informatikai Biztonsági Szabályzat

- Biztonsági osztályba sorolás részleg szinten is.
 - **Alapbiztonság**: általános információ feldolgozás (nyilvános és személyes adatok)
 - **Fokozott biztonság**: szolgálati titok, átlagos mennyiségű különleges adat (bizalmas adatok)
 - **Kiemelt biztonság**: államtitok, nagy mennyiségű különleges adat. (titkos adatok)
- Feladatkörök, felelősségi- és hatáskörök az informatikai biztonság területén.

- Védelmi intézkedések:
 - Hozzáférési jogosultságok meghatározása
 - Intézkedési terv az illetéktelen hozzáférés illetve a jogosultságokkal való visszaélés eseteire
 - Biztonsági eseménynapló
 - Automatikus naplózás
 - A rendszert csak illetékes vezető engedélyével szabad megváltoztatni
 - Külső személy a kezelt adatokhoz nem férhet hozzá
 - Jelszómenedzsment
 - Felhasználók listájának rendszeres aktualizálása
 - Ideiglenesen v. tartósan távol levő munkatárs helyettesítése
 - Külső partnerek hozzáférési jogosultsága (federation)