IT biztonság
2020/2021 tanév ősz

2020.09.05. ELTE IT BIztonság Speci

Bemutatkozás

NOREG Információvédelmi Kft.
SZIGORÚAN BIZALMAS

E-GROUP
SECURE
BUSINESS AUTOMATION

SOPHOS

IBM

BALASYS

H1 SYSTEMS

brightdea.hu

2020.09.05. ELTE IT BIztonság Speci

A kurzus célja

- Ismertetjük a vállalati IT biztonsági rendszerek feladatait, elemeit, felépítését. A téma tárgyalása során kiemelten kezeljük a *módszertani, irányítási szempontokat*. Bemutatjuk a biztonsági rendszerelemek működési elvét, valamint az egyes védelmi intézkedések bevezetésének és üzemeltetésének lépéseit.
- *Nem hacker tanfolyam*!!!

  Heti 90 percben lehetetlen

- A cél egy *szemléletmód átadása*
- Informatikusként tudni kell, hogy milyen eszközei, lehetőségei vannak a „sötét oldalnak”
- Programozóként meg aztán pláne! Programozók írják a programokat (amiket aztán a hackerek támadnak.)

Agenda

- Az információbiztonság alapjai
- Az információbiztonság irányitási rendszerei
- Sérülékenység elemzés és kezelés
- Kriptográfiai protokollok
- Határvédelmi technológiák
- Behatolásvédelem
- Üzemeltetés biztonság
- Fizikai biztonság
- Vírusvédelem
- Dokumentumvédelem

Fejezetek:

- Biztonsági kockázatok elemzése
- Szabályozások, módszertanok
- Naplófeldolgozás és elemzés
- Incidens menedzsment
- Szervezetek és biztonság-tudatosság, GDPR
- SSH/TLS

Előfeltételek

- Alapvetően nincs, de előnyt jelent
  - Valamilyen programozási nyelv közép szintű ismerete
  - Felhasználói szintű linux ismeret
  - Hálózati alapismeret (TCP/IP)
- A tárgy sikeres elvégzése

  SOK-SOK MUNKA

Számonkérés

- A félév végén egy **vizsgateszt** (feleletválasztós, 4 lehetőségből mindig egy a helyes)

A tárgy honlapja

- Az előadások anyaga (és egyéb):
  http://compalg.inf.elte.hu/~attila/Teaching.html
  lapon.

Miért fontos az IT biztonság?

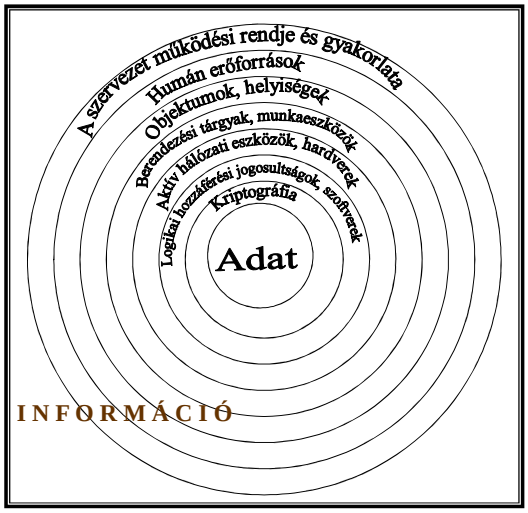
- A szervezetek informatika nélkül működésképtelenek
- Az informatikai függőség egyre nagyobb
- Az informatikai rendszerek fenyegetettsége kritikus
- A szervezeti adatok mindig informatikai adatok
- Létszükséglet a szolgáltatások folytonossága és az adatok bizalmas kezelése

Információbiztonság

Az információbiztonság az információ számos különféle "bizalmi" aspektusával foglalkozik. Az információbiztonság nem korlátozódik a számítógépes rendszerekre, sem az elektronikus vagy gépi úton olvasható információkra. Az információ vagy adatok bármilyen formában történő megőrzésére vagy védelmére vonatkozik.

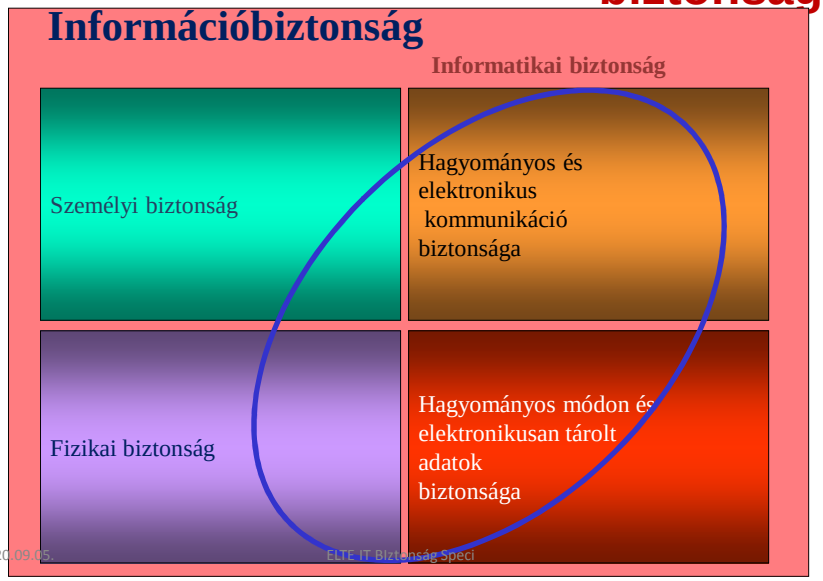
www.wordIQ.com

Adat vs. információ



Mindig az információt védjük!!!

Információbiztonság vs. informatikai biztonság



Informatikai biztonság

Az informatikai biztonság a védelmi rendszer olyan, a védő számára kielégítő mértékű állapota, amely az informatikai rendszerben kezelt **adatok** bizalmassága, hitelessége, sértetlensége és rendelkezésre állása, illetve a **rendszerelemek** rendelkezésre állása és funkcionalitása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

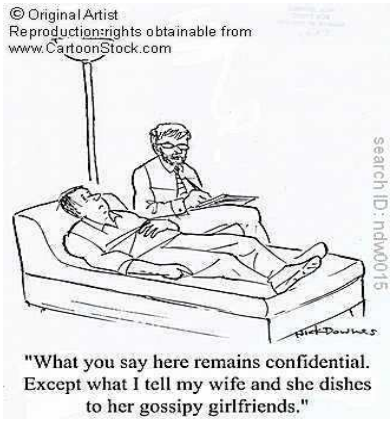
Információ/adatbiztonság

Amit meg kell őrizni:

- Bizalmasság (titkosság)
- Sértetlenség (változtatás nem történt, hiteles az adat, információ valódisága, letagadhatatlan, elszámoltatható)
- Folyamatos rendelkezésre állás (megbízhatóság, megbízható működés)
- Funkcionalitás (szolgáltatás minősége)

Az első hármat CIA-elvnek is nevezik (Confidentiality, Integrity, Availability)

Bizalmasság



Az információ/adat esetében a bizalmasság azt jelenti, hogy azokhoz csak az arra jogosultak és csak az előírt módokon férhetnek hozzá.

Sértetlenség

Az információt/adatot csak az arra jogosultak, szabályozott módon változtathatják meg.

Rendelkezésre állás

Az a tényleges állapot, amikor egy informatikai rendszer szolgáltatásai állandóan, illetve egy meghatározott időben rendelkezésre állnak, és a rendszer működőképessége sem átmenetileg, sem tartósan nincs akadályozva.

Biztonság és kockázat

- Nincs teljes biztonság, csak minimális kockázat.
- A biztonság nem más, mint **tudatos kockázatvállalás**

Szótár

- Fenyegetés – **Threat**
- Sérülékenység – **Vulnerability**
- Kockázat – **Risk**
- Védelmi intézkedés – **Countermeasure**
- Védelem – **Safeguard**
- Vagyontárgy – **Asset**
- Kitettség – **Exposure**

Biztonsági alapelvek

- Ismerd meg magad és az ellenséged
- A biztonság kompromisszumok kérdése
- Mindent nem védhetünk 100%-os biztonsággal
- A védelem legyen egyenszilárdságú
- A védelem ne kerüljön többe, mint a védendő érték
- A biztonság nem egy állapot, hanem egy folyamat
- Mindig az egyszerű megoldást válasszuk
- Legyen a védelem több szintű

Információbiztonság, mint folyamat

1. Információvagyon felmérése, értékelése
2. Fenyegetések számba vétele
3. Kockázatok meghatározása
4. Kockázatok kezelése
5. Védelmi intézkedések foganatosítása
6. Védelmi intézkedések nyomon követése
7. GOTO 1

Védelmi intézkedések

Elvárások:

- Teljes körű (a rendszer összes elemére)
- Zárt (minden fenyegetés)
- Folytonos (megszakítás nélkül)

PreDeCo-elv

- Preventív intézkedések
  - Pl.: biztonsági frissítések telepítése
- Detektív intézkedések
  - Pl.: IDS rendszerek
- Korrektív intézkedések
  - Pl.: backup/visszaállás

Védelmi kontrollok

- Adminisztratív kontrollok
  - Policy-k, eljárások, oktatás
- Fizikai kontrollok
  - Backup-ok, kábelezés, kontroll zónák
- Technikai/Logikai kontrollok
  - Hálózati architektúra, tűzfalak, titkosítás, rendszeres audit

Adminisztratív védelem

- Törvények
- Szabványok, műszaki normák
- Ágazati végrehajtási utasítások
- Helyi szabályzatok
  - Informatikai Szabályzat
  - Dokumentumkezelési Szabályzat
  - Katasztrófa-elhárítási terv

Fizikai védelem

- Vagyonvédelmi megoldások
  (videó, beléptető, behatolás-jelző…)
- Tűzvédelem
  (tűzjelző és oltórendszer…)
- Üzemeltetés védelem
  (szünetmentes megoldások, redundancia…)

Technikai/Logikai védelem

- Informatikai betörésvédelmi megoldások
- Mentési rendszerek, archiválás
- Vírusvédelem
- Jogosultságkezelés
- Titkosítás, kriptográfia
- Tűzfal
- …

Az informatikai biztonsági környezet

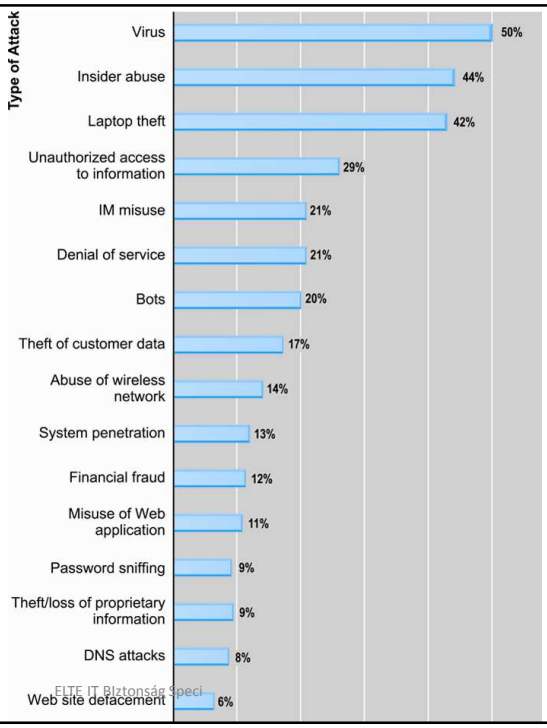
A **fenyegetettség** állapota:

ha az informatikai biztonsági környezet valamely eleme olyan állapotban van, hogy fennáll a bizalmasság, a sértetlenség, vagy a rendelkezésre állás sérülése, akkor az adott elem a fenyegetettség állapotába került
ez az állapot éppen ellentétes a biztonságéval,
a fenyegetettség állapotában az informatikai biztonsági rendszer elemét – illetve a sikeres támadáshoz szükséges titkot, kulcsot, stb. – *felfedhetik*, *módosíthatják*, vagy *megsemmisíthetik*

Honnan származnak a fenyegetések?

- Belső támadók
  - Hitelesített felhasználók, akik olyan adatokhoz vagy erőforrásokhoz akarnak hozzáférni, ami sérti a legkevesebb jogosultság elvet.
  - Lehet szándékos vagy vétlen támadás.
  - A belső támadók veszélyesebbek.
- Külső támadók:
  - Nem hitelesített felhasználók, akik a hitelesítési eljárások megkerülésével férnek hozzá az adatokhoz.
  - Hackerek, crackerek…

Honnan származnak a fenyegetések? (Cybercrime)



Source: Based on data from Computer Security Institute, 2009.

Mekkora a veszteség per alkalom?

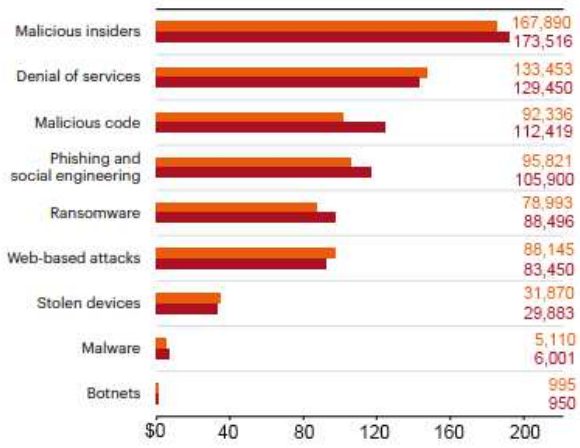


FIGURE 12
Average annualized cyber crime cost weighted by attack frequency

Legend
Consolidated view
n = 254 separate companies

FY 2016
FY 2017

Mekkora a veszteség összesen?

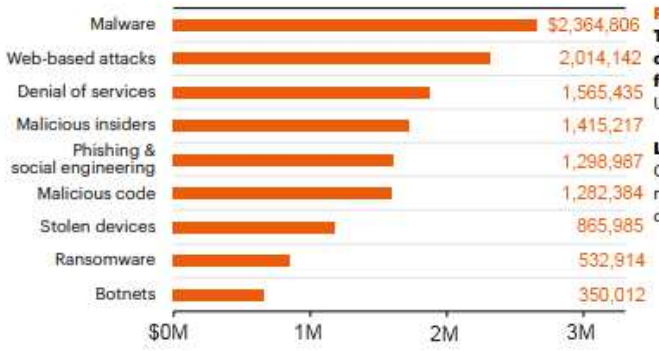


FIGURE 13
Total annualized cyber crime cost for attack types
US$ millions

Legend
Consolidated view
n = 254 separate companies

Fenyegetés típusok

- A fenyegetések kihasználásával egy támadó hozzáférést szerezhet a rendszerhez, alkalmazásokat futtathat, információt olvashat, hozhat létre, adhat hozzá és törölhet.
- Néhány példa lehetséges fenyegetésekre:
  - **Adat remanencia (data remanence):** Akkor következik be, ha egy mágneses adattárolót felülírtak vagy töröltek, de továbbra is kinyerhető belőle információ. http://en.wikipedia.org/wiki/Data_remanence
  - **Átejtés (spoofing):** Akkor következik be, amikor egy személy vagy egy alkalmazás másnak adja ki magát az adatok meghamisításával, így szerezve jogosulatlan hozzáférését. Pl. az IP spoofing során a támadó hamisított IP címmel megbízható hosztnak adja ki magát. http://en.wikipedia.org/wiki/Spoofing_attack

Fenyegetések

- **Beágyazás (tunneling):** Egy biztonsági rendszer megkerülése alacsonyszintű rendszerfunkciók elérésével. Pl. HTTP tunelling, melynek célja legális forgalomba ágyazott nem legális tartalommal kikerülni a tűzfalat. http://en.wikipedia.org/wiki/Tunneling_protocol
- **Célzott adatbányászat (targeted data mining):** Adatbázisok áttekintése meghatározott információkért, melyek érzékeny adatokat szolgáltathatnak a rendszerről. http://en.wikipedia.org/wiki/Data_mining
- **Fizikai hozzáférés (physical access):** Fizikai hozzáférés egy hálózathoz, berendezéshez vagy támogató rendszerhez.
- **Hátsókapu (backdoor):** Olyan szoftverbe vagy hardverbe épített eljárás, melynek segítségével ki lehet kerülni az adott entitás hitelesítési eljárásait. http://en.wikipedia.org/wiki/Backdoor

Fenyegetések

- **Jelszótörés (password cracking):** olyan eljárás, melynek segítségével a hitelesítést szolgáló jelszavak visszaállíthatók, pl. gyenge lenyomatból vagy brute force módszerrel. http://en.wikipedia.org/wiki/Password_cracking
- **Kártékony kód (malicious code):** Olyan kód, mely végrehajtása közben megsérti a biztonsági szabályzatot, és a felhasználó tudta nélkül károkat okoz.
  http://en.wikipedia.org/wiki/Malware
- **Kémkedés (spying):** Hagyományos eszközökkel (pl. mikrofon, kamera) elkövetett jogosulatlan információszerzés.
  http://en.wikipedia.org/wiki/Spying
- **Kifigyelés (shoulder surfing):** Érzékeny adatok direkt leolvasása a képernyőről.
  http://en.wikipedia.org/wiki/Shoulder_surfing

Fenyegetések

- **Kisugárzás (emanation):** A hardvereszközökből származó elektromágneses sugárzásból visszaállított információk megszerzése. http://en.wikipedia.org/wiki/TEMPEST
- **Közbeékelődéses támadás** (man-in-the-middle attack): olyan támadás, ahol a támadó a két fél közé, számukra láthatatlanul kapcsolódva mindegyik fél felé a másik partnerének adja ki magát. http://en.wikipedia.org/wiki/Man-in-the-middle
- **Kukabúvárkodás (dumpster diving):** A támadás célja leselejtezett (vö. kidobott) iratokból érzékeny információk visszaállítása. http://en.wikipedia.org/wiki/Dumpster_diving
- **Lehallgatás (eavesdropping):** a hálózat adatforgalmának monitorozása abból a célból, hogy érzékeny adatok birtokába jusson a megfigyelő.
  http://en.wikipedia.org/wiki/Eavesdropping

Fenyegetések

- **Megszemélyesítés (impersonation):** a támadás során a támadó egy hitelesített személynek adja ki magát, így szerez nem hitelesített hozzáférést, pl. lopott jelszóval.
  http://en.wikipedia.org/wiki/Impersonation
- **Mobil kód (mobile code):** Olyan szoftver, ami a hálózaton keresztül érkezik, és a helyi gépen hajtódik végre, általában a felhasználó engedélyével, de károkat okozhat a tudta nélkül. Pl. rosszindulatú ActiveX vezérlők.
  http://en.wikipedia.org/wiki/Mobile_code
- **Objektum újrafelhasználás (object reuse):** Az a lehetőség, hogy egy érzékeny adat rendelkezésre áll egy nem hitelesített felhasználónak, pl. egy érzékeny adat megmarad a swap memóriában, amit a gép egy másik felhasználója is láthat.

Fenyegetések

- **Buffer túlcsordulás (buffer overflow):** Egy alkalmazás több adatot ír a memóriaterületére, mint amennyit lehetne, így felülír esetlegesen más alkalmazáshoz tartozó érzékeny memóriaterületet. A felülírás pl. tartalmazhat kártékony kódot vagy kikerülhet hitelesítési eljárást.
  http://en.wikipedia.org/wiki/Buffer_overflow
- **Rejtett csatorna (covert channel):** Olyan kommunikációs csatorna, melyen a legális csatornák kapacitását használva nem engedélyezett adatforgalom halad keresztül. Az időzített csatornán az adás előfordulása, a tárolási csatornán a memória adott területének írása/törlése szolgáltat információt.
  http://en.wikipedia.org/wiki/Covert_channel

Fenyegetések

- **Személyes ráhatás (social engineering):** olyan gépfüggetlen eljárás, melynek lényege az, hogy a támadó a rendszerrel dolgozó emberektől megszerzett adatok segítségével tör be a rendszerbe. http://en.wikipedia.org/wiki/Social_engineering
- **Szimatolás (sniffing):** Információszerzés a hálózati csomagok elfogásának segítségével. A lehallgatással szemben (ami általános hálózati forgalomra vonatkozik) a szimatolás kimondottan csomagkapcsolt hálózatokra értelmezhető.
  http://en.wikipedia.org/wiki/Packet_sniffer
- **Visszajátszás (replay):** A hitelesítési eljárás kijátszása egy hálózati csomag elfogásával és későbbi visszaküldésével. http://en.wikipedia.org/wiki/Replay_attack

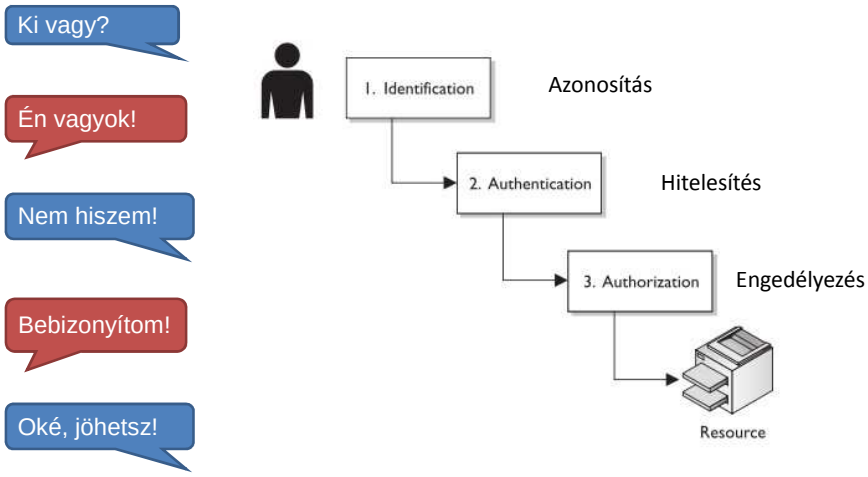
Fenyegetések 2020

1. **Cloud Vulnerability**
   - Érzékeny adatok a felhőben
2. **AI-Enhanced Cyberthreats**
   - Adaptív kártékony kódok
3. **Blockchain based small contracts**
   - Kódot tartalmaz
4. **Social engineering attacks**
5. **Fakenews**

Hozzáférés-ellenőrzés

- A hozzáférés-ellenőrzés olyan biztonsági mechanizmusok gyűjteménye, amely meghatározza, hogy a felhasználók mit tehetnek a rendszerben, azaz milyen erőforrásokhoz férhetnek hozzá, és milyen műveleteket hajthatnak végre.
- Azok a védelmi intézkedések tartoznak ide, melyek szabályozzák, hogy egy felhasználó
  - milyen felhatalmazással férhet a rendszerhez,
  - milyen alkalmazásokat futtathat,
  - mit olvashat, hozhat létre, adhat hozzá és törölhet egy információból.
- Három lépésből áll:
  - azonosítás (identification) ,
  - hitelesítés (authentication),
  - engedélyezés (authorization)
- A hozzáférés-ellenőrzés része az elszámoltathatóság.

Azonosítás, hitelesítés, engedélyezés



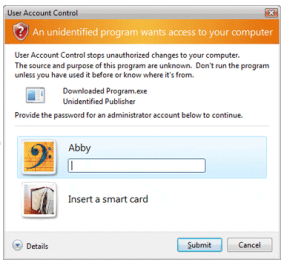
McGraw-Hill: CISSP All-in-One Exam Guide 3rd Edition (Osborne Media)

Hozzáférés-ellenőrzés elvei

- Feladatok szétválasztása (Separation of Duties)
  - Célja, hogy egy folyamat lépéseit különböző személyek végezzék el.
  - Ehhez a folyamatot meg kell tervezni.
  - Megakadályozza, hogy egy személy a teljes folyamatot ellenőrizze és manipulálja.
  - Például egy könyvelési osztályon nem fogadhatja be ugyanaz a személy a számlákat, és nem kezdeményezheti ezek kifizetését.

Hozzáférés-ellenőrzés elvei

- Legkevesebb jogosultság (Least Privilege)
  - Az elv betartásával a rendszer a felhasználók és az alkalmazások erőforrásokhoz való hozzáférését csak a legszükségesebbekre korlátozza.
  - Ehhez meg kell határozni a felhasználók munkájához szükséges jogosultságok minimális halmazát.
  - A felhasználók ehhez a halmazhoz kapnak csak hozzáférést, se többhöz, se kevesebbhez.
  - Példa a Windows User Account Control (UAC) megoldása.



Hitelesítés

- Tudás alapú – Something you **know**
- Tulajdon alapú – Something you **have**
- Tulajdonság alapú – Something you **are**

A jó hitelesítés során a **háromból legalább kettőt**, **egymástól függetlenül** kell használni! Ez az erős autentikáció vagy többlépcsős hitelesítés.

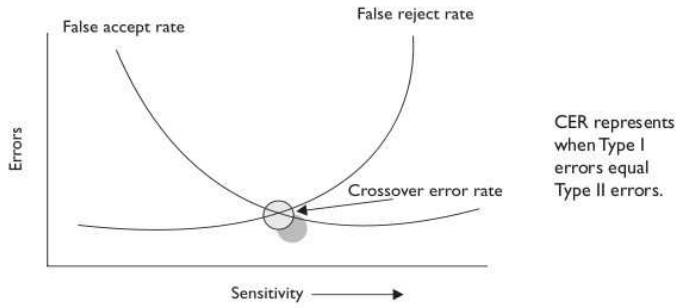
Tudás alapú: Jelszavak

- Jelszó politika (pl. korlátozott élettartam)
- Jelszó menedzsment (ne legyen szótári alakú, kisNAGY+szám+speckar, min8kar, …)
- Jelszó hashelés
- Jelmondatok
- Lehetséges támadások:
  Brute-force vagy szótár alapú támadás, lehallgatás, social engineering

Tulajdonság alapú: Biometria

(Ujjlenyomat, Retina, Írisz, Hang, Tenyér, Aláírás, Arc)

- Type 1 Error (hibás visszautasítási ráta)
- Type 2 Error (hibás elfogadási ráta)

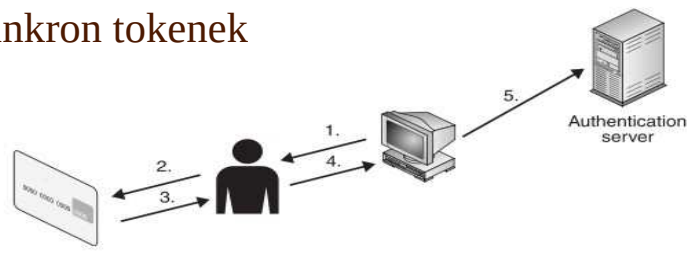


McGraw-Hill: CISSP All-in-One Exam Guide 3rd Edition (Osborne Media)

Tulajdon alapú: One Time Password

One Time Password = Dynamic password

- Szinkron tokenek
  - Számlálón alapuló token
  - Időn alapuló token
- Aszinkron tokenek



McGraw-Hill: CISSP All-in-One Exam Guide 3rd Edition (Osborne Media)

Azonosítás, hitelesítés - módszerek

- Azonosítás

Alapértelmezés: elutasítás (deny/no access)

- Hitelesítés

- **Centralizált**

RADIUS (A kliens fogadja a felhasználói kéréseket, amit egy titkosított csatornán továbbít a szervernek. A szerver hitelesíti a felhasználót - pl. egy LDAP szerveren (http://padre.web.elte.hu/ldap.html) keresztül -, és vissza-küldi a felhasználóra vonatkozó konfigurációs információkat. UDP alapú)

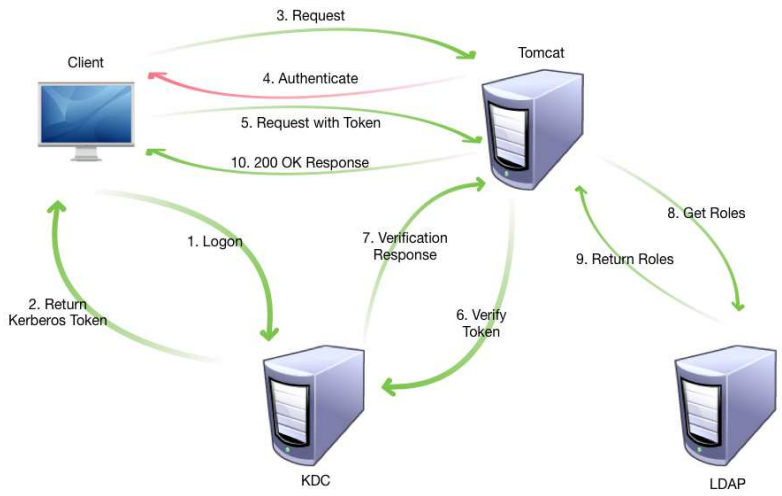
TACACS+ (Terminal Access Controller Access-Control System , TCP alapú, 49-es porton))

Single-sign-on, (SSO) ha egy felhasználó több rendszerhez szeretne hozzáférni

- **Decentralizált**

Kerberos (pl. Microsoft Active Directory, 88-as porton, nem szabványos)

Kerberos séma



Hozzáférés ellenőrzési modellek

- Discretionary Access Control (DAC)
  - Az objektum tulajdonosa mondja meg ki/mit tehet meg vele
  - Linux filesystem jogosultság
  - Windows ACL-ek
- Mandatory Access Control (MAC)
  - Az AC mechanizmus felülbírálhatja a tulajdonos döntését
  - „security labels” / „sensitivity labels”
  - SELinux

Olvasinvalók

- Shon Harris – All In One CISSP Exam Guide 4th ed.
- Harold F. Tipton, Kevin Henry – Official (ISC)2 Guide to the CISSP CBK
- http://biztostu.hu
- http://silentsignal.hu
- http://google.com :)
- A Kevin Mitnick által írt könyvek, főleg social engineering témakörben:
  - A megtévesztés művészete
  - A behatolás művészete
  - A legkeresettebb hacker

  Linkek:
  http://www.amazon.com/Art-Intrusion-Exploits-Intruders-Deceivers/dp/0471782661/
  http://www.amazon.com/Art-Deception-Controlling-Element-Security/dp/076454280X/
  http://www.libri.hu/konyv/a-legendas-hacker.html
  http://www.libri.hu/konyv/a-legendas-hacker-2.html
  Kevin Mitnick-ről szóló HACKERS 2 - Operation Takedown c. film (angolul)
  http://www.youtube.com/watch?v=nVPV5dzM0yY
  http://www.imdb.com/title/tt0159784/