# Az informatikai rendszerek elemei és azok sérülékenységei

## Elemei:

* Környezeti elemek
* Dolgozók
* Hardver elemek
* Szoftver elemek
* Adathordozók, adatok, dokumentumok
* A kommunikáció elemei

## Környezeti elemek:

* Nem védett vagy rosszul tervezett átviteli vezetékek
* Cégen kívüli személyek bent tartózkodása (állandó felügyelet nélkül)
* Cégen belüli személyek szükségtelen bent tartózkodása
* Nem felügyelt munkálatok az épületben
* Berendezések elhelyezése nem védett területen (pl.: utcán őrzés nélkül)
* Belépés nem biztonságos vagy a biztonság nincsen megfelelően betartva
* Védelmi intézkedések/berendezések megismerése jogosulatlanok számára

## Hardver elemek:

* Az eleme kis mérete és súlya esetén fennáll a lopás kockázata
* Érzékenyek az elektromágneses sugárzásra
* Kompromittáló kisugárzás lehetséges (pl.: képernyőről)
* Ütésérzékeny

## Szoftverek:

* Veszélyes programok használata
* Bonyolult felhasználói felületek
* Új szoftver vagy szoftververzió nem megfelelő telepítése
* Szükségtelenül nagy hozzáférési jogok (Super Userek)
* Ismeretlen programok használata (vírusok)
* Hitelesítési problémák:
  + nincs felhasználói hitelesítés
  + gyenge jelszó, ritkán kell változtatni
  + jelszó használata nem kötelező
  + közös jelszavak használata
* Távolról történő karbantartás

## Adathordozók sérülékenységei:

* Érzékenyek a mágnesességre, hőre, nedvességre (azaz a környezeti hatásokra)
* Nem védett tárolás és ellenőrizetlen használat
* Beállítható írásvédelem
* Könnyű szállíthatóság 🡪 nehezen ellenőrizhető, könnyen lopható

## Dokumentumok sérülékenységei:

* Hiányos adminisztráció
* Nem védett tárolás (lopás, tűz)
* Ellenőrizetlen sokszorosítási lehetőségek
* Selejtezésnél, megsemmisítésnél nem elé nagy körültekintés

## Adatok sérülékenységei:

* Adatvesztés-károsodás adódhat hardver / szoftver hibákból
* Hibás manuális adatmódosítás
* Adatok törlése vagy megváltoztatása tévedésből vagy szándékosan
* Adatok jogosulatlan másolása

# A biztonság tervezési elvei, a támadások formái, összetevői

## A biztonság tervezési elvei:

1. **Feltérképezni a vállalatot**
2. **Megvalósíthatósági tanulmány elkészítése**
3. A **vállalat célkitűzéseivel összhangban** lévő **biztonsági politika kialakítása** és **követelmények megfogalmazása**. (Fontos szempont a cég üzleti érdeke)

* A legfontosabb építőelemek:
  + **Központilag menedzselt vírusvédelem**
  + **Virtuális magánhálózatok (VPN)** kialakítása, menedzselése
  + **Hitelesítés – azonosítás** (tervezéskor fontos hány faktoros, milyen típusú legyen)
  + **Aktív tartalomszűrés** (vállalati hálózatra belépő és elhagyó dokumentumok vizsgálata)
  + **Tűzfal**(ak)
  + **Biztonsági ellenőrzőprogramok** (sebezhetőségek rendszeres ellenőrzésére)
  + **Behatolás-detektáló rendszerek** (milyen szabályok mentén legyen)
  + **Felhasználó és hozzáférés menedzsment** (csoportházirend, Active Directory)
  + **Adatmentő rendszer**
* **Régebben a védelmen volt a hangsúly** (vírusvédelem, tűzfal).

**Manapság menedzselés irányba fordult** (régi módszerek megfelelő menedzselése).

* **Biztonsági rendszerek tervezésekor érdemes követni:**
  + **Nyilvános rendszerterv és használt biztonsági protokoll**
  + **Alapértelmezés, hogy nem férhet hozzá valamihez a felhasználó**
  + **Utólag beépíteni a biztonságot nehezebb**
  + **Windows NT vonulat:** Mindenkinek minden jogosultság megadása, utána elvétele, amire nincs szüksége (NEM BIZTONSÁGOS)
  + **Novel vonulat:** Senkinek semmi joga és adjuk meg később a szükséges jogokat
  + **„Barátságos” rendszert kell kialakítani, mert emberek fogják használni** (túl szigorú előírások esetén megpróbálják megkerülni majd azokat)
  + **„Teljes hatalommal bíró” rendszergazda (Super user) kerülése, ha lehet**
  + **Költségek**
  + **Menedzsment** (-tel egyeztetés a tervünkről)

## A picture containing diagram, line, font, symbol Description automatically generatedA hálózati támadások formái

### Passzív támadás

**Csak lehallgatás történik.**

A támadó nem módosítja az átviteli csatorna tartalmát.

### A picture containing diagram, font, line, white Description automatically generatedAktív támadás

**A támadó is küld üzenetet a csatornán.**

* üzenetmódosítás
* megszemélyesítés
* visszajátszás
* szolgáltatás megtagadás

### A picture containing font, text, diagram, white Description automatically generatedCsomag szintű támadások

* Az **IP cím hamisítása** (**blind spoofing** [hamísítás])
  + pl.: elhiteti A-val, hogy B-vel kommunikál
  + **Cél**: nem információhoz való hozzáférés, hanem **más akadályozása**
* A picture containing font, diagram, line, white

  Description automatically generated**RST támadás**
  + **Reset-tel kapcsolat bontási kérelmet juttat el a B-hez.**
  + B az azt hiszi, hogy az A befejezte vele a kommunikációt, ezért megbontja a kapcsolatot.
  + **C támadó B nevében kommunikálni A-val ellen. Ennek hatására az A gépet védő tűzfal B-t kitiltja**
* **Védekezés:** a tűzfalak bizonyos forrás IP címeket csak bizonyos irányból fogadnak el.
* A picture containing text, diagram, line, font

  Description automatically generated**Smurf támadás**
* a DoS családba tartozó támadás.
* **A támadó az áldozatot szeretné kiiktatni működés ügyileg**
* **A támadó az áldozatott megbombázza adatokkal**, hogy ne legyen képes más tevékenység elvégzésére, hogy **ezzel legyen elfoglalva, amit a támadó küldött neki.**
* Az **üzenetet vevő gépek válaszukkal teletömik az áldozat gép hálózatát**, de a sajátjukat is, így ők maguk is áldozatok.
* **IP broadcast**
  + IP-hálózatokban a broadcast pont-többpont címzési és adattovábbítási módot jelent, ahol a küldő a hálózat minden tagjának továbbítja ugyanazt az adatfolyamot.
  + **Minden IPv4-hálózatban értelmezett egy broadcast IP-cím, melyre küldött üzenetet a hálózat valamennyi eszköze feldolgozza.**
* **ICMP (Internet Control Message Protocol):**
  + **Hibaüzenetek**
  + **Tesztcsomagok**
  + IP-vel kapcsolatos információs üzenetek **létrehozása**
* **Védekezés**: a routerek IP broadcast-ot ne engedjenek át
* **SYN flood**
  + Ha a **rosszindulatú C támadó** az **A nevében nagy mennyiségű SYN csomagot küld B-nek** akkor **ezzel kimeríti B erőforrásai**t és az **nem lesz képes fogadni a valódi kéréseket.**
  + **SYN: a TCP fejlécének 14. bitje, jelzi, ha egy új kapcsolat felépítése kezdődik**
  + **TCP** (Transmission Control Protocol): **egy hálózati modell**
  + Az IP hálózatok - így az internet is **legnépszerűbb szolgáltatásai (SMTP, HTTP, FTP) TCP kapcsolatot alkalmaznak.**
* **Védekezés**: syn cookie használata, mikro blokkok használatával
* **Xmas, Ymas** (A TCP fejrészben az URG bittől balra levő két bitet átállítja, mert ez a 2 bit 0 értéket várna el alapértelmezettként. Így ó információt szerezhet a TCP/IP protocol stack implementációjáról.)

### Hálózati szintű támadások

* **Switch-ek elleni támadás**
  + **Normál működése**: keretek továbbítása csak arra a portra, ahol a címzett található.
  + **A támadónak bent kell lennie a belső hálózatban.**
  + **Switchek üzemmódja:**
    - **Statikusan megadhatjuk** azt, mely **IP című belső hálózati munkaállomás** vagy szerver, **melyik porton érhető el.**
    - Legközelebb jön ennek a gépnek valamilyen külső megkeresése, akkor tudja, hogy melyik portra továbbítsa a kérést vagy választ.
  + **Támadás:**
    - Kellően **sok különböző MAC címmel a switch táblát megtölti**, akkor a működés fenntartása érdekében **minden keretet minden portjára kiküld** (fail open). **Ezzel a forgalom lehallgathatóvá válik.**
    - **Amikor jön egy valós kérés a switch nem fogja megtalálni a megfelelő összerendelést a táblájában, mert már tele van hamis adatokkal.**
    - **Mivel az üzenet továbbítás a feladata, ezért kifogja küldeni minden portján, így a támadó letudja hallgatni az adatforgalmat.**
* **ARP poisoning**
  + A támadó kéretlen és **hamis ARP válaszokat küld**, amelyben a **kérdéses IP címhez a saját MAC címét tünteti fel.**
  + **ARP (Address Resolution Protocol, azaz címfeloldási/ címlekérdező protokoll)** a számítógépes hálózatokon használatos **módszer az IP-címek és MAC-címek** egymáshoz rendeléséhez.
  + **ARP (Address Resolution Protocol) = Címlekérdező protokoll. Üzenetszórásos hálózatokon broadcast** (minden gépnek szóló) **üzenettel megszerzi az információt (IP cím - MAC cím összerendelés) és elraktározza (cache).**
* A picture containing text, font, white, diagram

  Description automatically generated**ICMP (Internet Control Message Protocol) redirect**
  + Egy interneten használt protokoll, melynek segítségével értesülhetünk a hibákról, illetve azok típusáról, valamint hálózati diagnosztizálásban lehet a segítségünkre.
  + **Nem egyfajta támadási forma történik, hanem ezeknek a kombinációja.**
  + **SYN csomagot küldeni a B nevében az A-nak**, egy kapcsolat felépítési kérést, de a B nevében.
  + **Az A válaszát, amit B-nek szánt C fogja megkapni**
  + **Egy router egy számítógép számára egy jobb útvonalat tud megadni.** A támadó **ezzel maga felé tudja irányítani a megtámadott gép forgalmát.**
* **Védekezés**: accept\_redirects kikapcsolása.
* **RIP (Routing Information Protocol ) távolságvektor hamisítása**
  + **Egy távolságvektor, egy adott célponthoz.**
  + **Egy célponthoz táblázatában tárolja:**
    - A célpont IP címét
    - Az odavezető út költségét
    - Az odavezető út első routerét
    - Időzítőket
  + **A támadó megfogja hamísítani az útvonalat és maga fele fogja vezetni az üzeneteket** a routerek becsapásával
* A picture containing text, diagram, font, white

  Description automatically generated**Source route IP opció**
  + A **privát hálózattoknak** létezik egy **Gateway**-je
  + **A Gateway** egy olyan intelligens eszköz, amely **képes útválasztó feladatokat is ellátni**, azaz a beérkező vagy megkapott **adathalmazt, a lehető legrövidebb úton juttatja a célhálózat felé.**
  + **A támadó el tud bújni több router mögé.**
* **A picture containing text, diagram, font, white

  Description automatically generatedBanki támadás, DNS (cache) ellen való támadás**
  + **A weben keresztül szeretnénk banki műveleteket végezni.**
  + Az ügyfél a **saját internetszolgáltatóján keresztül** elküldi a saját bankjának az URLcímét.
  + **Az internetszolgáltató, megkérdezi a saját DNS szerverén**, hogy **milyen IP-cím tartozik ehhez** a névhez.
  + Ez alapján **megnyitásra kerül adott bank honlapja** az ügyfélnél.
  + Támadás:
    - A honlapoknak van egy **TTL** ideje (**Time To Live**)
    - **TTL idő lejár**, a támadó az internetszolgáltatónak **küld egy kérést**, hogy **szeretné ezt a banki oldalt megnézni**.
    - Rögtön **küldi rá a választ, hogy** az internet szolgáltató névkiszolgálójához, hogy **ehhez a névhez az általa megadott IP cím tartozik**
    - **Az internetszolgáltató ezt a hozzárendelést fogja elfogadni.**
    - Utána a valós DNS szerver hiába mond bármit, az internetszolgáltatóm nem fogja elfogadni neki.
    - Akkor amikor **az ügyfél leakarja kérdezni a banki oldalt**, a**z ügyfél internetszolgáltatója a támadótól fogja megkapni**, hogy **milyen IP tartozik az adott névhez.**
    - Ez a támadónak az IP-címe lesz, ha elkészít egy másolat honlapot, amit az ügyfél használni fog.

## Támadási modellek

* **Algoritmus jellegű:**
  + **Ismeretlen nyílt szövegű támadó** (Chipertext only): A leggyengébb támadó, aki megcsapolja a csatornát. Ő csak azt látja mi a rejtett szöveg. Elfogja a rejtett szöveget, de fogalma sincs a nyílt szövegről.
  + **Ismert nyílt szövegű támadó** (Known plaintext): Ő két helyen csapolja meg a csatornát, ahonnan küldik és ahova érkezik. Ő ismeri a nyílt és a rejtett szöveget is. De nem tudja befolyásolni
  + **Választott nyílt szövegű támadás** (Chosen plaintext): Nem csak megcsapolja, hanem befolyásolni is tudja a nyílt szöveg kódolását.
  + Ezek alapvetően algoritmikus támadások.
* **Lehet egyéb is!**
  + **Social engineering**
  + **Betőrés, szabotázs**
  + **Side-channel attack**: az algoritmusnak a vannak fizikai implementációja, ami miatt működik.

**(**Egy processzornak az áram felvétele, függ attól, hogy mit csinál. Plusz információkat.)

* + **Reverse Engineering:**

(Az áldozattal el kell hitetni, hogy ő a kezdeményező pl.: hiba előidézése után kiadják magukat szerelőnek)

* **Védelem:**
  + **Titkosítás, tűzfalak**
  + **Jelszókezelés fontossága**
  + **Vírusvédelem**
  + **Oktatások**

# 3. Szimmetrikus és aszimmetrikus titkosítási módszerek.

**Kriptográfia**: titkosan írás tudománya

**Kriptoanalízis**: titkosan írt üzenetek jogosulatlan feltörése

**A kriptográfia célja:**

* **Titkosítás**
* **Integritásvédelem**: ha megváltoztatják az üzenet tartalmát azt tudjuk detektálni
* **Hitelesítés** (feladó személye)
* **Letagadhatatlanság**: ne mondhassuk, hogy más küldte az üzenetet, mint aki

**Kerckhoff-elv:**

* **Minél kisebb információt tartsunk titokban (kulcs)**, ne az egész algoritmust
* Az algoritmus által nyújtott védelem nem lehet magasabb, mint a kulcs védettségének mértéke
* Okok:
  + **Egyszerűbb a kicsi kulcsot titokban tartani** (mint a teljes algoritmust)
  + **Egyszerűbb a kulcsot lecserélni**, mint az algoritmust
  + **Egyszerűbb a kommunikáció, ha az algoritmus közös**
  + **Nyilvános algoritmus esetén a hibák hamarabb kiderülnek**

**Támadási modellek**

* **Ismeretlen nyílt szövegű támadó** (Ciphertext only): a támadó csak lehallgatja a csatornát
* **Ismert nyílt szövegű támadó** (Known plaintext): a támadó tudja az összetartozó nyílt szöveget és a titkosított szöveget is, de ő is csak lehallgat
* **Választott nyílt szövegű támadás** (Chosen plaintext): Nem csak lehallgat, hanem befolyásolni is tudja a nyílt szöveg kódolását.

**Biztonság fajtái:**

* **Feltételes (algoritmikus):** addig ad biztonságot, **amíg a támadó erőforrásai egy bizonyos határ alá esnek**
  + **Brute force** (összes lehetséges kulcsot kipróbálja)
  + Kulcstér = összes lehetséges kulcs halmaza → minél nagyobb, annál nehezebb a brute force
* **Feltétel nélküli:** a kulcs random és az üzenettel azonos hosszúságú
  + Ez az **OTP titkosítás**
  + **Titkosítás XOR művelettel**
  + **Probléma: kulcs hossza megegyezik az üzenet hosszával**, ha a kulcsot el tudjuk juttatni titokban akkor az üzenetet is

**Szimmetrikus kulcsú rejtjelezés (Private key)**

* Lényege, hogy mind a **küldő** mind a **fogadó** **ugyanazzal** **a** **kulccsal** végzi a kódolást és a **dekódolást**.
* Ez azt jelenti, hogy ezeknek a rendszereknek a **védettségi szintje akkora, mint a kulcs védettségi szintje.**
* Algoritmikus gyengeség, ha nem ismerjük a kulcsot, de feltudjuk törni.
* **A kulcsot titokban kell kicserélni.**

**Aszimmetrikus kulcsú rejtjelezés (Public key)**

* **Nem kell titokban kulcsot cserélni.**
* A titkosításhoz szükséges kulcsból nem lehet kiszámolni a dekódoláshoz szükséges kulcsot.
* A **dekódoló** **kulcs** **titkos**, a **kódoló** **kulcs** **nyilvános**. Hiteles, de nem titkos kulcs-csere csatorna kell.
* **A kódolás a címzett kódolójával történik.**

**Session key (egyszer használatos titkosító kulcs)**

* Hibrid titkosítási módszer (szimmetrikusan és asszimetrikusan is kódolt)

## Szimmetrikus rejtjelezők:

* Kulcs védettsége = védettségi szint
* **Kell egy titkos kulcs-csere csatorna**
* **Szubsztitúciós rejtjelezők** (karakterek ugyanott maradnak):
  + **Shift rejtjelező:** abc eltolása valahány betűvel
  + **Monoalfabetikus helyettesítő:** minden betűnek egy másikat feleltetünk meg

**(Probléma**: a betűgyakoriságokat megőrzi)

* + **Homofóniás helyettesítés:** monoalfabetikus továbbfejlesztése
  + **Polialfabetikus helyettesítés:** ciklikusan használja a kulcsot
  + **Vignere kódoló:** fedi a betűgyakoriságokat, de nem teljesen
  + **Affin** rejtjelező
  + **Hill** rejtjelező
* **Transzpozíciós rejtjelezők** (karakterek nem változnak, de a pozíciójuk igen)
  + **Gyakoriság elemzés nem segít** a törésben
  + Pl.: oszlop-transzpozíciós rejtjelező
* **Modern blokkrejtjelezők, sorozat rejtjelezők**
  + egyszerű lépések, de azt sokszor hajtjuk végre

## SP struktúra (helyettesítés + permutáció)

* A picture containing text, screenshot, font, number

  Description automatically generated**S doboz** pl. belemegy 6 bit és kijön 4 bit, nem invertálható művelet
* **P doboz**: megcseréli a bitek sorrendjét
* **S doboz határozza meg a biztonságot**

## DES rejtjelező (SP struktúrájú)

* **Algoritmikus gyengesége nem derült ki az évek során**
* **A kulcstér mérete idővel kicsinek bizonyult**
* **Az S doboz készítése és az elvárások vele szemben tapasztalatiak**
* **Támadása**
  + **Differenciális kriptanalízis:** a differenciális egyenletlenségét használja ki

(a bemeneti differenciákra nem egyenletes differenciák jelenek meg)

* + **Linearitás problémája:** A kimenő bitek előállíthatók a bemenő bitek valamilyen írásbeli kombinációjaként.
* **Továbbfejlesztések**: 3DES, AES

## RSA algoritmus

* **Támadása:**
  + **Feltörhető faktorizációval**, amire egyelőre nincs hatékony algoritmus. Ha tudnánk gyorsan faktorizálni, akkor törhető.
  + Speciális helyzetekben törhető
  + **Shor algoritmus: kvantumszámítógépen futtatva feltörné**
  + Nem kizárt, hogy törhető faktorizáció nélkül
* **ECB üzemmód:** Electronic Code Book
  + Felszeletelem 64 bites darabokra
  + Mindegyik 64 bites darabot lecserélem a titkos szövegre
  + Utána leírom őket ugyanúgy egymásután
  + **Probléma:** Egy rejtett blokknak mindig pontosan ugyanaz a nyílt blokk felel meg
* A diagram of a block encrypted key

  Description automatically generated with low confidence**CBC (Ciphet Block Chaining) mód:**
  + **Nem a nyílt szöveget kódolok**, hanem az elött ráxorolom az előtte lévő rejtett szöveg blokkot
  + **Az első esetében kell egy inicializáló vektor**
  + Hiába ugyanaz két nyílt blokk **az előző rejtett blokk bonyolultabbá fogja tenni**

# 4. Az operációs rendszerek biztonsági szolgáltatásai

## Alapvető követelmények az operációs rendszerrel szemben:

* **Megbízhatóság**
* **Elérhetőség**
* Méretezhetőség (**skálázhatóság**)
* **Kezelhetőség**
* **Együttműködő**: Biztosítani a különböző rendszerek zökkenőmentes összekapcsolását
* Költségkímélő legyen

## Együttműködő:

* **Együttműködik az XML-alapú alkalmazásokkal és szolgáltatásokkal.**
* **A különböző programok tudjanak egymással kommunikálni.**

## Megbízhatóság:

* **Kitudja szolgálni a hozzá intézet kéréseket** (ha a körülmények nem változnak).
* **Megbízhatóság követelményét tudja biztosítani**, növeli a biztonságot:
  + Hálózati terheléselosztás
  + **Nyelvfüggetlen futtatórendszer**
  + Elosztott hitelesítési rendszer támogatása
  + **Jó memóriakezelés**
  + Szilárd **rendszerarchitektúra**
  + **Diagnosztikai eszközök** (a rendszer állapotának megfigyelésére)
  + **Indítás csökkentett módban**
  + **Fájlvédelem**
  + Helyreállítási konzol
  + **Biztonságimásolat-készítő segédprogram**
  + **Automatikus rendszer-helyreállítás** (ASR)

## Elérhetőség

* **Az alkalmazások, szolgáltatások és rendszerek rendelkezésre állásának mértéke**
* **Tervezett vagy váratlan üzemszünete csekély** (elérhetőség szempontjából magas színvonalú)
* A diagram of a computer network

  Description automatically generated with low confidence**Hálózati terheléselosztás:**
  + **Több szerveren elosztja a terhelést**

(bejövő hálózati forgalmat)

* **A hálózati terheléselosztás előnyei:**
  + **Beállítható, hogy a különböző hálózatokra mekkora terhelés jusson**
  + A fürt **dinamikusan bővíthető**
  + A teljes adatforgalom egyetlen kiszolgálóra továbbítható
  + A fürt mindegyik gépe ugyanazzal az IP címmel rendelkezik
  + **Ha egy gép meghibásodik a rendszerben a többi átveszi a helyét** és elosztják a terhelést
  + Ha megjavítottuk a fürtből kivett állomást utána újra visszatudjuk kapcsolni a fürtbe
* **Kevesebb kiszolgáló-újraindítás** (operációs rendszer fejlődése miatt)
* **A kiszolgáló indítása tükrözött kötetről**
* **Felhasználóállapot-áttelepítő eszköz** (felhasználói beállítások, fájlok és dokumentumok rögzítése és helyreállítása)
* **Válságkezelési szolgáltatások** (távoli felügyeleti és rendszer-helyreállítási műveletek végrehajtására)

## Méretezhető (Skálázható)

* **Fürtözés** lesz az egyik megoldás
* Elosztott fájlrendszerrel történő rendszerindítás képessége.
* Felfelé és oldalra méretezés
* Az eddigieknél nagyobb kötetméret
* **Fizikai címek kiterjeszthetőek**
* **Skálázható hardver** (több CPU használható)
* **I2O támogatás**
* **Szimmetrikus multiprocesszálás** (OS bármely elérhető processzoron tud végrehajtási szálakat futtatni)
* **Hálózati terheléselosztás**
* **Kiszolgálófürtök**

## Kezelhetőség

* **Jól felügyelhető**
* Vállalati szintű **felügyeleti szolgáltatások:**
  + **Active Directory**
  + **Csoportházirend**
  + Parancssori segédprogramok
* **WMI** (Windows Management Instrumentation)
* **Távtelepítő szolgáltatás (RIS)**
* Távtelepítési szolgáltatás (RIS)
  + **Távtelepítési kiszolgálóról való alkalmazás telepítés az ügyfél számítógépre** (hálózaton keresztül)
  + **Egyszerűsíti az alkalmazások kezelését, javítja a hiba-helyreállítási hatékonyságát**
* **Távoli asztal felügyeleti célokra**. (A számítógép a hálózat bármely számítógépéről felügyelhető)
* **Eredő házirend** (Csoportházirendet használó számítógépeken és felhasználókon alkalmazott házirend-beállításokat tesztelhetjük)
* **Engedélyezéskezelő**

# 6. A távoli munkavégzés biztonsági problémái. Windows Server komponensek.

## A távoli munkavégzés biztonsági problémái

* **Egyre nagyobb igény a távoli elérésre**
  + Távmunkások
  + Partnerek, beszállítók, stb.
* **Levelezőrendszerek biztosítása**
  + **Belső levelezőrendszer használata**
  + Webes felületen chatbox használata
  + **Nem minden megy titkosítva**
  + A **hitelesítés** **titkos**, de a **kommunikáció** **nem**.
* **Gyakran szükséges:**
  + **A desktop elérése (Remote Desktop)**
  + HTTPS-en keresztül különböző alkalmazások elérése
  + **VPN**
  + **SSH**
* **Problémák: A távoli elérés sosem biztonságos**
  + **Házirend érvényesítése**
  + **Tűzfal** **és** **vírusvédelem** **megfelelő** **a** **követelményeknek**
  + Biztonságos-e a távoli gép?
  + DE ez **már** **nem** **gond**, mert **az** **operációs** **rendszerek** **beépítették** **a** **kellő** **eszközöket**
* **Levelezés, csoportmunka:**
  + **VPN**
  + **Outlook**
  + Pop3, IMAP
  + …
* **Fájl megosztások elérése**
  + **SSL-en keresztül a SharePoint segítségével**
  + **VPN-en keresztül - karantén alagút** (ha nincs SharePoint)
* **VPN karantén: beteg vagy gyógyulj meg elv**
  + Jön a **kliens,** **be** **akar** **csatlakozni** a fájlszervere
  + **Megvizsgáljuk milyen állapotban van** a gép, az előírásainknak megfelel-e
  + Ha **nem felel meg** nem a fájlszerverhez fogjuk csatlakoztatni, hanem egy **VPN karanténba** tesszük
  + **Töltse** **le** a webszerverről azokat, **amik** **neki** **hiányzanak**
  + **Újra** **megvizsgáljuk** a kliens munkaállomását, **ha** **megfelel** akkor **megkaphatja** **a hozzáférést**
* **Alkalmazások futtatása, távfelügyelet:**

Helyi erőforrások használata Remote Desktopon keresztüli munkához

## SSH

* **SSH** (Secure Shell, biztonságos héj)
  + **Segédprogram, protokoll, titkosító eszköz**
  + **Cél: két számítógép között egy titkosított kommunikációs csatorna létrehozása**
* **SSH funkciói:**
  + Minden megoldható lenne SSH-val, de túl drága a cégeknek
  + **TCP** **segítségével** **kapcsolódik** a géphez, **felhasználónév** és **jelszó** megadás **után** **fájl** **átvitelekre** **lehet** **használni**
* **SSH biztonsági összetevői:**
  + **SSH segítségével a hitelesítés kivitelezhető**
  + **Titkosítást használ** (**DES**, 3DES)
  + **Adatépség biztosítása**
  + Ellenőrzés
  + SSH lehetővé teszi **port átirányításra**
* **SSH kiszolgálók:**
  + OpenSSH (ingyenes)
  + SSH2 (nem üzleti használatra ingyenes)
  + VanDyke Software
* SSH ügyfelek:
  + OpenSSH
  + PuTTY
  + WinScp
  + SecureCrt

## VPN- protokollok

### PPTP (Point-to-Point Tunneling Protocol)

* **A PPP kibővítése**
* **Egyszerű, gyorsan beüzemelhető**
* Hitelesítés MS-CHAPv2 jelszó alapú szabvány szerint
* **Nem igényel különösebb infrastruktúrát**
* **Egyszerűen NAT-olható**
* **Teszt üzemmódban tökéletesen megfelel**
* Nagyon titkos esetekben nem használják ezt a protokolt. Abban az esetben PKI infrastruktúrát kell kiépíteni VPN-hez

## Windows Server komponensek

* **RDP - Remote Desktop Protocol**
* **RRAS - Routing and Remote Access Service**
* **VPN - Virtual Private Network**
* **CMAK - Connection Manager Administration Kit**

(Ez **lehetővé** **teszi**, hogy **egy** **teljes** **VPN** **kapcsolatot** **egy** **exe-ébe** **becsomagoljunk**, mindenféle **beállítással** **együtt**)

### Routing and Remote Access Service

* **Betárcsázós** **és** **VPN-es** **távoli** **elérést** **képes** **támogatni**
* **Site-to-site kapcsolatok létrehozásának támogatására**
* **NAT** **szerverként** **működni**
* **LAN** **routerként** **működni**
* **A** **fentiek** **összes** **kombinációja**
* **Távelérési házirendek készíthetők**
* VPN karantén
* **Tartalmaz egy viszonylag egyszerű tűzfalat**

# 7. A felhasználók azonosítása, hitelesítése és jogosultságaik kezelése. A felhasználói csoportok és a csoportjogok. Az engedélyek.

## Hitelesítés

* A **rendszer** **ellenőrzi**, hogy az adott **felhasználó** **tényleg** **az-e**, akinek mondja magát
* Lehet **egyfaktoros** **vagy** **többfaktoros** hitelesítés
* Mai **legbiztonságosabb** **protokoll**: **Kerberos** (szimmetrikus kulcsú titkosítás)

## Felhasználók azonosítása

* **Tudás alapú azonosítás 🡪 jelszó**
  + A felhasználó tudására épül
  + Egyszerű és olcsó
  + Erős jelszavak megjegyzése nehéz az ember számára
* **Birtok alapú azonosítás 🡪 kulcs**
  + A felhasználó birtokában lévő tárgyra épül
  + Egyszerű, lehet olcsó és drága is
  + Ellopható, de ha észreveszik akkor le lehet tiltani
  + Másolás elleni védelem szükséges
* **Biometrián alapuló azonosítás**
  + Nagyon megbízható
  + A komoly megoldások drágák, az olcsók könnyen átverhetők
  + Jogi problémákat okozhat a biometrikus adatok tárolása
* **Megfelelő megoldás**: két különböző módszer egyidejű használata

## Engedélyezés

* A már hitelesített kérőnek **van-e jogosultsága az adott objektumhoz**
* Van-e jogosultsága/engedélye pl.: a mappához?
* **Az adott felhasználó / csoport milyen típusú hozzáféréssel rendelkezik**
* Engedély rendelhető (felhasználókhoz, csoportokhoz, …)

## Jogosultságok

* **Megadja a hozzáférés szintjét, szerepkörét az adott felhasználónak**
* A jogosultságokat pl. fájlokon, könyvtárakon lehet érvényesíteni
* **Hozzáférési szintek:** Teljes hozzáférés / Írás / Olvasás
* **Hozzáférés engedélyek öröklődése**

# 8. Címtárintegráció.

**Felhasználómenedzsment fontos mérföldköve**

* Integrált felhasználómenedzsment létrehozásához elengedhetetlen a felhasználói adatok valós idejű szinkronizációja

## A címtár

* **Hálózati objektumok** (kiszolgálók, kötetek, nyomtatók, a hálózat felhasználói, …) **adatainak tárolására alkalmas**
* Felhasználók azonosságának, jogosultságainak ellenőrzésére is tudjuk használni
* **Központosítva lehet felügyelni a hálózati erőforrásokat**
* A hálózat távfelügyelete automatizálható (házirend)
* **Címtár szükségessége:**
  + **Sok felhasználó esetén is kell tudnunk biztosítani a maximális teljesítmény és biztonságot**

(ehhez járulnak hozzá a címtárak)

* + **Korábban:** felhasználók nyilvántartása minden kiszolgálón külön-külön
* **Problémák:**
  + Nem elegendő az integrált felhasználómenedzsmenthez az Active Directory
  + **Heterogén infrastruktúra** hosszútávon:
    - Gyakran egyesülnek cégek, szétválnak, átalakulnak
    - Eltérő megoldások vannak a különböző cég egységekben, ezeket kellene központosítani, egységesíteni
  + **Egységesítés költséges:**
    - Időkiesés
    - Szakértelem szükséges
  + **Azért kell létrehozni integrált rendszert**, mert **a dolgozó hosszú idő után kap meg minden jogosultságot** később tud effektív munkát végezni, de **elsődleges probléma mikor elhagyja a céget** akkor **nehezen szűnik meg minden jogosultsága**
  + Ezekre a problémákra tűzoltásra találták ki a metacímtár
* **Active Directory**
  + **Felhasználó menedzsmentet** biztosító **szoftverazonosítókat** tudunk benne **tárolni**, **jelszavakat** tudunk **kezelni**, **csoportházirenddel** tudjuk **szabályozni**
  + Gépek távtelepítése
  + Szoftver-letöltési korlátozások
  + **Active Directory tartomány:** a Windows rendszergazdája által meghatározott számítógépek csoportja
* **Alapfogalmak**
  + **Domain (tartomány):**

Számítógépek olyan csoportja, amely egy hálózatrészt alkot, és közös címtáradatbázist használ

* + Domain controller (tartományvezérlő):

Windows tartományokból felépülő környezetben o**lyan számítógép, amelyen Active Directory szolgáltatás fut**

* **Metacímtárak**
  + Identitásmenedzsment szükséges feltétele
  + Integráltan tartalmazza a csatolt adatforrások fontosabb információit
  + A metacímtárban gyűjtjük össze a vállalat teljes nyilvántartását
  + A következőkkel kapcsolatban létezik nyilvántartás:
    - Levelezőrendszerek
    - Active Directoryban van nyilvántartásunk
    - Munkaügyön
    - Adatbázisok
    - Telefonkönyv
  + Ezeket mind összegyúrni egy címtárba
  + Össze lehet kapcsolni a különböző rendszereket, különböző mezőket

## Tivoli Directory Integrator

* **A TDI működése**
  + **Adatszinkronizálást és cserét hajt végre különböző adatbázisok és címtárak között.**
  + Úgy kell elképzelni, mint egy futószalagot
  + Mindenféle adatforrást becsatlakoztatunk a futószalagra
  + A rendszeren belül rendelkezni kell ahhoz megfelelő elemzővel, hogy a becsatlakoztatott adatokkal tudjunk mit kezdeni
  + A szalagon történhet vele több minden is:
    - Adatokat összeválogatása
    - Többnek a becsatlakoztatása adatforrásként és egy közös összeállítása
  + Végig mennek az adatok vagy történik velük valami, vagy nem
  + Majd lesz egy kimenet belőle: pl.: bemenet: CSV-> kimenet: XML
* **A TDI jellemzői**
  + Két rész (Javaban): IDE és Runtime Server
  + Platformok: Windows, Unix, Linux, AIX
* **Integrációs feladatok megoldása a felhasználói adatok szinkronizációjával példák**
  + A vállalati nyilvántartásból van valamilyen telefonszám nyilvántartásunk
  + Van egy bérügyes nyilvántartásunk
  + Ezeket becsatlakoztatjuk az IDE-be és valami közöset kitudunk választani
  + Több telephelyes vállalatokat össze lehet ilyen formában kötni és összehangolni az adatokat

# 9. Felhasználó menedzsment MS és IBM alapon

* **N**
* **N**