

Informatikai és távközlési alapok II.



Tatabányai Szakképzési Centrum

**Széchenyi István Gazdasági
és Informatikai Technikum**

Bring Your Own Device (BYOD)

- Bármilyen eszközt
 - Laptop, telefon, PC, ebook olvasó
- Bárki
- Bárhol használhat

Online csoportmunka

- Egymással együttműködhetnek az emberek
 - az a folyamat, amikor mással vagy másokkal egy közös projekten dolgozunk.
- Cisco Webex Teams
 - Többfunkciós
 - Együttműködést segítő alkalmazás
 - Képek, videók, hivatkozások oszthatóak meg

Felhőalapú szolgáltatások

- Adattárolás
- Alkalmazások (szöveg és képszerkesztők)
- Nincs infrastruktúra beruházás
- Fontos a megbízhatóság (biztonság és rendelkezésreállítás)

Felhőtípusok

- **Publikus felhő:**

- **A publikus felhő által biztosított alkalmazások és szolgáltatások mindenki számára elérhetők.** A szolgáltatások lehetnek ingyenesek, de használat alapján fizetők is, ilyen az online tárhely bérlete. **A publikus felhő interneten biztosítja a szolgáltatásait.**

- **Privát felhő:**

- A privát felhő által biztosított alkalmazásokat és szolgáltatásokat egy bizonyos szervezet vagy felhasználói kör számára hozzák létre. A privát felhő üzemelhet a szervezet saját hálózatán belül, bár ennek létrehozása és üzemeltetése költséges. Üzemeltethető a szervezeten kívül is, ilyenkor természetesen szigorú hozzáférési biztonság megvalósításával.

Hibrid felhő

- A hibrid felhő kettő vagy több felhőből áll (pl.: részben privát, részben publikus), ahol mindegyik rész elkülöníthető objektum.
- Ugyanaz az architektúra köti őket össze
- A felhasználói jogaiktól függően különböző fokú hozzáférést kapnak a felhő szolgáltatásaihoz.

Közösségi felhő

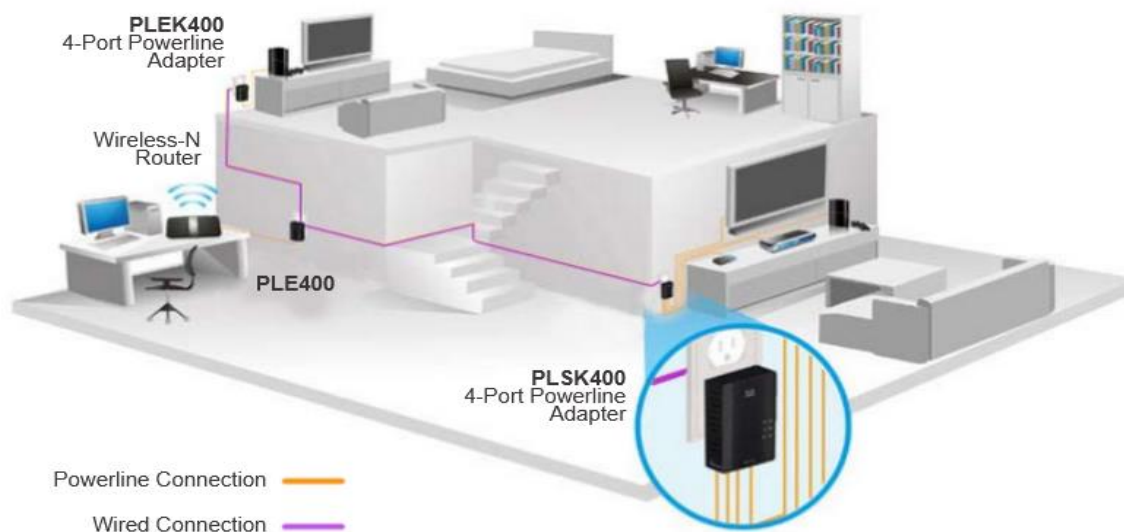
- A közösségi felhőt egy bizonyos kör vagy szervezet kizárólagos használatára hozzák létre
- A közösségi felhő funkcióit a közösség igényeihez szabják
- Például az egészségügyi szervezeteknek bizonyos szabályok és jogszabályok speciális hitelesítési és titoktartási előírásainak kell megfelelniük. A közösségi felhőt olyan szervezetek használják, amelyeknek hasonló szükségleteik és feltételeik vannak.
- A közösségi felhő hasonlít a publikus felhő környezetéhez, de meghatározott biztonsági, titoktartási és szabályozási előírásokkal.

Okosotthon

- Okos sütő
- Okos hűtő
- Okos mosó- és szárítógép
- Nem csak a jövő, hanem jelen is
- Jellemzően felhőt használnak

Hálózat konnektorból

- Kábeles összekötetés
- Már kiépített infrastruktúra
- Más frekvencián küld adatokat
- Powerline



Vezeték nélküli kapcsolat

- **Vezeték nélküli internetszolgáltató**
 - Wireless Internet Service Provider, WISP
 - Hol használják?
- **Vezeték nélküli szélessávú szolgáltatás**
 - Az otthoni és kisvállalkozások számára egy másik vezeték nélküli megoldás a vezeték nélküli szélessávú hozzáférés
 - Hasonló, mint mobiltelefon hálózatoknál

Hálózatbiztonság (1.8)

- **Vírusok, férgek és trójai programok:**
 - Rosszindulatú szoftvereket vagy kódokat tartalmaznak, és a felhasználó eszközén futnak.
- **Kémprogram (spyware) és reklámprogram (adware)**
 - A felhasználó eszközére telepített programok, amelyek titokban információkat gyűjtenek a felhasználóról.
- **Nulladik napi (zero-day) támadás:**
 - Más néven nulladik órás támadás, egy biztonsági rés ismertté válásának napján megjelenő támadás.
 - **Legveszélyesebb**

Hálózatbiztonság

- **Személyes fenyegetés**

- Egy rosszindulatú személy felhasználói eszközöket vagy hálózati erőforrásokat támad meg.

- **Szolgáltatás-megtagadásos támadás**

- Lelassít vagy elérhetetlenné tesz szolgáltatásokat és folyamatokat egy hálózati eszközön.

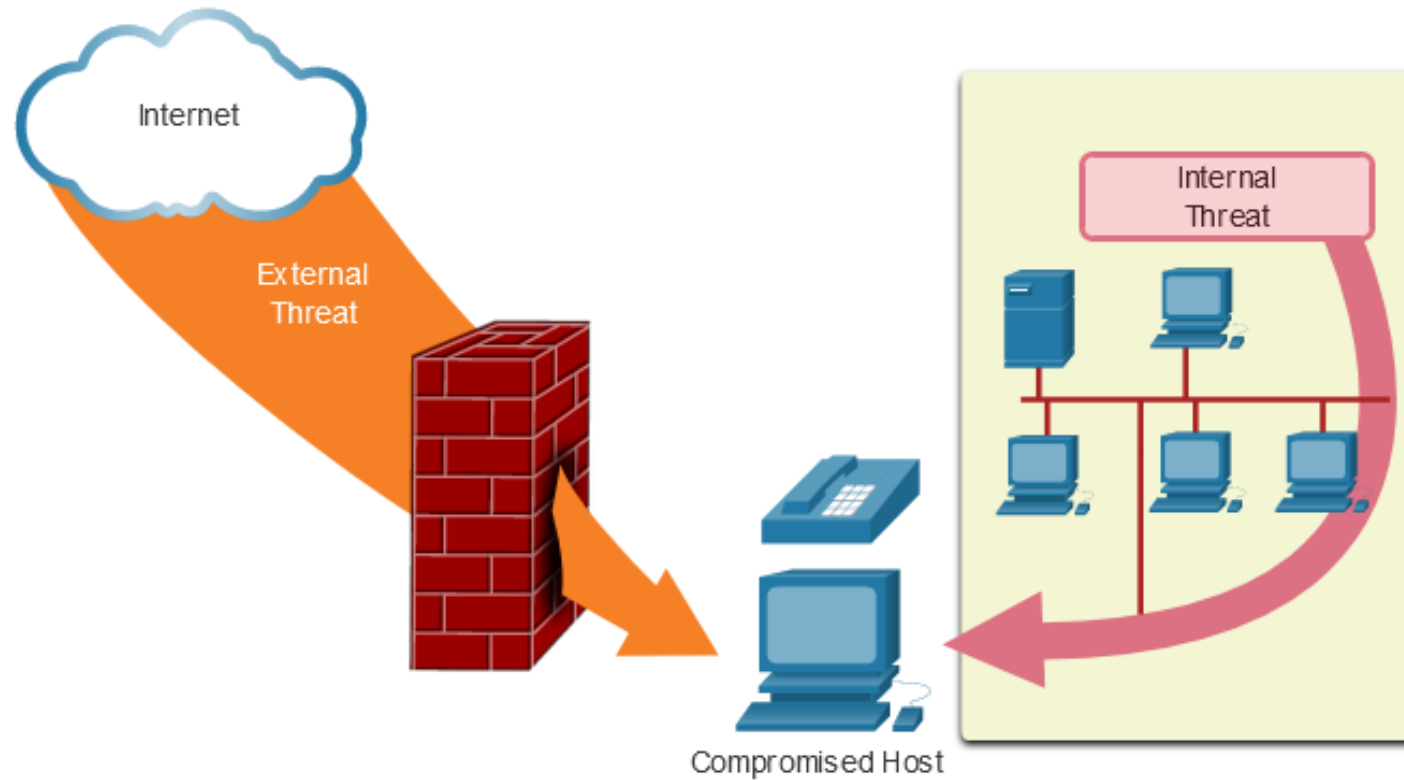
- **Adatlehallgatás és –lopás**

- Ez a támadás személyes adatokat rögzít egy szervezet hálózatából.

- **Személyazonosság-lopás**

- A támadó egy felhasználó belépési adatait lopja el, hogy privát adatokhoz férjen hozzá.

Honnan jöhet fenyegetés?



Védelem

Hálózatok gyakran alkalmazott biztonsági elemei:

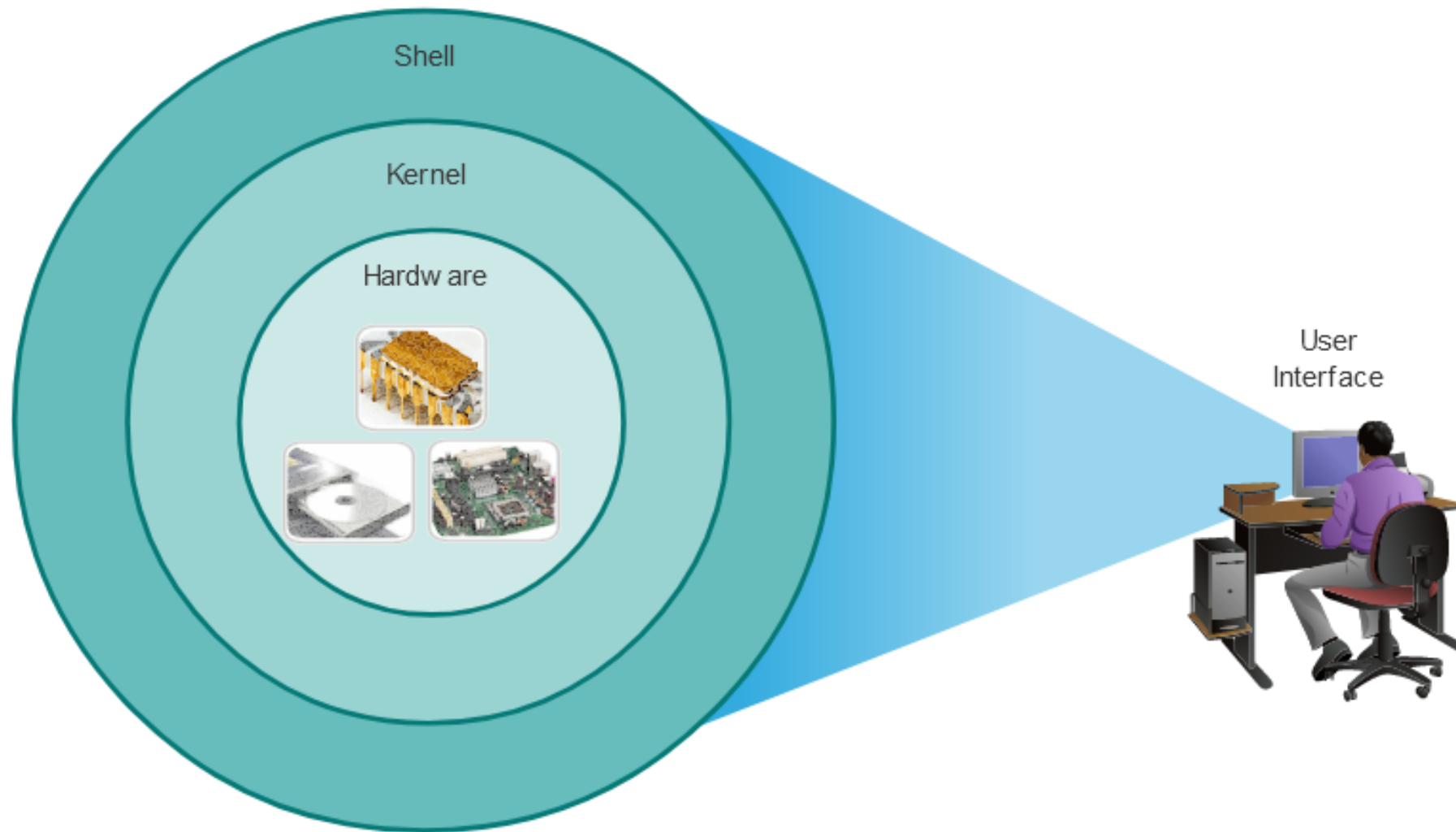
- Vírus-és kémprogramvédelem
- Tűzfal szűrés
- Dedikált tűzfalrendszerek
- Hozzáférés-szabályozó listák (Access control lists, ACL)
- Behatolás-megelőző rendszerek (Intrusion prevention systems, IPS)
 - 0 day hibál
- Virtuális magánhálózatok (Virtual private networks, VPN)

Cisco IOS

- Operációs rendszer (OS) fut
 - Otthoni routereknél firmware-nek hívjuk
- OS kommunikál a hardverrel és a felhasználóval
- Létezik CLI = command line interface
- Létezik GUI = graphical user interface
- IOS = Internetwork Operating System

CLI

- Kis erőforrás
- Tanulni kell
- Minden feladat megoldható ami grafikusan is
- Kötött struktúra
- Szinte mindent CLI-ből fogunk konfigurálni



Miért kell konfigurálni?

- Alapvetően jól működik
- De biztonságossá kell tenni
- Vállalat működéséhez kell alakítani

Konzol

- Sávon kívüli elérést biztosító fizikai menedzsment port a Cisco eszközökön
- A sávon kívüli = ez egy dedikált felügyeleti csatorna kizárólag az eszköz karbantartására
- Előnye, hogy az eszköz akkor is elérhető, ha semmilyen hálózati szolgáltatás nincs még beállítva, mint például a kezdeti konfiguráció idején.
- A konzolkapcsolat létrehozásához a terminálemulációs szoftvert futtató számítógépet egy speciális konzolkábelrel kell az eszközhöz csatlakoztatni.

Secure Shell (SSH)

- Az SSH a javasolt sávon belüli módszer, hogy a hálózaton keresztül, virtuális interfész segítségével biztonságos parancssoros kapcsolatot létesítsünk
- A konzolkapcsolattól eltérően az SSH-kapcsolatok aktív hálózati szolgáltatásokat igényelnek az eszközön, beleértve az aktivált és címmel beállított interfészt.

Telnet

- A Telnet a parancssor nem biztonságos távoli elérési módja hálózaton keresztül, virtuális interfész segítségével.
- Az SSH-től eltérően a Telnet nem kínál biztonságos, titkosított kapcsolatot, használata legfeljebb elkülönített teszthálózaton javasolt.
- A felhasználói hitelesítés, a jelszavak és a parancsok egyszerű szöveggént kerülnek elküldésre a hálózaton. Ha tehetjük, használjunk SSH-t a Telnet helyett!

AUX

- sávon kívüli elérést
- betárcsázós telefonkapcsolat

Terminál emuláció

Néhány terminál emulációs program:

- PuTTY
- Tera Term
- SecureCRT
- HyperTerminal
- OS X Terminal

Elsődleges módok

Parancsmód	Leírás	Készenléti (prompt) jel
Felhasználói EXEC mód	• Korlátozott felügyeleti parancsok. • Néha megtekintő vagy lekérdező módnak is nevezik.	Switch> Router>
Privilegizált EXEC mód	• Ebben a módban minden parancs és funkció elérhető. • A felhasználó bármilyen lekérdező és beállító parancsot használhat.	Switch# Router#

Globális konfig mód és alkonfigok

- Az eszköz konfigurálásához a felhasználónak globális konfigurációs módba kell lépnie, amelyet röviden globális konfig módnak nevezünk.
- Prompt: Switch(config)#
- **Vonalkonfigurációs mód** - Konzolos, SSH-, Telnet vagy AUX-hozzáférés konfigurálására szolgál.
- **Interfészkonfigurációs mód** - Switchport vagy router hálózati interfész beállítását végezzük innen.

IOS parancsok

- Felhasználói EXEC -> privilegizált exec: enable
 - Visszafelé: disable
- Globális konfigurációba lépés: configure terminal
 - Kilépés privilegizáltba: exit
- Vonalkonfiguráció:
 - Line {vonal típusa} {vonal száma}
 - line console 0
- Interfészkonfig
 - Hasonló mint a vonal
 - Interface FastEthernet 0/1