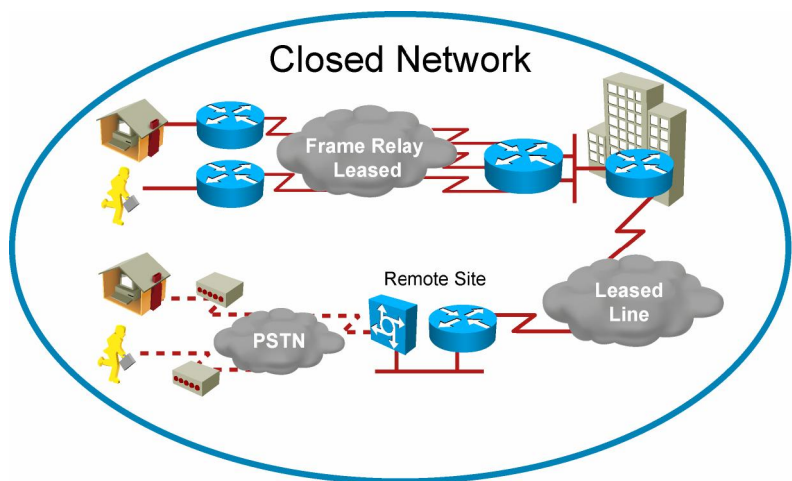


Alapvető technológiai áttekintés

Hálózat biztonság



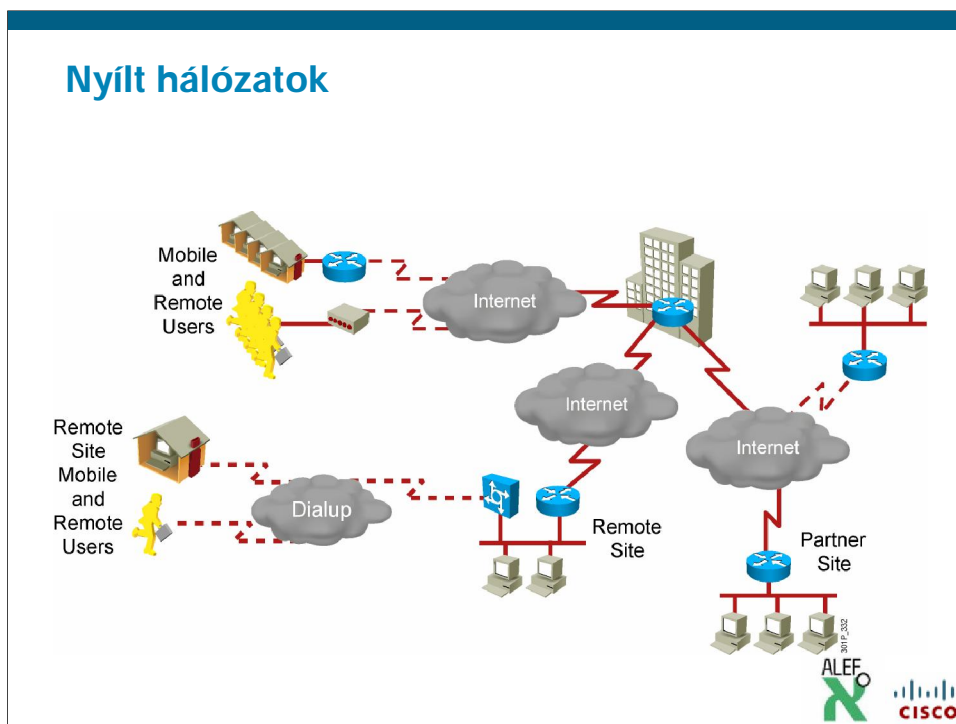
Zárt hálózatok



Zárt hálózatok: a belső támadások fenyegetése megmarad!!

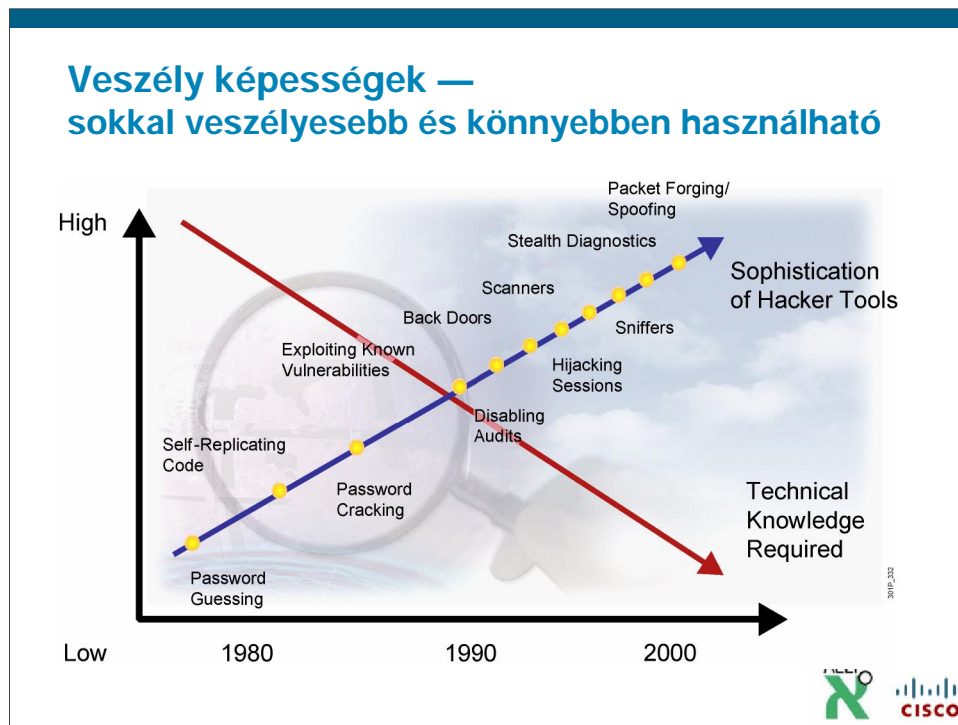
A legegyszerűbb módja egy hálózat külső támadásoktól való megvédésének a külvilágtól való teljes elzárása. Egy zárt hálózat egy hitelesített site-okhoz és részekhez engedi a hozzáférést; egy zárt hálózat nem engedi meg a kapcsolatot a nyilvános hálózathoz.

Mivel nincs külső kapcsolat, a hálózat tervezésekor ez figyelembe vehető a külső támadásoktól való védelemnél. Azonban, a belső fenyegetések még fennállnak. A hálózati visszaélések 60-80 %-a a hálózat belsejéből ered!



Nyílt hálózatok

Napjainkban, a vállalati hálózatok hozzáférést igényelnek az Internethez és egyéb nyilvános hálózatokhoz. Vállalati hálózatoknál nem rendkívüli, hogy számos hozzáférési pontjuk van nyilvános és egyéb privát hálózatokhoz. Nyílt hálózatoknál a biztonság különösen fontos.



Veszély képességek – sokkal veszélyesebb és könnyebben használható

Az ábra is mutatja, hogy a hacker támadások növekszenek és a hozzá szükséges szakértelem pedig csökken. Az elmúlt 20 évben a nagy nyílt hálózatok növekedésével a biztonsági veszélyek is jelentősen megnövekedtek. A hackerek több hálózati sebezhetőséget fedeznek fel és a hackelési eszközök használata sokkal egyszerűbb. Letölthetők különböző alkalmazások, amelyek kicsi vagy egyáltalán nem szükségesek hacker ismereteket követelnek. Különböző alkalmazások, amelyek hibaelhárítást, fenntartást és optimalizálást végeznek, rossz kezekbe kerülve, rosszindulatúan használhatóak!

Sophistication of hacker tools: hacker eszközök elterjedése

Self replicating code: önismétlő kód

Exploiting known vulnerabilities: ismert gyengeségek kihasználása

Back doors: hátsó ajtók

Scanners: szkennerek

Stealth diagnostics: titkos diagnosztika

Packet forging/spoofing: csomag hamisítás/beccsapás

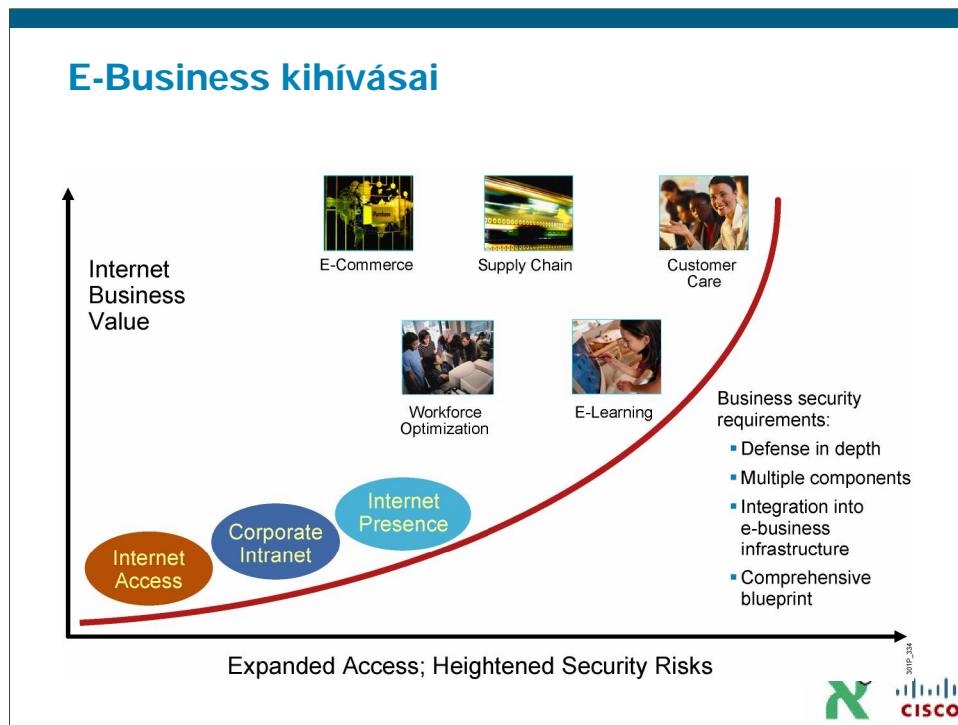
Password guessing: jelszó kitalálás

Password cracking: jelszó feltörés

Disabling audit: audit letiltás

Hijacking sessions: viszony eltérítés

Sniffers: snifferek



Ezen az ábrán a különböző hálózatzbiztonsági igények kiegyensúlyozása látszik.

A teljes biztonsági kihívást két fontos szükséglet között mérlegelve találjuk meg: nyílt hálózatok támogatják a kialakuló üzleti kívánalmakat és kezdeményezik az információ szabadságot, szemben a privát, személyes és stratégiai üzleti információk védelmével.

A biztonság a hálózat tervezés és kivitelezés elterébe került. Számos üzletben, a túlélésért szükséges megengedni a hálózati erőforrásokhoz való hozzáférést és biztosítani kell, hogy adatok és erőforrások biztonságosak legyenek, amennyire lehetséges. A hálózat biztonságpolitika létesítése kell, hogy az első lépés legyen egy hálózat biztonságos infrastruktúrára való lecserélésénél.

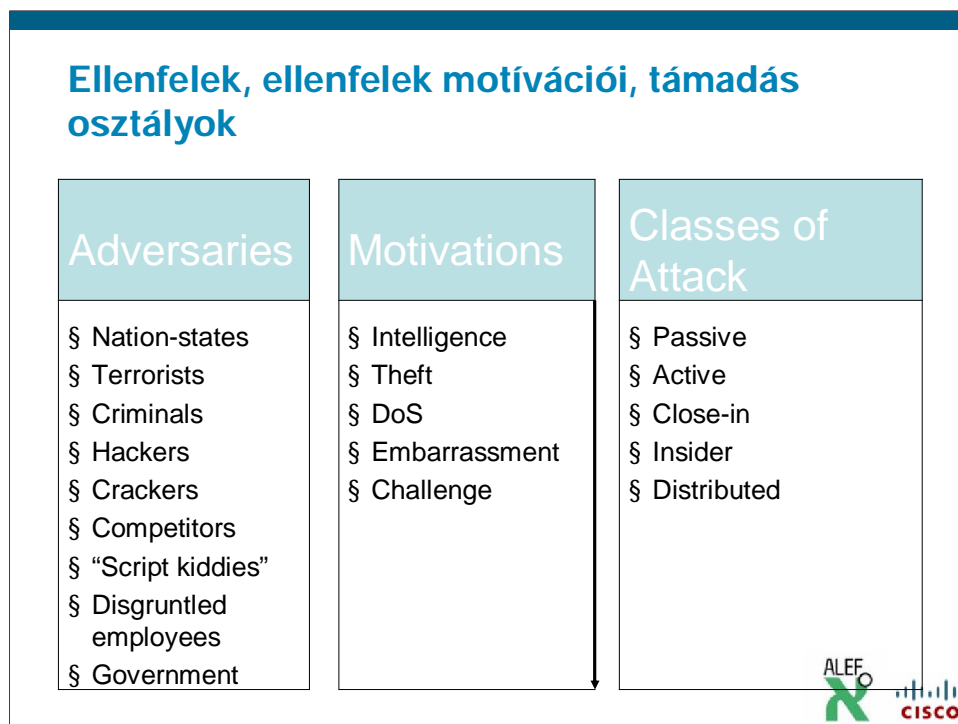
Az Internet elvárásokat készíti a cégekkel szemben, hogy erősebb kapcsolatot építsenek ki a felhasználókkal, szolgáltatókkal, partnerekkel és alkalmazottakkal. Az e-kereskedelem felszólítja a cégeket, hogy sokkal agilisebbek és versenyképesebbek legyenek.

Egy vállalati hálózaton a menedzserek megnyitják a hálózatukat a felhasználóknak és alkalmazásoknak, sokkal nagyobb kockázatnak kitéve a hálózatukat. A megoldás a biztonsági követelmények kiterjesztése. A biztonság alap követelmény kell, hogy legyen az üzleti stratégiában.

Ezeknek a hálózatoknak nemcsak biztonságosnak kell lenniük, hanem támogatniuk kell hang, video és adat átvitelt is, konvergálva egy multi-service környezethez.

Üzleti biztonsági elvárások:

- Defense in depth: mélyreható védelem
- Multiple components: többszörös összetevők
- Integration into e-business infrastructure: e-kereskedelem infrastruktúrába való integráció
- Comprehensive blueprint: széleskörű tervezet



Ellenfelek, ellenfelek motivációi, támadás osztályok

Ellenfelek:

Nation-states: nemzetek

Competitors: konkurencia

Hacker: általában jó szándékú, nagy tudású. Cracker: rossz szándékú.

Script kiddies: szkript-gyerek: Képzetlen, mélyebb szakmai ismeretekkel nem bíró **hacker**, aki a valódi szakemberek által készített segédeszközök (**exploit**-ok) felhasználásával próbál feltörni szervereket, saját céljaira.

Disgruntled employees: elégedetlen alkalmazottak

Government: kormányzat

Motívciók:

Theft: lopás

DoS Denial of Service: Ez a támadások egy speciális fajtája, amikor a támadó szándéka nem információszerzés vagy annak megsemmisítése, hanem egy adott szolgáltatás működésének megbénítása.

Embarrassment: fizetési nehézség

Támadás osztályok:

Passive attack: észrevétlen forgalom elemzés, esetleg archiválás, a kommunikáció tartalmának megváltoztatása nélkül. Betartja a protokoll szabályokat!

Active attack: a támadás során a lehallgató általában képes megváltoztatni a kommunikáció tartalmát, függetlenül attól, hogy tudja-e értelmezni vagy sem.

Close-in attack: azokat a hálózatokat, rendszereket tudja módosítani, amelyekhez fizikailag hozzáfér. Fizikai közelséget ér el a hálózathoz való titkos hozzáféréssel, vagy hozzáférés nyitásával, vagy mindkettővel.

Insider attack: belső támadás: a belső támadás lehet rosszindulatú, vagy nem rosszindulatú. Rosszindulatú belső támadók szándékosan hallgatónak, lopnak vagy károsítják az információt, hamisan használják az információt, vagy kitiltják a többi jogos felhasználót. Nem rosszindulatú támadások tipikusan gondatlanságból, ismerethiányból, a biztonság szándékos rászédéséből erednek.

Distributed attack: szétszórott támadás: hardver vagy szoftver rosszindulatú módosítása. Ezek az alkalmazások rosszindulatú kódokat mutatnak, mint a back door amely jogtalan hozzáférést biztosít az információkhoz vagy a rendszerhez egy későbbi időpontban.

Gyakori fenyegetések

- Physical installations
 - Hardware threats
 - Environmental threats
 - Electrical threats
- Reconnaissance attacks—Learning information about a target network by using readily available information and applications
- Access attacks—Attacks on networks or systems for these reasons:
 - Retrieve data
 - Gain access
 - Escalate their access privileges
- Password attacks—Tools used by hackers to compromise passwords



Gyakori fenyegetések

Fizikai fenyegetések:

- az eszközök nem biztonságosan zárható helyen vannak
- túl magas, vagy túl alacsony a hőmérséklet, vagy túl magas a páratartalom
- elektromos fenyegetés: az épületben túl sok a feszültség ingadozás

Felderítéssel támadások: a rendszer, a szolgáltatások, a gyengeségek felderítése és feltérképezése. Az első tipikus ilyen támadás az élő IP címek kiderítése egy hálózatban. Ezután jöhet a futó alkalmazások, operációs rendszerek kiderítése, amelyeknek a hibái közismertek. A különböző alkalmazások által használt portok kiderítése.

Hozzáféréssel támadások: ezek a támadások az ismert gyengeségeket használják ki az autentikációs szolgáltatásokban, FTP szolgáltatásokban és a web szolgáltatásokban.

Password támadások: a felhasználói azonosítók és jelszavak különböző módszerekkel történő kiderítése és ennek későbbi felhasználása.

Jelszó alapú támadások

- Here are password attack threat-mitigation techniques:
 - Do not allow users to use the same password on multiple systems.
 - Disable accounts after a certain number of unsuccessful login attempts.
 - Do not use cleartext passwords.
 - Use “strong” passwords; for example, “mY8!Rthd8y” rather than “mybirthday.”



A jelszó alapú támadások ellen különféle módokon védekezhetünk:

- Ne használjuk ugyanazt a jelszót a különféle rendszerekhez való hozzáférésekhez
- Bizonyos számú sikertelen belépés után tegyük elérhetetlenné a hozzáférést. Ez a módszer segít megelőzni a jelszó próbálgatással történő belépést.
- Ne használjunk titkosítatlan jelszavakat. Használjunk vagy egyszer használatos jelszót, vagy kódoljuk a jelszavunkat.
- Használjunk „erős” jelszót, ne legyen könnyen kitalálható, legyen benne kisbetű, nagybetű, szám, egyéb más karakter.

Összefoglalás

Összefoglalás

- Zárt-, nyitott hálózatok
- Támadás típusok a hálózatok ellen



