14 - Problematika bezpečnosti počítačových sítí

Fyzická bezpečnost

- zamezení přístupu nepovolených osob k prvkům sítě
- ochrana sítě před přírodními vlivy
  - zemětřesení, povodně
  - příliš vysoká / nízká teplota, vlhkost
- lze využít kamerový dozor, uzamčení, autentizaci, separaci datových záloh

Sociální inženýrství

- vyjednávací a komunikační metoda, která přinutí uživatele, aby prozradil určitou informaci
- vyvolá v člověku dojem, že se situace liší od skutečné
- příklad použití - přinucení uživatele, aby zadal své heslo na pochybnou stránku, která vypadá podobně jako pravá
  - **Phising**
  - stránka má jinou URL, můžou v ní být chyby ze strojového překladu

Škodlivý software

Malware

- počítačový program určen k poškození jiného systému
- obecné označení pro ostatní viry, spyware, adware…

Adware

- škodlivý software, který se typicky dostane do prohlížeče
- sám o sobě není škodlivý
- znepříjemňuje používání uživatele neustálým vyskakováním reklam
- adware si nainstaluje většinou uživatel nevědomky, ovšem s instalací souhlasí
- adware neodesílá žádná citlivá data přes internet, pouze otravně ukazuje reklamy
- typicky je přidán k programům zdarma, aby se autorovi zaplatil jejich vývoj

Spyware

- odesílá z počítače data bez vědomí uživatele, "špehuje uživatele"
- může odesílat pouze historii navštívených stránek nebo nainstalované programy
  - shromaždovaní dat, lepší cílená reklama
- ovšem spyware může zároveň odesílat citlivá data, jako jsou např. čísla platebních karet a hesla
- keyloggery

Exploit

- využívá programátorskou chybu, aby se útočník dostal do systému přes "díru v kódu"
- chyby v kódu mohou být neúmyslné a nebo úmyslné
  - autor kódu si může nechat tzv. "zadní vrátka" pro své vlastní pozdější využití
- obvykle je úmysl nainstalovat nežádoucí software a nezanechat po sobě stopu
  - software poté na zařízení páchá škody

Počítačový virus

- vytváří kopie sebe samého za využití jiných souborů
- může se přenášet i mezi zařízeními (např. přes USB disk)
- snaží se přebrat kontrolu nad PC

Počítačový červ

- oproti viru se červ šíří sám bez závislosti hostitele
- většinou se šíří přes síť
- automaticky rozesílá kopie sebe sama na další zařízení
- kromě kopírovaní se jeho škodlivá část snaží poškodit zařízení

DoS

- Denial of Service
- z jednoho počítače se posílá co nejvíce požadavků na určitý stroj
  - typicky na server nějaké webstránky
- útočník se snaží přehltit stroj požadavky tak moc, že nebude moci přijímat další
- útok cílový stroj zpomaluje a dokáže ho i úplně shodit
- v dnešní době je většinou použití jednoho počítače málo

DDoS

- Distributed Denial of Service
- stejný princip jako DoS
  - ovšem je rozdělen mezi více zařízení
- tím vzniká větší množství útočníku a větší efektivita
- těžší na odhalení než DoS, protože agresivita se rozloží mezi jednotlivá zařízení

Botnet

- síť uživatelů, kteří většinou netuší, že se v ní nacházejí
- do Botnetu se dostanou nevědomky
- celý Botnet je centrálně řízen z jednoho místa
- může vykonávat velké množství operací, jako je např. rozesílání spamu nebo DDoS útoky

Man in the Middle

- odposlech komunikace mezi dvěma účastníky
- pro každého z nich předstírá, že je ten druhý
- stává se aktivním prostředníkem

Ransomware

- zašifruje data uživatele a požaduje po něm výkupné
- peníze se typicky posílají přes kryptoměny z důvodu anonymity
  - podle ID kryptoměnové peněženky nelze vypátrat jejího autora
- může šifrovat soubory na pevném disku, nebo zamknout celý systém

---

Zabezpečení switche

MAC address flooding

- zaplavení MAC adresami, které se snaží vyčerpat paměť switche (CAM tabulky)
- zasílá velké množství rámců s neplatnými MAC adresami
- podobný princip, jako DoS
- switch se po naplnění tabulky začne chovat jako hub a posílat broadcasty, protože nemá místo na nové záznamy
  - díky tomu útočníkova stanice dostává informace, které pro ni nejsou určeny

DHCP snooping

- bezpečnostní funkce, která filtruje nebezpečné DHCP zprávy

1. po prvním startu jsou všechny porty nedůvěryhodné

2. některé se nastaví jako důvěryhodné (port s DHCP serverem a trunky, kterými jsou propojeny switche)
3. pokud packet DHCP serveru přichází z nedůvěryhodného portu, je zahozen

Port security

- metoda, která na daném portu kontroluje, zda packet přichází z povolené MAC adresy
- pokud se do zásuvky připojí jiné zařízení, tak se podle rozdílné MAC adresy přeruší komunikace

Zabezpečení bezdrátových sítí

WEP

- Wired Equivalent Privacy
- původni šifrovací systém, který byl už prolomen
- stále je podporován, ovšem není bezpečný

WPA

- Wifi Protected Access
- novější způsob ochrany
- při použití silného hesla je prakticky neprolomitelné
- implementováno na síťových kartách

WPA2

- nejnovější verze
- je založena na dodatku IEEE 802.11i