12 - Problematika bezpečnosti počítačových sítí

# Fyzická bezpečnost

* K serverům a jiným prvkům IT infrastruktury se nesmí dostat nepovalaná osoba – zamezení odcizení/poškození
* Autorizace pro vstup do určitých částí budovy
* Uzamčení serveroven, uzamčení racků, kamerové systémy, alarm, ochranka, ...
* Brát ohled přírodní vlivy, např.
  + Neumisťovat server do spodních pater v zátopových oblastech
  + Pod střechu, kde praží slunce
* Klimatizace, přepěťové ochrany, záložní zdroje, ...
* Stínění kabelů – vést kabel např. kovovou trubkou u stropu

# Sociální inženýrství

* Manipulace lidí za účelem provedení určité akce nebo získání určité informace
* Pretexting
  + Vytvoření smyšleného scénáře a přesvědčení oběti o jeho legitimnosti, aby následně provedla akci nebo vyzradila informace
  + Útočník po telefonu předstírá, že oběť vyhrála jakousi soutěž a chce po ní osobní informace („aby mohl poslat cenu“)
* Phishing
  + Získávání citlivých údajů na internetu pomocí zasílání falešných zpráv, které se tváří jako pravé (útočník se vydává za banku a chce údaje k ověření)
  + Záměna písmena f za ph má původu ze slova „phreaks“, což byla hackerská skupina v USA

# Zranitelnost

* Slabina v systému (bug, chyba v kódu)

# Exploit

* Nástroj, který dokáže využít slabiny (znatelnosti)

# Hrozba (threat)

* Jakákoli akce, která může zranit, zničit nebo jinak ovlivnit cenné věci (data na disku)

# Podvržení adres

* Změna IP adresy (v packet headeru)
* Slouží k zamaskování IP adresy útočníka

# DoS a DDoS

* (distributed) denial of service
* DoS způsobuje nedostupnost dané služby (většinou zahlcením dotazů)
* DDoS je DoS prováděný z vícero zařízení
  + Tyto zařízení většinou útok neprovádí dobrovolně, ale jsou ovládané pomocí škodlivého softwaru
  + Takovýmto zařízením se poté říká zombie a síti zombie botnet

# MITM – Man-In-The-Middle

* Útočník odposlouchává komunikaci mezi dvěma konci – přesměrování síťového provozu
* Může také komunikaci upravovat, oboustranně se vydávat za toho na druhém konci
* Útočník může získat citlivá data nebo se za někoho vydávat

# Průzkumné útoky

* Útok, při kterém útočník shromažďuje veškeré možné informace před tím, než zaútočí

# Malware

* Název pro úmyslně škodlivý software
* Trojský kůň
  + Malware schovaný v užitečném softwaru (hra, filmy)
* Virus
  + Vkládá svůj kód do spustitelných souborů
  + Replikuje se, potřebuje hostitele (software)
  + Zabírá místo na disku a snižuje výkon
* Worm
  + Replikuje se po síti
  + Nepotřebuje hostitelský software
  + Zatěžuje síť
* Ransomware
  + Zašifrování dat oběti
  + Požadováno výkupné (většinou v kryptoměnách)

# Zabezpečení síťových prvků

* ARP Flooding
  + Zaplavení MAC adresami (vyčerpá se kapacita ARP tabulky)
  + Switch poté začne framy rozesílat jako broadcast
  + Obranou je Port Security
    - Povolí jen určité MAC adresy nebo určitý počet MAC adres
* DHCP Starvation
  + Útočník opakovaně rozesílá DHCP requesty za účelem vyčerpání adresního poolu
  + Ostatní uživatelé poté nedostanou adresu
* DHCP Spoofing
  + Útočník odpovídá na DHCP requesty (namísto DHCP serveru)
  + Nastaví sebe jako výchozí bránu nebo DNS server
  + Díky tomu může zachytávat provoz na síti
* DHCO Snooping
  + Obrana proti DHCP Spoofing
  + Na přepínači lze nastavit trusted a untrusted porty
  + U nedůvěryhodných portů lze omezit počet DHCP requestů, nebo je úplně zakázat
* BPDU guard
  + Zamezuje posílání BPDU na určitém portu (znamená připojení nepovoleného switche)

# Zabezpečení bezdrátových sítí

## WEP – Wired Equivalent Privacy

* Šifrování omunikace
* Symetrická šifra
* Snadno prolomitelné

## WPA – Wi-Fo Protected Access

* Reakce na nedostatky WEP
* Šifra RC4
* TKIP – Temporary Key Integrity Protocol – Pro každý paket je používán jiný klíč (považován za nedostatečně bezpečný)

## WPA2

* Šifra AES
* Prolomeno – KRACK (2017)

## WPA-Personal (WPA-PSK – pre-shared key)

* Domácí použítí, nevyžaduje autentifikační server

## WPA-Enterprise

* Využití autentifikačního serveru (RADIUS)

## IEEE 802.1X

* Standard popisující zabezpečení přístupu do sítě a odesílání EAP zpráv po místní síti
* Suplikant, autentifikátor a autentifikační server
* Suplikant (klient) se nemůže dostat do chráněné části síte, dokud není jeho identita ověřena
* Suplikant předá požadované údaje autentifikátoru
* Ten je přepošle autentifikačnímu serveru, který rozhodne, jestli může suplikant přistoupit k síti, či nikoli

## EAP – Extensible Authentication Protocol

* Autentifikační framework
* Umožňuje výrobcům snadno vyvíjet a nasazovat nové autentifikační metody (EAP metody)

## AAA – Authentication, Authorization, Accounting

* Autentifikace – identita uživatele (kdo jsi?)
* Autorizace – k čemu máš přístup?
* Účtování – monitorování využívání sítě

## RADIUS

* AAA client/server protokol
* Back-end pro 802.1x autentifikaci