25. Bezpečnost v počítačových sítích

Bezpečnost v počítačových sítích a obecně v informatice je velmi důležitá.

Důvody útoků/proniknutí a proč se chránit:

- **Získání dat**
  - Získání důležitých, citlivých dat konkurence, které můžou následně být využity k obchodování a dalším věcem. V dnešní době jsou informace o konkurenci, o nových poznatcích a plánech velmi ceněná
- **Sabotování**
  - Útočníkovi jde o narušení dané sítě nebo zpomalení. Nebo o to, aby nemohla probíhat klasická komunikace. Důvodem je škodit, nebo upozornit na špatné praktiky (politiků, bank..) Jedná se i např. o DDOs útoky

Z těchto důvodů je potřeba mít dostatečně ochráněnou a zabezpečenou sít.

Základní bezpečnostní předpoklady

- Fyzicky nedostupné prvku
  - Schované kabely; zamknuté racky; nepřístupné zásuvky…
- Vypínat neaktivní porty

Port Security

Jedná se o prvotní ochranu na switchích.

Port security je jednoduchá a zajímavá metoda zabezpečení přístupu do sítě. Na portu, kde je nastavena, kontroluje, zda pakety přichází z povolené MAC adresy. Pokud tedy uživatel připojí do zásuvky jiné zařízení, nebude moci komunikovat.

Pro nastavení Port security musí být port ve statickém módu (trunk, access, ale ne dynamic)

Dále se volí, co se děje při porušení pravidel, tedy pokud přijde komunikace z MAC adresy, která není povolena (a dosáhlo se maxima). Default je shutdown.

Možnosti jsou:

- **Protect** – nepovolená komunikace je zahazována, povolené MAC adresy stále komunikují
- **Restrict** – pošle informativní SNMP trap
- **Shutdown** – port se zablokuje, přepne do stavu Error-disabled (pro opětovné zapnutí je třeba jej nejprve vypnout)

Pokud se port přepne do Error-disabled stavu, tak je třeba zásah administrátora, aby jej opět zapnul. Je však možno nastavit i automatické znovuzapnutí portu po určité době.

Může se nastavit kolik MAC adres pro port (nebo určitou VLANu) je povoleno (například pokud je do portu připojen switch). Defaultní hodnota je 1.

Pokud se nezadá žádná povolená MAC adresa, tak se používají adresy dynamicky (dočasně se ukládají pro aktuální komunikaci až do maxima). Nebo lze MAC adresy zadat ručně jako statické adresy. U dynamických adres lze nastavit, aby se tyto adresy ukládaly do běžící konfigurace (vytvoří se statický záznam, ale pokud se neuloží konfigurace, tak se po restartu smažou).

K porušení pravidel dojde také v případě, kdy je MAC adresa zadaná pro určitý port a tato adresa se objeví na jiném portu tohoto switche.

Ve výchozím stavu po zapnutí Port security, je povolena jedna MAC adresa, která se používá dynamicky, tedy první zařízení, které začne komunikovat. Pokud se pokusí komunikovat další zařízení, dojde k zablokování portu.

Hlavní příkazy pro zobrazení informací o Port security jsou

```
SWITCH#show port-security          // info pro všechny interface
SWITCH#show port-security address // tabulka MAC adres a související info
SWITCH#show port-security interface f0/1 // detailní info pro interface
```

Nastavení Port Security

```
SWITCH(config)#interface f0/5      // konfigurace daného portu switche
SWITCH(config-if)#switchport port-security  // zapnutí port security
SWITCH(config-if)#switchport port-security maximum 1  //  počet  MAC adres, 1 je default
SWITCH(config-if)#switchport port-security violation shutdown
// při porušení zablokovat port, default
SWITCH(config-if)#switchport port-security mac-address sticky
// napevno uložit dynamickou MAC adresu
```

Dalším typem zabezpečení je rozdělení sítě do jednotlivých **VLAN**. Síť pak je rozdělena na jednotlivé části, z nichž má každá jiný přistup a ochranu. Např. část sítě s citlivými daty firmy je oddělena do samostatné VLANy, která je odříznuta od internetu.

Dále se vytvoří VLANa, která oddělí síť pro vedení firmy, pro zaměstnance, a pro studovnu.

Dalším zabezpečením je použít routery, které vlastně jsou vstup mezi celosvětovou sítí (internet) a zde pomocí firewallu kontrolovat nežádané přístupy a požadavky z venčí. Firewally je dobré použít od více vydavatelů.

Access Control List; ACL

Seznam pravidel, která řídí přístup k nějakému objektu. ACL jsou používány v řadě aplikací, často u aktivních síťových prvků, ale třeba také u operačních systémů při řízení přístupu k objektu (souboru). Pokud někdo požaduje přístup k nějakému objektu, tak se nejprve zkontroluje ACL přiřazený k tomuto objektu, zda je tato operace povolena (případně povolena komu)(když ne tak to zablokuje). Layer 2 switch = pouze směr in.

any = 0.0.0.0 255.255.255.255

host = 10.0.5.2 0.0.0.0

Důvody zavedení ACL

- Kontrola šířky pásma → omezení provozu
- Policy Based Routing
- Identifikace, klasifikace
- Vynucení síťových politik

Stručná charakteristika a vlastnosti

- ACL je sekvenční (řazený) seznam pravidel; permit (povolit) a deny (zakázat)
- ACL můžeme identifikovat číslem nebo jménem (pojmenované ACL)
- Nová pravidla se přidávají vždy na konec seznamu
- Používá se pravidlo first-fit. Seznam se prochází od začátku ke konci, a pokud dojde ke shodě, tak se dále neprochází
- Každý neprázdný seznam má na konci defaultní pravidlo, které zakazuje vše (deny any)
- Prázdný seznam povoluje vše
- Je dobré umísťovat více specifická pravidla na začátek a obecná (subnety apod globální) na konec
- Pokud se v ACL vyhodnotí deny, tak se odešle ICMP host nedosažitelný (unreachable)
- Filtrování (používání ACL) zpomaluje zařízení (stojí výpočetní výkon)

Dělení ACL

- **Standard ACL** – starší a jednodušší verze ACL s méně možnostmi konfigurace
- **Extended ACL** – novější a složitější ACL s více možnostmi

Dále se ACL (standard a extended) dělí na číslovanou a pojmenovanou. Udává se číslem nebo pojmenováním

Standard ACL – standardní ACL

- Používá čísla 1 - 99 a 1300 - 1999 v rozšířeném módu
- Je jednoduché na konfiguraci
- Filtruje (dívá se) pouze podle zdrojové adresy a používá se jako odchozí
- Používá se pro blokování provozu blízko cíle
- Konfigurace standard i extended ACL se provádí stejně, rozlišuje se podle použitého čísla.

Extended ACL – rozšířené ACL

- Používá čísla 100 – 199 a 2000 – 2699 v rozšířeném módu
- Filtruje (dívá se) na IP adresu zdroje i cíle
- Kontroluje řadu položek v hlavičce vrstvy 3 a 4 (protokol, port apod.)
    - Ve **3. vrstvě** ISO/OSI, tedy v IP hlavičce kontroluje: IP adresy, protokol, údaje z ToS (Type of Service – prioritu 802.1q a službu)
    - Ve **4. vrstvě** kontroluje v **TCP hlavičce**: porty a protokoly, **v UDP hlavičce**: porty
- Může blokovat provoz kdekoliv (nejlépe blízko zdroje)

Named ACL – pojmenované ACL

- Standard i extended ACL
- Umožňuje upravovat či mazat jednotlivá pravidla v ACL
- Jména se lépe pamatují
- Lze použít "neomezený" počet pojmenovaných ACL
- Jako jméno lze použít i číslo, ale to musí patřit do správného rozsahu

Numbered ACL – Číslovaná ACL

Konfigurace ACL se provádí ve dvou krocích

- **Vytvoření ACL** – nejprve se vytvoří pravidla podle typu ACL
- **Aplikace ACL na rozhraní** – následně se musí toto ACL přiřadit k nějakému objektu, v tomto případě interfacu, to se provádí vždy stejně

Standard ACL se umisťuje blízko cíle a měl by tedy být vždy odchozí – out.

Extended ACL se většinou nejlépe umístit co nejblíže ke zdroji a v tom případě je filtr vstupní – in.

Příklad zablokování pc na switchi

```
access-list 25 deny host 192.168.035 //zablokuje(deny) pc s touto ip
access-list 25 permit any          //povolení ostatním
show access-lists                  //vypíše accesslisty
(conf-if)#ip access-group 25 in    //použije se daný list(25) na tento port
```

IDS a IPS systémy

Bezpečnostní metody systémů IDS / IPS lze rozdělit přibližně do těchto tří hlavních oblastí:

- Detailní inspekce všech paketů (ať již mezi LAN a WAN, tak i pouze v rámci LAN) dle definovaných signatur, tj. definovaných známých řetězců
- Kontrola portů / protokolů / adres
- Komplexní sledování provozu sítě

Při nestandardní události pak systém vyhodnocuje, zda se nejedná o průnik nebo jiné narušení.

Může se jednat buď o krabici zařazenou na trase přenosu dat, nebo o software na serveru

IDS; Intrusion Detection Systém; Systém pro odhalení (detekováni) průniku

Obranný systém, který monitoruje síťový provoz a snaží se odhalit podezřelé aktivity. Hlavními činnostmi IDS systému je detekce neobvyklých aktivit, které by mohly vést k narušení bezpečnosti operačního systému nebo počítačové sítě a též možný aktivní zásah proti nim. Hlavním prvkem IDS je senzor, který obsahuje mechanismy pro detekci škodlivých a nebezpečných kódů a jeho činností je odhalování těchto nebezpečí.

Systém IDS by měl po detekci neobvyklé aktivity vygenerovat varování (Alert), provést zápis do logu, upozornit správce počítače a případně tuto činnost zastavit. Dále by měl být schopen rozlišit, zda se jedná o útok z vnitřní sítě nebo z externích sítí.

IDS systém je méně náročný na hardware než IPS.

IPS; Intrusion Prevention Systems; Systémy pro prevenci (předcházení) průniku

Snaží se předcházet útokům, aby k nim vůbec nedošlo (popř. automaticky sám je blokovat..)

Hlavní funkce IPS systémů jsou identifikace škodlivé činnosti, zaznamenávání informací o jejím průběhu, následném blokování této činnosti a také její nahlašování.

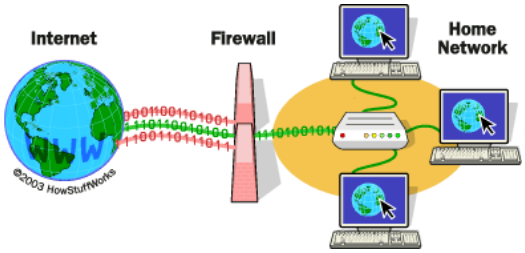
IPS jsou považovány za rozšíření IDS systémů, protože se i snaží útokům předcházet a ne jen detekovat.

Hlavní rozdíl oproti IDS systémům je, že systém IPS je zařazen přímo do síťové cesty (in-line), a tak může aktivně předcházet, případně blokovat detekovaný nežádoucí a nebezpečný provoz na síti. Konkrétněji, IPS

může provádět takové akce jako vyvolání poplachu, filtrování škodlivých paketů, násilné resetování spojení a/nebo blokování provozu z podezřelé IP adresy. Všechny tyto úkony často provádí ve spolupráci s firewallem. IPS také umí opravit chybný **cyklický redundantní součet** (**CRC**), defragmentovat proudy paketů, předcházet problémům s řazením TCP paketů, a čistit nežádoucí přenos včetně nastavení síťové vrstvy.

Většina IPS systémů využívá jednu ze tří detekčních metod: stavové detekce značek (signatur), odhalení provozních anomálií a odhalení protokolových anomálií.

Firewall



Slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení (kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje).

Ze začátku stačilo pouze pár pravidel (identifikace zdrojové, cílové adresy, port…), dnes je to již velice nedostačující.

Nové firewally se opírají přinejmenším o informace o stavu spojení, znalost kontrolovaných protokolů a případně prvky IDS. Na základě pravidel novější firewally dokážou i routovat.

Paketové firewally (filtry)

Pravidla přesně uvádějí, z jaké adresy a portu na jakou adresu a port může být doručen procházející paket (kontrola se provádí na 3. a 4. OSI). Na úrovní ACL.

Výhody

Rychlý

Nevýhody

Nízká úroveň bezpečnosti; U složitějších protokolů prakticky nepoužitelný.

Aplikační firewally (filtry)

Na rozdíl od paketových filtrů zcela odděluje sítě, mezi které je postaven. Veškerá komunikace přes aplikační bránu probíhá formou dvou spojení – klient (iniciátor spojení) se připojí na aplikační bránu (proxy), ta příchozí spojení zpracuje a na základě požadavku klienta otevře nové spojení k serveru, kde klientem je aplikační brána. Data, která aplikační brána dostane od serveru, pak zase v původním spojení předá klientovi. Kontrola se provádí na 7. vrstvě OSI

Server nevidí zdrojovou adresu klienta, který je původcem požadavku, ale jako zdroj požadavku je uvedena vnější adresa aplikační brány. Aplikační brány díky tomu automaticky působí jako nástroje pro překlad adres (NAT), nicméně tuto funkcionalitu má i většina paketových filtrů.

Výhody

Zabezpečení na vysoké úrovni u známých protokolů (FTP, kontrola příloh pošty)

Nevýhody

- Vysoká HW náročnost
  - Jsou schopny zpracovat mnohonásobně nižší množství spojení a rychlosti
  - Každý protokol vyžaduje napsání specializované proxy, nebo využití tzv. generické proxy, která ale není o nic bezpečnější, než využití paketového filtru
- Vysoká latence (kvůli 7. vrstvě)

Stavové firewally (filtry)

Provádějí kontrolu stejně jako jednoduché paketové filtry, navíc si však ukládají informace o povolených spojeních (**CTT**), které pak mohou využít při rozhodování, zda procházející pakety patří do již povoleného spojení a mohou být propuštěny, nebo zda musí znovu projít rozhodovacím procesem. To má dvě výhody – jednak se tak urychluje zpracování paketů již povolených spojení, jednak lze v pravidlech pro firewall uvádět jen směr navázání spojení a firewall bude samostatně schopen povolit i odpovědní pakety a u známých protokolů i další spojení, která daný protokol používá. Zásadním vylepšením je i možnost vytváření tzv. virtuálního stavu spojení pro bezstavové protokoly (UDP) a ICMP.

Výhody

- Vysoká rychlost; Efektivnější
- Dobrá úroveň zabezpečení
- Snazší konfigurace (než aplikační, paketové)

Nevýhody

- Nižší bezpečnost, než poskytují aplikační brány
- Hromada paměti (informace o spojeních…)

Nové firewally; Next-Generation Firewall

Firewally „další generace“ umí vše, co uměli staré firewally (NAT, filtrování paketů, VPN…). Cílem NGFW je zahrnout více vrstev OSI modelu, za účelem zlepšení filtrování síťového provozu na základě obsahu paketu.

NGFW provádějí hlubší inspekci než stavové firewally, zkoumají obsah paketu a hledají shodu (Virusy, malware, zranitelnost…).

Zapojení firewallu do sítě → sledování trafiku → statistika → blokace.

Dlouho trvá než se firewall “naučí“.

NFGW zaručují:

- Kompatibilita se “starýma“ firewallama
- Integrovaný IPS/IDS
- SSL dešifrování pro identifikování nechtěných zašifrovaných aplikací
- Logování trafiku
- Statistika
- Anomálie na síti (heuristická analýza)
- Antispam
- …

Ověření vůči radio serveru

Autentifikace.

Na základě přihlášení uživatele“

- Otevřít extra port
- Zařadit ho do určité VLANy
- Kontrolovat rychlost
- …