Analýza a zabezpečení počítačové sítě

Firewall, IPS, Netflow

Ing. Jakub Žák, redtoo

Základní informace o síti

- Z čeho se počítačová síť skládá?
- Switch, hub, router, firewall, servery, NAS,.....
- Úplná síťová dokumentace- schéma zapojení všech síťových prvků s IP adresami případně i informacemi o routingu a umístění jednotlivých zařízení.
- Dokumentace zapojení serverů
- Informace o aplikacích na serverech
- Procesy na správu a udržování dokumentace

Základní informace o síti

- Reálná situace- většina podniků tuto dokumentaci nemá. Komplikace v případě výpadku, řešení problému je mnohem komplikovanější
- Důsledek? Vyšší ztráty při výpadku sítě, delší doba řešení. V důsledku dražší než investice do správné dokumentace a hardwaru!
- Je důležité znát svoji síť, jak jí zmapovat?
- Základní rozdělení je na infrastrukturu (switche, routry, firewally, IPS,AP,...)
- Koncové body (PC, servery, tiskárny,...)

Mapování sítě a datových toků

- Základní nástroje- většinou zdarma
- **Netflow**- vyvinuto firmou Cisco, je součástí jejich zařízení. Ale i mnoho jiných výrobců netflow podporuje
  - Umožňuje získat informace o datách protékajících přes určité porty. Získané údaje obsahují IP adresy, porty, třídu služeb. Základní informace o datových tocích. Vytížení určitých linek, zjištění přetížení sítě,...
- **Síťový analyzátor(sniffer)**- může být softwarový (Wireshark) nebo hardware od různých výrobců. Je nutné zpracovat velké množství dat
  - Software- je nutné přesměrovat data na jeden systém, kde probíhá zachycení dat. Je nutná konfigurace v síti a ne vždy je to možné. Wireshark-zdarma
  - Hardware- speciální zařízení, zapojí se do sítě (pro uživatele je neviditelné). Následně je možné data analyzovat, nebo generovat statistiky (lze využít i firewall a IPS)

Zabezpečení sítě, koho se týká?

- Vládní organizace
- Nadnárodní koprporace
- Bankovní ústavy
- ....
- Menší a střední podniky?
- Hodnocení rizikovosti- je na rozhodnutí každé firmy
- Technologické firmy- Strojírenské, elektrotechnické, potravinářské, atd...
- ICS- industrial control systems (PLC, SCADA,...)
- Stroje konstruované na výrobu- maximální spolehlivost, dlouhá životnost, zabezpečení na okraji zájmu přesto je třeba připojení k síti.
- Málo prostoru na upgrade softwaru- většinou se „nešahá“ na to co funguje – Windows XP, WIN CE apod – velké bezpečnostní riziko

Bezpečnostní situace

- Velké téma součastnosti- mnoho velkých útoku medializováno
- Firmy se zajímají a začínají implementovat zabezpečení- komplexní problematika
- Pro oblast ICT zlomový rok 2010 ? Stuxnet
- Útoky na technologické sítě jsou možné a velmi snadné (SCADA,PLC většinou mají defaultní hesla). Externí přístup dodavatele pro servis-stroje na veřejné IP adrese...
- Nezabezpečený WIN XP- do 30 minut nakažen virem
- Falešný pocit bezpečí- nemáme viditelné problémy = vše je v pořádku
- Statistiky- nejvíce útoků vedených z Číny a Ruska
- Důvody:
  - Konkurenční boj
  - Průmyslová špionáž
  - Vydírání – zaplaťte pokud chcete svá data...

Zabezpečení na síťové úrovni

- Nejzákladnější krok- velmi často opomíjen
- **Správný design sítě** –
  - Členění sítě na funkční bloky oddělené firewallem
  - Vicerovňová hierarchie- každá úroven má jinou funkcni
  - Zabezpečené uživatelských portů:
    - Proti připojení cizích zařízení
    - Proti broadcast bouřím
    - Některým síťovým útokům
- Ulehčí a zlevní další zapezbečení

Firewall

- Základní a nejpoužívanější zařízení pro zabezpečení sítě
- Provádí filtrování paketů (datová jednotka, která se přenáší IP sítí)
- Základní parametry pro filtrování je Zdrojová a cílová IP adresa a protocol a port:

Source: 192.168.100.10

Destination: 8.8.8.8

Service: TCP 8080

- Statefull firewall – uchovává informace o datovém toku, zpětný provoz automaticky povolen
- Slabina?
- Provádí kontrolu do 4. vrstvy ISO/OSI -> malware, adware atd není rozeznán
- Dobrý začátek, ale sám o sobě nestačí

IPS

- IPS - Preventions System – zařízení, které přináší vyšší úroven zabezpečení sítě
- IPS většinou nefiltruje provoz na základě IP adres jako firewall, ale provádí hloubkovou analýzu paketů. To znamená, že vidí i služby které komunikují a dokáže rozeznat různé typy útoků a školivých kódů.
- Pokud je nějaká komunikace shledána podezřelou, je zablokována nebo je odesláno upozornění.
- Kontrola provozu se provádí na základě signatur, chování nebo exaktních pravidel
- Může chránit před DDOS útoky
- Může blokovat určité aplikace- Facebook, Torrent, chaty, atd
- Provádět Traffic shaping- omezit určité pásmo pro aplikace
- V některých případech spojen s Firewallem

Nadstandartní zabezpečení

- WEB application firewall- speciální zařízení na ochranu webových serverů/aplikací
- Proxy server – také může provádět filtering komunikace. Kategorizace webů- blokování některých kategorií, atd
- NAC – network admission control, systém řízení přístupu do sítě. Na základě identity uživatele je mu umožněn přístup na síť s určitými pravidly. Velmi pokročilé zabezpečení. Možnost trackování aktivit uživatelů!
- Logování aktivit- Firewall, IPS, WAF, proxy server- velké množství záznamů aktivit jak je zpracovat a uchovat?
- Pro úschovu log servery- důkeřité uchovat data pro případné dohledání hrozeb, útoků,...
- Zpracování dat- SIEM (security information and event management)- téma i na několik přednášek. Umožňuje data zpracovat do nějaké struktury aby se v nich dalo lépe vyledávat. Přidává logiku nad pouhé logy ze všech zařízení.
- Vytváření ticketů, notifikace, atd....

Investovat či ne?

- Každá firma by se měla investice do sítě zvážit. Platí i pro strojírenství
- Porovnat investice s přínosy- kolik lze ztratit peněz výpadkem sítě nebo ztrátou dat?
- Pokud se hacker rozhodne napadnout systém, dříve nebo později se mu to povede!!
- Smysl zabezpečení? – Ztížit útok tak, aby byl zisk menší než úsilí na překonání ochrany!!

Výhody a nevýhody

- Výhody:
  - Viditelnost komunikace s síti- reporty
  - Omezení nežádoucích aktivit (FB, chat, youtube,..)
  - Zvýšení rychlosti a spolehlivosti sítě = snížení nákladů
  - Jednodušší řešení problémů, jednodušší správa sítě
  - Vyšší bezpečnost dat
- Mínusy:
  - Investice
  - Zhoršení užvatelského komfortu (FB, youtube atd nefunguje)
  - Výpadky při implementaci
  - Je to změna, vždy se vnímá negativně

Otázky? Diskuze...

- Diskuze možná,....

DĚKUJI ZA POZORNOST