Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Bezpečnostní analýza síťového provozu

Viktor Kult

! ! !

Místo tohoto textu vložte PŘEDNÍ stranu zadání práce, které si můžete vyexportovat do PDF v IS.CZU.cz, pokud již máte schválené zadání i děkanem PEF.

! ! !

! ! !

Místo tohoto textu vložte ZADNÍ stranu zadání práce, které si můžete vyexportovat do PDF v IS.CZU.cz, pokud již máte schválené zadání i děkanem PEF.

V případě, že Vaše zadání je na více než 2 strany, vložte i další strany.

! ! !

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Bezpečnostní analýza síťového provozu" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 29.11. 2016 _____

Poděkování

Rád bych touto cestou poděkoval panu Ing. Martinu Havránkovi, Ph.D. za konzultace závěrečné práce a spolupráci na jejím vypracování.

Bezpečnostní analýza síťového provozu

Souhrn

Téma diplomové práce se týká problematiky informační bezpečnosti v oblasti korporátního prostředí. Literární rešerši tvoří informace získané studiem článků a odborné literatury z oblasti informační bezpečnosti. Byly vybrány zdroje se zaměřením na bezpečnostní rizika, bezpečnostní technologie a legislativní nařízení. Pozornost je zaměřena především na technologie podporující monitoring komunikačních toků v datové síti. Přehled o provozu v datové síti poskytuje důležité informace pro prevenci nebo vyšetřování bezpečnostních incidentů. Dále slouží jako zdroj informací pro plánování síťové infrastruktury. Dokáže odhalit poruchy nebo nedostatečné přenosové kapacity. Praktická část se věnuje implementaci monitorovacího systému v prostředí reálné korporátní sítě. Součástí praxe je analýza síťové struktury a volba vhodných nástrojů k samotné realizaci. Při volbě nástrojů lze využít bodovací metody vícekriteriální analýzy variant. Součástí integrace monitorovacího systému je také konfigurace aktivních prvků sítě. Následná analýza datových toků v síti přináší informace o nejaktivnějších uživatelích, nejpoužívanějších aplikacích nebo o zdrojích a cílech přenášených dat. To přináší zdroj cenných informací, které mohou být využity v případě poruchy na síti nebo bezpečnostního incidentu. Závěr práce je věnován shrnutí výsledků a pracovního postupu.

Klíčová slova: NetFlow, sFlow, IPFIX, IDS, IPS, DPI, NBAR, SIEM, TAP, SPAN, WORM, BOTNET

Analysis of data network traffic

Summary

Thesis topic concerns the issue of information security in corporate environments. Literature search includes information obtained by studying articles and literature in the field of information security. Resources were selected with a focus on the security risks, security technologies and legislative regulation. Attention is focused on technology that supports monitoring of communication flows in the data network. Overview of traffic operating a data network provides important information for the prevention or investigation of security incidents. Monitoring also serves as a source of information for the planning of the network infrastructure. It can detect faults or insufficient transmission capacity. The practical part is dedicated to implementation of the monitoring system in the real corporate networks. Part of the experience is the analysis of the network structure and choice of appropriate tools for actual implementation. When selecting tools, you can use the scoring method of multicriterial analysis options. The integration of the monitoring system is also the configuration of active network elements. Subsequent analysis of network traffic provides information about the most active users, most used applications or on the sources and targets of data transmitted. It provides a source of valuable information that can be used in case of failure on the network or security incident. The conclusion is a summary of the results and workflow.

Keywords: NetFlow, sFlow, IPFIX, IDS, IPS, DPI, NBAR, SIEM, TAP, SPAN, WORM, BOTNET

Obsah

1 Úvod 10

2 Cíl práce a metodika 11

2.1 Cíl práce 11

2.2 Metodika 11

3 Teoretická východiska 12

3.1 Network visibility 12

3.2 Komponenty Flow monitoringu 23

3.3 Bezpečnostní hrozby v datové síti 37

3.4 Nařízení a normy 49

4 Praktická část 52

4.1 Stanovení a formulace cílů 52

4.2 Monitorované prostředí 52

4.3 Použité nástroje 57

4.4 Návrh systému pro monitoring 61

5 Výsledky a diskuse 63

5.1 Agregované výsledky - celkové 63

5.2 Detailní informace o datových tocích 65

5.3 Diskuse 65

6 Závěr 67

7 Seznam použitých zdrojů 70

Seznam obrázků

Obrázek 1 - Souvislost mezi NetFlow a NBAR 18
Obrázek 2 - Přehled vstupních a výstupních informačních toků SIEM 21
Obrázek 3 - Monitoring při podpoře NetFlow síťovými prvky 24
Obrázek 4 - Monitoring při využití portu s odposlechem (SPAN) 24
Obrázek 5 - Využití TAP při monitorování síťového provozu 25
Obrázek 6 - SolarWinds – seznam aktivních exportérů (ukázka) 28
Obrázek 7 - sFlowTrend – průběh zatížení procesoru 29
Obrázek 8 - Scrutinizer – přehled nejpoužívanějších protokolů 30
Obrázek 9 - ManageEngine – přehled nejužívanějších protokolů 31
Obrázek 10 - nTop – žebříček nejaktivnějších uživatelů sítě 32
Obrázek 11 - PRTG – aktivita komunikace z různých podsítí 33
Obrázek 12 - Wireshark – barevné rozlišení podle typu komunikace 34
Obrázek 13 - InterMapper – uživatelé vykazující nejvyšší aktivitu 35
Obrázek 14 - Schéma administrativního pracoviště 53
Obrázek 15 - Schéma pracoviště na prodejně 54
Obrázek 16 - Připojení sondy na hranici MPLS páteře 56
Obrázek 17 - Schéma získávání agregovaných výstupů 62
Obrázek 18 - Graf – Nejaktivnější uživatelé 63
Obrázek 19 - Graf – Nejpoužívanější protokoly 64

Seznam tabulek

Tabulka 1 - Podpora NetFlow verze 9 významnými výrobci aktivních prvků 26
Tabulka 2 - Přehled OpenSource nástrojů 27
Tabulka 3 - Přehled placených nástrojů 36
Tabulka 4 - Přehled o podpoře exportu záznamů 55
Tabulka 5 - Bodové ohodnocení preferencí kritérií a výpočet vah 60
Tabulka 6 - Deklarace bodování pro jednotlivé úrovně kritérií 60
Tabulka 7 - Výpočet pořadí posuzovaných variant 61

1 Úvod

Vývoj v oblasti informačních technologií má za následek usnadnění lidského úsilí, které člověk odedávna vynakládá k získání, doplnění, předávání a zpracování informací. V rychlosti rozvoje, je oblast elektrotechniky a informačních technologií jedním z nejvýraznějších. Právě takový rozvoj umožnil začlenit informační technologie v nejrůznějších podobách do běžného života.

Práce s informacemi při využití moderních technologií vedla k vytvoření bezpečnostních postupů a nástrojů pro jejich ochranu. Zabezpečení a ochrana informací před jejich ztrátou stále nabývají na důležitosti. Elektronické zpracování informací využívá v současnosti stále větší okruh organizací. Jedná se o organizace státní správy i komerční podniky. Lze předpokládat, že státní organizace zpracovávají citlivé informace v nejrůznějších civilních registrech, ale i v oblasti bezpečnostních složek a obrany státu. U komerčních podniků a neziskových organizací jde většinou o různé druhy databází s informacemi o zákaznících, produktech a duševním vlastnictví. Řada takových subjektů se dnes nachází pod dohledem vládních (zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů) i komerčních nařízení.

Komerční i státní normy připisují odpovědnost za uložené informace samotným organizacím, které danými informacemi disponují. To podporuje snahy o posílení informační bezpečnosti, která je v této době důležitou součástí moderních informačních systémů.

V souvislosti s rozvojem informačních systémů došlo ke vzniku rozsáhlých a výkonných počítačových sítí. Prostředí veřejných (Internet) i privátních počítačových sítí je nedílnou součástí systémů pro zpracování a přenos dat. Ochrana informací v prostředí počítačové sítě se tak stává částí celkového systému informační bezpečnosti.

Jedním z důležitých součástí síťové bezpečnosti je přehled o provozu datové komunikace, kterou daná počítačová síť umožňuje. Za účelem získání přehledu o datové komunikaci vznikla řada technologií, která takový přehled umožňuje. Často používanou se stala technologie IPFIX (NetFlow), která svými komponenty a zpracováním získaných informací pomáhá utvářet obraz komunikace v rámci datové sítě. Předmětem praktické části této diplomové práce je integrace prvků zmíněné technologie a získání přehledu o datové komunikaci v prostředí informačních systémů komerční společnosti.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem diplomové práce je nalezení a identifikace autorizované i neautorizované datové komunikace v prostředí korporátní sítě použitím moderních informačních technologií.

Dílčím cílem je návrh a praktické ověření postupu k získávání, zpracování a vyhodnocení informací získaných pozorováním datových toků v kritických uzlech síťové topologie.

2.2 Metodika

V části literární rešerše budou představeny protokoly, metody a zařízení pro monitoring datových toků v síti. To umožní přiblížit vlastnosti a postupnou genezi jednotlivých technologií pro vzájemné porovnání. Zmíněny budou zejména technologie, kterých je dále použito v praktické části. Dále budou součástí rešerše zmíněna častá bezpečnostní rizika, která je možné prostřednictvím monitoringu datových toků odhalit.

V praktické části bude nejprve popsáno monitorované síťové prostředí. V dalším kroku budou zvoleny nástroje a body sítě pro získávání požadovaných informací. Nástroje budou voleny na základě jednotlivých vlastností metodou multikriteriálního rozhodování. V závěru praktické části budou nasbíraná data zpracována prostřednictvím statistických metod softwarových nástrojů. Po zpracování dat bude provedena jejich interpretace. V závěru práce budou vyhodnocena zjištěná fakta vyplývající z pozorování a posouzena úroveň zabezpečení v rozsahu zkoumaného prostředí. Uvedeným způsobem bude zároveň zdokumentován možný postup k provedení bezpečnostního auditu na úrovni datových toků.

3 Teoretická východiska

3.1 Network visibility

Využití Network visibility přináší nejsnazší způsob, jak získat přehled o tom jaké typy komunikací na síti probíhají. Do jisté míry umožňuje zjistit i to, jaké aplikace se na vytváření datových toků podílejí. Tyto informace získává o lokálních sítích (LAN) i o sítích rozsáhlých (WAN). Pokud má správce síťové infrastruktury takové podklady, tak teprve potom může efektivně a vědomě ovládat síťové aktivity. Získané informace o šířce přenosových pásem správce může využít třeba k preventivním opatřením, která zamezí nedostupnosti serveru se službami, které jsou kritické pro obchodní činnost firmy.

Průběžný dohled síťových aktivit na datové síti je přínosný k proaktivnímu vyhledávání kritických uzlů, které by mohly v budoucnu negativně ovlivnit datový provoz. K tomu se využívá vlastností nástrojů pro Network visibility, které jsou schopny detekovat překročení přednastavených prahových hodnot. Takto ošetřená síť umožňuje rychlé odhalení příčiny některých případných výpadků sítě.

Network visibility je užitečný pro monitorování všech aplikací, které na síti komunikují. Umožňuje zjistit, kdy a kým byla aplikace použita? Odpovědi na některé z těchto otázek vytváří užitečný přehled o komunikaci v síti. Vhodná kombinace monitorovacích nástrojů může správci nabídnout i mnohem detailnější informace o komunikaci aplikací jako jsou: porty transportního protokolu nebo IP adresy.

Dohled sítě může sloužit i k jiným účelům, než jen získávání aktuálních informací o datových komunikacích. Poskytuje také důležité informace o nárůstu datové komunikace v jednotlivých segmentech sítě. Zjištěné trendy růstu datových toků, umožňují rozhodování při plánování přenosových kapacit sítě.

Odhalení neautorizované komunikace je další výhoda Network visibility. Takový nežádoucí provoz může obsadit tak velkou část přenosové kapacity, že způsobí nedostupnost kritických podnikových aplikací. Pokud správce využije správné komponenty Network visibility, tak může sledovat aplikace, které při své komunikaci dynamicky mění porty transportního protokolu. Nástroje tohoto typu, je vhodné používat zejména na segmentech sítě typu WAN.

3.1.1 Datový tok (Network flow)

Datový tok lze charakterizovat, jako sekvenci paketů, které mají společnou zdrojovou a cílovou IP adresu, zdrojový a cílový port a stejný IP protokol.

Informace o sestavených datových tocích se ukládají do záznamů (flow records). Tyto záznamy obsahují souhrn základních informací o tom, které stanice se kterými komunikovaly, v jakém čase se komunikace odehrála, jakým způsobem výměna dat proběhla a ještě několik dalších informací o komunikaci v síti. Kontrola záznamů datových toků napomáhá odhalit, jaký typ provozu nám zabírá pásmo internetové přípojky. Nebo jaké chyby se objevují při chybě dostupnosti serveru. Současné síťové prvky mohou většinou reportovat datové toky, které přes ně prochází, aniž by zatěžovaly počítačovou síť. Podstatnou vlastností je to, že záznamy neobsahují přenášená data. Vytvoření takového záznamu není snadné zajistit, avšak množství dat uložených na disku je výrazně menší než v případě záznamů celého obsahu datových přenosů. Záznamy správci vypovídají o tom, že klient navštívil webový server z konkrétní IP adresy, kolik přenesl dat, ale neprezentují však obsah samotný.

3.1.2 Vývoj NetFlow

Vysokorychlostní routery a switche směrují provoz bez využití operačního systému. Směrování se tak netýká softwarového zpracování. Směrování paketu je tak prováděno na nejnižší možné vrstvě a to na úrovni samotného hardwaru. Společnost Cisco systems zavedla metodu směrování prostřednictvím Flows. V souvislosti s tím vnikla možnost zpřístupnění informací o Flow síťovým administrátorům pod názvem NetFlow. Za dobu své existence prošlo NetFlow několika vývojovými verzemi.

3.1.3 NetFlow verze 1

Verze 1 je nejstarší verzí, kterou společnost Cisco Systems vyvinula. Ostatní výrobci se prostřednictvím reverzního inženýrství snažili vytvořit NetFlow exportovací systém a vytvořit tak systém, který by byl s NetFlow kompatibilní. NetFlow verze 1 však obsahuje spoustu chyb a umožňuje získat jen málo užitečných informací. V současnosti se již nevyužívá.

3.1.4 NetFlow verze 5

Nejstarší široce vyvíjenou formou NetFlow je verze 5. Spousta velkých výrobců síťových prvků tento protokol implementovala. Záznam NetFlow verze 5 obsahuje 7 klíčových hodnot: zdrojová IP adresa, cílová IP adresa, zdrojový port, cílový port, IP protokol, vstupní interface a typ služby (TOS). Verze 5 dále poskytuje informace o směrování, IP adresu sondy a také několik přenosových charakteristik.

3.1.5 NetFlow verze 7

NetFlow verze 7 je podporována pouze nejvýkonnějšími Cisco switchi a routery. Jeho záznamy obsahují informace o přepínání a směrování, které nebyly poskytované verzí 5 jako například Next Hop adresa NetFlow.

3.1.6 NetFlow verze 8

NetFlow verze 8 zahrnuje množství sobě podobných formátů záznamů, které dokážou agregovat informace. To je výhodné v případě NetFlow u agregovaných vysokorychlostních linek. Zmenšuje se tím množství ukládaných dat. Cisco je jediný výrobce, který tuto verzi NetFlow podporuje.

3.1.7 NetFlow verze 9

NetFlow verze 9 je poslední verzí společnosti Cisco Systems. Tato verze umožňuje rozšíření třetím stranám. Tyto třetí strany pak mohou rozšiřovat záznamy o doplňující informace. Tato verze byla vyvinuta pro pouze malé množství komerčních produktů.

3.1.8 Standardizace

Počátkem milénia Internet Engineering Task Force vytvořila pracovní skupinu, aby pro Flow definovala jednotný, všem dostupný formát. Tato pracovní skupina vytvořila protokol na základech NetFlow verze 9 s malými obměnami pro lepší uživatelskou přívětivost. Poslední verze tohoto standardu je nazvána IP Flow Information eXport (IPFIX).

3.1.9 IPFIX

Standardní IPFIX je mnohem komplikovanější než předcházející verze NetFlow a používá výrazně více systémových zdrojů. Rozdíly mezi předchozími verzemi NetFlow jsou důsledkem přirozeného vývoje. Avšak rozdíly od původních verzí jsou zásadní. Administrátoři se naučili používat IPFIX nejen pro kontrolu datových toků ale i pro řešení řady bezpečnostních otázek. Doporučení, které se vztahuje k IPFIX bylo publikováno v roce 2013 pod označením IETF RFC 7011.

3.1.10 sFlow

Společnost Cisco systém vyvinula množství NetFlow verzí. Ostatní výrobci si uvědomili výhody exportování a reportování informací o datových tocích. Tato skutečnost dala vzniknout novému standardu známému jako sFlow. Umožňuje sledovat datový provoz na rozhraních směrovačů L3 ale i na rozhraních přepínačů L2. Výrobci jako 3com HP Extreme a Juniper podporují sFlow. Doporučení pro sFlow je publikováno jako RFC 3176 (IETF).

3.1.11 NetFlow vs. sFlow

NetFlow vzniklo za účelem analýzy datových IP toků. V okamžiku, kdy IP tok prochází rozhraním, důležité informace jsou načteny a uloženy do paměti (cache) v zařízení. Následně jsou tyto informace exportovány jako NetFlow do kolektoru v závislosti na nastavených podmínkách exportu. V tomto případě záznam o toku odpovídá každé konverzaci mezi dvěma klienty skrze konkrétní rozhraní. A protože NetFlow je zaměřeno na analýzu datových toků, tak sbírá informace o všech datových konverzacích, které skrz rozhraní prochází.

Analýza prostřednictvím sFlow je založena na sbírání vzorku paketové komunikace. Sbírá se 1 paket z „n“ (podle nastavení samplování). Z každého sebraného vzorku paketu je kopírováno prvních „x“ bytů (sFlow verze 5 kopíruje defaultně 128 bytů) a ty jsou v reálném čase prostřednictvím protokolu UDP exportovány jako sFlow datagramy. Prvních „x“ bytů paketu zahrnuje IP hlavičku, podle které získává potřebné

informace o datovém provozu. Protože však sFlow je zaměřeno na pakety, nezaznamenává tak informace o všech tocích, které přes analyzované rozhraní prochází. Nasbíraná data jsou vhodná pouze pro analýzy, do kterých není nutné zahrnovat všechny síťové konverzace. Datové toky, jejichž pakety nebyly obsaženy v sebraných vzorcích, se tak nemohou podílet na vzniku výsledků analýzy datového provozu a pro síťové administrátory, tak zůstávají neviditelné. V celkovém obrazu datového provozu tímto vznikají nekontrolované mezery.

Je zřejmé, že v případě obou monitorovacích systémů se jedná o rozdílné způsoby sběru podkladových dat, a to je třeba uvažovat při stanovení cílů u vytvářených analýz a statistik. Zvláštní výhodou sFlow je podpora méně rozšířených síťových protokolů (IPX, Appletalk) než jen IP protokolu, jako je tomu u NetFlow. Použití sFlow by bylo nevhodné například pro sběr dat jako podkladů k účtování za datové přenosy.

3.1.12 Flexible NetFlow (FNF)

Společnost Cisco systems vyvinula další generaci systému monitorování sítě, který využívá informací o datových tocích. Ve skutečnosti se jedná o rozšíření původního NetFlow o různá uživatelská přizpůsobení síťových analýz. Vzniklo Flexible NetFlow, které přináší možnost optimalizace síťové infrastruktury, snížení provozních nákladů a zlepšení kapacitního plánování. Užitečná je detekce bezpečnostních událostí s lepší pružností a rozšiřitelností. Možnost rozlišit IP provoz a určit jeho zdroj, cíl, časové údaje a informace o aplikacích jsou velmi důležité pro zajištění dostupnosti sítě, kontrole její výkonosti i k identifikaci poruch. Monitoring datových toků prostřednictvím Flexible NetFlow poskytuje podkladové informace pro přesné plánování přenosových kapacit datových spojů. Kvalitní kapacitní plánování přímo ovlivňuje nastavení šířky pásma pro využití jednotlivými aplikacemi (Quality of Service – QoS). To může sehrát důležitou roli v otázkách souvisejících s bezpečnostními útoky na dostupnost služeb (Denial of Service - DoS).

3.1.13 DPI (Deep Packet Inspection)

Technologie, která kontroluje síťovou komunikaci včetně přenášených dat, se nazývá DPI. Od NetFlow se zásadně liší právě tím, že s vytvořením záznamu o datovém toku také zkontroluje datovou část procházejících paketů přes kontrolní bod sítě. Kontrola datové části paketu může odhalit nesprávnou komunikaci protokolů vyšších vrstev, viry, spam, pokusy o proniknutí do sítě. Mohou být předem stanoveny podmínky za jakých je možno pakety dále směrovat a do jakých částí sítě. Užitek také přináší v tom, že zásadně rozšiřuje zdroje statistických informací. Podobně jako u NetFlow je více možností, jak získat pakety ke kontrole. Může toho být docíleno zrcadlením datového provozu na monitor port nebo pomocí optického splitteru TAP.

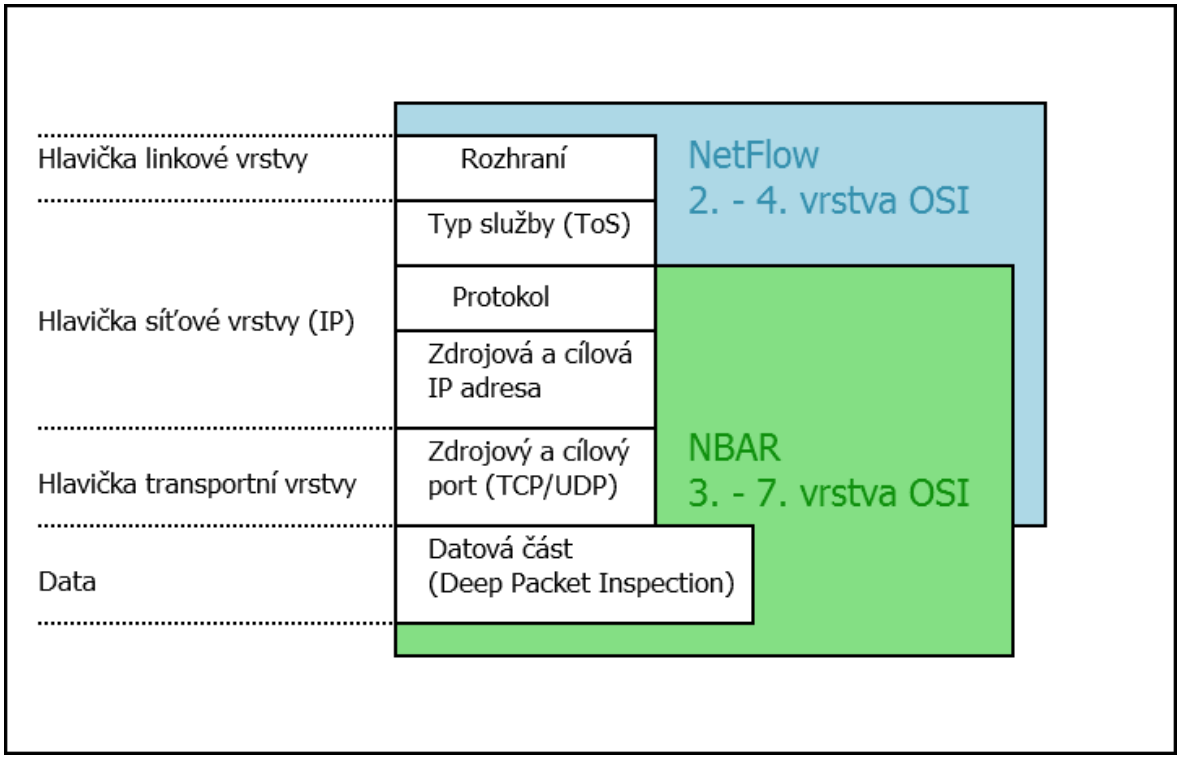
3.1.14 NBAR2 (Network Based Application Recognition)

Při využití některých síťových prvků společnosti Cisco systems, je možné rozpoznat přes 1000 různých aplikací, které tvoří datové toky v síti. Jedná se o rozšířenou funkcionalitu původní technologie DPI. NBAR2 k rozpoznání aplikací využívá soubor signatur, podle kterých je možné aplikace identifikovat. Vzhledem k přirozenému vývoji aplikací se časem aktualizuje i soubor signatur. Produkty Cisco aktualizaci umožňují bez přerušení datového provozu.

Při analýzách datových toků je třeba rozlišovat protokoly a aplikace. Zatímco protokoly využívají specifických portů, může několik různých aplikací využívat stejný jeden port. Víme, že spousta současných aplikací používá porty protokolu http a není úplně zřejmé, zda se jedná o data přenášená prohlížečem webových stránek nebo jiné aplikace. Rozpoznání aplikace na základě rozboru jednotlivých paketů tak může být obtížné nebo nemožné. Technologie NBAR dokáže spolehlivě určit, o jakou aplikaci se jedná na základě analýzy celého řetězce paketů až po sedmou (aplikační) vrstvu OSI modelu. Jedná se o klíčovou vlastnost, protože pokud už je nějakou aplikaci možné rozpoznat lze očekávat, že svým specifickým chováním bude ovlivňovat výkon a využívat zdroje datové sítě.

NBAR2 provádí kontrolu DPI nativně. Navíc dokáže na základě atributů rozdělovat aplikace s podobnými vlastnostmi do kategorií, podkategorií a skupin. Kategorizace aplikací usnadňuje agregaci reportů a snadnější úpravy konfigurace.

Obrázek 1 - Souvislost mezi NetFlow a NBAR



3.1.15 Cisco AVC (Application, Visibility and Control)

Cisco AVC je systém, který zahrnuje kombinaci více technologií. Jedná se především o vyžití podpory aktivních síťových prvků Cisco ASR 1000 (Aggregation Service Routers) a Cisco ISR G2 (Integrated Services Router Generation 2). Společně s nástroji pro management sítě tak vzniká velice efektivní integrovaný nástroj pro odhalování a řízení síťových aplikací. Správce sítě tak může získat přehled o aplikacích, které si vzájemně posílají data přes síťovou infrastrukturu. To je důležitý zdroj informací pro uplatňování řídících politik na komunikaci aplikací. Vhodná implementace komunikačních politik na síťovou strukturu umožňuje efektivně řídit síťové aplikace a vhodně využívat zdroje aktivních i pasívních prvků sítě.

Spuštěním softwarové podpory na některém z výše uvedených síťových prvků a využitím dalších nástrojů managementu sítě je možné vytvořit užitečné funkcionality.

Rozpoznávání aplikací – Využitím DPI je možno rozpoznat síťové aplikace bez ohledu na to, jaké komunikační porty využívají.

Monitoring výkonnosti – Funkcionality integrované v síťových prvcích poskytují možnost načítat a ukládat záznamy o tom, jaké aplikace jsou používány a jak využívají

zdrojů sítě. Z toho je následně zřejmý vliv jednotlivých aplikací na výkon sítě. Tyto záznamy prostřednictvím některého z exportních standardů (NetFlow, IPFIX) dále exportovány do části systému pro řízení sítě.

Kontrola sítě – Prostřednictvím aplikací pro řízení sítě je možné vizualizovat a interpretovat informace koncovému uživateli. Tímto způsobem je možné získat zpětnou vazbu o efektech implementované síťové politiky a podpořit tak optimalizaci výkonu celé sítě.

Řízení – Šířka využitého přenosového pásma jednotlivými aplikacemi a inteligentní volba přenosové trasy poskytují aplikacím možnost řízení výkonu sítě v reálném čase.

K realizaci Cisco AVC se využívá řada moderních technologií.

Nová generace DPI nazývaná **NBAR2** dokáže rozpoznat více než 1000 aplikací a zařadit je do definovaných kategorií. Aktualizace informací o aplikacích může proběhnout i bez přerušení provozu.

Infrastruktura Flexible NetFlow (**FNF**) a možnost exportu dat poskytuje zdroje pro řídící a analytické aplikace nejen společnosti Cisco, ale také řadu nástrojů vytvořenou jinými vývojáři.

Pro získávání informací o výkonu sítě jsou kontrolovány parametry sítě Application Response Time (**ART**) pro aplikace využívající transportní protokol TCP a Media Monitoring (**MMON**). Všechny tyto informace jsou exportovány pomocí FNF.

Nástroje pro reporty a řízení sítě jsou tvořeny množstvím aplikací pro rozbor síťových aplikací i měření výkonosti. Z významných spolupracujících vývojářských týmů lze zmínit ActionPacket, InfoVista, LivingObjects a Plixer.

Využití **QoS** usnadňuje optimalizaci řízení výkonosti aplikací.

Důležitou funkcionalitou je Performance Routing (**PfR**). Jde o inteligentní výběr směrovacích pravidel pro každou aplikaci. Tak je možné docílit toho, aby byla pro přenos dat vybrána ta cesta, která je pro danou aplikaci nejvhodnější.

3.1.16 SIEM (Security Information and Event Management)

Je známa spousta typů bezpečnostních incidentů, které vyžadují od správce sítě rychlou reakci. Posláním SIEM je pomoci k rychlejší a efektivnější reakci na bezpečnostní události.

Management SIEM v sobě integruje dvě důležité kategorie různých bezpečnostních aspektů. **SIM** (Security Information Management), jehož náplní je dlouhodobé ukládání událostí v síti, jejich analýzou i tvorba reportů a **SEM** (Security Event Management), který vyhodnocuje celou infrastrukturu, sleduje vzájemné vazby mezi událostmi a své výsledky oznamuje v reálném čase. Nejdůležitějšími vlastnostmi a funkcemi SIEM jsou:

- **Agregace:** Do systému lze zahrnout vstupní informace z velkého množství zdrojů (síťové prvky, servery, databáze, aplikace). Mít všechny informace o bezpečnostních událostech na jednom místě pomáhá předejít přehlédnutí malých avšak důležitých změn v síti.
- **Korelace:** Mezi záznamy o událostech v síti vyhledává společné znaky a spojuje je do celků, které spolu souvisí. Možnost nahlédnout na události v jednom časovém okně, nebo na vše, co jeden konkrétní uživatel udělal, poskytuje dobrý podklad pro diagnostiku bezpečnostních událostí. Tato technologie umožňuje provádět řadu korelačních analýz nad daty z různých zdrojů a ty pak transformuje do srozumitelných informací.
- **Upozorňování:** Automatizované korelační analýzy v reálném čase produkují množství důležitých a detailních upozornění, která napomáhají rozhodnout, na co je třeba se zaměřit právě v danou chvíli.
- **Informační panely:** Prostřednictvím informačních panelů je možné využívat data událostí a vytvářet z nich přehledné grafy. Tyto grafy mohou pomoci bezpečnostnímu analytikovi kontrolovat typické chování jednotlivých událostí, ale i odhalit nestandardní komunikace, které nejsou zřejmé z jednotlivých záznamů (logů).

V prostředí velkých korporátních sítí se objevují desítky až tisíce klientů, serverů a síťových prvků, které generují tisíce zpráv a upozornění do logů každý den. Tím vznikají značná množství uložených dat, která je těžko možné vyhodnocovat a zpracovávat ručně. SIEM umožňuje snadněji zpracovávat uložená data, aniž by bylo zapotřebí procházet dlouhé seznamy uložených událostí.

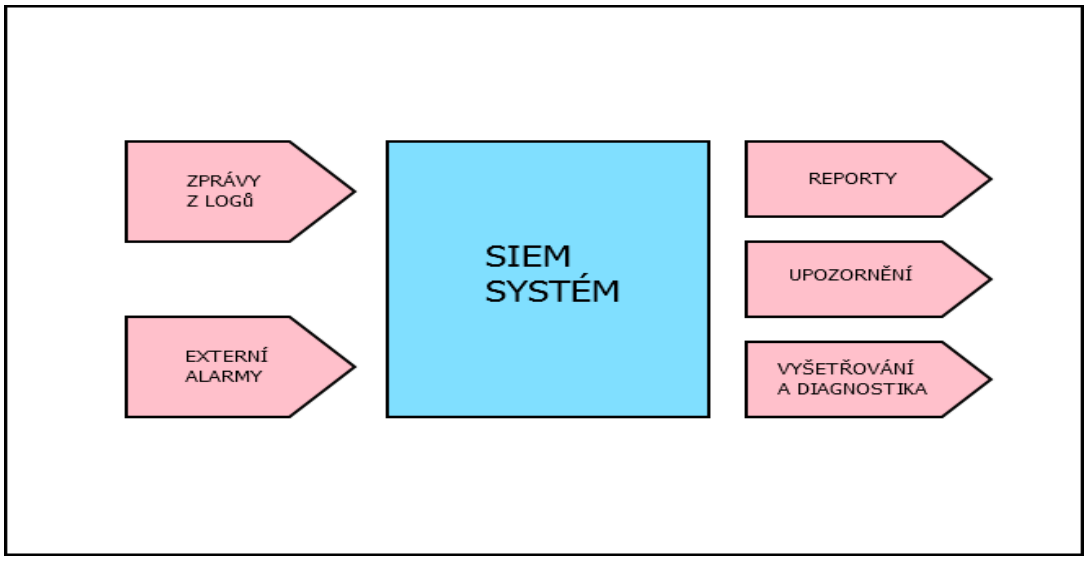
Při zpracování velkého množství vygenerovaných zpráv se zvyšuje riziko, že se analytik bude dlouhou dobu zabývat méně důležitými nebo bezvýznamnými událostmi

v síti, než se dopracuje k důležitým informacím, které pro podnikové informační systémy představují skutečné hrozby. Správné vyžití SIEM pomůže zprávy roztřídit a zvýšit tak produktivitu zpracování informací.

Systém SIEM poskytuje možnost náhledu na síť s ohledem na všechny její komponenty. Zaznamenané události je tak možné vyhodnocovat v kontextu celého pohledu na síť. Tak lze předejít tomu, že dojde k přehlédnutí souvisejících událostí.

Množství oddělených monitorovacích systémů může mít také za následek přehlédnutí souvislostí mezi událostmi v síti. Než je taková souvislost odhalena, tak to může trvat výrazně delší dobu než, když jsou všechna data vyhodnocována pouze jedním systémem. V okamžiku bezpečnostního incidentu může prodlení znamenat kritický dopad na podnikatelské aktivity.

Obrázek 2 - Přehled vstupních a výstupních informačních toků SIEM



3.1.17 DLP (Data Loss Prevention)

S ohledem na únik informací z organizací dochází nárůstu počtu incidentů. To představuje závažný problém pro všechny typy komerčních i státních organizací. Následkem toho organizace vynakládají spousty finančních prostředků i pracovního úsilí, aby bylo takovým únikům zabráněno.

Za posledních deset let došlo vývoji technologií, které usnadňují omylem nebo záměrně zaměstnancům vynášet z organizací utajované informace nebo informace o klientech. Data loss prevention (DLP) je součástí informační bezpečnosti, která může být implementována, aby rozpoznala taková rizika. Typický DLP systém dokáže minimalizovat, tyto zdroje zranitelností:

- Přenosná paměťová média USB klíčenky a hard disky, mobilní telefony, paměťové karty, CD/DVD média, zařízení připojitelná přes infraport, Bluetooth, Fire Wire nebo SCSI.
- Nahrávání souborů i těch šifrovaných na externí webová úložiště prostřednictvím běžných protokolů s využitím prohlížeče, jako jsou ftp, http, https. Tyto soubory pak mohou být napadeny na straně internetového úložiště i na straně počítače.
- Detekce situace, kdy přenosné počítače nejsou v síti organizace a kopírují se soubory do úložišť mimo organizaci.

Hlavním úkolem DLP je blokování pokusů při kopírování a nahrávání datových souborů některým z uvedených způsobů. V okamžiku, kdy se někdo ze zaměstnanců pokusí kopírovat nebo přenášet původní data, tak DLP tuto skutečnost automaticky zaznamená. DLP systém pomáhá zvládat taková rizika tím, že vytvoří záznam o tom, co bylo kopírováno. To může napomoci při analýze rizik případně i poskytne informace o tom, kdo ze zaměstnanců kopíroval data ze společnosti. Těchto vlastností může správce využít i v období, kdy některý ze zaměstnanců organizaci opouští. (KABAY, 2014, s. 428)

Systém vykonávající funkci DLP se nejčastěji skládá ze dvou základních komponent:

- **Síťová** – Nejčastěji se jedná o samostatné zařízení instalované jako součást síťové struktury. Ta se připojuje na perimetr privátní sítě, aby byl zajištěn přístup datovým komunikacím do internetu. Tam z procházejících datových toků kontrolují přenosy klasifikovaných dat. Nejčastěji se činnost tohoto zařízení zaměřuje na síťové

protokoly, jako jsou: e-mail, ftp, http, https. K proaktivnímu zablokování nežádoucích přenosů informací je důležité implementovat spolupráci síťového zařízení DLP s PROXY, která dokáže komunikaci zablokovat. Toto komponenta se vyskytuje také jako součást bezpečnostních síťových prvků, jako třeba firewall.

- **DLP koncových bodů** – Jsou to systémy instalované na koncové stanice v síti. Obvykle se spouští jako služba, která monitoruje pohyby dat v rámci koncové stanice podobně jako v případě síťové komponenty. Navíc však dokáže kontrolovat datové přenosy uvnitř privátní sítě, šifrovat citlivá data a monitorovat pohyby dat při čtení, zápisu a změnách na pevných i přenosných paměťových mediích.

Vývojem systémů DLP se zabývá většina společností, které se svým zaměřením pohybuje v oblasti informační bezpečnosti. Z nejznámější lze jmenovat společnosti McAfee, Symantec nebo Cisco.

Pro DLP je patrné jeho využití při plánování současné informační bezpečnosti obzvláště v organizacích, které uchovávají v podobě datových souborů důležité strategické a obchodní informace na kterých závisí podnikatelská činnost společnosti. I společnosti uchovávající osobní nebo citlivé informace o svých klientech prostřednictvím DLP získávají nástroj, kterým mohou své informace o klientech chránit.

3.2 Komponenty Flow monitoringu

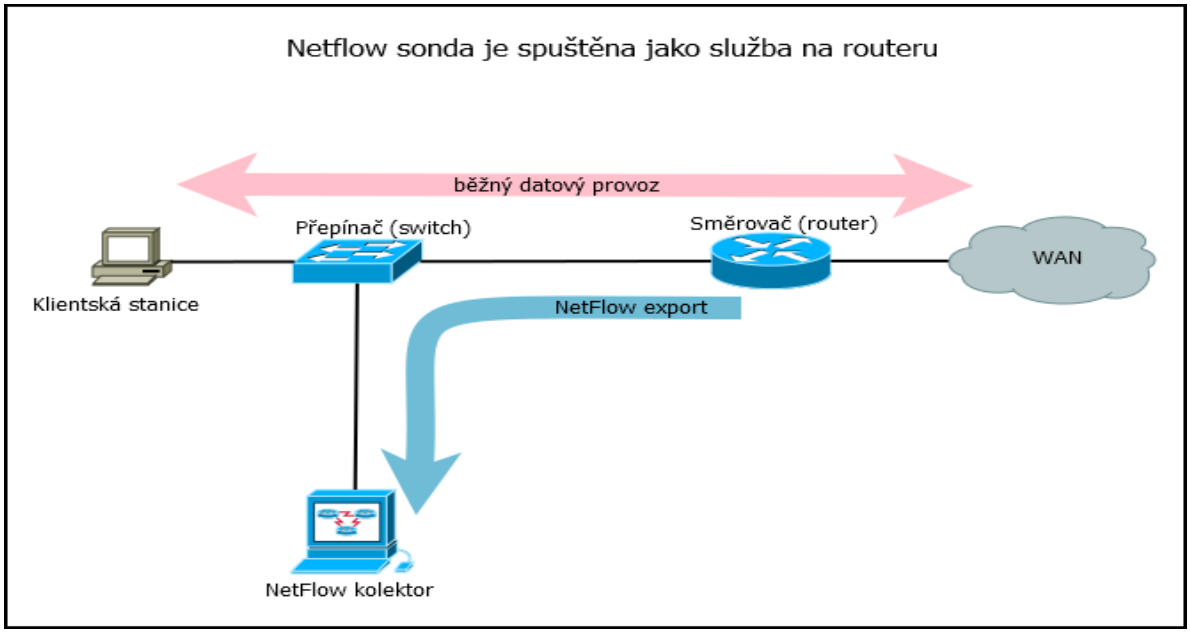
Celý systém pro získávání NetFlow/sFlow záznamů se skládá z několika základních komponent. Nejčastějšími součástmi jsou: exportér, kolektor a analytický software.

3.2.1 Exportér

Exportér zajišťuje sběr dat z uskutečněných datových toků. Tyto informace sonda získává z příslušných záznamů vytvořených v aktivních síťových prvcích nebo vytvořením záznamu z procházejícího provozu. Sonda získá záznam o datovém toku a odešle ho předdefinovanému kolektoru k dalšímu zpracování. Funkce exportéru může být realizována přímo spustitelná jako služba aktivních prvků sítě (*obrázek 3*), jako služba

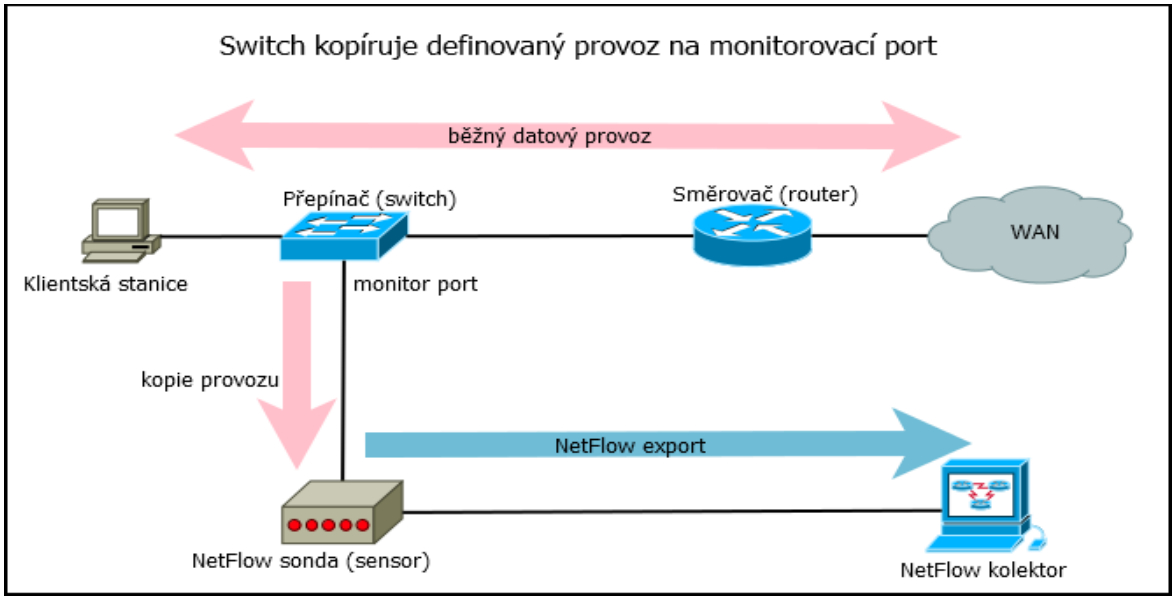
operačního systému severu anebo lze použít exportér v podobě samostatného zařízení (sonda, sensor).

Obrázek 3 - Monitoring při podpoře NetFlow síťovými prvky



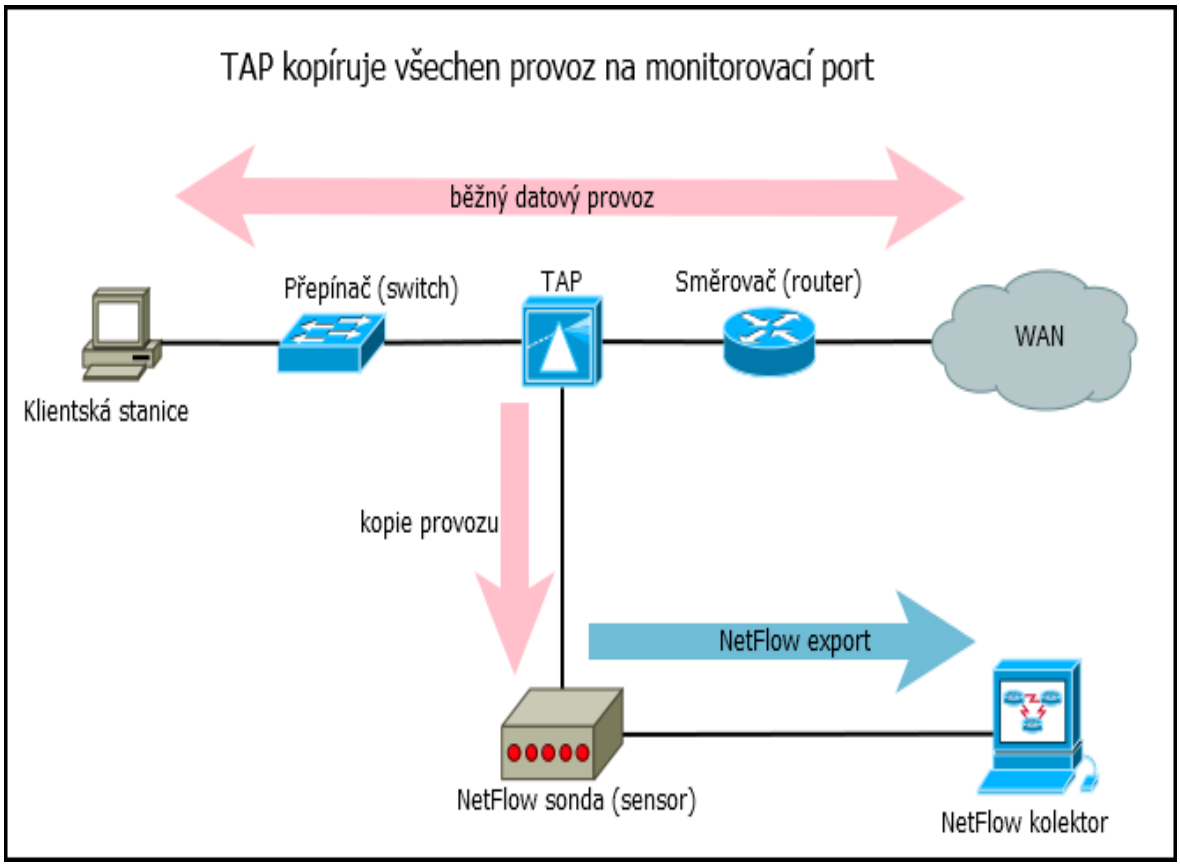
Samostatný exportér je možné připojit na port switche, na který je kopírován potřebný datový provoz (*obrázek 4*).

Obrázek 4 - Monitoring při využití portu s odposlechem (SPAN)



Další možností je přivedení měřeného provozu pomocí zařízení TAP (Traffic Access Point) přímo do sondy (*obrázek 5*). To je často jediné možné řešení v případě, že použité síťové prvky nepodporují službu exportu zpráv o datových tocích a zároveň nepodporují zrcadlení přenášených dat na monitorovací port switche (SPAN port).

Obrázek 5 - Využití TAP při monitorování síťového provozu



Tabulka 1 - Podpora NetFlow verze 9 významnými výrobci aktivních prvků

Výrobce	Produktová řada
Cisco	• Cisco 2600 řada • Cisco 3600 řada • Cisco 7100 řada • Cisco 7200 řada • Cisco 7300 řada • Cisco 7400 řada • Cisco 7500 řada • Cisco 12000 řada • Cisco 800, 1700, 1800, 2800, 3800, 6500, 7300, 7600, 10000, CRS-1 • Catalyst switches: 45xx, 55xx, 6xxx
3Com	• 8800 řada
Adtran	• NetVanta 3200, 3305, 4305, 5305, 1524, 1624, 3430, 3448, 3130, 340,344
Juniper Networks	Nepodporuje některá nastavení sběru dat.

3.2.2 Kolektor

NetFlow **kolektor** přijímá a ukládá záznamy získané prostřednictvím NetFlow / sFlow. Nad uloženými umožňuje provádět statistické a strukturální analýzy, vyhodnocovat a předpovídat trendy pro plánování kapacit. Uložené informace umožňují zpětné vysledování příčin bezpečnostních incidentů. Kolektory často disponují i řadou vizualizačních nástrojů, které přispívají ke srozumitelné a pravdivé interpretaci odečtených informací.

Samotné zařízení je ve své podstatě počítač se síťovou kartou a datovým úložištěm. Na takovém zařízení je spuštěna služba pro sbírání a ukládání informací o datových tocích. Na síťové rozhraní kolektoru jsou sondami prostřednictvím UDP protokolu (obvykle port 2055) zasílány záznamy o datových tocích. Pro výpočty statistik a vizualizace analýz bývá součástí kolektoru aplikace, která čerpá vstupní data z uložených záznamů.

3.2.3 Data flow management

Data získaná z exportérů mohou svým množstvím a způsobem uložení působit nepřehledně. Je to dáno velkým počtem záznamů z různých zdrojů. Takto nahromaděné množství dat je třeba roztřídit podle požadovaných kritérií, jako jsou: čas, zdrojové adresy, cílové adresy, protokoly a aplikace. Třídění je nezbytné pro zvýšení srozumitelnosti správci sítě, archivaci a dalšímu zpracování. Transformaci dat vykonává aplikace, která na vstupu přijímá data uložená z exportérů a na výstupu mohou být tabulky, grafy, upozornění nebo formátovaná data externí analytický systém. Analytická aplikace bývá nejčastěji součástí zařízení kolektoru. Typické je uživatelské rozhraní dostupné prostřednictvím prohlížeče webových stránek. V současnosti je k dispozici řada placených i neplacených aplikací (*tabulka 2 a 3*).

Tabulka 2 - Přehled OpenSource nástrojů

PRODUKT	POUŽITÍ	OPERAČNÍ SYSTÉM
Cflowd	Analýza provozu	UNIX
Flow-tools	Kolektor	UNIX
Flowd	Kolektor	BSD, Linux
FlowScan	Reporty pro Flow-tools	UNIX
IPFlow	Analýza provozu	Linux, FreeBSD, Solaris
NetFlow Guide	Tvorba reportů	BSD, Linux
NetFlow Monitor	Analýza provozu	UNIX
Netmet	Kolektor	Linux
NTOP	Bezpečnostní monitoring	UNIX
Stager	Reporty pro Flow-tools	UNIX
Nfdump / Nfsen	Analýza provozu	UNIX
SiLK	Analýza provozu	UNIX, Linux, Solaris, OpenBSD, Mac OS X

3.2.4 Nejpoužívanější kolektory

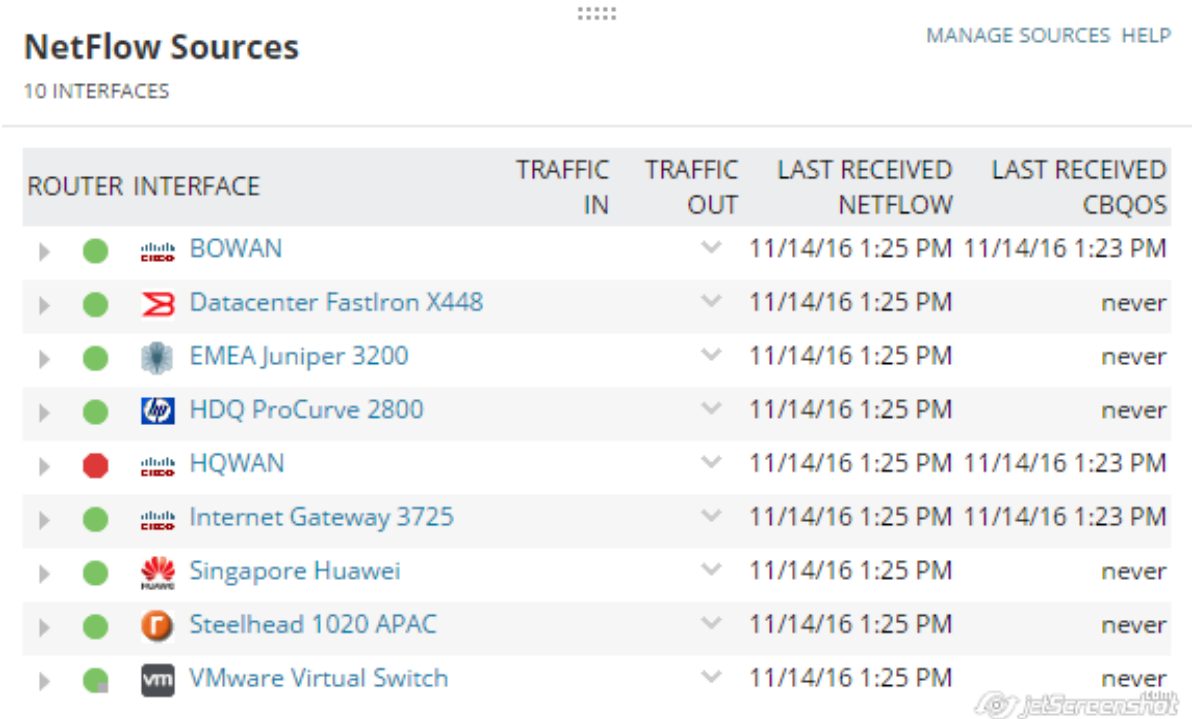
Pro sběr a zpracování záznamů o datových tocích je vhodné přiblížit detailnější popis těch produktů, které se v současnosti nejčastěji používají.

SolarWinds

Jedná se o jeden z nejoblíbenějších kolektorů, které jsou v současnosti k dispozici. Tento softwarový nástroj umožňuje řadit záznamy, vytvářet grafy a zobrazovat data různými způsoby. Tím usnadňuje analýzu datového provozu.

Poskytuje informace, které mohou být využity k identifikaci toho kteří uživatelé, aplikace a protokoly užívají největší šířku pásma v krátkém časovém intervalu. To lze využít pro optimalizaci datové sítě pro období provozních špiček.

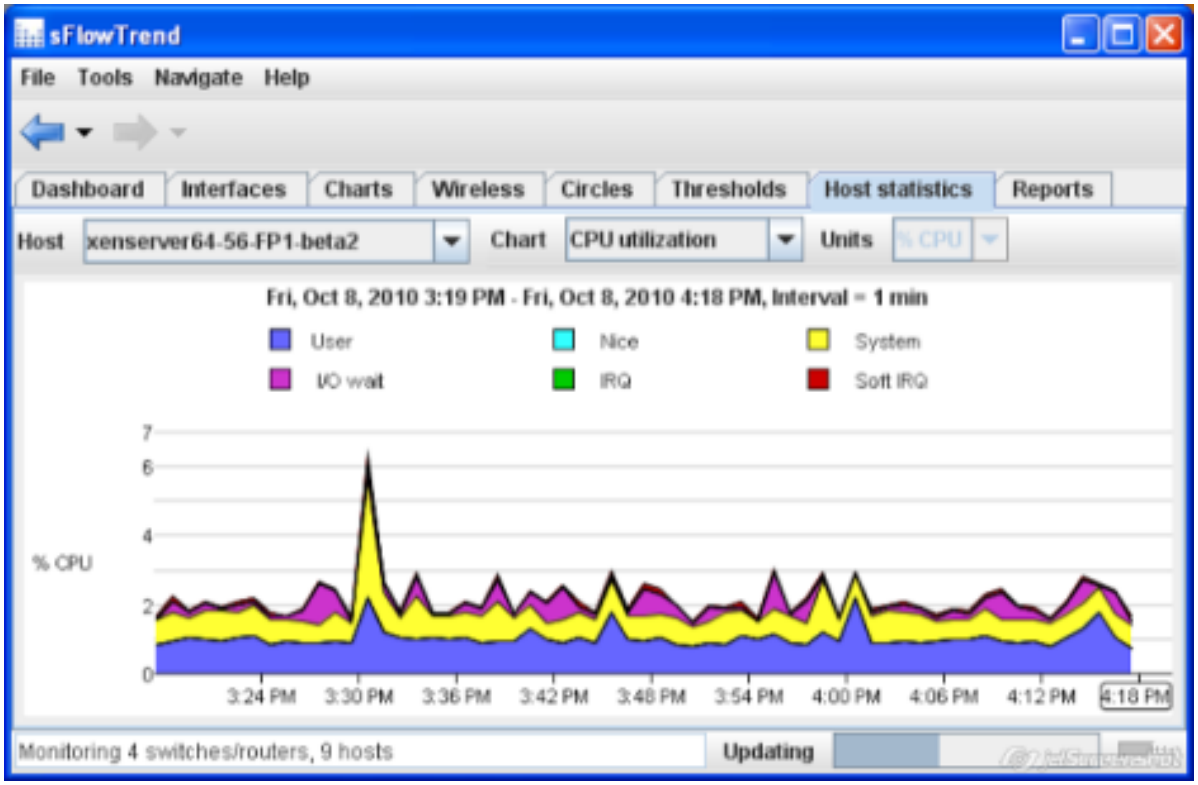
Obrázek 6 - SolarWinds – seznam aktivních exportérů (ukázka)



sFlowTrend

Tento nástroj společnosti inMon využívá standardu sFlow k vytváření náhledy využití šířky pásma v síti v reálném čase. Náhledy jsou doplněny o žebříček nejaktivnějších uživatelů a aplikací, které šířku pásma využívají. Tento typ informací napomáhá odhalit nedostatky sítě dříve, než se stanou kritickými. S nástrojem sFlowTrend lze sledovat i zatížení procesoru a využití operační paměti důležitých severů.

Obrázek 7 - sFlowTrend – průběh zatížení procesoru

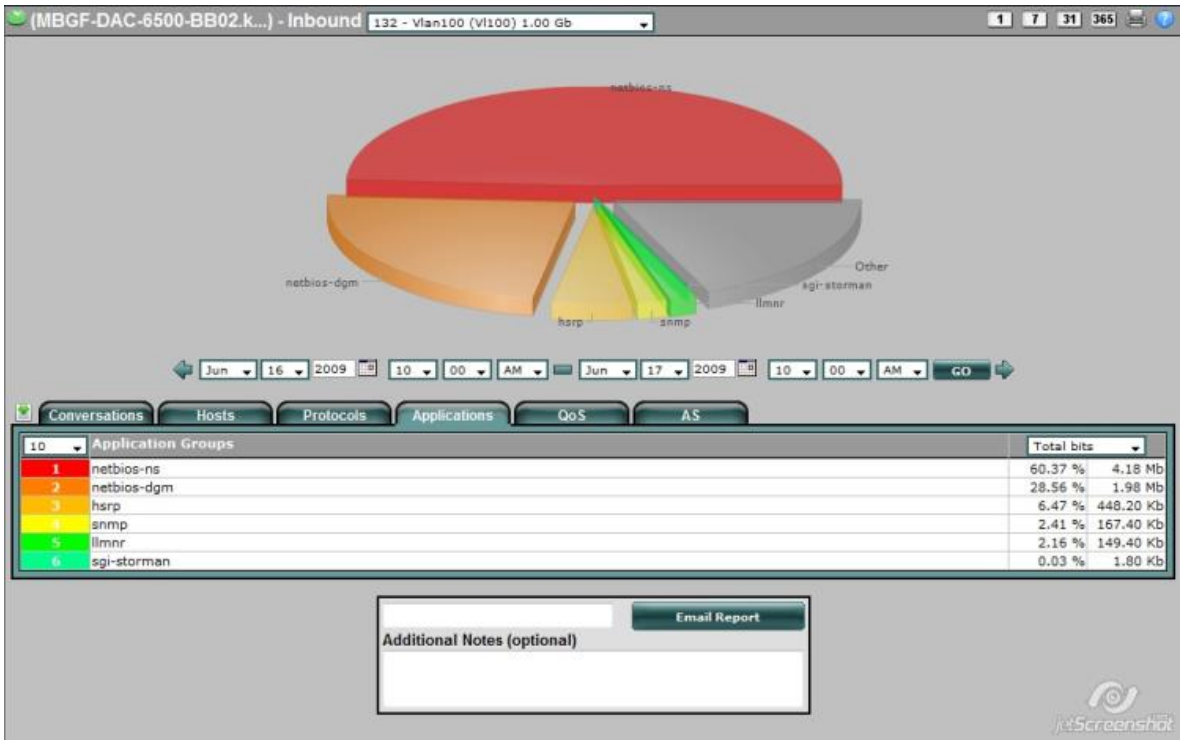


Tyto grafické výstupy poskytují aktuální i historická data, kde jsou dány do souvislostí výkony síťových uzlů a výkony serverů. Tím je možné získat celkový přehled o výkonosti celého síťového prostředí.

Scrutinizer

Společnost Plixer nabízí zdarma výkonný nástroj s podporou nejčastějších flow technologií pro sběr a analýzu datového provozu. To umožňuje nalezení neprůchodných částí sítě způsobených nesprávnou funkcí počítačů, přepínačů, směrovačů i dalších zařízení a aplikací. Scrutinizer umožňuje filtrovat výstupy nejrůznějšími užitečnými způsoby, ať už se jedná o časový úsek, počítač, aplikaci a další možnosti.

Obrázek 8 - Scrutinizer – přehled nejpoužívanějších protokolů

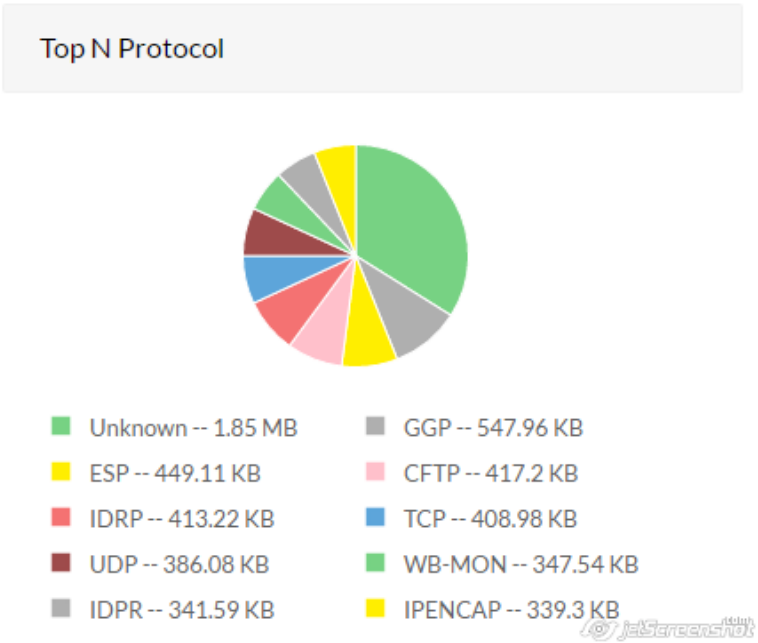


Neplacená verze umožňuje sbírání záznamů od neomezeného množství zařízení s omezením na 10 000 záznamů za sekundu a historii záznamů po dobu pěti hodin zpětně. Placená verze pak poskytuje 8 milionů záznamů za sekundu a historii po neomezenou dobu v závislosti na kapacitě zařízení.

ManageEngine

Je plnohodnotný nástroj získání přehledu o datovém provozu v síti. K tomu využívá zpracování záznamů ze všech běžných typů technologií (NetFlow, sFlow, jFlow). Dokáže v reálném čase poskytovat dostatek informací pro odhalení nedostatků síťové infrastruktury. Jedinečnou vlastností je to, že dokáže na základě IP adres sdružovat uživatele do jednotlivých oddělení nebo jednotlivých lokalit. Tuto vlastnost lze využít zejména při diagnostice problémů v síti mezi jednotlivými lokalitami.

Obrázek 9 - ManageEngine – přehled nejužívanějších protokolů

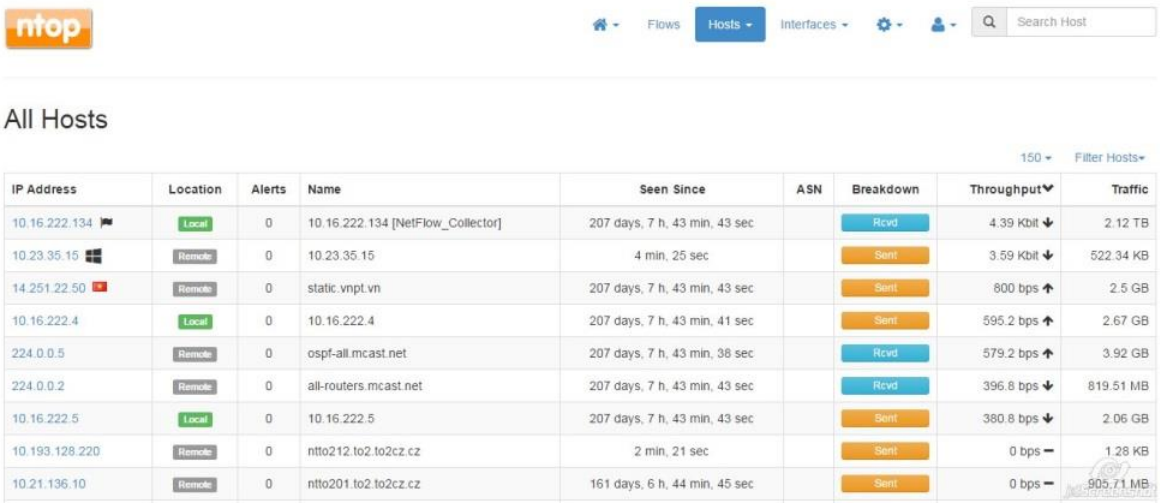


Jedinečnou vlastností je to, že dokáže na základě IP adres sdružovat uživatele do jednotlivých oddělení nebo jednotlivých lokalit. Tuto vlastnost lze využít zejména při diagnostice problémů v síti mezi jednotlivými lokalitami.

nTOP

Je to oblíbený a výkonný nástroj pro sbírání záznamů o datových tocích. Dokáže přijímat záznamy v různých formátech a ty v reálném čase konvertuje a zpracovává do grafických výstupů. Rozsah množství zpracovávaných formátů zpráv umožňuje sledovat datové toky v sítích s aktivními prvky nejrůznějších výrobců.

Obrázek 10 - nTop – žebříček nejaktivnějších uživatelů sítě



Kolektor nTop snadno napomůže svými informacemi k nalezení počítačů s nezvykle velkým počtem datových toků směrem do internetu. V takovém případě by se mohlo jednat o komunikaci iniciovanou škodlivým softwarem.

Paessler PRTG

PRTG přichází se spoustou užitečných vlastností, které pomáhají z nasbíraných záznamů odhalovat chyby v síti a vylepšovat celkovou výkonnost datové sítě. Je zaměřený na velký rozsah možností, při volbě ze kterých zařízení, získávat záznamy v potřebném okamžiku.

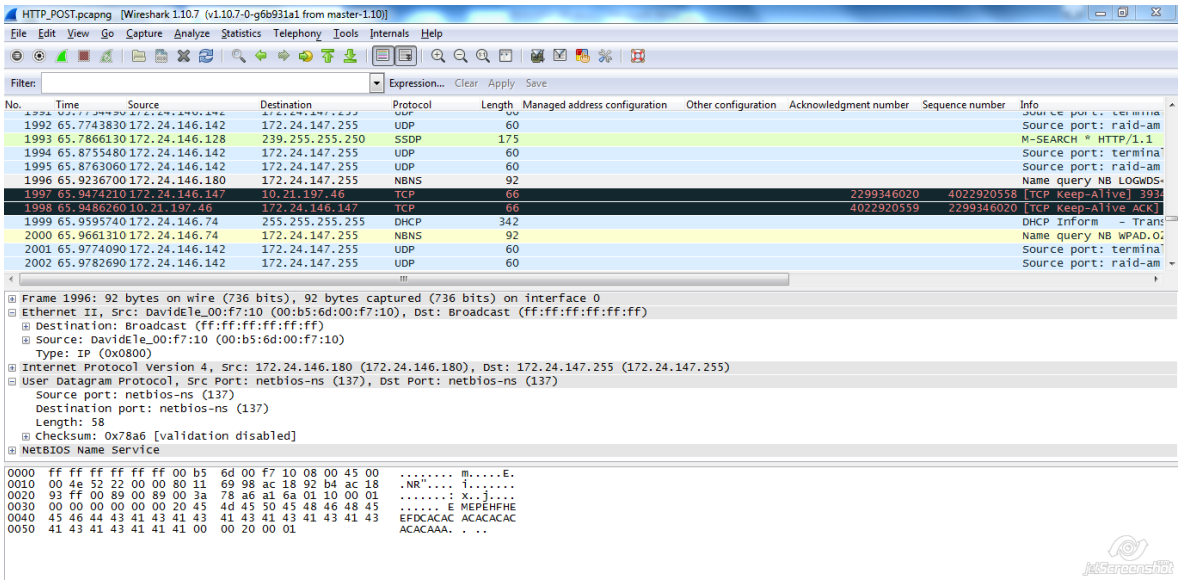
Obrázek 11 - PRTG – aktivita komunikace z různých podsítí

Tento nástroj umožňuje vzdáleně přistupovat ke zpracovaným informací prostřednictvím klientských aplikaci ze všech běžných zařízení. Další výhodou je rozsáhlá jazyková podpora včetně češtiny.

Wireshark

Je výkonný bezplatný a open-source kolektor a analyzátor. Wireshark dokáže prostřednictvím technologií pro záznam datových toků detailně zobrazovat data zachycených paketů. Detail přenášených dat je efektivním zdrojem informací pro správce sítí a pracovníky informační bezpečnosti. Zachycené pakety dokáže rozdělovat podle kategorií a ukládat je do souborů pro případnou analýzu v budoucnosti.

Obrázek 12 - Wireshark – barevné rozlišení podle typu komunikace

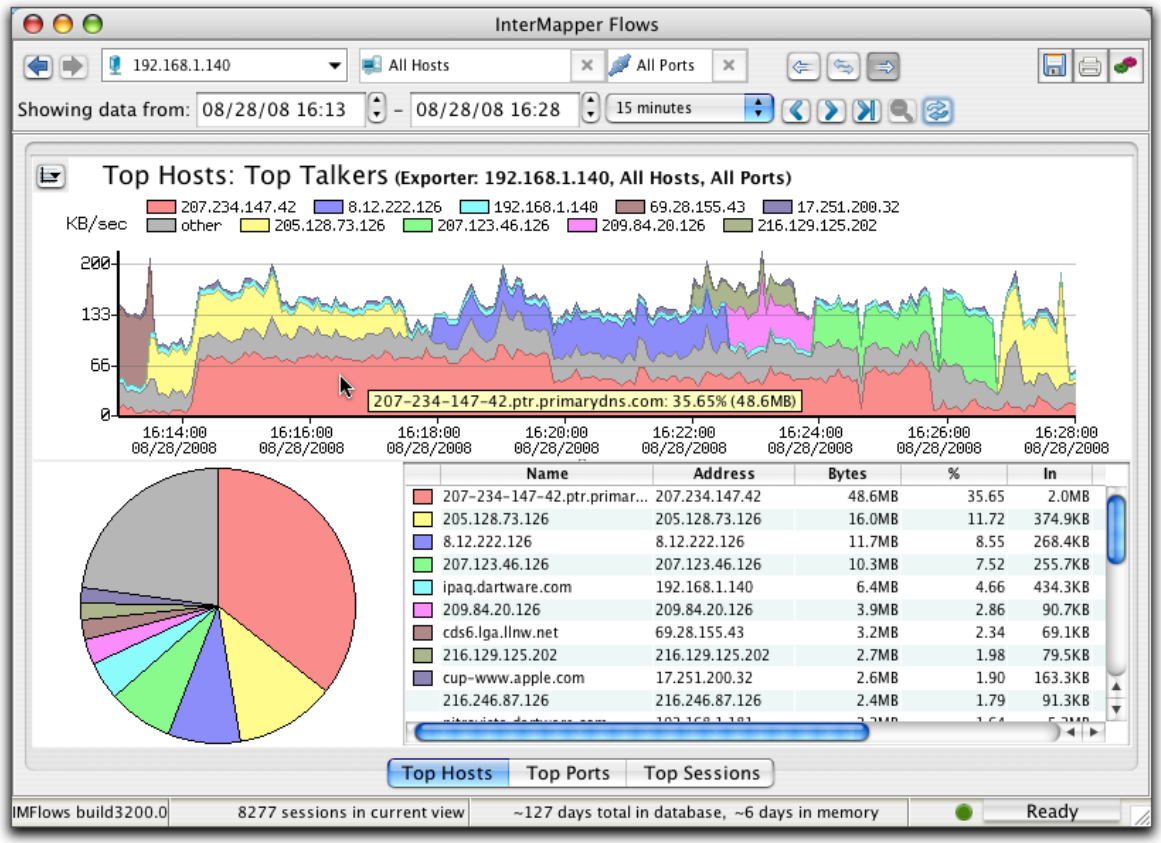


Wireshark se odlišuje od zmiňovaných nástrojů tím, že ho lze využívat v konzolovém režimu a tak poskytuje správci sítě Wireshark kontrolovat automatizovaně skriptem. Také je možné prostřednictvím tohoto nástroje přepnout kartu do promiskuitního režimu a používat ho jako měřící sondu.

InterMapper

InteMapper je výkonný nástroj pro monitoring, mapování a sledování aplikací, což umožňuje ovládání datové sítě a zachování její vysoké výkonnosti. Je to nástroj pro analýzu a archivaci záznamů pro sledování historických trendů.

Obrázek 13 - InterMapper – uživatelé vykazující nejvyšší aktivitu



Monitorování propustnosti sítě, sledování šířky pásma a mapování síťových služeb v reálném čase jsou vedle dalších těmi nejdůležitějšími funkcemi, které InterMapper poskytuje.

Tabulka 3 - Přehled placených nástrojů

PRODUKT	POUŽITÍ	VÝROBCE
Arbor PeakFlow	Analýza, Reporty	Arbor Networks
IBM Qradar	SIEM	IBM
FlowMon	Analýza, Reporty	Invea-Tech
StealthWatch	Analýza, Reporty	Lancope
NetFlow Analyzer	Analýza, Reporty	ManageEngine
NTBA	Behaviorální analýza	McAfee
Scrutinizer	Analýza provozu	Plixer
FlowTraq	Forenzní analýza	ProQSys
Mazu	Analýza provozu	Riverbed

3.3 Bezpečnostní hrozby v datové síti

Od dob vzniku počítačových sítí se jejich architekti a správci potýkají s množstvím aktivit, které ohrožují dostupnost služeb jednotlivých informačních systémů. Motivací těchto aktivit bývají často politické zájmy, oslabení obchodní konkurence, získání nebo manipulace informací i útoky pro účely testování nebezpečného software nebo zabezpečení sytému.

Jedním z nejstarších útoků na služby informačních systémů jsou tzv. DOS (Denial Of Service) útoky, které se snaží vytvořit velké množství síťových požadavků na informační systém. Zahlcení systému požadavky pak může způsobit jeho nedostupnost, zpomalení nebo dokonce zhroucení. Pro podniky, které využívají počítačovou síť pro zprostředkování svých produktů a služeb zákazníkům, může být takový typ útoku vážnou ekonomickou hrozbou.

Současné útoky začínají porušením vnitřní bezpečnosti, což je důsledkem toho, když je uživatel prostřednictvím nástrahy vytvoří odchozí spojení a získá tak spojení s místy v síti, kde jsou hostovány pro stažení všechny škodlivé druhy spustitelného softwaru, jako jsou keyloggery, Trojské koně, rootkity a ransomware. (CLARK, 2015, s. 93). S přihlédnutím k těmto faktům je zřejmé, že rizika napadení tak přináší sám uživatel uvnitř počítačové sítě.

Na úrovni datové sítě je možné detekovat komunikaci, která je typická pro škodlivý software. Jedním z nástrojů vhodných pro detekci veškeré datové komunikace je technologie IPFIX (NetFlow).

3.3.1 DoS útok

Význam analýzy síťového provozu narůstá v souvislosti s vyšetřováním bezpečnostních incidentů, při kterých je zneužita síťová infrastruktura. Jeden z nejčastějších incidentů nastává při útoku typu DoS (Denial of Service) nebo DDoS (Distributed Denial of Service). Útoky tohoto typu spočívají v napadení síťových zdrojů tak, aby došlo k jejich vyřazení z provozu. Cílem v takovém případě bývají aktivní síťové prvky, přenosová zařízení, servery a jejich služby. To má obvykle za následek nefunkční část kompromitované sítě nebo nedostupnost služby, která tuto část využívá.

Útočníci využívají nejrůznější možnosti k tomu, aby dokázali vytvořit natolik soustředěný útok, aby byl úspěšný. Primárně jde o neustálé napadání, dokud nedojde k vyřazení sítě z provozu. Obzvláště, pokud se jedná o postižení uživatelů korporátních sítí nebo poskytovatelů internetu, protože jsou nejčastěji odkázáni na protokoly TCP/IP. DoS útoky na korporátní sítě a poskytovatele internetových služeb mohou mít výrazný dopad na jejich hospodářské výsledky. DoS útoky je možno namířit proti hardwarovým zdrojům nebo operačním systémům, protože využívají internetový protokol IP. Útočné nástroje využívající IP (nejčastěji vytvořené pro Linux) mohou snadno cílit své útoky i na ostatní operační systémy, které využívají IP. Navíc využití IP protokolu na různých platformách se velice vzájemně podobají, a proto může jeden DoS útok postihnout většinu operačních systémů a účinek má na každý. Na všechny nové platformy se díky vývoji DoS útoků (díky spolupráci útočníků) za krátkou dobu (průměrně dva týdny) objeví mutace některého z předcházejících.

To, že DoS útoky mohou mít kritické následky, nelze brát na lehkou váhu. Cílené útoky několika zařízení proti jednomu se objevují od osmdesátých let minulého století; v roce 1999 se objevil DDoS útok, primárně byl vyvinut na útoky proti privátním sítím s využitím internetu. Nástroje DDoS útoku vyvíjejí soustředěný útok z více zdrojů na jediný cíl zároveň. (KABAY, 2014, s. 550)

3.3.2 Typy DoS útoků

Během vývoje DoS útoků dochází k neustálým inovacím a tím vznikají různé způsoby, jakými je možné napadat jednotlivé počítače i celé sítě. Podle způsobu realizace DoS útoku je v současnosti možné DoS útoky rozčlenit do několika typů.

Zahlcení (Saturation)

Tento typ útoku má za cíl vyčerpat omezené výpočetní zdroje počítačů nebo sítí tak, aby byl znemožněn nebo omezen jejich běžný provoz. Jedná se o zdroje typu, jako jsou vytížení procesorů, prostor na diskových úložištích, datové struktury, šířky přenosových pásem, přístupy k jiným počítačům nebo do jiných sítí a další potřebné zdroje jako chlazení nebo napájení.

Chyby nastavení (Misconfiguration)

Jde o úmyslné poškození nebo pozměnění nastavení počítače, serveru nebo síťového prvku. Změna nebo smazání konfigurace některého ze síťových prvků může způsobit výpadky sítě a síťových služeb. Útočník k tomu využívá nesprávně nebo nedostatečně dodržovaných zásad konfigurace ze strany správců sítí a služeb. Může se však jednat i o chyby zastaralých technologií, které nejsou ošetřeny ze strany výrobců, protože je podpora takových technologií ukončena z důvodu nahrazení novější.

Poškození (Destruction)

Tento typ útoku je založen na fyzickém zničení nebo poškození komponent sítě. Jako ochrana proti takovému útoku je vytvoření fyzického zabezpečení přístupu k serverům a aktivním prvkům sítě.

Narušení (Disruption)

Nerušení nebo úplné přerušení komunikace mezi dvěma zařízeními může vzniknout při nesprávném stavovém hlášení přenosových zařízení. Například protokol TCP řídí datové přenosy s využitím stavových zpráv. Manipulace s takovými zprávami dokáže efektivně zamezit datové komunikaci.

Je patrné, že značnou část DoS útoků je možné detekovat při sledování síťového provozu. Včasné odhalení neautorizované komunikace je důležitou součástí ochranných opatření na úrovni datové sítě.

3.3.3 Pokročilé intenzívní hrozby

Jedná se o hrozby útoků vedené proti jednotlivým konkrétním organizacím. Útočníkem v takových případech může být skupina, vládní agentura nebo i jedinec, který usiluje získání nějakých informací nebo atraktivních zdrojů. Za těmito účely jsou využívány sofistikované techniky, které umožňují skrýt vedený útok před odhalením.

Zákeřnost takovýchto útoků spočívá v tom, že je vedena zevnitř podnikové sítě. Bezpečnostní analytici je staví na úroveň moderní války vedené na kybernetickém bojišti.

Nepodceňujme pokročilé intenzívní útoky vedené proti našim organizacím v dnešní době. V nedávné studii organizace Ponemon institut (organizace zabývající se nezávislými průzkumy a studiemi v oblasti informační bezpečnosti) uvedlo 83% respondentů, že věří

v útok, který byl veden proti jejich organizaci. Politicky motivovaní hackeři i další útočníci se zaměřují na široké spektrum podniků a vládních subjektů (Chapple, 2012, s. 15).

Z této skutečnosti vyplývá, že pečlivě vytvořený a zabezpečený perimetr podnikové sítě nemusí být vždy dostatečně chráněn. Hackeři aplikující tento moderní způsob útoku budou využívat stále modernější a sofistikovanější postupy, aby získali příležitost vniknout do vnitřní sítě. V takovém případě je na straně správců sítě důležitým nástrojem právě NetFlow, aby umožnil detekovat právě probíhající útok, ale i události jemu předcházející. Analýza s využitím NetFlow a následný forensní rozbor umožňuje rychlou detekci i dříve neznámých typů útoků.

3.3.4 Hrozba uvnitř datové sítě

Ve spoustě případů nepřicházejí hrozby útoku z vnějšího perimetru privátní datové sítě, ale naopak z jejích vnitřních segmentů. Zdrojem takového rizika jsou nedůvěryhodné osoby, které však mají přístup citlivým informacím. Jedná se tak nejčastěji o stávající a bývalé pracovníky soukromých, vládních nebo rozpočtových organizací.

Americká federální vláda zažila v roce 2010 událost, kdy jediný armádní analytik způsobil masívní vyzrazení utajovaných informací na stránkách WikiLeaks (Chapple, 2012, s. 15).

Je zřejmé, že zabezpečení vhodnou architekturou a aktivními prvky sítě jako jsou například firewally se správnou konfigurací není před moderními útoky dostatečné. Tyto metody zabezpečení lze považovat jen jako součást celkové ochrany, protože nezabraňují přístupu k citlivým informacím osobám uvnitř sítě. Prostřednictvím technologie NetFlow lze detekovat neautorizované datové přenosy směrem do sítě i směrem do internetu. Je to možnost jak odhalit manipulaci s chráněnými daty i přenosy velkých datových objemů na neznámá místa v internetu.

3.3.5 Mobilita a neurčitá hranice sítě

Během několika posledních let dochází k rychlému rozvoji hardwaru přenosných zařízení. Nejmarkantnější je tento trend u zařízení, jako jsou notebooky, tablety a chytré telefony. Pro vysokou tržní poptávku po mobilních zařízeních došlo ke vzniku širokého množství nabízených produktů za různé ceny. Jejich vysoká dostupnost způsobila situaci, kdy je téměř každý člověk vybaven minimálně mobilním telefonem s přístupem na internet.

Mobilní zařízení jsou tak každodenně využívána pro přístup k informacím v internetu nebo privátních sítích.

Právě přístupy přenosné výpočetní techniky k citlivým informacím v privátních sítích nutí pracovníky informační bezpečnosti uvažovat jako tato zařízení jako zdroj možných rizik. Výhoda mobility se stává nevýhodou ve smyslu možné ztráty, zneužití nebo odcizení.

Je třeba si uvědomit, že sice lze nastavit organizační pravidla na používání mobilních zařízení pro přístup do privátní sítě, avšak není záruky, že taková pravidla nikdo neporuší.

V situaci, kdy je možné z mobilního zařízení přistupovat k jakýmkoli neveřejným nebo citlivým informacím je původní myšlenka firewallu jako rozhraní kontrolovaného přístupu do sítě značně zavádějící. Administrátoři a garanti bezpečnosti musí tento fakt brát v úvahu.

Sledování provozu uvnitř privátní sítě je jednou z nejúčinnějších možností zjistit informace o pohybech informací v podobě datových toků. Aplikace technologie NetFlow je v takovém případě vhodným nástrojem pro mapování autorizované i neautorizované komunikace mezi privátní datovou sítí a mobilními zařízeními. Lze tak i zpětně dohledat znaky škodlivé komunikace předchozích bezpečnostních incidentů.

3.3.6 Virtualizace a monitoring

Narůstající nároky na výpočetní výkony různých informačních systémů zvyšují tlak na rozvoj virtualizace. Běžně používané kancelářské aplikace, hry i složité podnikové informační systémy využívají virtualizaci v podobě cloudových řešení. Hlavní je provoz více virtuálních serverů na jedné hardwarové platformě. To je výhodné z hlediska efektivnějšího využití prostor velkých datacenter, dynamického rozdělení výpočetních zdrojů a celkové snížení dopadů na životní prostředí.

V prostředí virtuálních serverů je problematická analýza datového provozu v takové podobě, ve které se implementuje v prostředí, kde jsou jednotlivé prvky sítě jako samostatná zařízení. Pro přístup k síťovým zdrojům jednotlivých virtuálních serverů se využívá virtuální switch. Takový virtuální switch je součástí softwaru pro management virtuálních serverů. Mezi nejznámější patří třeba Hyper-V nebo V-Sphere.

Při návrhu datové infrastruktury a datových center by měl správce přihlédnou k možnostem monitoringu datového provozu v prostředí virtuálních serverů. Prostředí V-Sphere (IPFIX od verze 5.0.0) i Microsoft Hyper-V (sFlow od verze 3.0) umožňuje provádět analýzu datových toků.

3.3.7 Malware

Jedná se o souhrnné označení pro škodlivý software. Jeho název vznikl spojením anglických slov Malicious software. Škodlivé programy tohoto typ jsou známy též jako viry. Jeho cílem je narušení bezpečnosti počítače nebo mobilního zařízení za účelem ovládnutí operačního systému nebo přístupu ke chráněným informacím. Často se vyskytují v podobě malých fragmentů svázaných se spustitelným programem. Může tak být zakryt některou používanou aplikací. Pro Malware je typické to, že byl vyvinut tak, aby škodil uživateli a využil k tomu každého nedostatku softwarové výbavy nebo chyby uživatele.

3.3.8 Worm a Botnet

Běžný virus se může šířit prostřednictvím jiného běžně používaného programu jako jeho součást. Malware typu Worm dokáže ke svému šíření využívat počítačovou síť ke které je hostitelský počítač připojen. Automatickým šířením v prostředí počítačové sítě může způsobit napadení velkého počtu počítačů během poměrně krátké doby. Takto napadené počítače se mohou dostat pod kontrolu útočníka. Afektované počítače pod jednotnou kontrolou útočníka tvoří skupinu zvanou Botnet. Útočník dokáže ovládat Botnet jednotně a to mu umožňuje snadno plánovat útoky typu DDoS. Kontrola velkého množství počítačů umožňuje koordinovaně napadat síťové služby za účelem sabotáže nebo získání chráněných informací.

Analýza datového provozu dokáže odhalit šíření škodlivého softwaru v síťovém prostředí. Stejně tak umožňuje zaregistrovat koordinovaný útok na síťové prvky nebo služby.

3.3.9 Forensní analýza paměti (RAM)

Monitoring datových toků v privátní síti poskytuje obraz o komunikaci jednotlivých komponent různých informačních systémů. Avšak není to jediný účinný nástroj na ochranu proti škodlivému Malware. Podrobná analýza operační paměti je další efektivní zbraní.

Znalost toho, jak zachytit a rozčlenit obsah paměti počítače nám rozšiřuje možnosti reakce na bezpečnostní incidenty, detekce malwaru a schopnosti digitální forensní analýzy. Přestože kontrola pevného disku nebo zachycený paket může přinést přesvědčivé důkazy, je to často obsah paměti RAM, který umožňuje rekonstruovat to, co se stalo před napadením, během napadení nebo zda nehrozí napadení pokročilým útokem (CASE, 2014, s. 17).

3.3.10 Lidský faktor

Jistým rizikem pro bezpečnost informací je jakákoli osoba uvnitř společnosti, která má přístup k informačním systémům anebo alespoň do prostor společnosti. Může se jednat o kmenové zaměstnance, smluvní zaměstnance nebo o dodavatele služeb, jako je úklid, údržba nebo správa informačních technologií.

Tyto osoby lze rozdělit do několika kategorií:

Aktuální zaměstnanci, kteří pracují přímo pod vedením organizace. Tato kategorie zahrnuje běžné zaměstnance, dočasné zaměstnance, smluvní zaměstnance a konzultanty. Většina těchto osob má přístup do prostor společnosti, interní sítě a pracuje s interními informacemi společnosti.

Odcházející zaměstnanci znamenají v oblasti informační bezpečnosti nejvyšší riziko. Do této kategorie spadají zaměstnanci, kteří byli nebo budou přeloženi na jinou pracovní pozici, smluvní spolupracovníci nebo konzultanti, jimž má vypršet smlouva a další osoby, které mají v blízké době ukončit spolupráci se společností. Tyto osoby mají stále přístup k interním informacím a mohou zamýšlet se je získat. Motivací může být také poškození společnosti ze msty.

Bývalí zaměstnanci jsou ti, kteří již ve společnosti nejsou zaměstnáni nebo smluvní partneři, kteří se společností již nemají platnou smlouvu o spolupráci. Tyto osoby mají znalost vnitřního prostředí a bez ohledu na využití přístupových práv dokážou společnosti způsobit škodu dlouho po tom, co byla jejich spolupráce ukončena. Bývalí pracovníci mohou být vysoce motivováni k tomu, aby zaútočily na prostředky bývalých zaměstnavatelů.

Poskytovatelé služeb zastávají spousty důležitých rolí, aby se společnost mohla věnovat svým hlavním podnikatelským aktivitám. Obvykle se jedná o služby jako je úklid prostor, správa budov nebo správa informačních technologií. Poskytovatelé služeb za posledních několik let natolik rozšířili své aktivity, že se často podílejí na hlavní podnikatelské činnosti podniků. V současnosti je běžné, že dodavatel přímo podporuje prodej podniku tím, že zprostředkovává kontakt se zákazníkem. Ne každý dodavatel potřebuje přístup do prostor nebo k informačním systémům, ale je třeba si uvědomit, že spousta z nich ano.

Je na zvážení vedení společnosti, zda by specifickou službu měli vykonávat vlastní zaměstnanci nebo zaměstnanci dodavatele. Vlastní zaměstnanci podléhají bezpečnostním postupům a politikám, které si společnost sama stanovila a sama si je spravuje. Naproti tomu jsou zaměstnanci dodavatele, kteří podléhají jiným bezpečnostním nařízením. Avšak za bezpečnostní postupy zaměstnanců dodavatele nese odpovědnost dodavatel sám. Přístup dodavatelů k interním informacím je jistě bezpečnostním rizikem, ale takové riziko často přináší i vlastní zaměstnanci.

Obchodní partneři jsou obvykle osoby nebo organizace, které spolupracují za účelem naplnění společného podnikatelského cíle. Přístup k informacím v takovém případě bývá na úrovni nejvyšších manažerů partnerských organizací. Taková situace může přinášet jistá rizika při sdílení informací v rámci obchodního partnerství, ale nemusí přinášet rizika pro jiné interní informace.

Lze předpokládat, že současné organizace mají ve své struktuře hlavní organizační jednotky (vedení organizace, prodej, zákaznická podpora a produktový vývoj) a podpůrné organizační jednotky (IT, finanční oddělení, logistika, lidské zdroje a další).

Zaměstnanci potřebují k vykonávání jejich pracovní náplně přístupy k souvisejícím informacím. Obchodník přecházející ke konkurenci mívá přístup k informacím o

zákaznících a o produktech, někdo další k informacím o vývoji a to je intelektuální vlastnictví související se současnou i budoucí podobou produktu. Zaměstnanci zákaznické podpory mohou mít přístup k osobním informacím zákazníků, které mohou posloužit pro zneužití identity (KABAY, 2014, s. 422).

Oblast informačních technologií je z pohledu bezpečnosti velice citlivá, ale také velice užitečná z pohledu moderního podnikání. Většina současných organizací uchovává a zpracovává informace prostřednictvím elektronických systémů. Správci informačních technologií mívají často nekontrolovaný přístup ke všem těmto informacím. Je na vedení každé organizace, aby posoudilo rizika, která z takové situace vyplývají.

Podle příčiny vzniku bezpečnostních incidentů ze strany osob je lze rozdělit do několika typů: nedopatření, úmyslné ohrožení a neúmyslné ohrožení (KABAY, 2014, s. 425).

Nedopatření jsou incidenty způsobené nějakou chybou. Například pokud zaměstnanci nedodržují správné postupy a obcházejí bezpečnostní nařízení, nebo když nejsou dostatečně proškoleni a neznají správný postup. Také může dojít k odeslání údajů o zákazníkovi na nesprávnou adresu. To může nastat ve chvíli, kdy má odesílatel nastavené automatické doplňování adres příjemce. Systémy na ochranu informací tak nemusí takový incident zaznamenat. Tento typ chyby může v oblasti finančnictví znamenat velký problém, při kterém došlo k porušení legislativních nařízení.

Spousty dalších nedopatření nastává během změn, inovací a údržby informačních systémů. Programátor netestovaným skriptem snadno smaže záznamy z databáze. Správce snadno zapříčiní ztrátu dat na porouchaném disku tím, že nezajistil zálohování.

Úmyslné ohrožení má za cíl poškodit organizaci nebo zajistit přínos útočníkovi. Nespokojení správci mohou zasáhnout do informačních systémů tak, že způsobí zastavení chodu celé společnosti. V minulosti bylo zaznamenáno množství zlomyslných zásahů ze strany současných i bývalých administrátorů.

Některé organizace disponují hodnotnými informacemi, na které se útoky přímo zaměřují. Zaměstnanci kopírují databáze osobních informací a snaží se je zpeněžit na černém trhu. V jiných případech jde o intelektuální vlastnictví organizace, které se zaměstnanec snaží získat, aby ho sám mohl nabízet za účelem zisku. Zaměstnanec může tyto informace využít v novém zaměstnání nebo je nabídnout konkurenci. Tento typ

incidentu se často vztahuje na vývojáře softwarového vybavení, na jehož vývoji se podílely.

Neúmyslné ohrožení je takové, které způsobí pracovník záměrně, ale nikoli za účelem poškození společnosti. Častým motivem je zvýšení pracovní produktivity prostřednictvím nedodržení správných postupů a bezpečnostních politik. Byly zaznamenány události, kdy zaměstnanci vyexportovali interní data na internetové úložiště bez zabezpečení přístupu. Indexovací služby internetových vyhledávačů umožnily taková data snadno nalézt. V okamžiku, kdy pracovník odesílá interní informace prostřednictvím elektronické pošty do vlastní schránky, vzniká riziko, že se informace dostanou do nesprávných rukou darováním nebo odprodejem vlastního počítače. Rizikové situace nastávají i během vzdáleného přístupu k informacím z domova nebo ze služební cesty. Rychlý přístup k potřebným informacím ze vzdálených lokalit může být často pro podnikání velmi důležitý. Využití vzdáleného přístupu zvyšuje nároky na fyzickou bezpečnost, protože vzniká riziko odcizení z nedostatečně nebo vůbec nezabezpečených prostor jako jsou automobily nebo veřejné prostory.

Analýza síťového provozu nedokáže zabránit nebezpečnému chování uživatelů a správců sítě, ale dokáže napomoci při identifikaci komunikace, která únik interních informací způsobila. Jako nástroj aktivní ochrany interních informací byl vyvinut systém DLP (Data Loss Prevention), který manipulaci s informacemi dokáže zaznamenat ale i ji aktivně zabránit.

Systémy dostupné prostřednictvím internetu

Narůstající trend poskytování služeb informačního systému prostřednictvím internetu externí firmou zvyšuje bezpečnostní riziko více než v případě využívání interních systémů ve vlastní správě. V případě, že některý zaměstnanec ukončí s organizací pracovní poměr, je poměrně snadné neprodleně zrušit přístupy do prostor, sítě a aplikací. Je to velice důležitý úkon v případě bývalého zaměstnance, který má přístup k interním informacím a mohl by mít motivaci k poškození organizace.

Ale v případě informačních systémů, ke kterým se přistupuje přes internet, může bývalý zaměstnanec mít stále k těmto systémům přístup v podstatě odkudkoli. Bývá náročné neprodleně odcházejícímu pracovníkovi odebrat přístupová práva k systémům provozovaných externí firmou a pokračující platnost uživatelského účtu tak zvyšuje riziko

zneužití těchto systémů. Na některé z bývalých pracovníků to může působit přísně, ale zrušením přístupu lze spolehlivě snížit riziko zneužití.

Využívání takto provozovaných systémů může organizacím výrazně snížit náklady na informační technologie, než kdyby si je organizace provozovaly sami. Pracovníci odpovědní za informační bezpečnost musí úzce spolupracovat s oddělením lidských zdrojů a správci informačních technologií. Je třeba zajistit, aby odcházejícímu pracovníkovi byl neprodleně zamezen přístup k systémům poskytovaným externím dodavatelem.

Poskytovatelé služeb

Spousta organizací uplatňuje přísná bezpečnostní pravidla na své vlastní zaměstnance, ale nejsou nijak chráněny ze strany zaměstnanců externích dodavatelů. Množství organizací zahrnuje své bezpečnostní politiky a procesy do smlouvy o spolupráci a považuje to za dostatečné předcházení rizikům. Externí dodavatel však nemusí dodržování bezpečnostních postupů a politik provádět dostatečně intenzivně. Může za tím být zvýšení zisků z kontraktu nebo nedostatek financí v rozpočtu.

Například externí dodavatel čelící neustálé fluktuaci zaměstnanců by mohl obcházet vstupní prověření nebo zaškolení nastupujících proto, aby proces zaměstnání urychlil. Nedostatečné bezpečnostní politiky na straně externího dodavatele mohou vést ke kompromitaci klientských informací.

V případech, kdy jsou veškeré informační systémy dodávány externím dodavatelem, mají zaměstnanci dodavatele přístup k veškerým informacím klienta. Konkrétně poskytovaná služba elektronické pošty je vysoce riziková, protože umožňuje snadné vyhledávání přesně formulovaných informací. Klientská organizace je tak vystavena riziku, že přijde o informace související intelektuálním vlastnictvím.

Správci systémů

Správci informačních systémů běžně disponují správcovskými přístupovými právy k informačním zdrojům, na kterých jsou uchovávána citlivá data. Prostřednictvím takových práv mohou záměrně napadat služby informačních systémů, které jim neumožňují přímý přístup k informacím. Například je možné poškodit data aplikací nebo mazat informace v databázích i jejich zálohách. Obnovení takto ztracených informací je značně obtížné. Riziko je obzvláště vysoké v případech malých organizací, kdy jediný správce má možnost

ovládat provoz serverů, aplikací, sítí, elektronické pošty a zálohování. Taková osoba mívá často i pod kontrolou správu uživatelských účtů a přístupových práv. U větších organizací je mnohem jednoduší oddělit jednotlivé administrátorské role tak, že jejich práva jsou přidělena pouze na nutné množství systémů. To výrazně snižuje riziko poškození dat než v případě, kdy jsou veškeré systémy pod kontrolou jediné osoby.

Ve velkých organizacích s tisíci serverů, kde se využívá rozdělení výpočetního výkonu, správce často disponuje právy, které mu umožňují spustit skript, který dokáže smazat data na discích všech severů zároveň. Takové riziko klade důraz na úpravu rozsahu přístupových práv správců, aby nemohlo dojít plošnému poškození informačních systémů.

Zmíněná rizika nelze odstranit implementací analýzy síťového provozu, ale lze většinu případů odhalit na základě uložených záznamů, které umožňují zpětné vyšetření událostí v prostředí datové sítě.

3.4 Nařízení a normy

3.4.1 Zákon o kybernetické bezpečnosti

Od 1. Ledna 2015 vešel na území České republiky v platnost zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Zákon vznikl s cílem zajištění bezpečného fungování informační společnosti České republiky. Zákon nezakládá civilní ani trestní odpovědnost pachatelů kybernetických útoků. Avšak vytváří systém bezpečnostních opatření, která mají předcházet výskytu kybernetických incidentů. Dalším cílem je stanovení minimálních požadavků na standardní zabezpečení kritické informační infrastruktury a významných informačních systémů. Správci kritické informační infrastruktury a významných informačních systémů mají možnost kontaktovat Národní centrum kybernetické bezpečnosti (govCERT.cz), který se podílí na standardizaci a osvětě v prostředí kybernetické bezpečnosti.

Tvůrci přijatého návrhu vycházeli ze dvou zásad a třech pilířů:

1. Zásada – Minimální zásah do práv soukromých subjektů
2. Zásada – Individuální odpovědnost za bezpečnost vlastních systémů

1. Pilíř – Bezpečnostní opatření
2. Pilíř – Hlášení kybernetických bezpečnostních incidentů
3. Pilíř – Protiopatření, reakce na bezpečnostní incident

K zákonu kybernetické bezpečnosti náleží též prováděcí předpis č. 316/2014 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti. Předpis je znám jako vyhláška o kybernetické bezpečnosti. Vyhláška definuje povinnosti jednotlivých subjektů kybernetické bezpečnosti. Předepisuje tak:

- Podobu bezpečnostní dokumentace
- Obsah a rozsah bezpečnostních opatření
- Kategorizaci bezpečnostních incidentů

  Kategorie III – velmi závažný kybernetický bezpečnostní incident

  Kategorie II – závažný kybernetický bezpečnostní incident

  Kategorie I – méně závažný kybernetický bezpečnostní incident

- Podrobnosti k hlášení o bezpečnostním incidentu
- Podrobnosti k hlášení o provedených protiopatřeních

Zákon o kybernetické bezpečnosti ukládá povinnosti těmto subjektům:

- Poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací
- Orgán nebo osoba zajišťující významnou síť
- Správce informačního systému kritické informační infrastruktury
- Správce komunikačního systému kritické informační infrastruktury
- Správce významného informačního systému

3.4.2 Zákon o ochraně osobních údajů

Zákon č.101/2000 Sb. o ochraně osobních údajů definuje, klasifikuje a upravuje nakládání s informacemi o osobách.

Tento zákon v souladu s právem Evropské unie, 1) mezinárodními smlouvami, kterými je Česká republika vázána, 1a) a k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států. (ČR, č.101/2000 Sb., § 1.)

Většina komerčních i státních organizací disponuje množstvím osobních údajů o svých zaměstnancích, klientech, zákaznících a obchodních partnerech. Při jakékoli manipulaci s daty, které obsahují osobní údaje, je třeba dbát zvýšené opatrnosti a respektovat zákon na ochranu osobních údajů.

3.4.3 Další zdroje nařízení v oblasti kybernetické bezpečnosti

HIPAA (Health Insurance Portability and Accountability Act) v oblasti zdravotnictví (www.hipaa.com)

GLBA (Gramm-Leach-Bliley Act, známý též jako Financial Services Modernization Act z roku 1999)

Basel_II (Doporučení bankovních zákonů a regulace vydaná Basel Committee on Banking Supervision) ve finančním sektoru
(www.bis.org)

PCI DSS (Payment Card Industry Data Security Standard) pro organizace zpracovávající transakce platebních karet
(www.pcisecuritystandards.org)

4 Praktická část

4.1 Stanovení a formulace cílů

Cílem praktické části je zajištění informací o datových tocích v reálném prostředí podnikové datové sítě. Jeho součástí je důkladné seznámení s topologií a použitými aktivními prvky sítě a seznámení s charakterem běžně využívané datové komunikace. Další součástí je výběr a implementace nástrojů potřebných k zajištění potřebných podkladů pro vyhodnocení celkového stavu komunikace v monitorovaném prostředí.

Vedlejším cílem je získat zkušenost s výběrem a implementací dostupných monitorovacích nástrojů a ověřit plánovaný postup v praxi.

4.2 Monitorované prostředí

Praktická část analýzy síťového provozu je v prostředí reálné a funkční podnikové sítě. Síť svou topologií odpovídá nejčastěji se vyskytujícím typům síťového propojení jednotlivých pracovišť komerční společnosti. Zvolená síť obsahuje pracoviště typu: administrativní budova, prodejna, centrum zákaznické podpory a datové centrum. Pracovní stanice s operačním systémem Windows 7 jsou pod společnou správou prostřednictvím Microsoft Active Directory (AD). Pro hlasovou komunikaci mají zaměstnanci k dispozici IP telefonii v podobě VoIP telefonních přístrojů. Přístup z pracoviště do Internetu je bezpečnostní politikou povolen výhradně přes PROXY. Prostory pracoviště jsou pokryty signálem pro bezdrátovou síť WiFi. Vzdálený přístup zaměstnanců vně prostorů společnosti k datovým službám a zdrojům je realizován prostřednictvím šifrovaného spojení k VPN koncentrátoru.

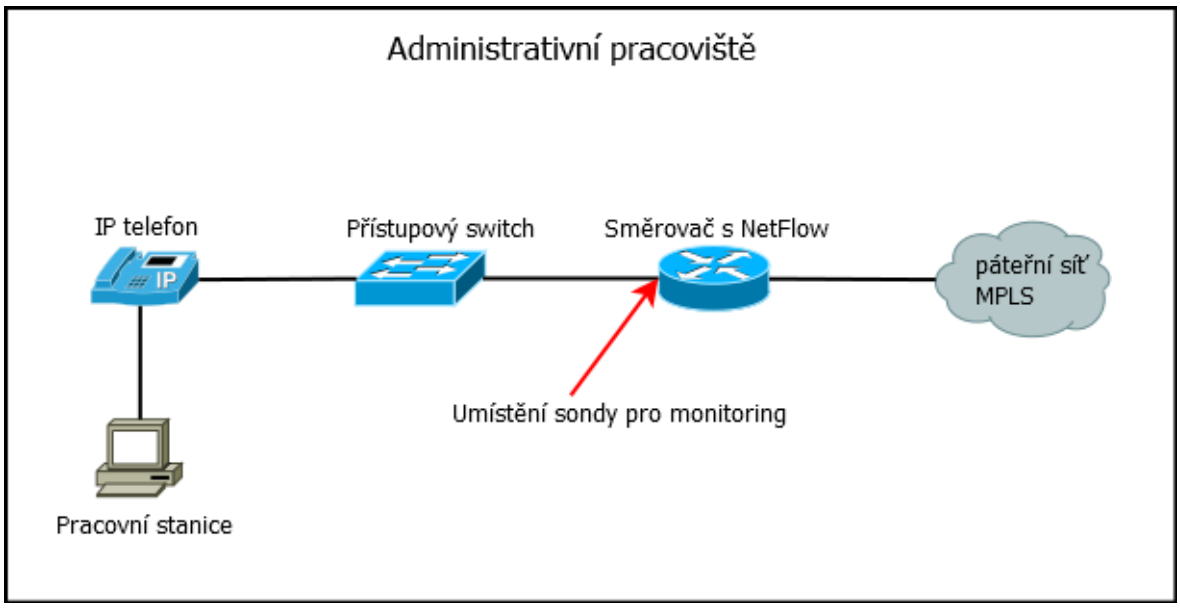
Z pohledu datové sítě existuje předpoklad, že většina datových toků bude procházet přes brány jednotlivých lokálních sítí (default gateway) včetně případné komunikace iniciované škodlivým softwarem směrem do internetu. Brána lokální sítě je tak vhodným uzlem k umístění sondy pro monitorování datových toků.

Pracoviště v administrativních prostorech

Datové toky, které je možné v případě monitorování administrativního pracoviště očekávat:

- Komunikace do datového centra – V datovém centru jsou hostovány servery s podnikovými informačními systémy, poštovní servery a servery pro správu pracovních stanic.
- Komunikace do internetu – Nařízení politiky podnikové bezpečnosti umožňuje komunikaci do internetu pouze prostřednictvím proxy severu.
- IP telefonie – Zařízení pro IP telefonii vytváří datové toky protokolu UDP přenášející hlas mezi jednotlivými pracovišti nebo na telefonní ústřednu, která je bránou pro odchozí hovory do dalších telefonních sítí. Je třeba zohlednit komunikaci VoIP signalizačního protokolu.

Obrázek 14 - Schéma administrativního pracoviště



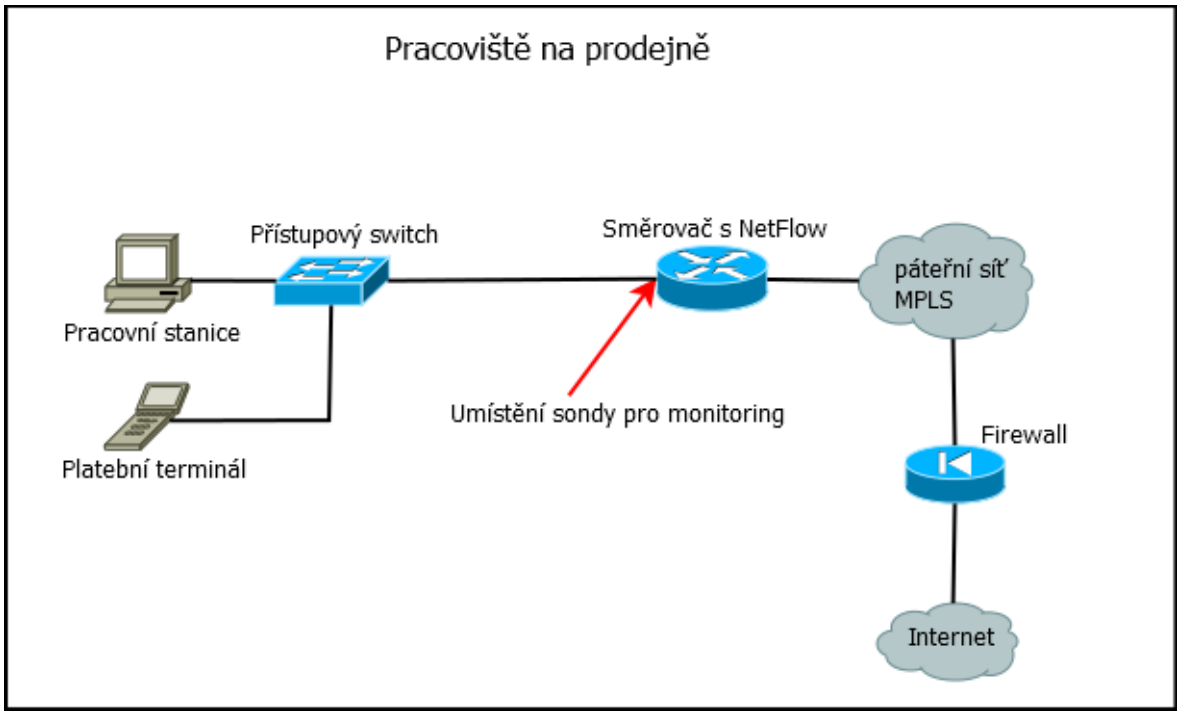
Monitoring je v takovém případě umístěn v uzlu sítě tak, aby zaznamenal aktivitu datových přenosů prostřednictvím NetFlow sondy. V okamžiku, kdy dojde na pracovišti k jakékoli datové komunikaci mimo lokální síť, je možné prostřednictvím NetFlow sondy získat záznam o navázaném datovém toku. Samotná sonda je v tomto případě součástí směrovače. Jde o službu, kterou lze na některých směrovačích nakonfigurovat a spustit.

Pracoviště na prodejně

Na rozdíl od administrativního pracoviště je předpokládán částečně jiný typ datových toků. Nestejný soubor datových toků je dán využitím specifických informačních systémů pro odbavení požadavků zákazníků. Další užitečnou informací pro monitoring datových toků je, že prodejny nevyužívají IP telefonii. Předpokládané typy komunikací tedy v případě prodejny jsou:

- Komunikace do datového centra – V datovém centru jsou hostovány servery s podnikovými informačními systémy, poštovní servery a servery pro správu pracovních stanic. Prodejny nadále využívají systémy management komerčních služeb a přístup k CRM.
- Komunikace do internetu – Nařízení politiky podnikové bezpečnosti umožňuje komunikaci do internetu pouze prostřednictvím proxy severu.
- Přímá komunikace do internetu – Jedná se o bezpečnostní výjimku, kterou bylo nutné přijmout za účelem přístupu terminálů pro platební karty k bankovní platební bráně.

Obrázek 15 - Schéma pracoviště na prodejně



Přesto, že se pracoviště prodejny liší v typech očekávané datové komunikace od administrativních prostor, je možné pro monitoring využít NetFlow sondu, která je integrovaná v místním směrovači.

Síťové prvky

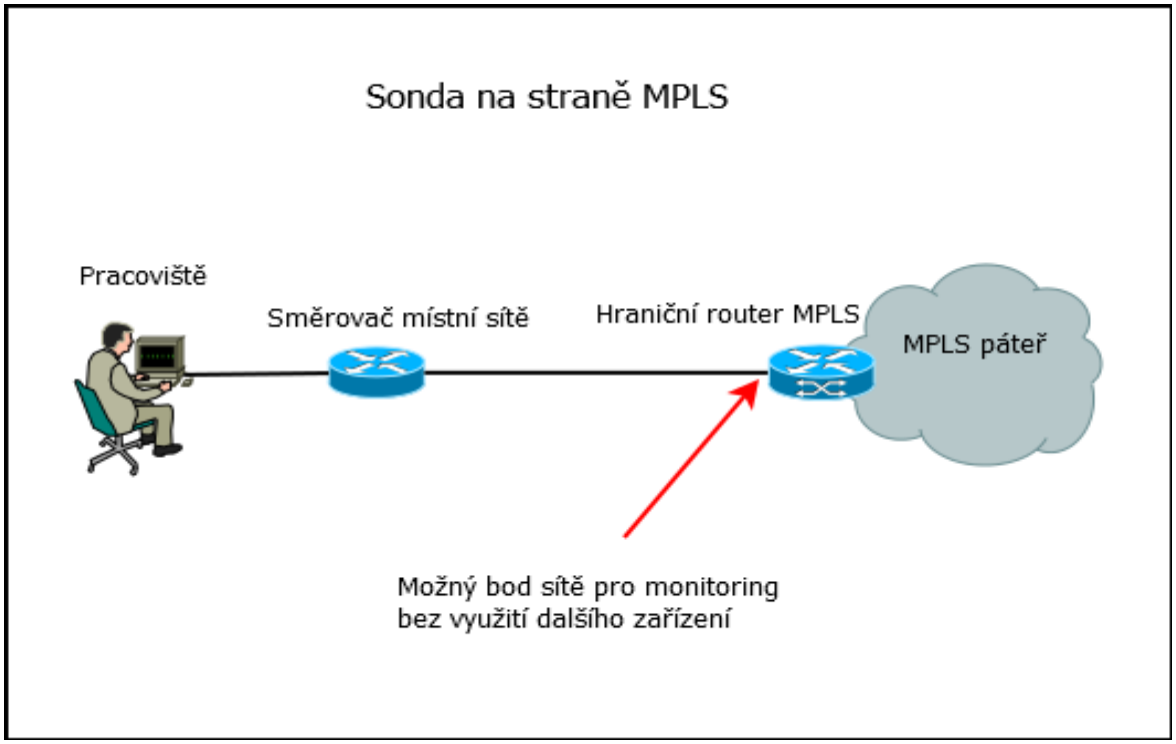
Součástí postupu je ověření, zda implementované síťové prvky lze využít pro export záznamů o datových tocích. Pokud směrovače lokálních sítí umožňují export záznamů, pak je třeba na těchto prvcích nakonfigurovat sběr a export směrem ke kolektoru. Pokud by součástí sítě byl aktivní prvek, který nepodporuje export záznamů, je třeba nalézt jiný způsob, jak umístit monitorovací sondu pro daný uzel sítě.

Tabulka 4 - Přehled o podpoře exportu záznamů

Umístění směrovače pro monitoring	Typ zařízení	Verze software	Podpora sledování toků
administrativní pracoviště	Cisco C4500	s72033_rp-IPSERVICESK9_WAN-M 12.2(33)SXJ6	Ano
administrativní pracoviště	Cisco C3750	C3750-IPSERVICESK9-M 12.2(25)SEE2	Ano
administrativní pracoviště	HP A5820X-24XG-SFP+	Comware 5.20	Ano
administrativní pracoviště	H3C S5600-26F	Comware 3.10	Ne
prodejna	Cisco C1921	C1900-UNIVERSALK9 M15.3(3)M4	Ano
prodejna	Cisco C2901	C2900-UNIVERSALK9-M 15.1(4)M3	Ano
Hranice administrativní sítě	Cisco Nexus N7k	n7000-s2-dk9.6.2.14	Ano
hranice MPLS páteře	Cisco 7606-S	c7600s72033_rp-ADVIPSERVICESK9-M	Ano

Dalším možným umístění sondy je na hraničním směrovači MPLS. To je však možné pouze v případě, že hraniční směrovač MPLS páteře export záznamů podporuje. Jestliže by ani tato možnost monitoringu nebyla možná, je nutné instalovat sondu jako samostatné zařízení.

Obrázek 16 - Připojení sondy na hranici MPLS páteře



Je patrné, že pokud bude sonda umístěna na straně hraničního směrovače, nebude možné získat záznamy o komunikaci v rámci lokálního směrovače. Z tohoto důvodu je třeba správně rozhodnout, zda tato změna nebude zdrojem neúplných podkladů pro vyhodnocení výsledků.

Pokud by se třeba jednalo o monitoring za účelem analýzy provozu do internetu, tato změna by se do výsledků nijak negativně neodrazila.

Ale v případě, že by došlo k samovolnému šíření škodlivého softwaru v rámci lokální sítě, nebude taková aktivita sondou na straně MPLS zaregistrována.

4.3 Použité nástroje

Volba nástrojů závisí na očekávané podobě výsledků, na rozsahu vstupních informací a vzájemné spolupráci mezi jednotlivými komponenty. S výhodou lze využít možností monitoringu, který poskytují samy implementované síťové prvky. Jako kolektor záznamů je třeba vybrat zařízení a softwarovou službu, která dokáže přijímat informace o záznamech ze všech typů použitých sond. U kolektoru je v tomto případě potřebná podpora příjmu a zpracování záznamů typu IPFIX, NetFlow a sFlow. Dále je nutné, aby kolektor neměl omezení na počet exportérů, které by mohlo působit nekompletní nebo zkreslené výsledky.

4.3.1 Výběr monitorovací sondy

Směrovače zkoumaného síťového prostředí ve většině případů umožňují získání záznamů o datových tocích prostřednictvím integrované NetFlow (sFlow) sondy. Na úrovni konfigurační změny lze získávat záznamy a exportovat je směrem ke kolektoru. Pro tyto účely lze využít sondy jako samostatného zařízení, ale k získání podkladových dat není třeba této možnosti využít. Na základě těchto informací je zvolen způsob získávání informací prostřednictví směrovačů Cisco, HP a H3C.

Ukázka a popis použité konfigurace sondy na směrovači

Cisco Catalyst řady C6500-E:

mls netflow

povolí zpracování na kartě PFC (Policy Feature Card)

mls flow ip full

specifikace zachytávaných záznamů (zachycení všech)

interface vlan *611*

ip route-cache flow

exit

povolí zachytávání záznamů na jednotlivých rozhraních

mls nde sender version 7

nastavení verze NetFlow pro exportér NDE (NetFlow Data Export)

ip flow-export source *Vlan600*

nastavení zdrojového rozhraní exportéru pro identifikaci zdroje záznamů v kolektoru

ip flow-export destination *10.16.222.134 2055*

specifikace adresy kolektoru

H3C (HP) Comware 5.20

sflow agent ip *10.5.112.49*

nastavení zdrojového rozhraní exportéru pro identifikaci zdroje záznamů v kolektoru

sflow collector 1 ip *10.16.222.134* ***port*** *2055*

specifikace adresy kolektoru

sflow version 5

nastavení verze sFlow

sflow interval 30

každých 30 sekund odešle záznamy do kolektoru

interface ethernet 1/0

sflow enable inbound

sflow sampling mode random

sflow sampling-rate 512

aktivace a nastavení samplování na jednotlivých rozhraních

Postupy konfigurace jsou uvedeny pro zdokumentování postupu. Není zde uvedena konfigurace pro každé monitorované rozhraní, protože se jedná o stejný způsob nastavení.

4.3.2 Výběr kolektoru

V současnosti je trhu množství nástrojů, které umožňuje zpracovávat získané záznamy. Tyto produkty se liší svými funkcemi a vstupními parametry. Mezi těmito nástroji je třeba zvolit takový, který dokáže zpracovat záznamy daných exportérů a poskytnout zpracovaný přehled o komunikaci monitorovaného prostředí. Z toho lze stanovit podmínky pro výběr kolektoru. Tyto podmínky slouží také jako zdroj informací pro použití bodovací metody vícekriteriálního výběru variant. Bodovací metoda je výpočetně nenáročná a na rozdíl od metody pořadí zohledňuje velikost odstupu mezi jednotlivými úrovněmi.

Varianty jsou tvořeny softwarovými produkty pro analýzu datového provozu, které jsou popsány v části literární rešerše.

Kritéria:

- Nejaktivnější uživatel – Zobrazení aktuálně nejaktivnějšího uživatele (uživatele s největším počtem datových spojení)
- Nejpoužívanější protokol – Zobrazení nejčastěji používaných portů pro určení typu datové komunikace
- Vytížení sítě – Celkový pohled na využití síťových zdrojů
- Flow technologie – Úroveň podpory technologií využitých pro export záznamů (sFlow, NetFlow)
- Náklady – Kritérium zohledňující ekonomický aspekt produktu

Bodové hodnocení preferencí kritérií a výpočet vah

Přidělení bodů jednotlivým kritériím bylo stanoveno subjektivně na základě preferencí, které vedou k uspokojující volbě nástroje, a zároveň poskytne potřebné zpracování datových záznamů. Bodová škála je uvažována v rozmezí od 1 bodu (nejhorší) po 10 bodů (nejlepší). Vypočtené váhy jsou pro přehlednost dále zaokrouhleny na dvě desetinná místa.

Výpočet vah jednotlivých kritérií:

$$\text{váha kritéria} = \frac{\text{bodové ohodnocení}}{\text{součet přidělených bodů}}$$

Tabulka 5 - Bodové ohodnocení preferencí kritérií a výpočet vah

Kritérium	Body	Váhy kritérií	Zaokrouhlení
Nejaktivnější uživatel	8	0,266666667	**0,27**
Nejpoužívanější protokol	5	0,166666667	**0,17**
Síť celkově	6	0,2	**0,2**
Podpora Flow	10	0,333333333	**0,33**
Náklady	1	0,033333333	**0,03**
Suma	30	1	1

Bodové hodnocení kritérií jednotlivých variant

U každé uvažované varianty nástroje jsou přiděleny body kritériu podle toho, do jaké míry splňují stanovené požadavky. Bodová škála je, jako u hodnocení významnosti kritérií uvažována v rozmezí od 1 bodu (nejhorší) po 10 bodů (nejlepší).

Tabulka 6 - Deklarace bodování pro jednotlivé úrovně kritérií

Počet bodů	10	9	7	6	5	2	1
Nejaktivnější uživatel	plně podporuje				částečně podporuje		nepodporuje
Nejpoužívanější protokol	plně podporuje				částečně podporuje		nepodporuje
Celkové využití sítě	plně podporuje				částečně podporuje		nepodporuje
Podpora technologií	více technologií				NetFlow a sFlow		pouze jedna
Náklady (kč)	0	4050	32400	41310	51000	102000	109000

Stanovení nejvhodnější kompromisní varianty

Pro stanovení pořadí kompromisních variant je v rámci výpočtu zohledněna váha každého kritéria a úroveň do jaké míry je kritérium naplněno. Nejvyšší celkové bodové hodnocení určuje nejvhodnější variantu produktu pro použití.

Výpočet bodového hodnocení variant:

$$\text{bodové hodnocení} = \frac{\Sigma \text{ počet bodů} * \text{váha kritéria}}{\text{součet přidělených bodů}}$$

Tabulka 7 - Výpočet pořadí posuzovaných variant

Produkt	Nejaktivnější uživatel	Nejčastější protokol	Celkový náhled na síť	Podpora Flow	Náklady	Bodové hodnocení
SolarWinds	10	10	10	10	6	9,88
sFlowTrend	10	10	10	1	10	7,03
Scrutinizer	10	10	10	5	2	8,11
ManageEngine	10	10	10	10	5	9,85
nTop	10	10	10	10	9	**9,97**
PeaslerPRTG	10	10	10	10	7	9,91
Wireshark	1	1	1	10	10	4,24
InterMapper	10	10	10	10	1	9,73
váha	0,27	0,17	0,2	0,33	0,03	

Nejvyšší bodové hodnocení (9,97 bodů) bylo vypočteno u varianty produktu nTop a vychází jako varianta, která nejlépe splňuje stanovená kritéria.

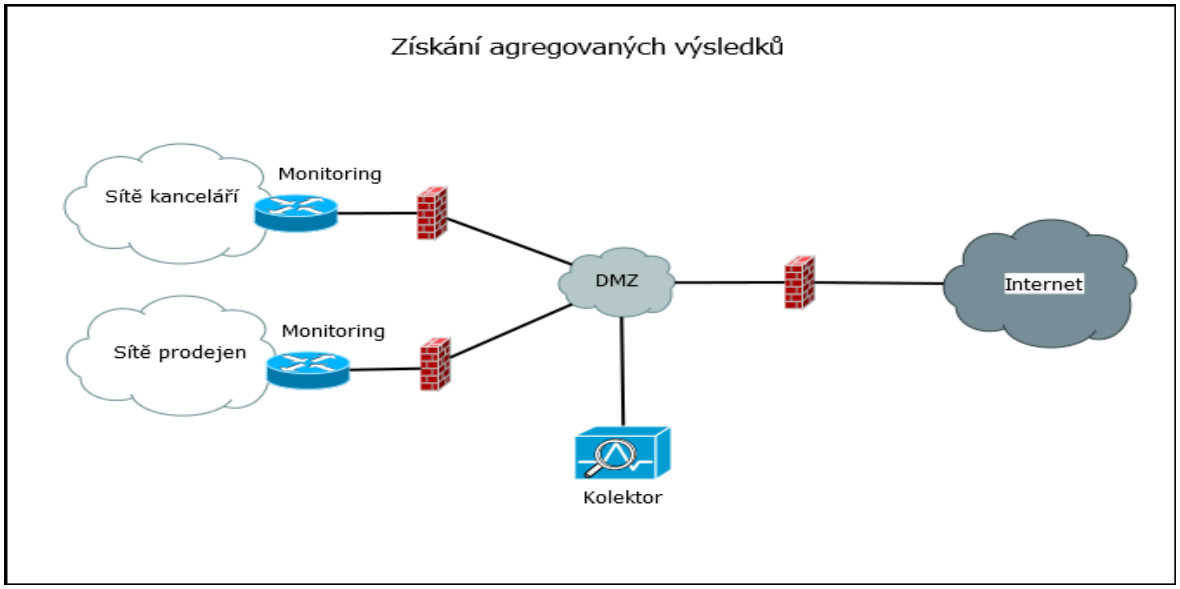
4.4 Návrh systému pro monitoring

V prostředí rozsáhlé sítě je třeba dbát na přehlednost sledovaných parametrů. Menší množství agregovaných výstupů může znamenat větší přehlednost. V případě šíření nebezpečného softwaru po síti celkový náhled napomůže odhalit jednorázový nárůst komunikace na portech protokolů, u kterých to nebývá běžné. Agregované výsledky v podobě grafů však nemusí na první pohled poskytnout dostatečně detailní informace, které mohou napomoci nalezení konkrétního uživatele sítě v případě bezpečnostního incidentu. Pro kontrolu datového provozu je proto třeba zajistit, aby měl správce přístup k agregovaným i detailním výstupům.

4.4.1 Agregované výsledky

Celkové výsledky je možné získat umístěním monitorovacího zařízení na síťový prvek, který je společný pro všechny uživatele daného segmentu. Získané záznamy lze pak snadno exportovat po síti směrem ke kolektoru pro další zpracování.

Obrázek 17 - Schéma získávání agregovaných výstupů



Ze schématu je patrné, umístění monitorovacích sond na perimetr síťových segmentů odděleně pro sítě prodejen a pro sítě administrativních prostor. Obě sondy tak zaznamenají veškerý datový provoz ke zdrojům v datovém centru nebo v internetu.

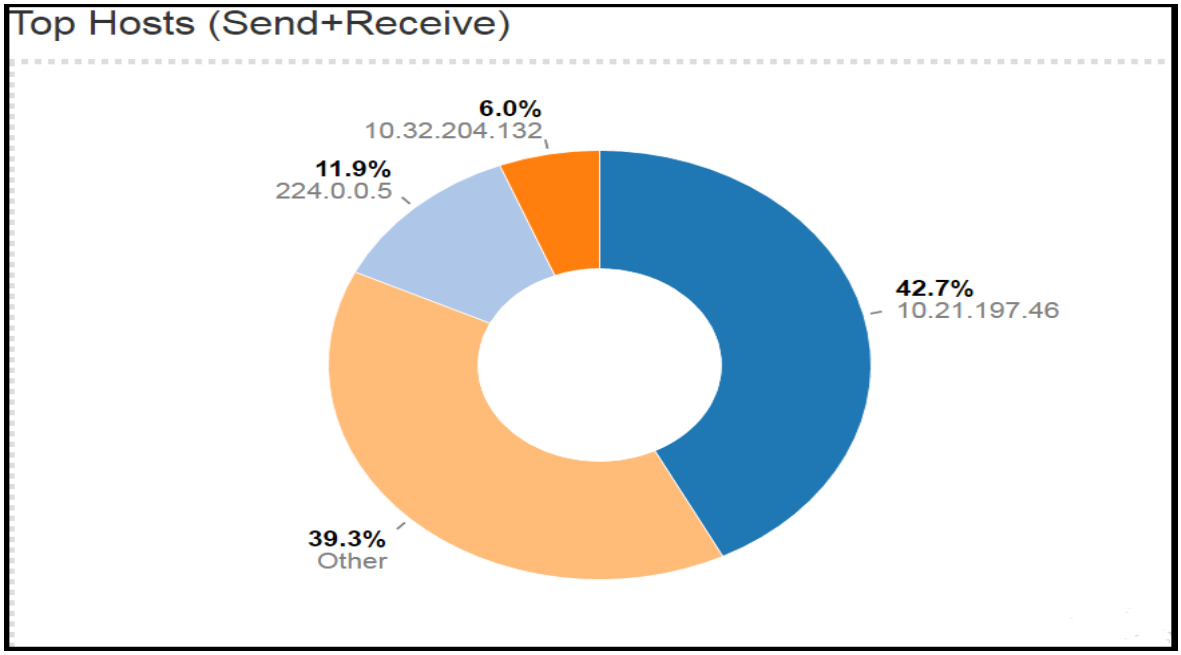
5 Výsledky a diskuse

Výsledkem analýzy datových toků v prostředí monitorované datové sítě jsou grafy, které přinášejí celkový náhled na stav sítě. Detailní výpisy záznamů umožňují identifikovat koncové body, typ komunikace a další parametry.

5.1 Agregované výsledky - celkové

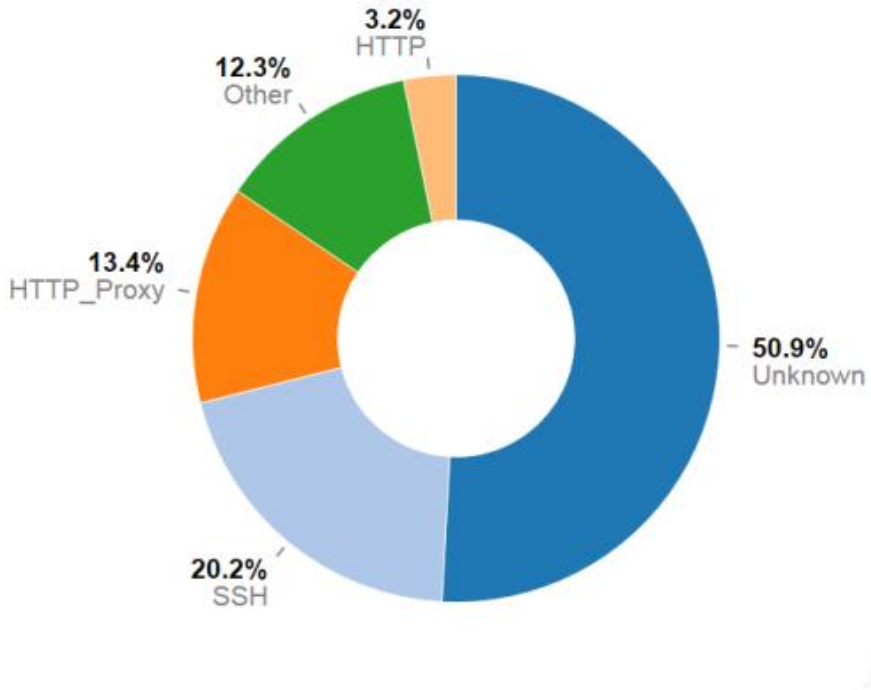
Hlavní součástí agregovaných výsledků jsou grafy, které vypovídají o celkovém využití síťové struktury. Pro potřeby identifikace datového provozu jsou grafické výstupy zaměřeny na zobrazení nejaktivnějších uživatelů sítě a na typy komunikace procházející perimetrem sítě. Zdrojem těchto výsledků jsou průměrné hodnoty, které poskytuje kolektor záznamů nTop (verze 2.0).

Obrázek 18 - Graf – Nejaktivnější uživatelé



42,7 % síťového provozu je komunikace do internetu prostřednictvím proxy serveru.
6,0 % z celkového vytížení sítě využívá server pro management pracovních stanic.
11,9 % síťového provozu využívá multicastový provoz (provoz aktivních prvků sítě).
39,3% tvoří zbývající skupina uživatelů, jejichž využití sítě není relativně výrazné.

Obrázek 19 - Graf – Nejpoužívanější protokoly



Z grafu nejpoužívanějších protokolů je patrné používání prohlížečů webových stránek. Popiskem „Unknown“ jsou označeny datové toky, které nástroj nedokáže sám identifikovat a dále interpretovat. Tento typ datového provozu není v celkovém náhledu blíže specifikován a lze o něm získat bližší informace z podrobného výpisu datových toků. Využití aplikací označené jako „Other“ znázorněné na grafu zahrnuje 12,3 % komunikace a reprezentuje skupinu identifikovaných protokolů, které svými přenosy dat nejsou relativně výrazné. Další skupina uživatelů používá šifrované spojení prostřednictvím protokolu SSH.

Výsledky byly zaznamenány během pracovní doby a jsou zajištěny na základě aktivity 2.372 uživatelů z 3.432 zaznamenaných datových toků.

5.2 Detailní informace o datových tocích

Nástroj nTop umožňuje získat přesné informace o konkrétním datovém spojení. To je nezbytná vlastnost pro identifikaci autorizované a neautorizované komunikaci v síťovém prostředí. K tomuto účelu slouží výpis všech záznamů o datových spojích. Prostřednictvím výpisu o datových spojích lze přistoupit i k detailním informacím každého záznamu. Detail záznamu obsahuje informace o IP adresách, mezi kterými komunikace proběhla, informace o transportním protokolu a portu transportního protokolu. Nástroj také zobrazuje počet přenesených paketů, objem dat a časové charakteristiky.

Detailní výpis záznamů v monitorované síti je možné získat z některých aktivních prvků sítě i prostřednictvím příkazové řádky CLI (Command Line Interface). Výčet záznamů prostřednictvím CLI umožňuje L3 switch Cisco Catalyst řady C6500-E. Toho je možné využít jako nouzové řešení v případě, že by došlo k bezpečnostnímu incidentu nebo nefunkčnosti části sítě a zároveň není v síti k dispozici kolektor záznamů.

5.3 Diskuse

Nejprve bylo nutné získat podrobné informace o prostředí, ve kterém analýza datového provozu probíhala. Tím vznikly podklady pro implementaci monitorovacího systému. Na základě takových podkladů lze rozhodnout, jaké nástroje a aktivní síťové prvky jsou pro monitoring potřebné.

Pro efektivní zachycení datových toků byly rozmístěny senzory a exportéry na uzlech sítě, přes které prochází veškerá datová komunikace monitorovaného síťového segmentu. V daném prostředí byly zvoleny směrovače, které bezprostředně sousedí s firewallem a tvoří perimetr sítě. Další možností je zachytávání záznamů na defaultních branách jednotlivých lokálních sítí. Sledování provozu zároveň na lokální síti a na perimetru sítě způsobuje to, že se záznam o jedné komunikaci dostává prostřednictvím dvou exportérů do kolektoru dvakrát. Takto vzniklé duplicity by bylo nutné odstranit, aby nedošlo ke zkreslení výsledků.

V monitorovaném prostředí bylo třeba se zaměřit na stávající možnosti aktivních prvků sítě a to především na jejich podporu pro získávání záznamů o datových tocích. Síťové prvky, které tvoří perimetr síťových segmentů (administrativní prostory a prodejny)

disponují NetFlow exportéry a umožňují tak získávat záznamy od datové komunikaci NetFlow verze 9.

Dále je vhodné specifikovat očekávané typy komunikací na základě používaných aplikací v daném segmentu sítě. To napomůže jako výchozí informace při hodnocení výsledků analýzy.

Informace generované kolektorem nepřetržitě umožňují vyhodnocovat aktuální stav síťové komunikace a v případě bezpečnostního incidentu je možné z těchto informací vycházet.

Implementovaný systém monitoringu nezaznamenal žádný typ nebezpečné komunikace do internetu ani využití nestandardních komunikačních protokolů.

Z dostupných výsledků vyplývá, že analýza datového provozu monitorované podnikové sítě nevykazuje známky aktivity škodlivého software ani přímé komunikace na neznámá místa v internetu. Zaznamenaná komunikace do internetu je pod kontrolou definovaných politik na proxy serveru a lze ji považovat za autorizovanou.

Monitorovací systém neumožňuje nijak aktivně zasahovat do řízení datové komunikace v síti. Systém by mohl být využit, jako zdroj informací pro automatický nástroj, který by mohl prostřednictvím SNMP (Simple Network Management Protocol) ovlivňovat konfiguraci síťových prvků a řídit datový provoz. Tím by se dalo zabránit nežádoucí komunikaci již při prvním výskytu.

6 Závěr

Analýza síťového provozu hraje významnou roli jako součást celkového zabezpečení informačních systémů. Tím, že umožňuje získávat informace o datové komunikaci, rozšiřuje úroveň zabezpečení informací. Datová síť je prostředím pro komunikaci většiny současných informačních systémů a to vytváří vhodné podmínky pro implementaci technologií pro analýzu datového provozu.

Z pohledu informačního zabezpečení analýza datového provozu zaujímá své místo vedle dalších technologií jako jsou protivirové programy, firewally nebo systémy IDS.

Často je analýza datových toků kombinována s jinými technologiemi a vytváří komplexnější systémy zabezpečení. Účinné použití analýzy datových toků je podstatou systémů SIEM nebo DLP. Jako součást těchto kombinovaných systémů tvoří efektivní nástroje pro preventivní odhalování neautorizované komunikace, která může být iniciována škodlivým softwarem nebo nesprávnou konfigurací aktivních prvků sítě. Včasné odhalení neautorizované komunikace v kombinaci s informací o zdroji a cíli usnadňuje odhalení příčin incidentů, dříve než dojde k samotnému ohrožení informačních systémů.

Uchovávání záznamů o datové komunikaci usnadňuje zpětné dohledání zdrojů a cílů neautorizované komunikace. Analýzou historie záznamů lze účinně odhalit datové přenosy, které vykazují známky přístupů k chráněným interním informačním zdrojům. V případě úniku interních informací z organizace díky uchovávaným záznamům existuje zdroj podstatných informací, který lze využít při vyšetřování incidentů tohoto typu.

Příčina úniku nebo ztráty informací bývá na straně samotných uživatelů. Uživatelé způsobují únik informací často, aniž by si to sami uvědomili. K takovým situacím přispívá nedostatečné proškolení, nepozornost a nezodpovědnost samotných uživatelů. Nástrojem pro ochranu před únikem je systém DLP, který kontroluje a vyhodnocuje datové přenosy a manipulaci s daty na straně uživatelských zařízení. Na koncových stanicích dokáže zabránit nebo zaznamenat kopírování na přenosná média. V síťovém prostředí DLP aktivně spolupracuje s proxy serverem, který neautorizované komunikaci do internetu zabrání.

Podle charakteru informací může způsobit jejich únik organizaci, z níž pochází, závažné problémy. Následky mají podobu ekonomických ztrát, ztrát intelektuálního vlastnictví, poškození zákazníka nebo trestního stíhání. V případě státních bezpečnostních

složek, vládních úřadů nebo výzkumných organizací může mít únik vnitřních informací fatální následky.

V souvislosti s rizikem a možným zneužitím informací strategického nebo osobního charakteru vznikla řada doporučení a norem upravujících přístup k informacím a jejich zpracování. Na úrovni legislativy České republiky vešly v platnost zákon č. 101/2000 ze dne 4. Dubna 2000 o ochraně osobních údajů a o změně některých zákonů (zákon o ochraně osobních údajů) a zákon č. 181/2015 ze dne 1. Ledna 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Podle jednotlivých odvětví podnikání organizace podléhají dalším nařízením, jako jsou HIPAA pro organizace zpracovávající informace v oblasti zdravotnictví nebo GLBA vztahující se na organizace v sektoru financí.

Budoucí vývoj technologií pro monitoring datového provozu by měl zohledňovat aktuální trendy vývoje informačních systémů. Pokud se v současnosti projevuje tendence o maximální využití technologií pro virtualizaci, je třeba se zaměřit na vývoj nástrojů pro sledování datového provozu mezi virtuálními zařízeními. V této oblasti existuje podpora na straně virtuálních přepínačů a vývoj nástrojů pro monitoring ve virtuálním prostředí pokračuje.

Aktuální trend, který přináší nová rizika v prostředí počítačových sítí je Internet věcí IoT (Internet of Things). V minulosti již byly zaznamenány útoky na informační infrastrukturu typu DoS. Tyto útoky byly vedeny prostřednictvím zařízení, která jsou připojena k internetu, ale sami o sobě nejsou typickými počítači s běžným operačním systémem. Jedná se zařízení, jako jsou televizory, teploměry, kamery nebo dětské chůvičky. Odolnost proti napadení takového zařízení závisí na tom, jaké zabezpečení provede jeho výrobce. Použití antivirového software je na těchto zařízeních téměř nemožné a zbývá jen kontrola datového provozu na úrovni sítí. Vývoj monitoringu v oblasti IoT má svůj význam, protože se často jedná o jediný účinný prostředek pro odhalení nestandardního chování v síťovém prostředí.

Využívání datových sítí přináší rizika, která je možné odhalovat sledováním datového provozu. V současném i budoucím prostředí informačních systémů nalezne analýza síťového provozu využití pro posílení bezpečnostních opatření.

Před samotnou analýzou je důležité v síťové topologii zvolit vhodné uzly pro umístění monitorovacích zařízení tak, že by bylo možné získávat hodnoty agregátní i dílčí.

Je však třeba dbát na to, aby nedocházelo k duplicitnímu monitorování téhož záznamu na dvou místech.

Pro bezchybný export záznamů je vhodné umístit kolektor v blízkosti měřících sond. V síťovém okolí kolektoru leze očekávat nárůst datových přenosů v podobě exportovaných záznamů. Často jsou segmenty sítě odděleny firewallem a je třeba zajistit potřebné prostupy pro exportované záznamy.

Součásti systému pro analýzu datového provozu musí svými vlastnostmi zohledňovat očekávané výsledky. Pro získávání a export záznamů lze využít sond a exportérů integrovaných v aktivních prvcích sítě.

Při volbě nástroje pro zpracování získaných záznamů lze využít bodovací metody vícekriteriální analýzy variant. Tím je možné zajistit nejvhodnější variantu z několika dostupných kompromisních řešení. S ohledem na stanovená kritéria nástroje vyšla nejvýhodnější varianta produktu nTop. Softwarový nástroj nTop zastává funkci kolektoru i nástroje pro zpracování a interpretaci získaných záznamů. Tento nástroj poskytuje agregované i detailní informace, což umožňuje získat analytický přehled o datovém provozu.

Analýzou datových toků v prostředí monitorované sítě nebyly nalezeny záznamy, které by prokazatelně dokládaly výskyt neautorizované komunikace. V oblasti autorizované komunikace vznikl přehled v podobě grafu o typech a množství používaných protokolů. Dále je prostřednictvím management konzole dostupná informace o aktivitách jednotlivých uživatelů a síťových služeb.

Implementovaný systém pro monitoring může posloužit jako základ k dalšímu rozšíření. V souvislosti s rozšířením by mohlo být užitečné vytvoření automatického řízení aktivních síťových prvků na základě informací získaných prostřednictvím monitorovacího systému. S využitím protokolu SNMP by bylo možné řídit konfiguraci síťových prvků a tím aktivně ovlivňovat datovou komunikaci.

Zprovoznění monitoringu datové sítě umožňuje správci nepřetržitý přístup k informacím, které napomáhají sledovat stav a zabezpečení celé informační infrastruktury. Aktivní monitoring datových toků lze zařadit do komplexu opatření informační bezpečnosti.

7 Seznam použitých zdrojů

Knižní publikace

CLARK, Gregory, QING, Li, 2015. *Security Inteligence: A Practitioner's Guide to Solving Enterprise Security Challenges*. 1. edition, Wiley. 363 s. ISBN 9781118896693.

CASE, Andrew, Levy, Jamie, Hale, Ligh, Michael 2014, *The Art of Memory Forensics*, Wiley. 914 s. ISBN 9781118825099.

KABAY, Michel E. Bosworth, Seymour Whyne, Eric, 2014. *Computer Security Handbook, Set,* Wiley. 2207 s. ISBN 9781118127063, ISBN 9781118851791.

DAVIDOFF, Sherri, Ham Jonathan, Geer Daniel E. *Network Forensics: Tracking Hackers through Cyberspace*, Pearson Education, Inc., 2013, ISBN-13: 978-0132564717, ISBN-10: 0132564718.

CHAPPLE, Mike. *Incident Response with NetFlow For Dummies, Lancope Special Edition*, John Wiley & Sons, Inc., 2014, ISBN 978-1-118- 88341-9.

PEREZ, André, *Network Security*, Wiley-ISTE, 2014, ISBN 9781848217584.

SIKORSKI, Michael, Honig Andrew, *Practical malware analysis, 1st Edition*, No Starch Press, Inc., 2012, ISBN-13: 978-1593272906, ISBN-10: 1593272901.

WOODY, Aaron, *Enterprise Security*, Packt Publishing, 2013, ISBN 981849685962.

COLLINS, John, *Security architect, Carreers in information security*, BCS Learning & Development Limited 2014, ISBN 9781780172200

EL-BAWAB, Abd El-Monem A., *Untangle Network Security*, Packt Publishing, 2014, ISBN 9781849517720

VACCA, John R., *Managing Information Security*, Elsevier Science, 2013, ISBN 9780124166882

Elektronické knihy a online monografické publikace

CHAPPLE, Mike, 2012. *NetFlow Security Monitoring: ForDummies*. Lanscope Special Edition. Hoboken: John Wiley & Sons. 48s. ISBN 978-1-118-33772-1

Oficiální dokument

Česko. Zákon č. 181/2015 ze dne 1. Ledna 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Česko. Zákon č. 101/2000 ze dne 4. Dubna 2000 o ochraně osobních údajů a o změně některých zákonů (zákon o ochraně osobních údajů).

Normy

IETF RFC 7011. 2013 [online]. *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information.* Dostupné z www: https://tools.ietf.org

IETF RFC 3176. 2001 [online]. *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks.* Dostupné z www: https://tools.ietf.org

Ústní a písemná sdělení

KOLOUCH, Jan. Seminář o informační bezpečnosti a služeb. Přednáška: Zákon o kybernetické bezpečnosti. *Cyklus zvaných přednášek.* Praha: CESNET v Praze 11. 2. 2015.