VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH MONITORINGU SÍŤOVÉ INFRASTRUKTURY PRO PORADENSKOU SPOLEČNOST

DESIGN OF NETWORK INFRASTRUCTURE MONITORING FOR A CONSULTING COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. Michal Flaxa

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Viktor Ondrák, Ph.D.

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Michal Flaxa**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2019/20

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Návrh monitoringu síťové infrastruktury pro poradenskou společnost

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Navrhnout management bezpečnosti.

Základní literární prameny:

ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky. Český normalizační institut, 2006.

ČSN ISO/IEC 27002:2005 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2005.

DOBDA L. Ochrana dat v informačních systémech. Praha: Grada Publishing, 1998. ISBN 80-71--9479-7.

DOUCEK P., L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

JORDÁN, V. a V. ONDRÁK. Infrastruktura komunikačních systémů III: integrovaná podniková infrastruktura. Brno: Akademické nakladatelství CERM, 2015. 136 s. ISBN 978-80-214-5241-1.

POŽÁR, J. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-8--7251-250-8.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2019/20

V Brně dne 29.2.2020

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Diplomová práce se zaměřuje na problematiku monitoringu dat v poradenské společnosti TG Community Holding a.s. Návrh spočívá ve vytvoření monitoringu sítě pro sledování provozu, především sledování velikosti objemu dat. Jednalo by se o sledování netypického dění na síti. Tato diplomová práce bude sloužit k implementaci navrženého řešení v holdingu.

Abstract

This master's thesis is focuses on problematic of monitoring data in consulting company TG Community Holding a.s. The design will consist of a create monitoring network for a traffic tracking primarily data volume size tracking. It would be a monitoring of atypical events on the network. This master's thesis will be used to implement the proposed solution in the holding.

Klíčová slova

monitoring, správa sítě, bezpečnost, ochrana proti úniku dat, sFLOW

Key words

monitoring, network management, security, data leak protection, sFLOW

Bibliografická citace

FLAXA, Michal. Návrh monitoringu síťové infrastruktury pro poradenskou společnost [online]. Brno, 2020 [cit. 2020-05-17]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/125652. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Viktor Ondrák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 17. května 2020

……..

podpis studenta

Poděkování

Můj obrovský vděk patří panu Ing. Viktorovi Ondrákovi, Ph.D. za vedení mojí diplomové práce, za jeho cenné a odborné rady i čas. V neposlední řadě patří moje poděkování rodině, přátelům a známým, kteří mě při psaní této práce podporovali.

OBSAH

ÚVOD

V dnešní době je velice snadný přístup k informacím. Lidé, firmy a různé útvary denně pracují s informacemi druhých, které jsou umístěny například v datových uložištích firem nebo cloudech. Data pohybující se na internetu, ale i vnitřních sítí jsou terčem mnoha útoků. Není proto divu, že státní celky i nadnárodní organizace se snaží řídit a zabezpečit nakládání s informacemi uživatelů normami či nařízeními.

V mé diplomové práci se budu podobným problémem zabývat. Firma, kterou jsem si vybral pro svoji práci a kde zároveň pracuji, podniká v oboru poradenství, denně zpracovává stovky dokumentů svých klientů a manipuluje s nimi více jak sto zaměstnanců. Dokumenty samozřejmě obsahují citlivé osobní informace. Pro zvýšení bezpečí pro klienty a předcházení problémům pro firmu, se pokusím zanalyzovat rizika s nimi spojená a zavést opatření, která by snížila míru rizik.

Vlastní návrh řešení, který vyberu po domluvě s vedením holdingu bude následně realizován ve firmě.

VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Cílem diplomové práce je zvýšení bezpečnosti v oblasti práce s daty, konkrétně návrh monitoringu síťové infrastruktury pro poradenskou společnost TG Community Holding a.s. Nyní na počítačové síti holdingu žádný monitoring není a je tedy žádoucí zavedení jakékoliv ochrany, snížení rizik úniku či ztráty důležitých dat. Vzhledem k cennosti a diskrétnosti dat by bylo vhodné monitorovat provoz na firemní privátní síti. Zavést jakékoliv možné opatření, které by snížilo riziko propuknutí hrozeb a analyzovat síťový provoz, aby například někdo nekopíroval větší množství dat, než je obvyklé nebo je nekopíroval do nepovoleného prostoru.

V první fázi diplomové práce se budu věnovat teoretickým východiskům, která budou potřeba pro následnou analýzu současného stavu a vlastní návrh řešení. Výstupem analýzy současného stavu bude analýza rizik, která bude sloužit jako vstup pro návrh vlastního řešení. Návrh bude zahrnovat výběr opatření proti rizikům, jejich implementaci a popis používání ve firmě.

1 TEORETICKÁ VÝCHODISKA PRÁCE

V této kapitole popíšu pojmy a technologie pro moji diplomovou práci. Teoretická východiska budou složit pro pochopení problematiky, kterou se budu v dalších kapitolách zabývat. Nejprve proberu základy počítačových sítí a poté rozeberu podrobněji problematiku informační bezpečnosti, managementu sítí, monitoringu, vzorkovacích technologií a ochranu proti úniku dat.

1.1 Počítačová síť

Jedná se o propojení více zařízení (např. počítačů), obecně označovaných jako "Hosts" propojených dohromady různými způsoby, které jim umožňují komunikovat, za účelem odesílání a přijímání dat nebo médií. Existují zařízení a média, která pomáhají při komunikaci mezi dvěma různými zařízeními. Jedná se o síťová zařízení jako je například Router, Switch, Hub, Bridge. Na počítačové síti se může vyskytovat nespočet počítačů a síťových zařízení. Příkladem počítačové sítě může být internet (7).

1.2 Dělení sítí

Počítačové sítě se mohou dělit různými způsoby. V následujících podkapitolách rozřadím sítě dle základních dělení tak, aby byly pochopeny jejich principy.

1.2.1 Podle rozsahu

Výchozí dělení počítačových sítí je podle rozsahu. Nejzákladnější dělení je na 4 rozsahy. Na LAN, PAN, MAN, WAN.

LAN *(Local Area Network)* – je skupina počítačů vzájemně propojených v malé oblasti, jako je kancelář, byt, patro, budova, firemní privátní síť. LAN se používá pro připojení dvou nebo více osobních počítačů v malém rozsahu prostřednictvím komunikačního média. Síť je levnější, protože je postavena na levném hardwaru, který nemusí obsluhovat obrovské toky dat. Data se v místní síti přenášejí rychleji než v sítích větších rozsahů. Lokální síť také poskytuje vyšší zabezpečení (7).

PAN (*Personal Area Network*) – je síť uspořádaná v rámci jedné osoby, obvykle v dosahu 10 metrů. Personal Area Network se používá pro připojení počítačových zařízení pro osobní použití. Zařízení, které se používají k rozvoji osobní sítě jsou notebooky, mobilní telefony, tablety, přehrávače médií a herní stanice (7).

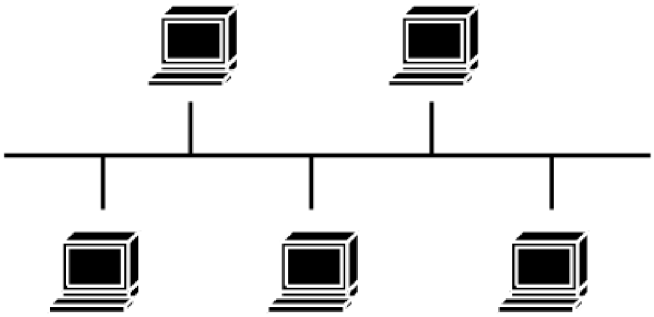
WAN *(Wide Area Network)* – je síť, která sahá přes velkou geografickou oblast, jako jsou státy nebo země. Široká oblast není omezena pouze na jedno místo. Může být propojena přes velkou geografickou oblast pomocí kabelu z optických vláken nebo satelitním spojením. Internet je jednou z největších WAN sítí na světě. WAN síť je široce používána v oblasti podnikání, státní správy a vzdělávání. Může jít o síť, kterou poskytuje provider (7).

MAN *(Metropolitan Area Network)* – je síť, která pokrývá větší geografickou oblast propojením více sítí LAN za účelem vytvoření větší sítě. Typicky firemní počítačová síť s více pobočkami. V MAN jsou různé LAN sítě vzájemně propojené prostřednictvím optických kabelů. Má vyšší dosah než LAN (7).

1.2.2 Podle topologie

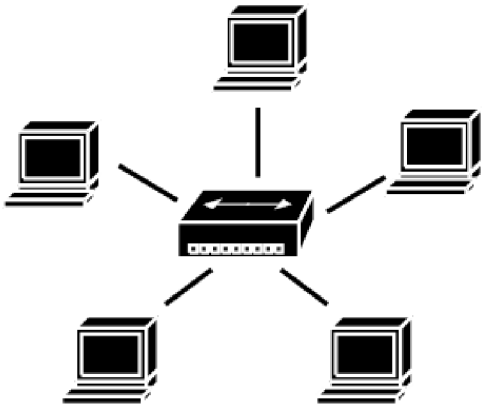
Dělení podle topologie je rozdělení podle toho, jak jsou uzly (počítače nebo síťové zařízení) v síti vzájemně propojeny. Topologii tvoří kabeláž, která určuje schéma zapojení. Níže budu popisovat fyzické topologie, nikoliv logické. Popíši základní topologie jako bus, star a ring (8).

Sběrnicová topologie *(Bus Topology)* – je typ topologie, ve které je každý počítač a síťové zařízení připojeno například T-konektorem k jednomu kabelu. Přenáší data z jednoho konce na druhý v jednom směru. V topologii sběrnice není žádná obousměrná funkce. Topologie sběrnice má sdílený páteřní kabelem. Náklady na kabeláž jsou ve srovnání s jinými topologiemi nižší. Pokud selže hlavní kabel, dojde k selhání celého systému. Pokud je síťový provoz hustý, zvyšují se kolize v síti. Abychom tomu zabránili, používají se v linkové vrstvě protokoly známé jako Pure Aloha, Slotted Aloha, CSMA/CD atd. Nicméně dnes se tato technologie téměř nepoužívá (8).



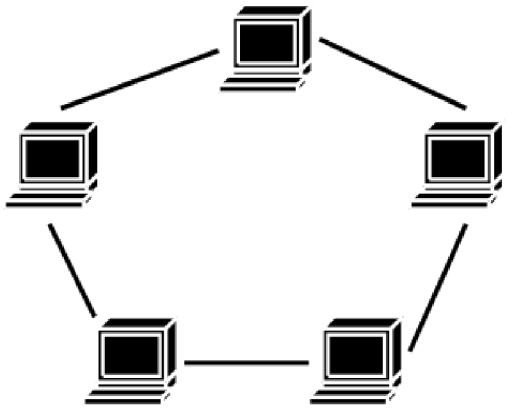
Obr. 1: Schéma topologie Sběrnice (10)

Hvězdicová topologie *(Star Topology)* – zde jsou všechna zařízení připojena kabelem k jedinému switchi. Tento switch je centrální uzel a všechna ostatní zařízení jsou k němu připojena. Jde o nejrozšířenější topologii. Každé zařízení vyžaduje pouze 1 port pro připojení ke switchi. Pokud switch, ke kterému je připojená celá topologie zkolabuje, celý systém se zhroutí. Náklady na instalaci jsou vyšší. Výkon je založen na jediném prvku, tj. switchi (8).



Obr. 2: Schéma topologie Hvězda (10)

Kruhová topologie *(Ring Topology)* – zde tvoří jednotlivé uzly, navzájem pospojované se svými sousedy, kruh. Možnost kolize je u tohoto typu topologie minimální. Levné instalace i rozšíření. Přidání nebo odebrání stanic může narušit celou topologii. Nevýhody jsou stejné jako u topologie sběrnicové. V případě poruchy je potřeba redundantní trasy. Používá se spíše pro specifické přístupové metody (např. IBM Token Ring). (8)



Obr. 3: Schéma topologie Kruh (10)

Další možnou topologií je **páteřní vedení** *(Backbone)*, kterou se propojují menší segmenty sítě. Po backbone je požadována vysoká přenosová rychlost.

1.3 Síťové architektury

Síťová architektura je standard počítačové sítě, který poskytuje technologický základ pro navrhování, budování a správu komunikační sítě. Má strukturu s různými vrstvami. Vrstvení je princip návrhu sítě, který rozděluje komunikační úkoly do několika menších částí. Každá část plní určitý dílčí úkol a spolupracuje s ostatními vrstvami. Používá se k zajištění komunikace mezi heterogenními zařízeními. K tomu slouží referenční model. Síťová architektura využívá dva referenční modely. První je ISO/OSI, který je hypotetický a TCP/IP, který je praktický (6).

Síťové architektury nikdo nevlastní. Každý může navrhovat hardware a software na základě síťové architektury. Síťová architektura TCP/IP, na které je založen internet, je otevřená a je přijímána jako celosvětový síťový standard. Používá se široce v LAN sítích, WAN sítích, ale také v malých a velkých podnicích (6).

1.3.1 Referenční model ISO/OSI

Model OSI byl vyvinut Mezinárodní organizací pro normalizaci (ISO) v roce 1984 a nyní je považován za architektonický model mezipočítačové komunikace. OSI je zkratka pro

Open System Interconnection referenční model, který popisuje, jak se informace ze softwarové aplikace v jednom počítači pohybují fyzickým médiem k softwarové aplikaci dalšího počítače. ISO/OSI se skládá ze sedmi vrstev a každá vrstva vykonává určitou síťovou funkci. Model ISO/OSI rozděluje celý úkol na sedm menších úkolů. Každá vrstva je samostatná, takže úkol přiřazený ke každé vrstvě může být prováděn nezávisle (5).

ISO/OSI model je rozdělen do dvou skupin – horní a spodní. Horní vrstva modelu se zabývá hlavně úkoly souvisejícími s aplikací a je implementována pouze v softwaru. Aplikační vrstva je nejblíže koncovému uživateli. Koncový uživatel i aplikační vrstva spolupracují se softwarovými aplikacemi. Spodní vrstva modelu ISO/OSI se zabývá problematikou přenosu dat. Fyzická vrstva je nejnižší vrstva modelu OSI a je nejblíže fyzickému médiu nebo je médiem samotným. Fyzická vrstva je zodpovědná za umístění informací na fyzické médium (5).

Na obrázku níže je vidět uspořádání vrstev v referenčním modelu ISO/OSI.

Obr. 4: Schéma referenčního modelu ISO/OSI (vlastní zpracování dle 7)

Fyzická vrstva pracuje s bity. Předává či přijímá bity z fyzického přenosového média (např. UTP, optické vlákno). Tato vrstva nerozumí významu bitů, ale zabývá se elektrickými charakteristikami signálů, modulováním signálu a metodám signalizace (5).

Linková vrstva je zodpovědná za přenos a integritu bitů při přenosu z uzlu na uzel. Přenesené bity z fyzické vrstvy jsou rozděleny do rámců. První a druhá vrstva jsou požadované pro každý typ komunikace (5).

Síťová vrstva stanovuje cestu mezi odesílatelem a přijímačem přes směrovače. Síťová vrstva pracuje s pakety. Routery jsou zařízeními třetí vrstvy. Jsou specifikované v této vrstvě a používají se k poskytování směrovacích služeb v rámci sítě. Používané protokoly pro směrování síťového provozu jsou známé jako protokoly síťové vrstvy. Příklady protokolů jsou IP a IPv6. Routery směrují (routing) na základě směrovací tabulky (5).

1.3.2 Architektura TCP/IP

Model ISO/OSI je pouze referenčním modelem. Byl navržen tak, aby popsal funkce komunikačního systému rozdělením na menší a jednodušší komponenty. Pokud ale mluvíme o modelu TCP/IP, ten byl navržen a vyvinut v 60. letech a je založen na standardních protokolech. TCP/IP je zkratka Transmission Control Protocol/Internet Protocol. Model TCP/IP je zkrácenou verzí modelu ISO/OSI. Na rozdíl od sedmi vrstev modelu OSI obsahuje vrstvy pouze čtyři (5). Vrstvy TCP/IP:

- vrstva síťového rozhraní,
- síťová vrstva,
- transportní vrstva,
- aplikační vrstva (5).

Tabulka 1: Přehled vrstev v síťových architekturách (16)

<table>
<tr><th>OSI</th><th>TCP/IP</th><th colspan="8">Aplikace a protokoly</th></tr>
<tr><td>7. aplikační
6. presentační
5. relační</td><td>Aplikační vrstva</td><td>telnet</td><td>FTP</td><td>TFTP</td><td>SMTP</td><td>RIP</td><td>DNS</td><td colspan="2">Ostatní</td></tr>
<tr><td>4. transportní</td><td>Transportní vrstva</td><td colspan="4">TCP</td><td colspan="4">UDP</td></tr>
<tr><td rowspan="2">3. síťová</td><td rowspan="2">Síťová vrstva</td><td colspan="4" rowspan="2">IP</td><td colspan="2">ICMP</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>ARP</td><td>RARP</td></tr>
<tr><td>2. linková
1. fyzická</td><td>Vrstva síťového rozhraní</td><td colspan="3">token ring</td><td colspan="3">ethernet</td><td colspan="3">jiné typy protokolů</td></tr>
</table>

Z tabulky vyplývají vrstvy modelu ISO/OSI, zastupující vrstvy architektury TCP/IP a protokoly, které jsou v nich zastoupené.

Architektura TCP/IP pomáhá navázat a nastavit spojení mezi různými typy počítačů. Funguje nezávisle na operačním systému. Podporuje mnoho směrovacích protokolů. Architektura TCP/IP má hierarchickou architekturu klient-server (5).

Vrstva síťového rozhraní odpovídá kombinaci vrstvy linkové a fyzické vrstvy modelu OSI. Protokoly přítomné v této vrstvě umožňují fyzický přenos dat (5).

Síťová vrstva zastupuje stejné postavení a funkci jako v referenčním modelu ISO/OSI. Definuje protokoly, které jsou zodpovědné za logický přenos dat v celé síti (5). Hlavní protokoly, které se nacházejí v této vrstvě, jsou:

- IP – je zkratka pro internetový protokol a je zodpovědný za doručování paketů od zdrojového hostitele k cílovému hostiteli tím, že adresuje na IP adresy v záhlaví paketů. IP má 2 verze:
    - IPv4 a IPv6. IPv4 je v současné době používán. IPv6 se však začíná pomalu používat, protože počet adres IPv4 klesá a je ve srovnání s počtem uživatelů omezenější.
- ICMP – zkratka pro Internet Control Message Protocol. Je zapouzdřen v IP datagramech a poskytuje informace o problémech v síti.
- ARP – zkratka pro Address Resolution Protocol. Jeho úkolem je najít hardwarovou adresu hostitele ze známé IP adresy. ARP má několik typů: Reverzní ARP, Proxy ARP a Inverzní ARP (5).

Transportní vrstva je taktéž stejná s transportní vrstvou modelu ISO/OSI. Je odpovědná za komunikaci mezi koncovými body a bezchybné doručování dat. Chrání aplikace horní vrstvy před složitostí dat (5). Dva hlavní protokoly přítomné v této vrstvě jsou:

- Protokol řízení přenosu TCP – poskytuje spolehlivou a bezchybnou komunikaci mezi koncovými systémy.
- Protokol UDP (User Datagram Protocol) – využívá nespolehlivý přenos. Vhodný pro přenos videa, audia. Je nákladově velmi efektivní (5).

Aplikační vrstva vykonává funkce vrstev aplikační, prezentační a relační z ISO/OSI modelu. Je zodpovědná za komunikaci mezi uzly a řídí specifikace uživatelského rozhraní. Některé z protokolů přítomných v této vrstvě jsou: HTTP, HTTPS, FTP, TFTP,

Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD (5). Základní protokoly:

- HTTP a HTTPS - HTTP znamená protokol přenosu Hypertextu. Používá ho World Wide Web (WWW) ke správě komunikace mezi webovými prohlížeči a servery. HTTPS je zkratka HTTP-Secure. Jedná se o kombinaci HTTP s SSL (Secure Socket Layer). Je účinný v případech, kdy prohlížeč potřebuje vyplnit formuláře, přihlásit se, ověřit a provést bankovní transakce.
- SSH - SSH znamená Secure Shell. Jedná se o software emulace terminálu, podobný Telnetu. Důvod, proč je SSH výhodnější, je kvůli jeho schopnosti udržovat šifrované připojení. Nastaví zabezpečenou relaci prostřednictvím připojení TCP/IP. SSH se dále věnuji v jedné z následujících kapitol.
- NTP - NTP znamená Network Time Protocol. Používá se k synchronizaci hodin v počítači s jedním standardním zdrojem času. Je užitečný v situacích, jako jsou bankovní transakce (5).

1.4 Aktivní prvky

Aktivní prvky tvoří část počítačové sítě, které určitým způsobem aktivně pracují se signály v síti (zesilují je, upravují, hodnotí atd.). Aktivní prvky jsou obvykle specifická zařízení umístěna v uzlech sítě a nejsou koncovými zařízeními (8).

1.4.1 Switch

Switch je termín pro zařízení v počítačové síti, které spojuje jednotlivá zařízení v síti (segmenty sítě). Přepínač je jedním z aktivních prvků sítě. Z technického hlediska switch kontroluje adresy odesílatele a příjemce obsažené v přenášeném datovém paketu a na základě toho směruje pakety pouze do portu toho zařízení, kterému je určen. Přepínač nahradil dříve používané rozbočovače, které pouze kopírovaly signál. Switche se nejčastěji používají v topologii LAN a používají protokol Ethernet (8).

Switch pracuje na druhé linkové vrstvě OSI modelu, která přenáší rámce. Rámec obsahuje mimo jiné zdrojovou a cílovou MAC adresu. Pokud je MAC adresa rámce nová, přepínač si jí uloží do tabulky MAC adres (7).

1.4.2 Aruba OS

Vzhledem k tomu, že v diplomové práci budu pracovat se switchi HP Aruba proberu nyní jeho firmware Aruba OS. Aruba nabízí dvě prostředí pro správu svých switchů. První je grafické prostředí, které běží v prostředí webového prohlížeče po připojení na switch přes IP adresu. Druhou možností správy switchů je přes CLI tedy Command-Line Interface. Příkazy, které jsou používány jsou podobné těm od Cisco. Veškeré potřebné příkazy jsou k dispozici v on-line dokumentaci HP (24).

1.4.3 Router

Router je zařízení používané k vytváření a správě místní sítě ve firemních nebo domácích sítích. Zprostředkovává připojení k internetu nebo k jiným částem sítě. Router pracuje na třetí vrstvě ISO/OSI modelu. Činnost, o kterou se stará, je routing – směrování. Směrovač ukládá informace o sítích, ke kterým se připojil, a z nich vybírá nejvhodnější cestu pro posílaní paketů. Router je na samém okraji LAN sítě, kde slouží jako připojení sítě k internetu (8).

Routery využívají směrovacích protokolů, které jim umožňují získávat informace o sítích mimo jejich oblast působení, přičemž nejvyužívanější je protokol IP. (7)

1.5 Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací je systém, který chrání informační aktiva před riziky. Rizika jsou řízena, zaváděna na ně opatření a ty jsou kontrolovány. Systém se označuje zkratkou ISMS z anglického Information Security Management System. ISMS podléhá řadě mezinárodních norem ISO/IEC 27000. Jde o systém standardů, pravidel, doporučení, postupů a kontrol pro zabezpečení vybraných aktiv společností. Pokud se takové řešení v organizaci zavede, vzniká tím nikdy nekončící proces hledání rizik, zajišťování opatření vypuknutí rizik a kontrol. Zavést jej mohou organizace jakékoliv velikosti nebo oboru, pro které jsou informace podstatou podnikání (2).

1.5.1 Základní pojmy ISMS

ISMS obsahuje mnoho specifických pojmů. Tyto pojmy budu využívat i v této práci, a proto zde vypíšu základní pojmy, které pomohou pochopit význam práce.

Aktivum je buď hmotná nebo nehmotná věc, která má pro organizaci nějakou cenu. Hmotným aktivem může být hardware organizace. Nehmotná aktiva jsou většinou informace o klientech, know-how organizace, software nebo informační systémy. Informace, které jsou součástí nějakého informačního systému pak nazýváme jako Informační aktiva (2).

Zranitelnost je slabá stránka aktiva. Je třeba znát zranitelná místa aktiva pro jejich dostatečné opatření proti hrozbám (2).

Hrozba je stav, kdy negativní vlivy působící na zranitelnosti aktiv ohrožují jejich bezpečnost. Působení hrozeb může přicházet z vnějšku organizace nebo vnitřku, kde se jedná o nejčastější výskyt hrozeb a nebo ze samotného aktiva. Dále se hrozby dělí na lidské, které mohou i nemusí být úmyslné, technologické, technické, kdy se typicky jedná o poruchy HW, fyzické a přírodní (2). Přírodní mají velmi malou pravděpodobnost v propuknutí hrozby.

Riziko je hodnota, která udává míru, s jakou může propuknout hrozba. Ta následně způsobí bezpečnostní incident. Skládá se ze zranitelnosti a hrozby (2).

Bezpečnostní událost nastane v okamžiku, kdy hrozba propukne. Jedná se o momentální ohrožení aktiva, které nemusí nutně znamenat, že je aktivum poškozeno (2).

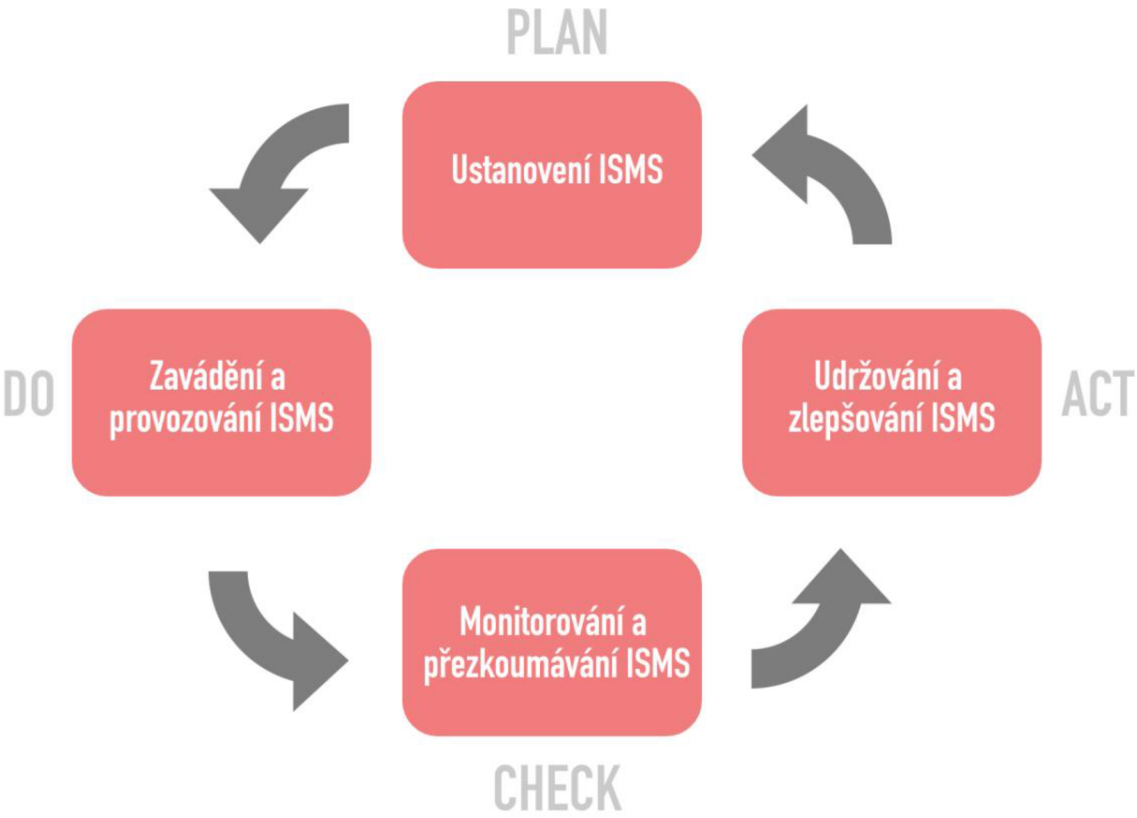
Bezpečnostní incident popisuje stav již porušeného aktiva po působení bezpečnostní události. V momentě, kdy mluvíme o bezpečnostním incidentu má aktivum změněné vlastnosti (2).

Dopad je důsledek bezpečnostního incidentu. Dopad se obvykle převádí na finanční hodnotu. Pak lze říci, jak velké poškození na aktivu způsobil. Újmy mohou být různých druhů a pro každou organizaci jsou negativní (2).

1.5.2 PDCA cyklus

PDCA neboli Demingův cyklus je metoda pro postupné zlepšování jakosti výrobků. Je přenositelná i na jiná odvětví, než jen na výrobu a lze ji využít i u ISMS. Vzhledem k tomu, že je ISMS nekončící proces, který se opakuje v cyklech, je model PDCA vhodnou metodikou pro vylepšování opatření hrozeb. PDCA je v původním znění zkratka z anglických slov Plan – plánuj, Do – vykonej, Check – kontroluj a Act – jednej (2).

V rámci norem ISO/IEC 27000 je cyklus formulován dle potřeby ISMS, a to jako ustanovení ISMS, zavedení a provoz ISMS, monitorování a přezkoumání ISMS, udržování a zlepšení kvality ISMS. „Plan“ v logice ISMS upřesňuje rozsah působení a uvádí, koho se týká. Nastavuje politiku ISMS, cíle, procesy, postupy a v neposlední řadě specifikace kompletního zadání. „Do“ aplikuje nastavení, které bylo v předchozím kroku stanoveno. „Check“ zajišťuje zpětnou vazbu na jejíž základě můžeme hodnotit úspěšnost, či neúspěšnost. „Act“ slouží pro implementování změn, vylepšení (2).



Obr. 5: PDCA cyklus dle ISMS (vlastní zpracování dle 2)

1.5.3 Analýza aktiv

Analýza aktiv se skládá z identifikace aktiv a následného hodnocení aktiv. Každá organizace bude mít seznam aktiv jiný dle jejich podnikatelského záměru. Je ovšem vhodné aktiva seskupit. Pro následující hodnocení je požadováno stanovit vlastníka aktiva a učinit ho plně zodpovědným za dané aktivum. Dle ISMS jsou většinou nejdůležitějším primárním aktivem informace. K identifikování přesných aktiv může pomoci dekompozice informačního systému (4).

Postup pro hodnocení aktiv si může organizace přizpůsobit podle vlastních metrik. Takových, které jim nejlépe ukáží, jaký dopad na organizaci by mělo ohrožené aktivum. K hodnocení využíváme klasifikační tabulky, kde si stanovíme základní stupnici a podle ní hodnotíme dopady na organizaci, při ohrožení daného aktiva. Tato tabulka by se měla sestavovat s vlastníky jednotlivých aktiv. Dále by se měly hodnotit dopady na jednotlivé bezpečnostní atributy. Těmi jsou dostupnost, důvěrnost a integrita. Přičemž se jako hodnotící kritérium využívá součet těchto atributů děleno třemi. Vzniklé číslo nám ukazuje míru dopadu (4).

1.5.4 Analýza rizik

Riziko popisuje stav, kdy existuje reálná pravděpodobnost vzniku škody. S hotovou analýzou hrozeb můžeme říci jaké rizika mohou působit na daná aktiva. V ISMS existuje seznam obecných rizik. Z tohoto seznamu lze vycházet a doplnit ho o vlastní rizika (4).

Analýza rizik s následujícími opatřeními je nejdůležitější částí Systému řízení bezpečnosti informací. Lze ji rozdělit do několika kroků. V první fázi se identifikují aktiva, dále se stanoví rizika, přijmou se nebo vyloučí a na závěr přijmeme opatření. Opět je hodnotíme tabulkami a k hodnocení můžeme využívat dvě klasifikační schémata, a to buď kvalitativní nebo kvantitativní. Kvalitativní analýza stanovuje pravděpodobnost, s jakou hrozba způsobí bezpečnostní incident. K hodnocení využívá klasifikační stupnici. Kvantitativní analýza je podrobnější a stanovuje pravděpodobnosti jednotlivých scénářů. Počítá s pravděpodobností výskytu hrozby, vyvolání bezpečnostní události a vyvolání incidentu. Tyto atributy analýzy se pak násobí mezi sebou a stanovují výslednou hodnotu rizika (4).

Míra rizika pak určuje i scénáře, které nastanou v případě jeho vypuknutí. Rizika s nízkým dopadem nemusí mít ani opatření, pokud nepředstavují velkou překážku pro aktivum. S rostoucí mírou dopadu se můžeme dostat až k takovému riziku, kdy je nutné okamžité řešení. V takovém případě aplikujeme opatření (4).

1.5.5 Řízení rizik

Abychom snížili možnosti propuknutí rizik či možné dopady, využíváme řízení rizik (risk management). Jedná se o nekončící proces pro zvýšení bezpečnosti informací. Dohlíží na to, aby veškeré činnosti spojené s řízením rizik byly vykonávány a řízeny. Proces řízení rizik je ucelený a lze ho definovat algoritmem (4).

Základním schématem pro řízení rizik jsou 4 po sobě jdoucí kroky. V první řadě se stanovují obecné věci, vybírají se metodiky a způsoby hodnocení. Druhým bodem je samotná analýza rizik. Dále se rizika vyhodnocují a určují se náležitá opatření. V neposlední řadě se rizikům určuje, jakým způsobem se budou opatřovat. Na závěr procesu se ptáme, zda riziko přijmeme. Pokud ne, tak se celý proces opakuje znovu. Zároveň je proces po celou jeho dobu trvání komunikován, monitorován a přezkoumáván (4).

1.6 Normy ISO/IEC 27000

Normy ISO/EIC 27000 je řada norem nazývána jako Systém řízení bezpečnosti informací neboli ISMS. Řada norem popisuje náplň výkonu řízení bezpečnosti. Zároveň sjednocuje světové používání do standardu. Dále rozeberu normy, které jsou potřeba k pochopení této práce, jinak je norem více a popisují například i postupy auditů, vyšetřování problémů a jiné (11).

ISO/IEC 27000 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

Je první normou z této série, která obecně poskytuje popis ISMS. Popisuje pojmy, termíny, definice jednotlivých norem a definují požadavky na ISMS (11).

ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

Specifikace požadavků na ustavení, zavedení, udržování a zlepšování ISMS. Norma vyžaduje splnění všech požadavků pro úplné splnění předpisů bez ohledu na velikost organizace. Dále jsou definovány požadavky na hodnocení a ošetření rizik (12).

ISO/IEC 27002 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Soubor postupů

Norma poskytuje standardy pro postupy v ISMS a dá se použít jako kontrolní seznam zavedených požadavků. Doporučuje postupy pro výběr, implementaci a řízení opatření. Norma nenařizuje, která opatření musí být aplikována, ale nechává rozhodnutí na organizaci. Skládá se z 14 hlavních kapitol a definuje 35 cílů opatření, které slouží jako kontrolní. Opatření jsou pro ochranu informačních aktiv proti porušení integrity, dostupnosti nebo důvěrnosti (13).

ISO/IEC 27004 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Měření

Tato norma je pomocným nástrojem k měření efektivity řídících nástrojů ISMS organizace z norem ISO/IEC 27001 a ISO/IEC 27002 (13).

ISO/IEC 27005 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Řízení rizik bezpečnosti informací

Norma je návodem pro zavedení řízení rizik. Vymezuje základní kritéria, definuje rozsah a stanovuje organizační strukturu pro řízení rizik. Popisuje celý proces od hodnocení, redukce, akceptace a následné monitorování rizik. To vše, aby byly plněny požadavky normy ISO/IEC 27001 (13).

1.7 Management sítí

Pro správu sítí existuje norma dle ISO. Její název je Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4: Management Framework pod označením ISO/IEC 7498-4 (14). Norma ukládá základní funkce

managementu sítí. Mezi tyto funkce patří správa výkonu, správa konfigurace, účet a evidenční správa, správa poruch a správa bezpečnosti (15). Jednodušeji řečeno jde o kontrolu, plánování, rozvržení, rozmístění, koordinaci a monitorování sítě.

Správa výkonu slouží pro měření výkonnosti aktivních prvků a koncových uzlů. Existují dva způsoby provádění správy výkonu. Management reaktivní a proaktivní. Reaktivní management řeší problémy až nastanou nebo přesáhnou předem nastavenou hranici únosnosti. Proaktivní management se snaží problémům předcházet. Využívá simulačních metod při plánování změn v síti. Snaží se předpokládat co se stane, když nastane určitá situace (15).

Správa konfigurace zjišťuje konfiguraci prvků sítě. Zaměřuje se i na provádění změn konfigurací daných aktivních prvků jako jsou třeba switche, dále na koncových zařízeních atp. Na koncových uzlech může nastavovat aplikace, operační systém, doménové nastavení aj. U aktivních prvků nastavuje parametry chování (15).

Účetní a evidenční správa slouží pro monitorování využívání sítě uživateli, aplikacemi nebo procesy. Tato správa hlídá provoz, na jehož základě může optimalizovat, regulovat nebo zpoplatňovat využívané zdroje na síti. Sleduje uživatele a jejich chování, z čehož vede statistiky a záznamy (15).

Správa poruch detekuje chyby a poruchy na síti. Jde o nejpoužívanější oblast z důvodu včasných následných oprav pro co nejplynulejší běh sítě. Skládá se z detekce chyb, odstraňování chyb s následnou evidencí a vyhodnocením (15).

Správa bezpečnosti řídí přístupy uživatelů na síti k čemuž využívá access control list. Tím ověřuje přístupy uživatelů. Vede statistiky o neoprávněném chování uživatelů, pokud takové je (15).

Management sítě využívá ve většině případu architekturu síťové správy Manager – Agent. Manager je kolektorovým prvkem, který prostřednictvím svých agentů sbírá údaje, statistiky nebo další data z aktivních prvků a koncových zařízení. První způsob komunikace mezi managerem a agentem je tzv. pooling aktivity, kdy manager vyšle požadavek a agent mu odpoví. V druhém případě odesílá agent údaje bez vyžádání managera. Tato funkcionalita se jmenuje Trap (15).

1.8 Protokol SSH

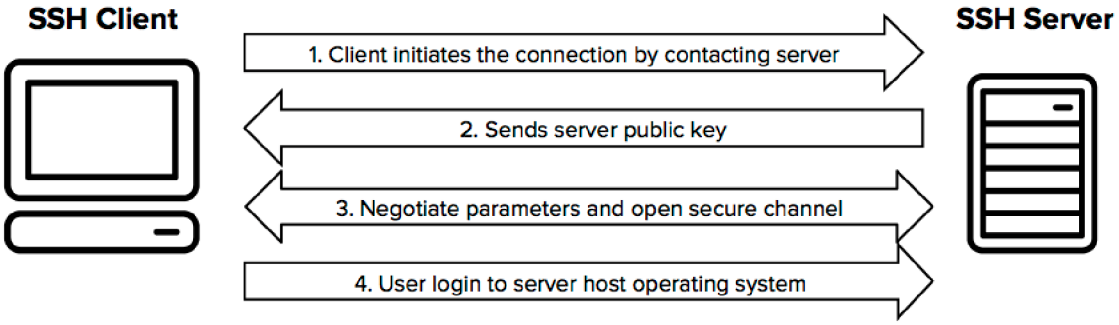
Protokol SSH je metoda pro bezpečné vzdálené přihlášení z jednoho počítače na druhý. Poskytuje několik alternativních možností pro bezpečnou autentizaci a chrání komunikaci se silným šifrováním. Je to bezpečná alternativa k nechráněným přihlašovacím protokolům jako je telnet, rlogin a nezabezpečeným metodám přenosu souborů jako je například FTP (23).

Protokol se používá v podnikových sítích pro:

- zajištění bezpečného přístupu pro uživatele,
- interaktivní a automatizované přenosy souborů,
- zadávání vzdálených příkazů (23),
- správa síťové infrastruktury a dalších systémových komponent.

Protokol pracuje v modelu klient – server, což znamená, že připojení je navázáno SSH klientem připojujícím se k serveru. SSH klient řídí proces nastavení připojení a používá k ověření identity serveru SSH kryptografii veřejného klíče. SSH protokol používá pro nastavení silné šifrovací a hashovací algoritmy, aby zajistil soukromí, bezpečnost a správnost integrity dat, která jsou vyměňována mezi klientem a serverem (23).

Obrázek níže popisuje proces nastavení zabezpečeného spojení SSH klient – server.



Obr. 6: Proces propojení SSH klient – server (23)

Ověření uživatele probíhá několika možnostmi. Nejběžnější je ověření heslem nebo autentizace pomocí veřejného klíče (23).

Metoda ověřování pomocí veřejného klíče je primárně používána pro automatizaci a správci systémů a sítí je používají pro jednotné přihlášení. Záměrem je mít kryptografický

klíčový pár – veřejný klíč a privátní klíč. Veřejný klíč se musí na serveru nakonfigurovat tak, aby autorizoval přístup a udělil ho každému, kdo má kopii soukromého klíče na server. Klíče používané pro ověření se nazývají SSH keys (23).

Po navázání spojení mezi SSH klientem a serverem jsou přenášená data šifrovaná podle předem stanovených parametrů. Během počáteční komunikace se klient a server dohodnou na použitém šifrovacím algoritmu a vygenerují šifrovací klíč, který bude používán po dobu komunikace. Provoz mezi komunikujícími stranami je chráněn standardními šifrovacími algoritmy jako je AES (Advanced Encryption Standard). Protokol SSH zahrnuje mechanismus, který zajišťuje integritu přenášených dat pomocí standardních algoritmů hash SHA-2 (Standard Hashing Algorithm) (23).

1.9 Vzorkovací technologie

Vzorkovací technologie je velmi rozšířený nástroj ve sledování provozu sítí. Tyto technologie sledují a analyzují pakety. Následně dokáží vyhodnotit, zda se jedná o typické, či netypické chování. Tato technologie neposkytuje 100% přesný výsledek, ale přesnost se dá kvantifikovat (16).

Vzorkovací technologie jsou aplikovány ve formě protokolů. Říká se jim Flow protocols. Mezi nejpoužívanější flow protokoly patří NetFlow a sFlow. Leč dělají tyto protokoly to samé, každý má odlišnou charakteristiku (16).

1.9.1 NetFlow

NetFlow vynalezla firma Cisco a používá ho ve svých zařízeních. Spuštěný protokol aktivuje na zařízeních export IP flow dat do kolektoru, kde je může administrátor analyzovat. Skládá se ze dvou komponent. První je NetFlow Cache, která shromažďuje informace o IP flow. Druhá část je mechanizmus NetFlow Export Mechanism, který odesílá dočasně uložená data do kolektoru (16).

Když přijde nový paket do switche, zařízení na základě nastavených atributů rozhodne, zda má odeslat datagram. Pokud se switch rozhodne směrovat datagram, vloží ho do mezipaměti. Mezipaměť NetFlow obsahuje následující informace:

- Cílová IP adresy
- Zdrojová IP adresa
- Cílové číslo portu
- Číslo zdrojového portu
- Zdrojové rozhraní
- Typ protokolu 3. vrstvy
- Byte ToS (16)
- Vstupní logické rozhraní (ifIndex)

V mezipaměti se pakety shromažďují a pokud splňují určitá kritéria, jsou odesílány dál do kolektoru NetFlow (16).

1.9.2 sFlow

S flow protokolem sFlow přišla firma HP v roce 1991. HP umožnilo používání sFlow všem bez ohledu na výrobce aktivních prvků. V procesu sledování provozu využívá náhody, aby zabránil v synchronizaci s periodicky se opakujícími vzory. To znamená, že každý N-tý paket zachytí a zanalyzuje. Získané data následně odešle do sFlow kolektoru jako sFlow datagramy. Taktéž jako NetFlow má dvě komponenty. sFlow Agent sbírá pakety na switchi nebo routeru a následně je odesílá do sFlow Kolektoru (16).

Klíčovou vlastností sFlow protokolu je náhodné vzorkování paketů, které umožňuje vypozorovat trend chování síťového provozu. Switche sbírají náhodné vzorky paketů a jako datagramy se odesílají do kolektoru (16).

Při nastavování sFlow na switchi se musí nakonfigurovat interval dotazování a vzorkovací frekvence. Interval dotazování počítá, kolik paketů prochází switchem. Vzorkovací frekvence se používá k určení procenta vzorkovaných paketů. Například, je-li rychlost připojení 10Mb/s a nastavila by se vzorkovací frekvence 1 z 200, sFlow by shromažďovalo 1 paket z každých 200, které prošly (16).

1.10 Data Leak Prevention

Data leak prevention (DLP) v češtině Prevence proti úniku dat je funkcionalita firewallu FortiGate, která zabraňuje úniku citlivých dat z privátní sítě. Funguje na principu definování vzorů pro citlivá data. Pokud DLP zachytí tento vzor, zablokuje nebo zaznamená průchod firewallem. Konfigurace vzorů probíhá nastavením filtrů na základě typu souboru, velikosti, výrazů nebo pravidel. DLP může sledovat nejen provoz ze sítě ven, ale i vstup do sítě zvenčí a to způsobem, kdy zachytí daný soubor a archivuje jej (17).

2 ANALÝZA SOUČASNÉHO STAVU

V této kapitole se budu zabývat představením firmy TG Community Holding a.s. (dále „TGC“), které v této diplomové práci vytvořím návrh monitoringu síťové infrastruktury. V následující části rozeberu současný stav této problematiky. Dále zanalyzuji důležité milníky pro návrh jako je proces práce zaměstnanců s daty, analýza ICT, rozeberu informační aktivum, provedu analýzu hrozeb a rizik. Nakonec shrnu celou analýzu současného stavu a vytvořím výstup pro návrh vlastního řešení.

2.1 Představení společnosti

Přestože mateřská společnost TG Community Holding a.s. byla založena v roce 2015, počátky činnosti sahají do roku 2011, kdy společnost začala nabízet služby v podobě energetických aukcí pro domácnosti a firmy pod názvem Terra Group, což bylo umožněno tzv. liberalizací trhu, kdy bylo všem odběratelům elektřiny či plynu umožněno svobodně změnit dodavatele komodit. Zejména díky změnám dvou energetických směrnic Evropské unie (19).

Dnes je holding TGC považován za jeden z největších správců služeb domácnosti v České republice. V současné době má více jak 100 000 klientů v podobě domácností a další tisíce firem. Holding TGC má 15 dceřiných firem a plánují se další rozšíření (20).

Obr. 7: Organizační struktura TGC (20)

2.1.1 Základní údaje

- Datum vzniku a zápisu: 19. listopadu 2015
- Obchodní firma: TG Community Holding, a.s.
- Sídlo: Karolíny Světlé 716/1, Líšeň, 628 00 Brno
- Identifikační číslo: 04576446
- Základní kapitál: 2 000 000,- Kč (18)
- Odhadovaný počet zaměstnanců: 150 + zhruba 250 externích (21)
- Roční obrat: 200 000 000 Kč (21) (ke 31.12.2018)

Obr. 8: Logo TG Community Holding a.s. (20)

2.1.2 Historie společnosti

Společnost byla založena již na konci roku 2011. Firma začala s poskytováním svých služeb klientům až na začátku následujícího roku, do té doby firma přijímala zaměstnance, kteří by obstarávali potřebnou administrativu. Paralelně se založila i dceřiná firma Zeus Solutions s.r.o. určená k poskytování IT služeb a vývoji vlastního CRM systému (22). Firma Zeus Solutions s.r.o. je správcem počítačové sítě holdingu a bude i realizátorem návrhu. Během následujících pár let společnost získala velkou přízeň u klientů, což vedlo k zapojování obcí, městských částí, firem a institucí. V květnu roku 2014 firma spustila svůj vlastní aukční portál, který využívá dodnes (22). V následujících dvou letech firma procházela a stále prochází rapidním růstem. Prvním krokem bylo zakoupení vlastního sídla v brněnské Líšni. To umožnilo nadále nabírat nové zaměstnance. V roce 2017 firma expandovala natolik, že musela pronajmout další nemovitost a udělat z ní hlavní pobočku pro své klienty (19).

2.1.3 Záměr holdingu

Po otevření trhu energetiky odběratelům se zavedly tzv. energetické aukce. Principem těchto aukcí je seskupování potencionálních odběratelů do větších skupin a jejich

zařazení do aukce. Dodavatelé si pak navzájem „podhazují“ cenové nabídky za elektřinu a plyn v závislosti podle toho, jak velký je počet odběratelů v daném kole aukce. Tímto způsobem účastníci mohou získat výrazně lepší ceny, než jsou aktuálně nabízeny na trhu. Tyto aukce jsou přístupné všem dodavatelům jak renomovaným, tak i těm méně známým. Společnost dává svým klientům na základě dohody o zastupování možnost zúčastnit se v těchto aukcích. Klienti se pak ve výsledku nemusí o nic starat a vše za ně zařídí společnost TGC (21).

Společnost během doby svého působení na trhu vyvinula celou řadu dalších služeb. Byla k tomu z části nucena i z důvodu neustálého zdražování energií. V poslední době především elektřiny. Energetické aukce dnes přestávají být natolik výhodné jako dříve. Společnost je dnes i dodavatelem energií (elektřiny a plynu), má firmu na správu pojištění, revize komínů, prodává doplňkové produkty k šetření vody a provozuje programy na šetření energií pro různá uskupení, jako jsou například města a obce (21).

Aktuálním záměrem společnosti je zejména spojení všech svých služeb do jednoho balíčku tzv. Komplexní domácnosti, který by klientům usnadňoval přehled a nabízel levnější řešení v oblasti energií, pojištění a správě domácnosti s důrazem na ekologii. V současné době je vyvíjen i klientský portál s mobilní aplikací, který by takové spojení umožňoval (21).

2.2 Současný stav

Budovy

TG Community Holding a.s. dnes používá k výkonu své činnosti dvě budovy v Brně. Budovu v Líšni a dvě patra v kancelářské budově na ulici Vídeňská. V Líšní sídlí vedení holdingu, účetní a IT oddělení. Serverovna zde není, je zde pouze místnost, kde je pár switchů. V kancelářské budově na Vídeňské je zbytek holdingu, část oddělení IT a především celý backoffice, který zpracovává dokumenty klientů. Dále se v suterénu budovy nachází serverovna.

Serverovna

Serverovna je osazena 3 servery, na kterých běží dalších x serverů virtuálních. Zprostředkovatel připojení k internetu optickým kabelem je společnost T-Mobile. S touto

společností holding spolupracuje více. Serverovna nemá vlastní diskové pole pro ukládání dat, ale využívá cloudové služby právě od T-Mobilu. Přístup na toto uložiště je možný pouze z firemní sítě. Dále od nich využívá například FortiGate. Jako switche se používají HPE Aruba 2530, 2540 a distribuční switche HPE 2930M, do kterých jsou zapojené předešlé switche a řízené RSTP.

Monitoring

Zatím se nepoužívá žádný způsob monitoringu sítě. Je zde však nutkavá potřeba pro alespoň částečný monitoring firemní sítě.

2.3 Proces práce zaměstnanců s daty

V tomto ohledu je třeba analyzovat hlavně oddělení backoffice a jeho zaměstnance. Ti pracují s daty klientů nejvíce a jsou tak největším rizikem v procesu zpracování dat. Každý zaměstnanec backoffice pracuje s interním CRM informačním systémem v němž přistupují k dokumentům.

Dokumenty se do CRM systému dostanou prostřednictvím obchodních zástupců, kteří využívají nástroj E-přihláška, kterou si firma taktéž sama vytvořila. Obchodní zástupce s tabletem na kterém běží aplikace E-přihláška, získá osobní informace s potřebnými dokumenty a souhlasem v podobě elektronického podpisu od klienta. V dalším případě může klient vyplnit E-přihlášku sám na webu. V obou případech se dostanou veškeré informace od klienta do CRM systému, kde je zpracovává zaměstnanec backoffice.

Zaměstnanec backoffice pak zpracovává informace, chystá návrhy smluv a vše spojené s předmětem podnikání holdingu TGC. Informace a dokumenty stahuje, upravuje, nahrává na firemní síťové uložiště. Z této práce lze vypozorovat typické a netypické chování zaměstnance. Nyní zaměstnanec může soubory odeslat kamkoliv chce, leč je vázán smlouvou proti tomuto jednání.

2.4 Analýza ICT

Veškerý hardware používaný v holdingu spadá do vlastnictví dceřiné firmy Zeus Solutions s.r.o. Ta poskytuje veškerou správu tohoto HW, zároveň provozuje počítačovou

síť, ale i vyvíjí a udržuje softwarové prostředky pro chod holdingu. IT DevOps oddělení, které se stará o počítačovou síť sídlí právě v budově na ulici Vídeňská, kde je i serverovna. Ve společnosti jsou definovaná vnitřní pravidla pro používání počítačové sítě, připojování se do sítě přes VPN, vytváření služeb na serveru, chování se na doménových počítačích a další různá pravidla, která jsou definována v groupware používaném firmou. K interní síti se dá připojit kabelem, přes Wi-Fi nebo vzdáleně pomocí VPN. Dále rozeberu jednotlivé skupiny ICT, které jsou používány v holdingu TGC.

2.4.1 Osobní počítače

Ve společnosti je používáno více jak 100 počítačů. Část z nich jsou stolní počítače pro kancelářskou práci a druhá část jsou přenosné počítače různých typů od těch základních po prestižní modely. Převládají počítače značky HP. Nejvíce je využíván operační systém Windows 10, v menší míře OS na bázi Linuxu a výjimečně počítače s MacOS. Veškerý SW, který je instalován většině zaměstnancům je buď freeware nebo s open source licencí. Pro připojování počítačů k firemní síti z venčí přes SSL-VPN se používá FortiClient v základní verzi.

Další zařízení, která by se dnes dala počítat do kategorie osobních počítačů jsou tablety. Používají je převážně obchodní zástupci k výkonu své pracovní náplně a je na nich nasazena E-přihláška. Všechny tablety jsou značky Lenovo využívající operační systém Android.

2.4.2 Server

V serverovně se nacházejí 3 fyzické servery. Všechny běží se systémem na bázi Linuxu – Centos. Na fyzických serverech jsou spuštěny další virtuální servery. Servery jsou využívány především pro IT vývojové oddělení. Jsou na nich testovací a demo prostředí pro vývoj.

Veškeré služby, které holding TGC potřebuje ke svému fungování jako provoz CRM systému BM, hostování webových stránek, provoz klientského portálu, databáze webů, aplikací atp. běží na cloudovém řešení serveru v prostředí IaaS (infrastructure as a service) od T-Mobilu. Na serverech běží OS Windows Server 2012 R2. Je zde využívána

adresářová služba Active Directory a to rovnou na dvou různých virtuálních serverech nezávislých na sobě, kvůli redundanci. Dále jsou na serverech služby typu DNS, DHCP, a NSP.

2.4.3 Datové toky ve společnosti

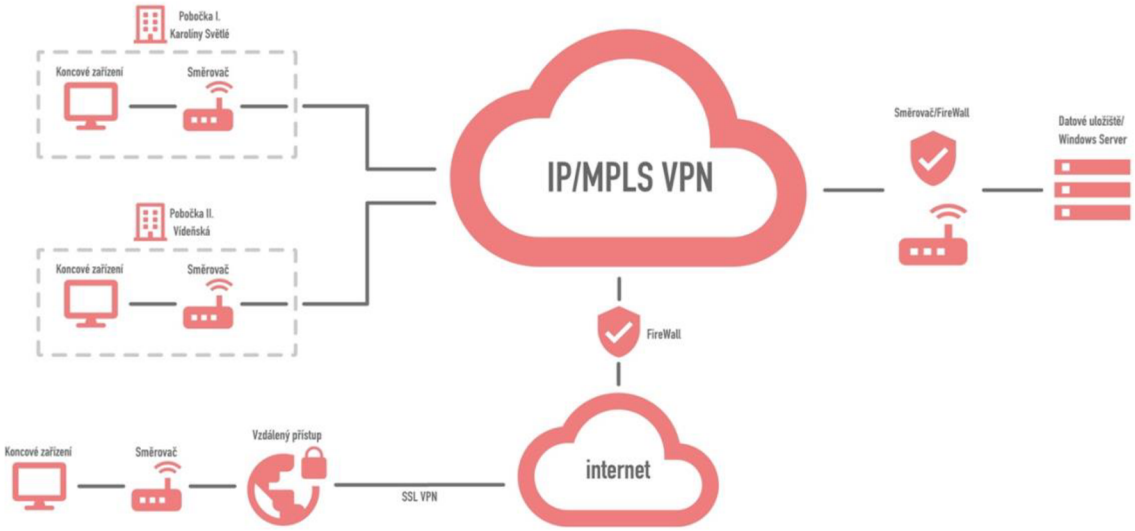
Společnost TGC využívá pro své připojení k internetu, propojení poboček, firewall a vzdálené připojení službu od T-Mobile (GTS) označovanou jako MPLS IP VPN. Služba zajišťuje veškerý provoz a oddělení firemní privátní sítě od internetu. Obě pobočky jsou tedy v jedné síti, přičemž existuje několik VLAN s odlišnými úrovněmi přístupových oprávnění dle oddělení.

Pro vzdálený přístup do firemní sítě je využívána SSL-VPN od Fortinetu. To umožňuje připojení zaměstnanců odkudkoliv z internetu. Přístupový bod pro VPN obstarává FortiGate, který je zakoupen v rámci služby Managed Firewall, taktéž od společnosti T-mobile.

T-Mobile firmě poskytuje diskové uložiště, které je sice umístěno fyzicky mimo firmu, ale je ve zmíněné privátní síti holdingu. Toto řešení by se dalo označit jako cloudové. Vzhledem k tomu, že je diskové pole obstaráváno Windows Serverem 2012 R2, lze využít služeb AD. Zaměstnanci jsou dále rozřazeni do User Group a každý uživatel v doméně má dle své skupiny přiřazené oprávnění k přístupu do specifických podsložek v rámci síťových disků. K síťovým diskům jsou připojeni pomocí SMB protokolu – Samba sdílení. Jinak tomu není ani u přístupu CRM BM k souborům. Datový tok souborů, které si zaměstnanci ukládají na své prostory v síťových discích, je obousměrný. Zaměstnanci mohou stahovat i nahrávat. Zcela rozdílnou problematikou je práce souborů CRM BM. V CRM BM pracuje zaměstnanec se soubory a informacemi klientů pouze v rámci CRM. Soubory nemůže stahovat do svého počítače. Do BM je zaměstnanec může nahrát přes E-přihlášku nebo speciální funkcionalitou v CRM. Z BM se soubory stahují pouze do oddělení tisku na jejich specifické místo na síťovém uložišti. Typickým souborem jsou smlouvy k tisku.

K síťovým diskům, ke své specifické sadě složek v rámci oddělení, má přístup každý zaměstnanec. Počítače zaměstnanců v síti napřímo komunikují přes službu MPLS IP VPN s datovým centrem T-Mobilu. Za zmínku stojí firewally. Ten, který je mezi MPLS

a internetem je FortiGate FireWall a ten, který je mezi MPLS a datovým uložištěm/Windows servery je firewall PfSense. Nákres využívané privátní sítě je níže.



Obr. 9: Schéma topologie (vlastní zpracování)

2.4.4 FortiGate

Firma pronajímá od společnosti T-Mobile službu Managed FireWall. Ta je využívána způsobem, který popisuje obrázek č. 9. Jedná se o balík služeb FortiGatu, který zahrnuje:

- VPN
- FireWall
- SSL inspekci
- Webfilter
- Application control
- IPS
- DLP

Tento balík je určený pro malé firmy. Neobsahuje FortiAnalyzer a není ho možné v rámci balíku dokoupit. FortiGate FireWall je připojený v tzv. HA clusteru. To znamená, že fyzicky jsou firewally dva a zapojeny do redundance tak, aby v případě výpadku jeden zastoupil ten druhý.

2.4.5 Komunikační infrastruktura

Holding TGC si nechal zhotovit komunikační infrastrukturu v budově v Líšni, již v počátcích své podnikatelské kariéry odbornou firmou. V budově na Vídeňské byla komunikační infrastruktura připravena a zbývalo si akorát kabely přidělat do patch panelů v serverovně a propojit aktivní prvky. Obě sítě mají dohromady potenciál připojení kolem 400 koncových zařízení, jsou ovšem zaplněné přibližně ze 70%.

2.4.6 CRM – Bussines Maker

Dá se říct, že CRM Bussines Maker je to nejdůležitější pro společnost. Při zakládání prvotního uskupení v roce 2011 byl právě tento vlastní CRM to, co odděloval tehdejší firmu Terra Group od konkurence a poskytoval jim výhodu. Jedná se o vlastními silami vytvořený CRM systém běžící ve webovém prohlížeči, který slouží pro správu databáze klientů a jejich dokumentů s automatizovanými úkony. Systém sám komunikuje s aukčními portály a dodává návrhy na nejlepší možné ceny energií. Dnes je CRM systém mnohem rozšířenější a umí více funkcí. Je denně udržován a dále vyvíjen.

2.4.7 E-přihláška

E-přihláška je nástroj k získávání nových zákazníků. Existuje v podobě aplikace na Android a v podobě webové aplikace. Jedná se o běžný elektronický formulář s elektronickým podpisem. Nástroj je napojen na CRM BM.

2.5 Informační aktivum

V mém návrhu budu pracovat pouze s jedním aktivem, které je pro analýzu vzhledem k zadání relevantní. Tímto aktivem jsou informace o klientech a dodavatelích. V této části informační aktivum blíže popíši, stanovím hrozby a s jakými riziky je spojeno.

2.5.1 Popis aktiva

Jedná se o nejdůležitější aktivum ve společnosti, protože tvoří její hodnotu. Toto nehmotné informační aktivum, které je součástí informačního systému CRM Bussines Maker, budu obecně nazývat jako Informace. Obsahuje všechny data o klientech, dodavatelích a soubory s nimi spojené. Má velkou hodnotu jak peněžní, tak i bezpečností. S jeho manipulováním a uchováváním ve firmě souvisí vysoká zodpovědnost vůči klientovi i dodavateli a nakládání s ním podléhá Zpracování osobních údajů dle čl. 13 nařízení GDPR.

2.5.2 Zranitelnost aktiva

S mým vybraným aktivem, tedy informacemi, se zajisté pojí zranitelnosti, které určitě má. V tabulkách níže určím klasifikační metodou zranitelnosti aktiva. Každou zranitelnost ohodnotím klasifikačním stupněm ve škále 1-4. Stupnice je popsána v tabulce č. 2.

Tabulka 2: Klasifikační schéma zranitelností (vlastní zpracování)

Klasifikační stupeň	Klasifikační kritérium (příklady)
1 - Nízká zranitelnost	je potřeba k zneužití fyzický přístup
2 - Střední zranitelnost	útočník musí být na stejné síti
3 - Vysoká zranitelnost	útočník musí být na stejné síti, ale vyžaduje speciální výbavu a znalost
4 - Kritická zranitelnost	známá zranitelnost, lze ji zneužít odkudkoliv bez speciálních znalostí

V následující tabulce vypíši zranitelnosti. Některé z nich jsou obecnějšího typu a původu, některé jsou určena firemním prostředí TGC.

Tabulka 3: Klasifikace zranitelnosti informačního aktiva (vlastní zpracování)

Zranitelnost	Úroveň
Krádež	4
Internet	2
Firemní síť	3
Zpracování dat	3
Firewall	1

CRM	**2**
Ukládání dat	**2**
Fyzické poškození HW	**1**
Výpadek napájení el. sítě	**1**
Nastavení oprávnění	**3**

Z tabulky Klasifikace zranitelností informačního aktiva vyplývají méně i více zranitelné oblasti. Nejvýznamnějšími zranitelnostmi jsou krádež, firemní síť, zpracování dat a nastavení oprávnění.

2.5.3 Bezpečnostní události

V tabulce níže definuji na základě předchozí analýzy zranitelností, možné incidenty a události na ně navázané.

Tabulka 4: Identifikace možných incidentů a bezpečnostních událostí (vlastní zpracování)

Aktivum	Zranitelnost	Incident	Událost
Informace	Internet	Neoprávněné získání dat	Získání přístupu k datům klientů
		Nedostupná (zašifrovaná) data	Získání přístupu k databázi
			Získání přístupu do CRM
			Získání přístupu do infrastruktury
			Nelegální činnost
			Útok počítačového viru
	Firemní síť	Nedostupná data	Získání přístupu k databázi
			Získání přístupu do CRM
			Získání přístupu do infrastruktury
		Interní napadení klientských dat	Získání přístupu k databázi
			Získání přístupu do CRM
			Získání přístupu do infrastruktury
			Nelegální činnost
			DDoS útok
	Zpracování dat	Chyba při ukládání dat	Chyba programu
			Chyba HW
	Firewall	Vniknutí do firemní sítě	Chybná konfigurace
	CRM	Chyba při zpracování dat	Chyba programu
			Chyba programátora

			Vadná komponenta CRM
		SW chyba	Chyba programu
			Chyba programátora
			Vadná komponenta CRM
		Poškození dat	Chyba programu
			Chyba programátora
			Vadná komponenta CRM
	Ukládání dat	Chyba při ukládání dat	Poškozený HW
		Poškozená data	Poškozený HW
	Fyzické poškození HW	Nedostupná data	Lidská chyba
	Nastavení oprávnění	Porušení práv	Získání přístupu do nepovolených oblastí
			Nedbalost zaměstnance
		Získání dat v rozporu s právy	Získání přístupu do nepovolených oblastí

2.5.4 Hrozby

Práce a uchovávání informačního aktiva přináší hrozby jak pro klienta, dodavatele tak pro společnost. Klient, při předání svých informací společnosti samozřejmě souhlasí se Zpracováním osobních údajů. Dodavatelé jsou pak vázáni smlouvou. Firma se dle nich musí řídit, jinak by porušovala zákony. Čemu ovšem z hlediska firmy nejde předejít jsou hrozby plynoucí z práce zaměstnanců s informacemi a další vnější hrozby. Zaměstnanec může účelně i neúčelně svým chováním informace ohrozit. Základní ochrana proti účelnému ohrožení je smlouva, kterou má každý zaměstnanec uzavřenou se zaměstnavatelem, aby k němu nedošlo.

Prvním typem neúmyslného ohrožení informací je únik dat způsobený neurčitým typem počítačového viru. Každý počítač, se kterým zaměstnanec pracuje, je opatřen antivirovým programem, síť je zabezpečena FireWallem FortiGate. I přesto je možné, že tato situace nastane. O další typ poškození dat by se mohl postarat RansomWare. Ten by mohl způsobit zašifrování dat a tím je znehodnotit, což by mohlo mít katastrofální dopad na chod společnosti. Vzhledem ke stavu zabezpečení BM CRM systému je i s nízkou pravděpodobností možný DDoS útok, který by mohl činnost firmy na neurčitou dobu vyřadit.

Další hrozbou je zaměstnanec se špatným úmyslem. Jako špatný úmysl se může brát prodej nebo poskytnutí informací konkurentovi atp. Dnes je těžké se proti takovému počinu ubránit. Obzvlášť na pracovišti backoffice, kde je vysoká fluktuace zaměstnanců. Takový zaměstnanec by pak mohl stáhnout informace o klientech i dodavatelích buď na externí přenosné uložiště nebo je poslat přes internet. V extrémním případě by mohla nastat ještě jedna situace. Pokus o násilné neoprávněné vniknutí do počítače a následně i do CRM systému typicky prolamováním hesla cizí osobou nebo zaměstnancem s nekalým úmyslem.

2.5.5 Rizika

Vzhledem k mé problematice a tomu, jak mám dané a jednoznačné aktivum, se s ním pojí předpokládané hrozby. Ty jsem si popsal v předchozí části této podkapitoly a v tabulce jsem ještě pár obecných hrozeb přidal. V této části ohodnotím hrozby kvalitativní metodou a určím váhu rizika, se kterou by mohl nastat bezpečnostní incident. Nejprve jsem vytvořil klasifikační schéma, podle kterého budu hodnotit možná rizika zvolených hrozeb.

Tabulka 5: Klasifikační schéma pro kvalitativní metodu (vlastní zpracování)

Klasifikační stupeň	Riziko
1	Velmi nízká
2	Nízká
3	Střední
4	Vysoká
5	Velmi vysoká

Kvalitativní analýza rizik je v tabulce níže. Rozdělil jsem ji hierarchicky od aktiva, incidentu, který obecně popisuje nežádoucí stav, přes možné události a hrozby s nimi spojené. V posledním sloupci hodnotím, s jakým rizikem nastane z hrozby bezpečnostní incident.

Tabulka 6: Kvalitativní analýza rizika (vlastní zpracování)

Aktivum	Incident	Událost	Hrozba	Riziko
Informace	Neoprávněné získání dat	Útok počítačového viru	Zašifrování dat	2
			Smazání dat	1
			Poškození dat	2
			Únik dat – krádež	2
		Nelegální činnost	Krádež dat zaměstnancem	4
			Úmyslné poškození dat zaměstnancem	4
	Interní získání dat	Nedbalost zaměstnance	Nezamknutý počítač	4
		Nelegální činnost	Krádež dat zaměstnancem	5
			Úmyslné poškození dat zaměstnancem	5
	Zneužití dat	Neoprávněné vniknutí	Krádež dat	2
		Technické selhání	Selhání HW	3
			Chyba SW	4
	Poškozená data	Technické selhání	Selhání HW	2
			Chyba SW	3
		DDoS útok	Zkolabování firemní počítačové sítě	3
	Nedostupná data	Útok počítačového viru	Zašifrování dat	2
			Smazání dat	2
			Poškození dat	2
			Únik dat – krádež	3
		Technické selhání	Selhání HW	2
			Chyba SW	3
		DDoS útok	Zkolabování firemní počítačové sítě	3

Z kvalitativní analýzy rizik vyplynulo více závažnějších hrozeb. Nejrizikovější hrozby jsou dvě. První je krádež dat zaměstnancem. Druhá je úmyslné poškození dat zaměstnancem. Následují hrozby, které mají nižší, ale přesto vysoké riziko. Mezi ně patří například nezamknutý počítat zaměstnance, čehož by mohl zneužít jiný zaměstnanec s nekalým úmyslem nebo chyba softwaru či hardwaru. Hrozba se střední hodnotou rizika je v analýze zastoupena zkolabováním firemní počítačové sítě, které by předcházela událost v podobě DDoS útoku. Ten může být vyvolaný z venku, nebo i z vnitřku sítě, pokud by se vir, který vyvolá DDoS útok dostal například chybou SW do interní sítě.

Z analyzovaných hrozeb jsem vybral nejvýznamnější. Ty, které měly vysokou míru rizika a ty, které jsou důležité z hlediska podnikatelské činnosti společnosti. V následující tabulce popisuji, jak by se jejich propuknutí analyzovalo na firemní síti a navrhuji opatření, které by mohly hrozbám snížit míru rizika nebo alespoň upozornit na jejich propuknutí. Tím by mohli zaměstnanci včas zareagovat a snížit alespoň dopad hrozby.

Tabulka 7: Významné hrozby s návrhem na jejich opatření (vlastní zpracování)

Hrozba	Bezpečnostní událost	Návrh opatření
Krádež dat zaměstnance	Netypické chování na síti – stahování nebo nahrávání většího (než je obvyklé) objemu dat	Sledování toků na firemní síti, nastavení limitů pro nahrávaná nebo stahovaná data, sledování přijímaných a odesílaných typů souborů (filtrování)
Poškození dat zaměstnancem	Netypické chování na síti – vyvolání netypického úkolu, nahrávání dat na jinou než požadovanou adresu	Sledování toků na firemní síti, sledování přijímacích adres a jejich filtrování
Nezamknutý počítač	Jiný zaměstnanec s nekalým úmyslem záměrně zneužije tuto příležitost	Ukládání provozu sítě pro zjištění historického chování subjektů na síti
Chyba SW	Aplikace působící na síti začne chybně komunikovat nebo přestane fungovat	Sledování aplikací a jejich chování
Chyba HW	HW prvek sítě začne chybně komunikovat či přestane fungovat	Mapování sítě
DDoS útok	Netypické zatížení sítě	Detekce takového chování
Krádež (vlivem viru)	Zařízení napadené virem vykazuje netypické chování, odesílá na neověřené adresy	SSL inspekce, Webfiltr, sledování a filtrování příjemců, filtrování odesílaných a přijímaných souborů

2.6 Požadavky investora

Vedení holdingu TGC projevuje zájem ve zvýšení bezpečnosti dat svých klientů. Vzhledem k seskupení holdingu a snahy využít jeho maximální potenciál, chce vedení, aby projekt realizovala dceřiná firma Zeus Solutions. Hlavním úkolem je snížení rizika u těch hrozeb, kde konfiguruje zaměstnanec a data klientů, se kterými pracuje. Vzešel tedy požadavek na tuto firmu, aby přišla s návrhy, které by posunuly zabezpečení dat. Z provedeného návrhu bude navazovat během léta 2020 realizace řešení. Podmínka

vedení Zeus Solutions je využití dosavadních aktivních prvků a řádné zdokumentování dle vnitřních pravidel.

Požadavky investora v bodech:

- Zvýšení bezpečnosti pro klienty.
- Zajistit zabezpečení proti úniku informací z firemních síťových disků.
- Monitorování provozu.
- Funkční řešení využívající stávající HW a kapacity.
- Řádná dokumentace řešení do stávajícího systému dokumentování.
- Výběr vhodných technologií.
- Minimální náklady na realizaci.

2.7 Shrnutí analýzy současného stavu

Analýza současného stavu podtrhuje požadavek vedení holdingu TGC k vytvoření zabezpečení počítačové sítě proti úniku dat. Vyplývá z ní, že žádné takové řešení nyní neexistuje.

V analýze současného stavu jsem představil holding TGC, zadavatele projektu a prostředí firmy jako místo realizace návrhu. Analýzou ICT jsem přiblížil stav a vybavení, kterým holding disponuje a popsal datové toky ve společnosti. V poslední části jsem se věnoval informačnímu aktivu. Podrobil jsem analýzám informační aktivum, a to informace společnosti. Stanovil jsem nejvýznamnější hrozby, které působí na toto aktivum. Určil jsem, jak by se tyto hrozby mohly projevit a navrhl opatření, které by snížilo jejich míru rizika a dopad. Tento seznam určitě není konečný a časem mohou hrozby přibývat či ubývat.

V návrhu vlastního řešení se pokusím právě tyto vybrané hrozby zredukovat, snížit míru jejich dopadu nebo alespoň snížit jejich pravděpodobnost způsobení bezpečnostního incidentu. Vzhledem k zadání je vhodné povýšit úroveň zabezpečení dat, leč není na špatné úrovni, jak hlídáním provozu na vnitřní síti, tak hlídáním provozu na výstupu do internetu.

3 VLASTNÍ NÁVRH ŘEŠENÍ

Ve vlastním návrhu řešení se budu věnovat v první řadě výběru technologií, které zredukují nebo sníží dopad významných hrozeb vybraných v závěru analýzy současného stavu. Podrobně popíši události hrozeb, které je potřeba sledovat, aby bylo možné včasně reagovat na jejich propuknutí. Poté se zaměřím na samotnou implementaci řešení redukující rizika. V závěru porovnám míru hodnot rizik po návrhu opatření.

Jak již bylo zmíněno v závěru analýzy současného stavu, je požadováno sledovat toky na firemní privátní síti a soubory procházející ze sítě a do sítě. A to z důvodu citlivých dat, se kterými se ve firmě pracuje. Je žádoucí přijít s řešením, které by upozorňovalo na netypické dění na síti, sledovalo její vytíženost, nejpoužívanější aplikace, adresy, zatížení sítě počítači zaměstnanců či odhalilo DDoS útok.

3.1 Návrh bezpečnostních opatření

V analýze současného stavu jsem si stanovil významná rizika a k nim jsem popsal stavy, kdy se pozná stav, jakmile se hrozba promění v bezpečnostní incident. Úkolem bezpečnostních opatření je snížit míru rizika nebo alespoň snížit dopad hrozeb.

Udělal jsem rešerši opatření, která by odpovídala navrhovaným opatřením z tabulky č. 7 a zároveň požadavkům investora. Výsledkem rešerše jsou tyto možnosti pro opatření:

- Monitoring toků na firemní síti
- FortiAnalyzer + FortiClient
- Ochrana proti úniku dat

Dále se pokusím přiblížit jednotlivé varianty a co by opatření redukovala, případně cenový odhad implementace.

Monitoring toků na firemní síti

Monitoring má různé podoby a mohu využít řadu různých technologií a protokolů. Dá se postavit na vlastních skriptech nebo na bezplatných či komerčních řešeních. Vzhledem k tomu, že u většiny případů hrozeb jde o sledování toků na firemní síti, byl by monitoring

vhodným řešením pro snížení rizik či dopadu. Mohl by včasně upozorňovat na nežádoucí dění a zaměstnanci z DevOps by tak mohli ihned reagovat.

FortiAnalyzer + FortiClient

Společnost TGC využívá na své firemní síti balíček služeb od Fortinetu. Obsah služeb balíčku je rozepsaný v analýze současného stavu. Fortinet nabízí další služby, které ovšem nejsou součástí balíčku, který využívá TGC. Tyto další služby jsou v dražším balíku služeb. Zmíněnými službami jsou FortiAnalyzer a placený FortiClient. Řešení s těmito službami by pokrylo sledování toků na firemní síti, monitorování koncových stanic, logování aktivity, centrální přehled o chodu jednotlivých stanic a monitorování toků i na VPN. Řešení by tedy pokrylo naprostou většinu hrozeb. Nevýhodou je cena, která by se v tomto případě lišila oproti monitoringu toků závratným způsobem.

Ochrana proti úniku dat

Toto řešení je velice úzce zaměřené a pokrylo by menší počet hrozeb, ale o to efektivněji. Řešení ochrany proti úniku dat by podstatně snižovalo hodnotu rizika u hrozeb, u nichž je toto opatření navrhnuto. Ochrana proti úniku dat filtruje na firewallu soubory, které skrze něj prochází. To se u společnosti TGC dá velice dobře specifikovat, jelikož jejich zaměstnanci pracují pouze s několika typy souborů. Ochrana proti úniku dat je dokonce součástí balíku služeb od Fortinetu, který společnost využívá. Nyní se pouze tato funkcionalita nevyužívala.

Tabulka 8: Významné hrozby s návrhem na jejich opatření (vlastní zpracování)

Kritérium	Monitoring	FortiAnalyzer + FortiClient	Ochrana proti úniku dat
Počet redukovaných hrozeb / snížení dopadu	7	7	2
Náklady	Žádné nebo vyšší v řádu tisíců	Nárůst o desítky až stovky tisíc za rok	Stejné jako aktuální

První i druhé navrhované řešení pokryje všechny hrozby nebo alespoň jejich části. Třetí řešení je specifické na míru poslednímu navrhovanému řešení. Jeho účinnost v redukci hrozeb bude nejvyšší. První dvě řešení především snižují zásadním způsobem dopad.

U monitoringu mohou být náklady nulové nebo jednorázové a v řádech nižších tisíců. Záleží na výsledném řešení. Každopádně investor požaduje minimální náklady, takže nižší náklady mají vysokou prioritu. Řešení od Fortinetu poskytuje největší výhody z jeho používání, je ale problém jeho cena. Ta se přiděluje individuálně. Nyní firma využívá služeb základního balíku od Fortinetu. Povýšení na balík služeb s FortiAnalyzerem a plnou verzí FortiClienta a s řadou dalších funkcionalit by znamenalo nárůst nákladů o desítky až stovky tisíc za rok. Takový finanční náklad rozhodně neodpovídá požadavkům investora. Ochrana proti úniku dat je v současnosti součástí základního balíku od Fortinetu. Tím pádem by jeho používání nepřineslo další finanční zatížení.

3.1.1 Vybrané opatření

Z navrhovaných opatření nejvíce vyhovuje požadavkům na redukci hrozeb a požadavkům investora první navrhované řešení – monitoring. Proto ho vybírám jako opatření pro většinu hrozeb. Monitorovacích systémů existuje více. Vzhledem k tomu, že v návrhu opatření je třeba sledovat toky, zaměřím se na monitoring využívající flow protokoly.

Řešení od Fortinetu není bohužel v tuto chvíli možné. Jeho možnosti a komplexnost jsou velkou pákou pro pořízení, ale cena za toto řešení je vysoká. Navíc je řešení placené paušálně. Náklady se tedy mohou dostat opravdu vysoko. To pro společnost TGC není v tuto chvíli možné.

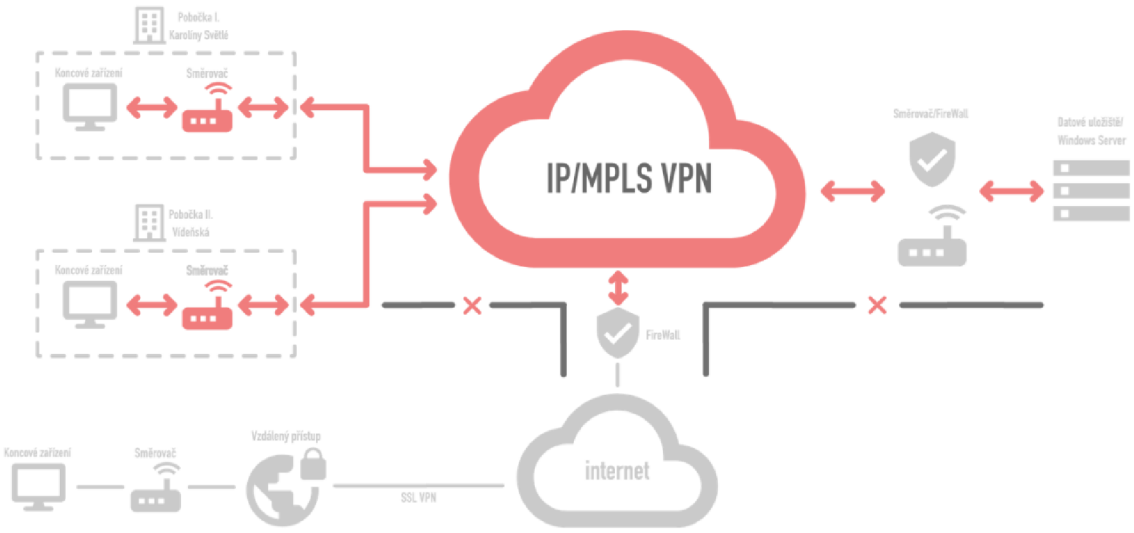
Dalším zaváděným opatřením bude ochrana proti úniku dat. Jeho implementace nebude stát žádné náklady navíc a zároveň bude snadná.

3.2 Sledované toky

Dle požadavků investora vyplývá, že chce sledovat v první řadě vnitropodnikové toky. Z hlediska bezpečnosti by bylo samozřejmě lepší sledovat i toky z internetu do sítě, naopak i provoz na VPN, ale takové řešení by vyžadovalo značně větší investici, což by vzhledem k požadavkům investora nebylo obhájitelné.

Pro představu, jaké kanály přesně budou sledovány, jsem vytvořil schéma (obrázek č. 10). Na schématu jsou červeně vyznačeny toky, které budou sledovány. Toky v síti budou

konkrétně monitorovány na pobočce Vídeňská a pobočce Karolíny Světlé. Dále bude vidět kompletní provoz před firewallem FortiGate, který je na hranici s internetem. Taktéž bude vidět provoz, který jde do datového centra z poboček a zpět. Nebude sledován provoz (tmavě šedé linky s červenými křížky) mezi pobočkami a internetem, stejně tak mezi datovým centrem a internetem. Monitoring nepokryje provoz za firewallem, tedy mezi firewallem a VPN.



Obr. 10: Schéma sledovaných toků (vlastní zpracování)

3.3 Monitorované události

V analýze současného stavu jsem vybral hrozby, uvedl stav, v jakém se hrozba projevuje a navrhl opatření. V této kapitole se pokusím tyto události více rozvést. Nadpisem bude hrozba a pod ním popsána událost.

Všechny případy událostí a jejich opatření by se na monitorovacím systému musely nastavit buď v administraci monitoringu, nebo pomocí vlastních skriptů. Postupem času se budou nastavené hodnoty sledovaných událostí zpřesňovat tak, aby stanovené metriky odpovídaly co nejvíce skutečnému dění a neohlašovaly falešné události.

3.3.1 Krádež dat zaměstnancem

Ve společnosti TGC je nastavený systém pro práci s daty klientů. Data jdou obvykle z E-přihlášky do CRM BM, kde s nimi zaměstnanci backoffice dále pracují. Způsob, jakým s nimi zaměstnanci na backoffice pracují je striktně daný. Dá se tedy vypozorovat a stanovit, kam mají toky dat od každého zaměstnance směřovat. Lze stanovit seznam adres, odkud kam má komunikace směřovat. Pokud by toky vedly jinam, než by bylo stanoveno, jednalo by se o netypické chování. Monitorovací systém by pak upozornil nadřízeného o netypickém chování.

Další možností je měření přijímaného a odesílaného objemu dat. Všechny soubory potom, co projdou CRM BM, mají redukovanou velikost. Soubor jednoho klienta, vzhledem k podnikatelské činnosti, by neměl přesáhnout 20 MB. Zaměstnanci na backoffice vždy pracují s daty jednoho klienta. Pokud by tedy zaměstnanec ze svého zařízení odesílal větší objem dat v jednom toku, než by byl stanovený limit 20 MB, šlo by opět o netypické chování. Následně by nadřízená osoba dostala upozornění e-mailem.

V obou případech by mohlo jít o krádež, pokud by se splnily podmínky.

3.3.2 Poškození dat zaměstnancem

Jak bylo zmíněno u krádeže dat, je práce zaměstnance backoffice striktně daná. U této hrozby jde o podobný typ monitorování. Pokud by zaměstnanec vyvolal akci, která by byla jiného než obvyklého charakteru, došlo by opět k upozornění nadřízeného.

Dalším případem je možnost, kdy by jakýkoliv zaměstnanec zjistil, že jsou data určitým způsobem poškozená. V monitorovacím systému by v takovém případě šlo dohledat co se v historii dělo s danými daty.

3.3.3 Nezamknutý počítač

V tomto případě by monitorovací systém mohl opět posloužit pro vhled do historie zařízení. Pokud by někdo zneužil nezamknutý počítač ke krádeži či poškození dat, dalo by se zjistit alespoň jaké soubory byly odcizeny nebo poškozeny. Případně co daný člověk

dělal na síti. Pokud by docházelo ke krádeži nebo poškozování dat, měly by zareagovat předchozí dva případy – mělo by dojít k notifikaci nadřízeného.

3.3.4 Chyba SW

Monitorovací systém by sledoval aplikace běžící na firemní síti a kontroloval jejich stav. Pokud by nějaká aplikace zatěžovala síť nad limit, přestala by fungovat nebo by aplikace potřebná pro běh a podporu podnikatelské činnosti firmy přestala fungovat, monitorovací systém by upozornil DevOps. Existoval by seznam, kde by právě byly aplikace vypsány a vedeny jako kriticky důležité.

3.3.5 Chyba HW

Monitorovací systém by sledoval stav sítě, mapoval všechny prvky na síti a tím by sděloval aktuální stav. Pokud by nějaký prvek vypadl, například switch, ohrozil chod firemní sítě a tím i podnikatelskou činnost, přišla by notifikace DevOps oddělení.

3.3.6 DDoS útok

Pokud by došlo k DDoS útoku, zvýšil by se na firemní síti rapidně provoz. Opět by došlo k notifikaci DevOps.

3.3.7 Krádež (vlivem počítačového viru)

V první řadě je žádoucí ochrana dat. Ta je již zajištěna FireWallem FortiGate, antivirovými programy na koncových zařízeních a dalšími nápomocnými nástroji jako například SSL inspekce nebo webfiltr. Další ochranou je mnou navrhované opatření ochrana proti úniku dat. Ta se nastavuje přímo na firewallu. Jejím úkolem je filtrovat příchozí a odchozí soubory. Zde je opět možné přesně stanovit jaké soubory mohou projít a jaké ne.

Pokud vir i přes ochranu na firemní síti projde dovnitř, je na řadě monitorovací systém. Ten by opět sledoval netypické dění tak, jako u prvních dvou hrozeb.

3.4 Výběr monitorovacího sytému

V této části se zaměřím na výběr konkrétního řešení pro monitorování toků na firemní síti společnosti TGC.

3.4.1 Výběr flow protokolu

Monitorovací systém má sledovat toky. Proto se zaměřím na použití monitoringu s flow protokolem. Nejrozšířenějšími a nejvíce používanými typy flow protokolu jsou sFlow a NetFlow. Jejich používání je ověřené a jsou od renomovaných značek v odvětví počítačových sítí. Proto se i já budu rozhodovat pro jeden z těchto dvou.

Teoretické nastínění toho, co je sFlow a NetFlow jsem uvedl již v první části této práce. Zde tyto protokoly porovnám a uvedu atributy, které mě budou zajímat u výsledného výběru.

3.4.2 Porovnání flow protokolů

Základní rozdíl je použitelnost. NetFlow funguje jen na produktech Cisco, zatímco sFlow funguje na produktech více různých výrobců. Rozdíl je i v kolektorech pro tyto technologie. Pro NetFlow jich je více. To může být pro sFlow omezením. Na rozdíl od NetFlow může sFlow shromažďovat provoz z vrstev OSI 2 až 7, protože není omezené na sledování IP přenosů, což je největší rozdíl mezi těmito technologiemi. Díky tomu, že NetFlow nepracuje s náhodnými vzorky jako sFlow, je díky tomu přesnější, vizualizuje kompletní stav sítě. sFlow je také pomalejší. Obecně je NetFlow pohodlnější a rozsáhlejší.

Tabulka 9: NetFlow vs sFlow porovnání (vlastní zpracování)

Vlastnosti	NetFlow	sFlow
Výrobce	Cisco	Více výrobců
Zachycování paketů	Ne	Částečně
Počítadlo paketu na portu	Ne	Ano
Sběr dat v reálném čase	Částečně	Ano
Podpora protokolů	**NetFlow**	**sFlow**

IP/ICMP/UDP/TCP	Ano	Ano
Ethernet/802.3	Ne	Ano
Packet Headers	Ne	Ano
IPX	Ne	Ano

3.4.3 Porovnání kolektorů

K tomu, aby flow protokoly fungovaly korektně, je potřeba mít server, který bude shromažďovat a vyhodnocovat data. Takovéto funkcionalitě se říká kolektor a analyzátor. Nyní se budu zabývat porovnáním kolektoru, který bude splňovat, pokud možno, tyto parametry:

- Open-source licence nebo alespoň trial verze na vyzkoušení.
- Přehledné analytické statistiky.
- Přehledné „top“ seznamy pro výpis zdrojových adres, které nejvíce vytěžují síť.
- Přehledné „top“ seznamy pro výpis aplikací, které nejvíce vytěžují síť.
- Varovné upozornění (notifikace do e-mailu).
- Vytvoření mapy sítě.
- Běh aplikace ve webovém rozhraní na apache serveru, pro jednoduchý přístup odkudkoliv.
- Detekce botnetu.

Výběr kolektoru budu provádět průzkumem na internetu. Žádoucí jsou takové kolektory, které budou nejvíce odpovídat požadovaným parametrům. Do tabulky níže jsem vypracoval rešerši různých kolektorů.

Tabulka 10: Porovnání kolektorů (vlastní zpracování)

Název	OS	Flow protokol	Licence	Přehledy	Mapování sítě	Reporting
SolarWinds	Win	NetFlow, sFlow	30 dní trial, poté 1500$ +	uživatelů, aplikací, protokolů	Ano	Ano
sFlowTrend	Linux	sFlow	Omezení na 5 switchů a historie dat 1h nazpět, Pro	uživatelů, aplikací	Ano	Ano

			verze neomezena			
Plixer Scrutinizer	Linux, Win	NetFlow, sFlow	Omezení na 10000 analyzovaný toků za sekundu, 5h historie; SSRV verze neomezeno (Pay per device)	Time frame, uživatel, aplikace, protokol	Ano	Ano
Paessler PRTG	Win	NetFlow, sFlow	30 dní trial, poté 1300€ +	Uživatel, aplikace, protokol, pokročilé přehledy	Ano	Ano, push notifikace do telefonu
Intermapper	Win	NetFlow, sFlow	30 dní trial, poté placené	Uživatel, aplikace, protokol, pokročilé přehledy	Ano	Ano
NfSen	Linux	NetFlow	Open source	uživatelů, aplikací, protokolů	Ne	Pouze v prohlížeči
FlowViewer	Linux	NetFlow	Open source	Vlastní filtry	Ne	Pouze v prohlížeči
Nprobe/Ntopng	Linux, Win	NetFlow, sFlow	Nprobe omezení na 25000 flows, poté placené 50$; Ntopng Open source	Uživatel, aplikace, protokol, pokročilé přehledy	Ano	Ano

3.4.4 Výběr řešení monitorovacího systému

Z předešlých porovnání flow protokolů a kolektorů mi vzešlo více možných řešení. Zde se pokusím porovnat mnou vybrané možnosti řešení pro monitoring. Vezmu v potaz flow protokol, operační systém serveru a hardware.

Z vybraných kolektorů pro Windows je vhodným kandidátem Paessler PRTG. Odpovídá všem stanoveným požadavkům. Navíc je do 100 senzorů zdarma. Používání kolektoru a analyzéru Paessler PRTG dává větší smysl s protokolem NetFlow. Nevýhodou je nutnost použití Cisco switchů. Vzhledem k možnostem společnosti TGC je možné použití virtuálního Windows serveru od společnosti T-mobile, na kterém by kolektor s analyzérem mohl fungovat.

Z možných kolektorů pro Linux je nejvhodnějším řešením Nprobe s analyzérem Ntopng. Řešení odpovídá všem potřebám a je tak vhodným kandidátem. Skládá se ze dvou samostatných SW. První je Nprobe, který funguje jako kolektor a druhý Ntopng, který funguje jako samostatný analyzér. Výhodou je, že toto řešení poskytuje stejné možnosti jako ostatní placené řešení, ale je levnější. Vyzkoušet se dá zdarma a analyzér je dokonce s open source licencí. Kolektor Nprobe je na otestování omezený na 25 000 toků a pak se dá koupit v základní verzi za 50 dolarů, což je sice proti požadavkům investora, ale jde o velice zanedbatelnou částku. Jak Nprobe, tak Ntopng lze upgradovat o další funkcionality za příplatky, které ve srovnání s konkurencí nejsou tak vysoké. Toto řešení je postavené na využití stávajícího HW. Tzn., že by se použil sFlow protokol, protože switche ve společnosti ho podporují a taktéž je k dispozici linuxový server, který je na pobočce Vídeňská.

V tabulce jsem zpracoval a porovnal obě možné verze. Náklady jsem rozpočítal na rok provozu.

Tabulka 11: Porovnání řešení monitoringu (vlastní zpracování)

Možnost	Flow protokol		Doba instalace
	Výhody	Nevýhody	
Win Server + NetFlow + nové switche	Rozmanitost řešení Více kolektorů Přesnější Podpora firewallů Nevzorkuje Funkční na WAN	Omezení na Cisco produkty Odchytává pouze IP přenosy na 3 vrstvě Kolektor od 3. strany	5 MD
Linux server + sFlow + stávající switche	Shromažďování dat z vrstev OSI 2-7	Pomalejší Kolektor od 3. strany	2 MD

	Cena řešení							
Možnost	**Cena za server**	**Provoz serveru**	**Switche**	**Kolektor**	**Licence za OS**	**Konfigurace**	**Správa**	**Celkem**
Win + NetFlow + nové switche	42 000 Kč	0 Kč	105 246 Kč	0 Kč	4 050 Kč	10 000 Kč	48 000 Kč	**209 296 Kč**
Linux + sFlow + stávající switche	0 Kč	7 000 Kč	0 Kč	1 250 Kč	0 Kč	4 000 Kč	60 000 Kč	**72 250 Kč**

V tabulce jsem nejprve porovnal výhody a nevýhody NetFlow a sFlow. Jak je vidět, Netflow má více výhod, ale rozdíly mezi nimi nejsou až tak zásadní. To již ukázala i předchozí část, kde jsem se zaměřil na porovnání flow protokolů. Dále jsem se věnoval době instalace. U řešení s NetFlow by doba instalace byla delší, protože by se musely vyměnit i switche. Ty současné NetFlow nepodporují. Kvůli tomu je doba instalace delší. Nespornou výhodou sFlow je okamžité nasazení bez nutného dokupování HW.

V další části tabulky jsem porovnával cenu implementace a ročního provozu monitoringu. V první řadě jsem se zaměřil na server. Pokud by se mělo použít řešení s Windows, pak je tu možnost virtuálního serveru od společnosti T-mobile. Ta si účtuje za základní server 500 Kč měsíčně plus 6 Kč za 1 Gb. Do tabulky jsem zanesl roční cenu s 500 Gb. Linuxový server by nestál nic, protože společnost TGC má server navíc. V případě Win serveru pak společnost nemusí platit za provoz. Naopak je tomu u vlastního serveru. Cena 7000 Kč je odhad za roční spotřebu serveru. Pokud by bylo žádoucí jít do nové infrastruktury s NetFlow bylo by potřeba vyměnit distribuční switche přes které prochází veškerý provoz. Bylo by potřeba vyměnit tři switche HP Aruba 2930M za switche Cisco Catalyst 2960X-24TS-L, který stojí jeden 35 082 Kč s DPH. Další na řadě jsou licence. V případě PRTG kolektoru by cena byla nulová, protože vývojáři poskytují svůj SW zdarma, pokud síť nemá více jak 100 senzorů, což by v případě společnosti TGC bylo splněno. Muselo by se ale zaplatit za licenci Windows Server Standard 2019, která stojí 4 050 Kč s DPH. Naopak u linuxového řešení by cena za OS byla nulová, ale kolektor je zpoplatněný částkou 1250 Kč (50 dolarů). Vzhledem k době instalace jsem vypočítal další položku – konfiguraci, která popisuje cenu doby instalace, kdy 1 MD stojí 2000 Kč zaměstnance DevOpa. Pro správu na windowsovém nebo linuxovém serveru musí být vyhrazena speciální osoba. Pokud by to měl být Windows administrátor, byla by roční správa, kterou odhaduji na 2 MD za měsíc, levnější než ta, kterou by prováděl administrátor linuxu.

Sečtení nákladů jednotlivých možností pak ukazuje značný nepoměr, kdy by cena za verzi s NetFlow stála za roční provoz téměř 210 000 Kč. Kdežto verze využívající sFlow a stávající HW vyjde v ročním provozu na necelých 73 000 Kč. To udává, vzhledem k požadavku investora na minimální náklady, jasnou převahu pro řešení s sFlow. Navíc řešení utvrzuje další požadavek investora, a to využití stávajícího HW. I když řešení s sFlow nenabízí takové možnosti jako to s NetFlow, je řešení s sFlow kompromisem především pro investora. Obě řešení by zredukovala rizika podobným dílem. Další

výhodou linuxového řešení je využívání především linuxových technologií v oblasti DevOps ve firmě Zeus Solutions, která má na starost IT podporu společnosti TGC.

Pro vlastní návrh řešení tedy vybírám možnost sFlow protokolu aplikovaného na stávajících switchích a nainstalování kolektoru nProbe s analyzérem ntopng na server firmy Zeus Solutions.

3.5 Zprovoznění serveru

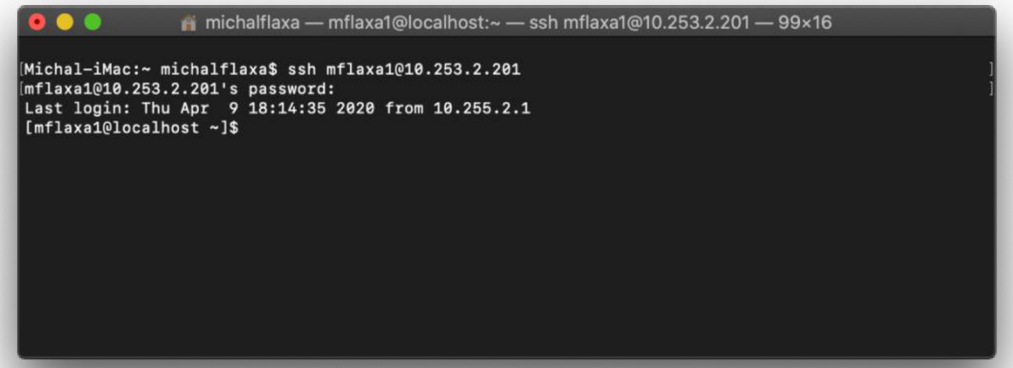
Nejprve popíši zapojení, nastavení serveru a instalaci OS. Server bude fungovat jako kolektor a analytický server pro monitoring. Vzápětí nastavím další aktivní prvky pro provoz monitoringu na síti.

Firma Zeus Solutions disponuje několika servery. Pro prvotní testovací provoz monitoringu byl vyhrazen starší nepoužívaný server, na který bude potřeba nainstalovat operační systém. V rámci zachování firemní struktury serverů a používání, pokud možno open source softwaru, je doporučeno nainstalovat stejný OS jako na ostatní servery. Tím je právě volná linuxová distribuce založená na Red Hat Enterprise Linuxu – CentOS.

3.5.1 Instalace operačního systému CentOS

Na server je nejprve nutné nainstalovat zmíněný CentOS. Instalace probíhá stejným způsobem jako u každého jiného OS. Jako paměťové médium pro instalaci jsem použil flash disk, na kterém jsem umístil instalační soubor s OS. To jsem připojil do serverového počítače, kde jsem v boot menu vybral možnost instalace z USB flash disku. Poté se rozběhne instalace. Ta probíhá sama a první požadovaná interakce je až na vybrání úložiště na které se má OS nainstalovat. Pak instalátor vyzve k vytvoření uživatele, jeho a administrátorského hesla. To je z hlediska instalace vše, zbytek proběhne automaticky sám a po rebootu naběhne operační systém do svého prostředí. Jak je vidět na obrázku č.12 CentOS se ovládá přes příkazový řádek.

Základním úkonem po naběhnutí serveru bylo ještě zjištění IP adresy serveru, která se následně umístila do VLANy, která je izolovaná od internetového připojení, jinak vidí všechny switche a koncové zařízení v rámci celé privátní firemní sítě.



Obr. 12: Terminál připojený přes SSH na server (vlastní zpracování)

Následuje umístění serverového počítače do racku v serverovně pobočky Vídeňská, kde se server připojí na zařízení UPS a ke switchi. Dokonfiguruje se přístup k serveru přes daný port, otestuje se a server je připravený.

3.5.2 Vzdálené připojení a správa

Pro pohodlnou správu serveru je vhodná vzdálená správa. Ta se provádí pomocí SSH připojení a dnes je toto připojení možné přes kterýkoliv operační systém skrze terminál (u Windows CMD či PowerShell). Nyní popíši reálný příklad připojení na náš připravený server.

Pro připojení přes SSH na server musí být uživatel připojený ve vnitřní firemní síti buď na ethernetovém kabelu nebo na firemní Wi-Fi síti, kde potřebuji certifikát. To není vždy možné a pokud se uživatel nenachází fyzicky v dosahu sítě, musí se připojit prostřednictvím VPN. Toho dosáhne tak, že má ve svém počítači nainstalovaný FortiClient. Přes který se může pohodlně přihlásit pomocí svého doménového účtu do firemní sítě. Když už je uživatel v síti, může bez problémů zapnout terminál a přihlásit se přes SSH. Příkaz pro připojení pak vypadá následovně:

```
ssh mflaxa3@10.253.2.201
```

Neboli

```
ssh uživatel@místo_připojení
```

Pak uživatel zadá heslo, které si nastavil v CentOS a je připojen k serveru. Takto bude probíhat každé připojení, když bude potřeba nainstalovat komponenty, doplňky, kolektor či nastavovat potřebné věci. Obdobným způsobem se připojíme i pro správu switchů.

3.6 Konfigurace sFlow

Pro správné fungování monitoringu je potřeba zapnout sFlow na switchích. K popisu konfigurace bude sloužit tato kapitola.

Pro vzdálené připojení na switche platí podobný postup jako pro vzdálené připojení k serveru. V obou případech je nutné mít uživatelský profil, kterým se pomocí SSH a zadáním příslušné IP adresy, připojíme na dané zařízení. V tomto konkrétním případě na switch. Na switchi se uživatel ověřuje vůči RADIUS serveru, který je v datovém centru u T-mobilu v rámci firemní privátní sítě. Postupně se takto budeme připojovat na všechny switche na kterých chceme zapnout sFlow. V mém případě jsem začal od distribučního switche a pokračoval po switchích vnořených hlouběji v síti. Celkově bude sFlow nastaveno na 14 switchích HP Aruba.

První příkaz, který slouží pro aktivování sFlow a nastavení jeho směrování, tzn. kam má posílat data je následující:

```
sflow 1 destination 10.253.2.201
```

Tento příkaz říká – aktivuj sFlow pod instancí 1 (z možných třech) a posílej tyto data do destinace 10.253.2.201, což je analytický server, na kterém záhy nastavím kolektor.

Dalším příkazem říkám switchi jakou frekvencí má sFlow vzorkovat.

```
sflow 1 sampling all 100
```

Příkaz říká – vzorkuj každý 100 paket na všech portech. Pokud by bylo žádoucí, mohl bych zde nastavit určité porty. To, ale v našem případě, není potřeba. Pokračuji s nastavením, které je vyžadované.

```
sflow 1 polling all 60
```

To nám říká, sesbírej data za poslední minutu a odesílej je kolektoru. Pro potvrzení nastavení je potřeba ještě pár příkazů.

```
write memory (wr m)

show sflow agent

show sflow 1 destination
```

Tím potvrdíme nastavení a vypíšeme informace o nastaveném sFlow pro kontrolu. V reálném provedení to pak vypadá následovně, jako na obrázku č.13 a č. 14.

```
sw-d01.brn02.core.terragroup.cz(config)# sflow 1 destination 10.253.2.201
sw-d01.brn02.core.terragroup.cz(config)# sflow
 <1-3>                 The sFlow instance to configure.
sw-d01.brn02.core.terragroup.cz(config)# sflow 1 sampling
 [ethernet] PORT-LIST  Enter a port number, a list of ports or 'all' for all ports.
 0                     Disable sampling.
 <50-16777215>         The sampling rate; approximately 1/N packets will be sampled.
sw-d01.brn02.core.terragroup.cz(config)# sflow 1 sampling all 100
sw-d01.brn02.core.terragroup.cz(config)# sflow
 <1-3>                 The sFlow instance to configure.
sw-d01.brn02.core.terragroup.cz(config)# sflow 1
 destination           Configure the sFlow collector address.
 polling               Configure sFlow polling.
 sampling              Configure sFlow sampling.
sw-d01.brn02.core.terragroup.cz(config)# sflow 1 polling
 [ethernet] PORT-LIST  Enter a port number, a list of ports or 'all' for all ports.
sw-d01.brn02.core.terragroup.cz(config)# sflow 1 polling all
 0                     Disable polling.
 <20-2147483647>       The polling interval in seconds.
 [ethernet] PORT-LIST  Enter a port number, a list of ports or 'all' for all ports.
sw-d01.brn02.core.terragroup.cz(config)# sflow 1 polling al
 0                     Disable polling.
 <20-2147483647>       The polling interval in seconds.
sw-d01.brn02.core.terragroup.cz(config)# sflow 1 polling al
 0                     Disable polling.
 <20-2147483647>       The polling interval in seconds.
sw-d01.brn02.core.terragroup.cz(config)# sflow 1 polling all
 0                     Disable polling.
 <20-2147483647>       The polling interval in seconds.
sw-d01.brn02.core.terragroup.cz(config)# sflow 1 polling all 60
 <cr>
sw-d01.brn02.core.terragroup.cz(config)# sflow 1 polling all 60
sw-d01.brn02.core.terragroup.cz(config)# wr m
sw-d01.brn02.core.terragroup.cz(config)# show sflow agent
 SFlow Agent Information
  Version             : 1.3;Aruba;WC.16.08.0003
  Agent Address       : 10.253.1.3
  Source IP Selection : Outgoing Interface

sw-d01.brn02.core.terragroup.cz(config)# show sflow
 agent                 Show sFlow agent information for the switch.
 <1-3>                 The sFlow instance to show information for.
sw-d01.brn02.core.terragroup.cz(config)# show sflow 1
 destination           Show sFlow collector information.
 sampling-polling      Show sFlow sampling and polling information.
sw-d01.brn02.core.terragroup.cz(config)# show sflow 1
 destination           Show sFlow collector information.
 sampling-polling      Show sFlow sampling and polling information.
```

Obr. 13: Prostředí PowerShell – konfigurace sFlow 1. (vlastní zpracování)

```
sw-d01.brn02.core.terragroup.cz(config)# show sflow 1 destination
 SFlow Destination Information

  Destination Instance      : 1
  sflow                     : Enabled
  Datagrams Sent            : 58
  Destination Address       : 10.253.2.201
  Receiver Port             : 6343
  Owner                     : Administrator, CLI-Owned, Instance 1
  Timeout (seconds)         : 2147483455
  Max Datagram Size         : 1400
  Datagram Version Support  : 5
  OOBM Support              : Disabled

sw-d01.brn02.core.terragroup.cz(config)# show sflow 1 destination
 SFlow Destination Information
  Destination Instance      : 1
  sflow                     : Enabled
  Datagrams Sent            : 61
  Destination Address       : 10.253.2.201
  Receiver Port             : 6343
  Owner                     : Administrator, CLI-Owned, Instance 1
  Timeout (seconds)         : 2147483450
  Max Datagram Size         : 1400
  Datagram Version Support  : 5
  OOBM Support              : Disabled

sw-d01.brn02.core.terragroup.cz(config)# show sflow 1
 destination           Show sFlow collector information.
 sampling-polling      Show sFlow sampling and polling information.
sw-d01.brn02.core.terragroup.cz(config)# show sflow 1 sampling-polling
 SFlow Sampling Information

        | Sampling                    Dropped | Polling
  Port  | Enabled      Rate Header    Samples | Enabled Interval
  ----- + -------  -------- ------ ---------- + ------- --------
  1       Yes(1)        100    128          0   Yes(1)        60
  2       Yes(1)        100    128          0   Yes(1)        60
  3       Yes(1)        100    128          0   Yes(1)        60
  4       Yes(1)        100    128          0   Yes(1)        60
  5       Yes(1)        100    128          0   Yes(1)        60
  6       Yes(1)        100    128          0   Yes(1)        60
  7       Yes(1)        100    128          0   Yes(1)        60
  8       Yes(1)        100    128          0   Yes(1)        60
  9       Yes(1)        100    128          0   Yes(1)        60
  10      Yes(1)        100    128          0   Yes(1)        60
  11      Yes(1)        100    128          0   Yes(1)        60
  12      Yes(1)        100    128          0   Yes(1)        60
  13      Yes(1)        100    128          0   Yes(1)        60
  14      Yes(1)        100    128          0   Yes(1)        60
  15      Yes(1)        100    128          0   Yes(1)        60
  16      Yes(1)        100    128          0   Yes(1)        60
  17      Yes(1)        100    128          0   Yes(1)        60
  18      Yes(1)        100    128          0   Yes(1)        60
  19      Yes(1)        100    128          0   Yes(1)        60
  20      Yes(1)        100    128          0   Yes(1)        60
  21      Yes(1)        100    128          0   Yes(1)        60
  22      Yes(1)        100    128          0   Yes(1)        60
  23      Yes(1)        100    128          0   Yes(1)        60
  24      Yes(1)        100    128          0   Yes(1)        60

sw-d01.brn02.core.terragroup.cz(config)# show sflow 1 destination
 SFlow Destination Information

  Destination Instance      : 1
  sflow                     : Enabled
  Datagrams Sent            : 93
  Destination Address       : 10.253.2.201
  Receiver Port             : 6343
  Owner                     : Administrator, CLI-Owned, Instance 1
  Timeout (seconds)         : 2147483386
  Max Datagram Size         : 1400
  Datagram Version Support  : 5
  OOBM Support              : Disabled

sw-d01.brn02.core.terragroup.cz(config)#
```

Obr. 14: Prostředí PowerShell – konfigurace sFlow 2. (vlastní zpracování)

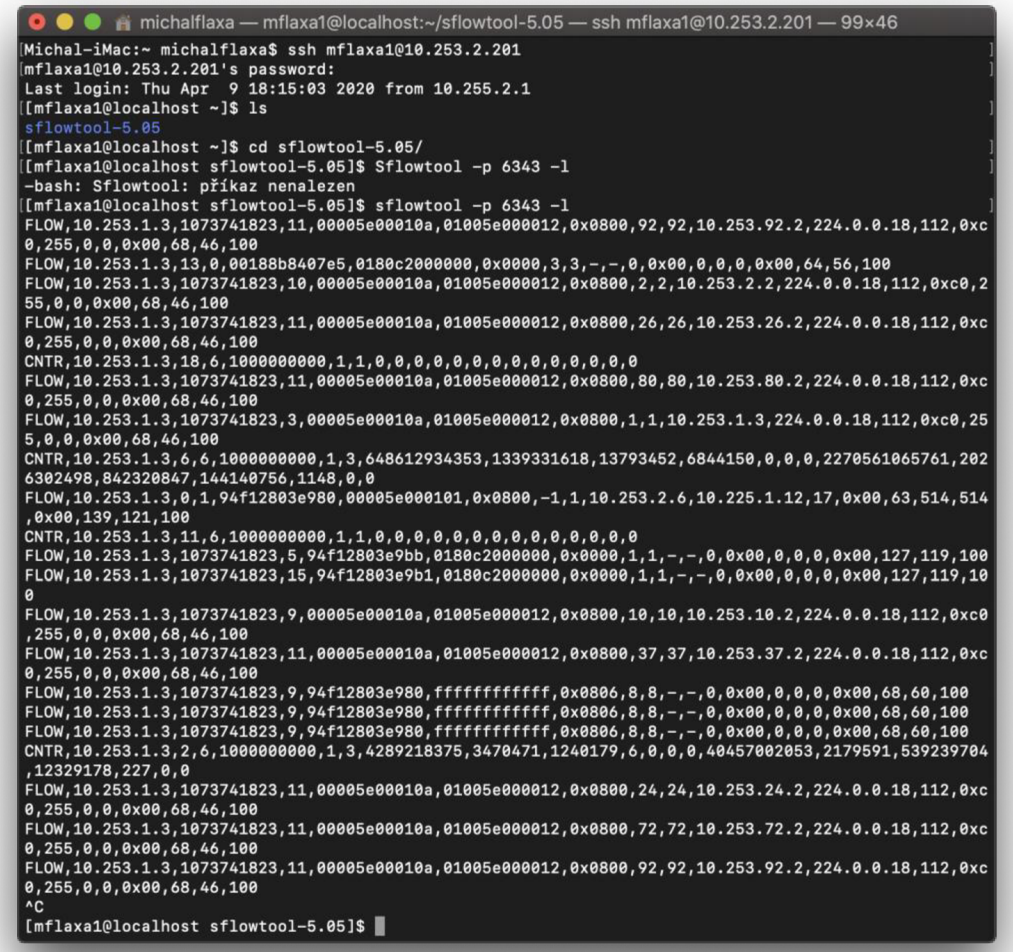
Na obrázcích 10. a 11. je vidět jak celý proces konfigurace, tak výpis nastavení, který je vypsaný několikrát po sobě. To je proto, aby bylo vidět, že sflow skutečně odesílá ze switche datagramy. Je vidět měnící se číslo za položkou Datagrams sent po zadání příkazu *show sflow 1 destination.* Lze vidět i potvrzení, že polling opravdu funguje na všech portech switche a to konkrétně na obrázku č. 14 za příkazem *show sflow 1 sampling-polling.*

3.6.1 Testovací provoz

Pro testovací provoz je potřeba nainstalovat kolektor na server. Zvolil jsem nejjednodušší možný kolektor pro ověření funkčnosti. Tím je sFlowToolkit. Tento kolektor je doporučený dle vývojářů sFlow. SFlowToolkit je nástroj, který nemá grafické rozhraní a funguje pouze v příkazovém řádku. Vzhledem k tomu, že server nemá prozatím přístup k internetu, pro instalaci kolektoru se musel dočasně přesunout do jiné VLAN, která přístup má. Samotnou instalaci tohoto kolektoru popisovat nebudu. Tu popíši až pro kolektor, který bude vybrán jako konečný. Po instalaci kolektoru se VLAN opět přepne do svého původního umístění. Nástroj se ovládá příkazy. Zde je jeden základní, kterým si ověříme funkčnost.

```
Sflowtool -p 6343 -l
```

Tento příkaz ve zkrácené podobě vypíše datagramy, které kolektor aktuálně přijímá na svém TCP/UDP portu 6343. Příklad je na obrázku č. 15.



Obr. 15: Terminál – otestování příjmu datagramů (vlastní zpracování)

Na obrázku č. 15 je vidět výpis přijatých datagramů za krátkou časovou jednotku (1-2 sekundy). V dobu měření nebyl na firemní síti příliš velký provoz. Jeden datagram je vždy řádek, který začíná slovem „FLOW“. Jednotlivé datagramy obsahují mnoho užitečných informací, jako například zdrojové IP adresy, IP adresy switche, informaci o VLAN, použité porty na přepínači a další informace. Tyto informace bude přijímat i navrhovaný sFlow kolektor, který převede datagramy do uživatelsky přívětivějšího zobrazení, bude je analyzovat, sestavovat statistiky atp.

3.7 Kolektor a analyzér provozu

V jedné z předchozích kapitol jsem vybíral kolektor s analyzérem pro monitoring firemní sítě. Z rešerše mi vzešlo, že nejvhodnější řešení je od firmy Ntop, a to v kombinaci kolektoru Nprobe s analyzérem Ntopng. V této kapitole provedu instalaci a konfiguraci jednotlivých komponent, představím prostředí Ntopng, jeho možnosti a předvedu, jak se řešení chová v produkčním provozu.

3.7.1 Zprovoznění kolektoru a analyzéru

Kolektor a analyzér budu instalovat na server, který jsem si pro činnost monitoringu již připravil. Verze operačního systému, na který budu Ntop instalovat je CentOS 7. Pro účel instalace si přepnu server do jiné VLAN, která má přístup k internetu. Po instalaci jej přepnu zpět do své vyhrazené VLAN, kde server nemá přístup k internetu. Instalaci a konfiguraci budu provádět vzdáleně přes SSH připojení, které jsem zde již také popsal, přejdu tedy rovnou na instalaci.

Celá instalace bude probíhat dle dokumentace Ntop, kde jsem se dočetl, že pro instalaci na CentOS mohu využít Yum package manager, který je již součástí OS. V první řadě je vhodné Yum aktualizovat, aby stáhl poslední verze balíčků, mezi nimiž jsou i instalační balíčky od Ntop. Tento úkon je potřeba vykonat jako root, tedy jako *sudo*. K tomu slouží příkaz:

```
sudo yum update
```

Pro doplnění dalších balíčků, potřebných pro plnou funkčnost monitoringu je ještě potřeba doplnit knihovnu balíčků.

```
rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-
7.noarch.rpm

cd /etc/yum.repos.d/

wget http://packages.ntop.org/centos-stable/ntop.repo -O ntop.repo
```

Po aktualizaci yum knihovny balíčků může přijít na řadu stažení a instalace Nprobe, Ntopng a dalších potřebných SW.

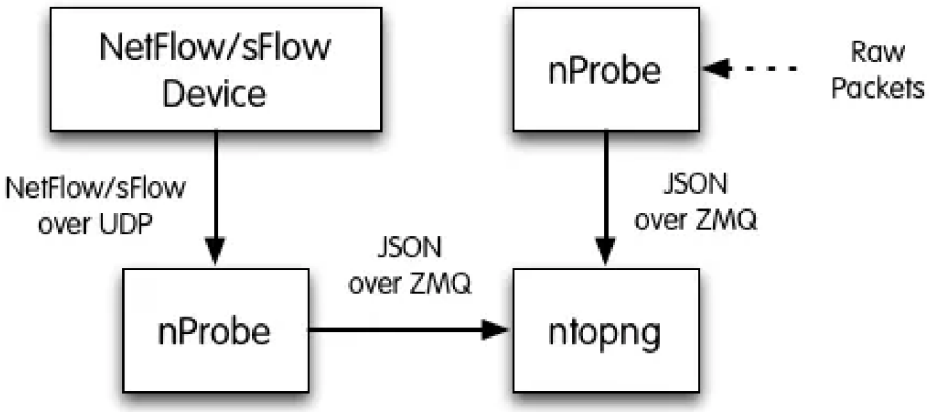
```
sudo yum install pfring-dkms n2disk nprobe ntopng cento
```

Během instalace je potřeba potvrdit stažení, jinak není potřeba nijak reagovat. To je k instalaci vše a dále je potřeba nakonfigurovat kolektor a analyzér.

Nyní přichází na řadu konfigurace Nprobe. U něj je potřeba nastavit režim fungování do módu kolektor, a to z toho důvodu, že jej lze využívat v dalších dvou módech. Dále mu musíme říci, na kterém portu má naslouchat, aby zachytával sFlow datagramy. Příkaz bude vypadat následovně:

```
nprobe -3 6343
```

Kde, -3 znamená provoz v módu kolektoru a 6343 je port, kam sFlow posílá své datagramy. Takto nastavený kolektor bude zachytávat požadované sFlow a bude s ním korektně pracovat. U kolektoru není potřeba nic jiného konfigurovat. Automaticky předává data analyzéru Ntopng. Jak mezi sebou dva dané SW komunikují je vidět na následujícím obrázku č. 16.



Obr. 16: Schéma komunikace nProbe s ntopng (25)

Aby nProbe začal fungovat je potřeba ho spustit. O to se postará následující příkaz:

```
sudo systemctl start nprobe
```

Nyní je nProbe spuštěn a funguje, jak je potřeba. Dále je potřeba nakonfigurovat a spustit analyzér Ntopng.

Ntopng funguje jako webová aplikace. Aby fungovala, potřebuje prostředí. Na serveru může být spuštěna na localhostu a následně se bude dát k serveru připojovat, přes jeho IP

adresu, a tak se bude kdokoliv s přístupovými údaji moci připojit odkudkoliv z firemní sítě k monitoringu. První potřebný příkaz je následující:

```
ntopng -i tcp://127.0.0.1:5556
```

Tento příkaz říká, že má analyzér běžet na localhostu na portu 5556. Následně musíme říci kolektoru, aby posílal data právě na tuto adresu localhostu. To zajistí následující příkaz:

```
nprobe --zmq "tcp://*:5556" -i none -n none --collector-port 6343 -T
```

Nezbytnou součástí je povolení používaných portů na firewallu OS. Na CentOSu je to Firewalld. Pokud by se tak nestalo, tak by Firewalld porty blokoval a nedošlo by k monitorování sítě.

```
sudo firewall-cmd --permanent --add-port=6343/tcp
```

Tento příkaz povolí danému portu komunikovat, aniž by ho firewall blokoval. Je potřeba zadání příkazu opakovat a pokaždé přidat číslo daného portu. V našem případě je potřeba zadat ještě port 5556. V základu je nastavení zobrazení Ntopng na port 3000. Pro náš konkrétní případ jsem port přepnul na port 80. Ten je taky potřeba přidat do neblokovaných portů firewallem. V poslední řadě je potřeba resetovat a spustit všechny služby. To zařídí následující sada příkazů:

```
sudo systemctl restart nprobe

sudo systemctl restart firewall

sudo systemctl start ntopng
```

Nyní je vše nastaveno tak, jak je potřeba. Pokud bude potřeba nastavit další konfigurační možnosti, lze je nastavit v konfiguračních souborech nprobe.conf a ntopng.conf.

Pro potvrzení funkčnosti stačí přejít do webového prohlížeče na počítači, který je ve firemní síti, zadat IP adresu serveru, port a monitoring by měl fungovat. V našem případě je adresa následující:

```
http://10.253.2.201:80
```

Monitoring zobrazí uživateli přihlašovací okno. Pro prvotní přihlášení slouží přihlašovací údaje – login: admin, heslo: admin. Následně ntopng požádá uživatele o změnu hesla a po zadání se zobrazí základní nástěnka monitoringu ntopng.

3.7.2 Prostředí ntopng

Software ntopng od Ntop má velice jednoduché, přehledné, ale funkční zobrazení. Pozadí aplikace je buď světlé, nebo, jak je oblíbené v dnešní době, v tmavém provedení.

Vrchní lišta zobrazuje v prvé řadě (bráno zleva doprava) možnost přepínání monitorovaných rozhraní. V našem případě je pouze jedno. Dále provoz na síti ukazovaný v upload/download Mbit/s. Následuje zobrazení sumarizovaných ukazatelů pro počet toků, zařízení, varovných hlášek atp. Ke konci vrchní lišty najdeme vyhledávání, oznamovací centrum a ikonu pro uživatele, kde jsou možnosti spojené s jeho účtem.

Na levé straně je lišta s jednotlivými položkami. Položky rozeberu jednotlivě shora dolů.

Dashboard/Nástěnka

Nástěnka zobrazuje základní sdělení a lze se přes ní dostat na ostatní položky menu. Zobrazuje aktuální stav dění na síti v přehledných grafech. V nichž zobrazuje IP adresy zařízení, které aktuálně vytěžují nejvíce síť, stejně tak porty a aplikace. Nástěnka je taktéž uvítací obrazovka Ntopng.

Alerts/Upozornění

Zde jsou historicky zaznamenávány upozornění týkající se chyb, netypického dění, varování, dosažení limitů apod.

Flows/Toky

Podrobný historicky řazený výpis toků. U každého toku je vidět o jakou šlo aplikaci, protokol, jeho cestu, dobu trvání, přenesená data a další. Všechny možnosti se dají filtrovat.

Hosts/Hostitelé

Položka hostitelé zobrazuje všechny hostitele podle jejich IP adres, kteří v síti vykonaly nějakou činnost. Jsou řazeni historicky a dají se filtrovat mnoha způsoby. U každého

hostitele se dá zjistit jeho vytěžování sítě, jaké protokoly, aplikace využívá nejvíce, kolik přenesl dat, jeho toky a mnoho dalšího.

Interface/Rozhraní

V podstatě zobrazuje to samé jako Hosts, ale souhrnně pro celé rozhraní. Za zmínku zde stojí přehled, který zobrazuje vytížení rozhraní (firemní sítě) historicky v grafu. Lze tak například vypozorovat výkonost celé firmy z hlediska zpracovaných dokumentů klientů v určitém období.

Settings/Nastavení

Ntopng disponuje opravdu širokou možností nastavení. Kromě běžných nastavení uživatelů, prostředí, umožňuje například nastavit i upozornění, pokud by uživatelé navštěvovali nepovolené stránky či aplikace. Lze zde i nastavit kategorie stránek a aplikací, které uživatelé navštěvují nejčastěji a řadit je tak do skupin. Taktéž je možné ručně nastavovat všechny možné nastavení týkající se opatření hrozeb.

Developer/Vývojář

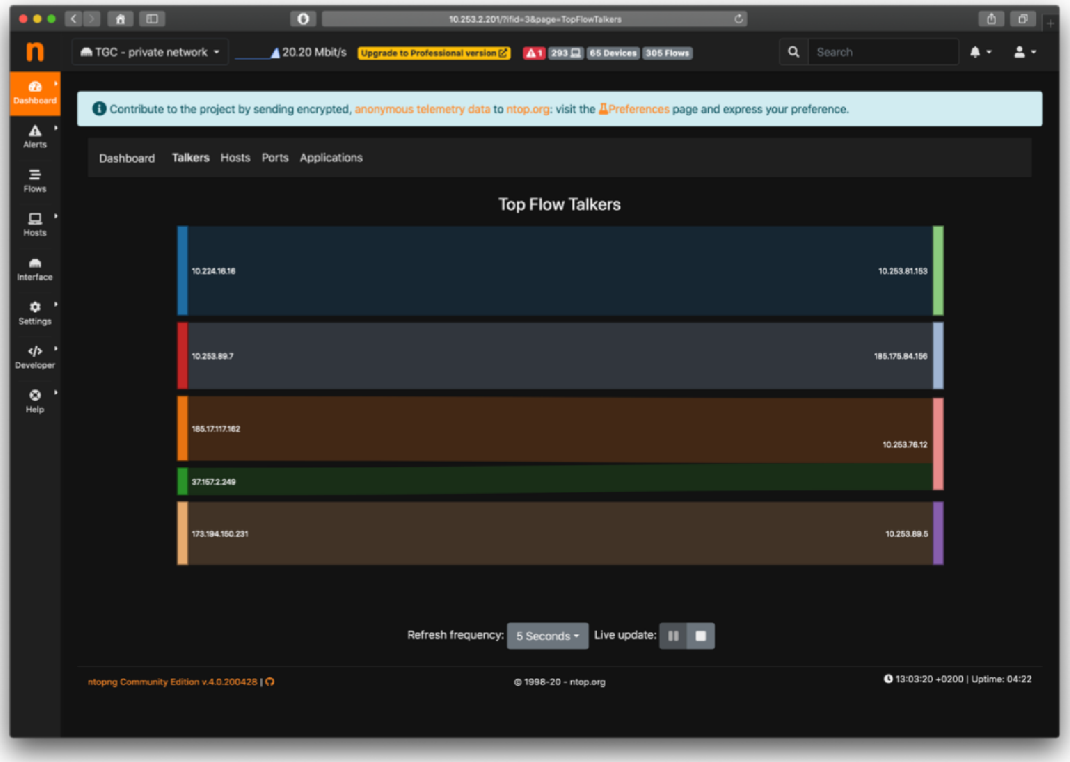
Tato sekce má na starost správu pluginů a především správu vlastních skriptů. Vlastní skripty lze využít pro konkrétnější akce, které se stanou při propuknutí bezpečnostních událostí.

Poslední položkou je Help/Nápověda. Ta poskytuje nápomocnou dokumentaci.

Ntopng ukládá data na harddisk serveru. Z něhož je možné číst data zpětně do minulosti. Lze například tvořit přehledy výkonnosti jednotlivých uživatelů, oddělení firmy apod.

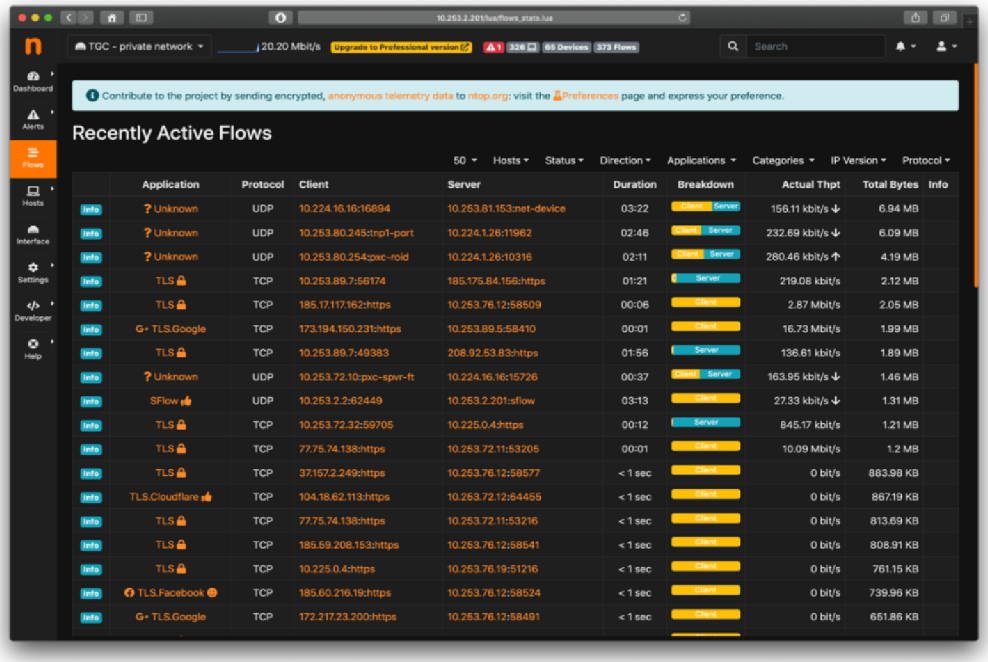
3.7.3 Produkční provoz

V této části předvedu výstup produkčního provozu nasazeného Ntopng monitoringu na firemní privátní síti. Ntopng pracuje v produkčním provozu, tak jak se od něj očekává. Dle momentálního dění v danou dobu ukazuje informace, které se dají považovat za skutečné. Všechny statistiky se obnovují dle nastavení, ale v mém případě jsem si nastavil obnovovací frekvenci zobrazení na 5 sekund. Tzn., že každých 5 sekund se zobrazí aktuální situace dění na síti. Zobrazení aktuální situace provozu znamená vypsání právě probíhajících toků na interní firemní síti. Všechny přijaté datagramy se ukládají přímo na HDD serveru, na kterém je monitoring.



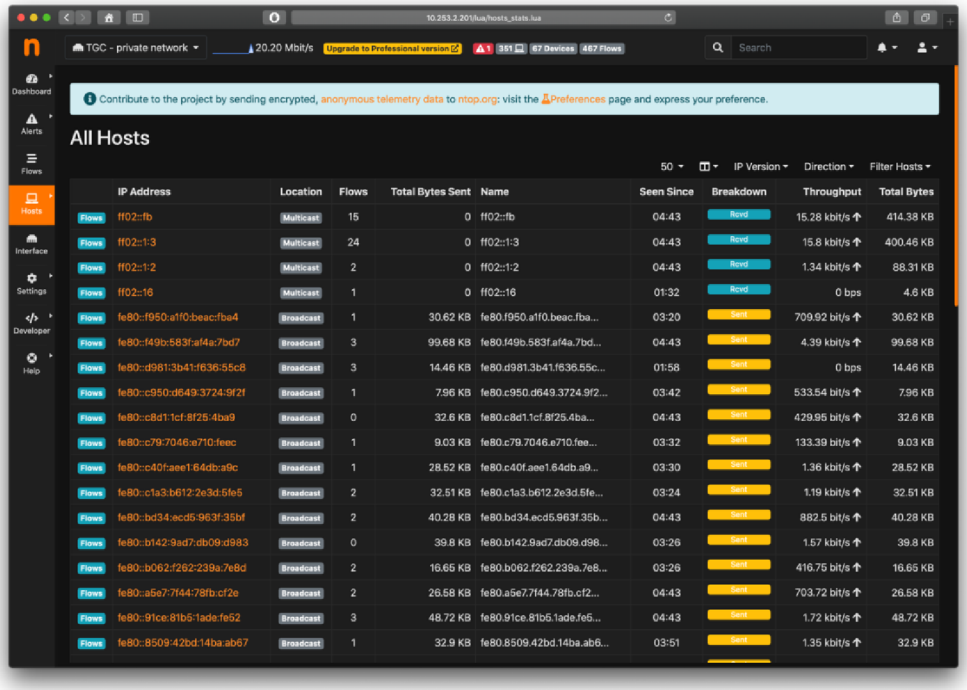
Obr. 17: Nástěnka monitoringu Ntopng (vlastní zpracování)

Na obrázku č. 17 je vidět nástěnka monitoringu Ntopng, na které jsou vidět aktuální toky, které nejvíce vytěžují síť. Tok je vždy zobrazen s počáteční a konečnou IP adresou. Dále je možné ze základního zobrazení vidět v horní liště počet aktuálně komunikujících zařízení, počet aktuálních toků či upozornění na netypickou událost na síti, jako v mém případě.



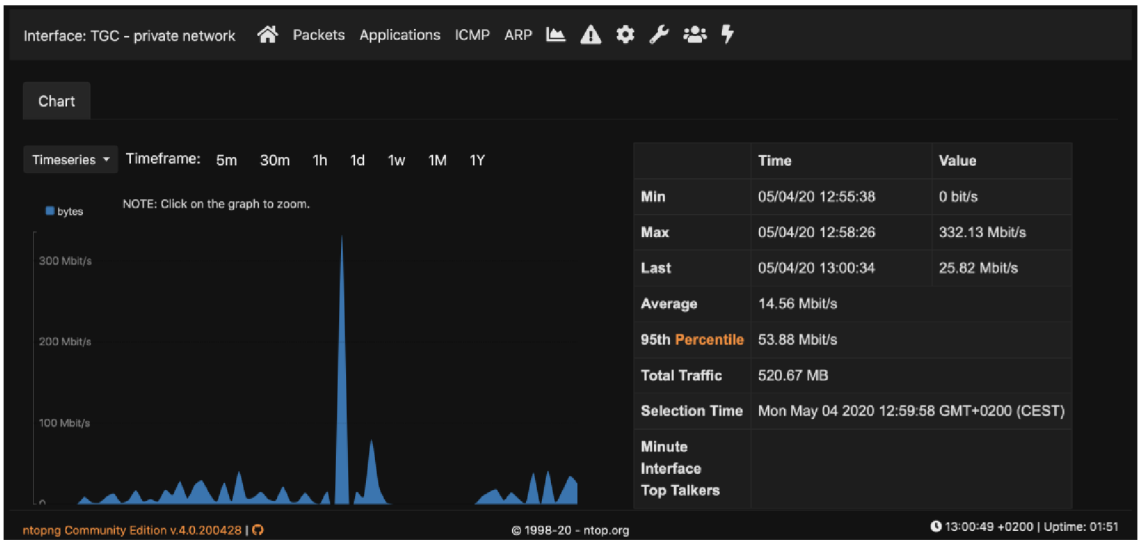
Obr. 18: Monitoring Ntopng – přehled posledních toků (vlastní zpracování)

Užitečným přehledem je zobrazení toků, které je možné různě filtrovat. Přehled zobrazuje aplikaci, použitý protokol, adresy klienta a serveru, které je možné dále rozkliknout, dobu trvání relace, přenesené bity.



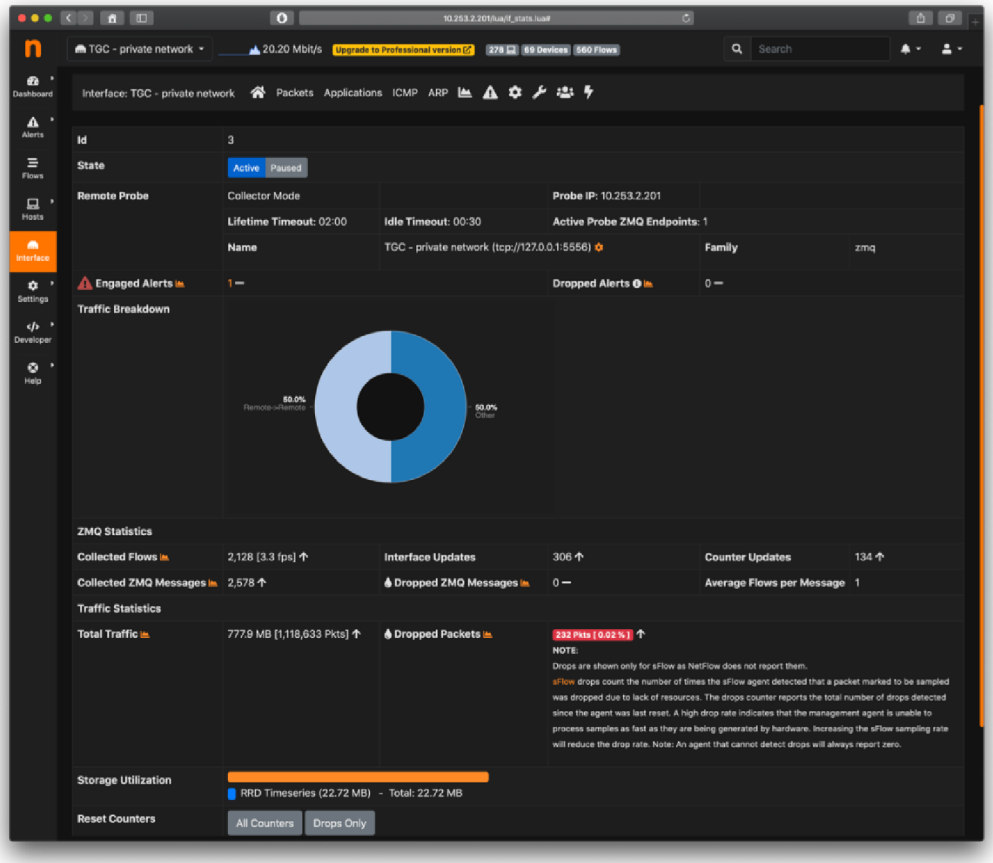
Obr. 19: Monitoring Ntopng – přehled hostů (vlastní zpracování)

Dalším přehledem je zobrazení všech Hosts na síti, který navazují nebo navazovaly komunikaci. Jsou zde taktéž rozmanité možnosti filtrování, stejně tak jako detail po rozkliknutí každého zařízení.



Obr. 20: Monitoring Ntopng – přehled hostů (vlastní zpracování)

Velice užitečným nástrojem je zobrazování historických statistik jako je ta na obrázku č. 20. Z takové statistiky lze například vypozorovat trend provozu či momenty, kdy je síť přetížena. Na obrázku je krátká statistika z pěti minutového provozu v době ladění funkčnosti monitoringu, proto je zde extrémní vrchol i propad v objemu provozu dat na síti. Jak je ale vidět v časové ose, lze nahlédnout až 1 rok zpětně.



Obr. 21: Monitoring Ntopng – celkový přehled rozhraní (vlastní zpracování)

V neposlední řadě je na obrázku č. 21 přehled statistik celého rozhraní, tedy firemní privátní sítě. Zobrazená data jsou zachycena za krátkou dobu provozu, v podstatě ihned po započetí běhu monitoringu.

Monitoring Ntopng samozřejmě obsahuje další funkcionality, zde jsem uvedl pouze některé z nich. Dalšími užitečnými funkcemi mohou být především notifikace, upozornění a výstrahy, které se dají upravovat na míru. Ty se dají například zasílat na e-mail. Lze i nastavit detekci botnetu. Díky možnosti přidání vlastního skriptu je možné schopnosti monitoringu široce obohacovat.

Výběr tohoto monitoringu splňuje téměř všechny požadavky, které byly před výběrem stanoveny. Nesplňuje pouze dva požadavky. Prvním je vytvoření mapy sítě, která se však dá vyřešit dokoupením pluginu v hodnotě cca 15 euro. Druhým nesplněným požadavkem je licence. Byla požadována open-source. Tuto licenci má pouze jedna část monitoringu

– Ntopng, druhá – nProbe, je zpoplatněna. Nicméně částka 50 dolarů je zanedbatelná a firmou přijatelná.

3.8 Ochrana proti úniku dat

Firma Zeus Solutions vyžívá dlouhodobě služeb společnosti T-mobile. Využívá balíček služeb Managed FireWall. Je rozsáhlý a stojí měsíčně značný obnos peněz. Ochrana proti úniku dat je součástí firewallu FortiGate, který je používán na firemní síti společnosti TGC. U Fortinetu má toto řešení název Data Leak Prevention (DLP), neboli prevence proti úniku dat. Toto řešení zatím nebylo zprovozněno. Proto vidím jako příležitost DLP nakonfigurovat a spustit. Řešení by značně pomohlo snížit rizika dvou zmíněných hrozeb. Z toho důvodu řadím DLP do opatření rizik. Z tohoto důvodu nemá smysl porovnávat či vybírat jiné služby tohoto typu, protože by se investice do zavádění nového balíku služeb podobného typu nemohla nikdy vyplatit. Zůstanu tedy u služby FortiGate DLP.

3.8.1 Požadované/zakázané soubory

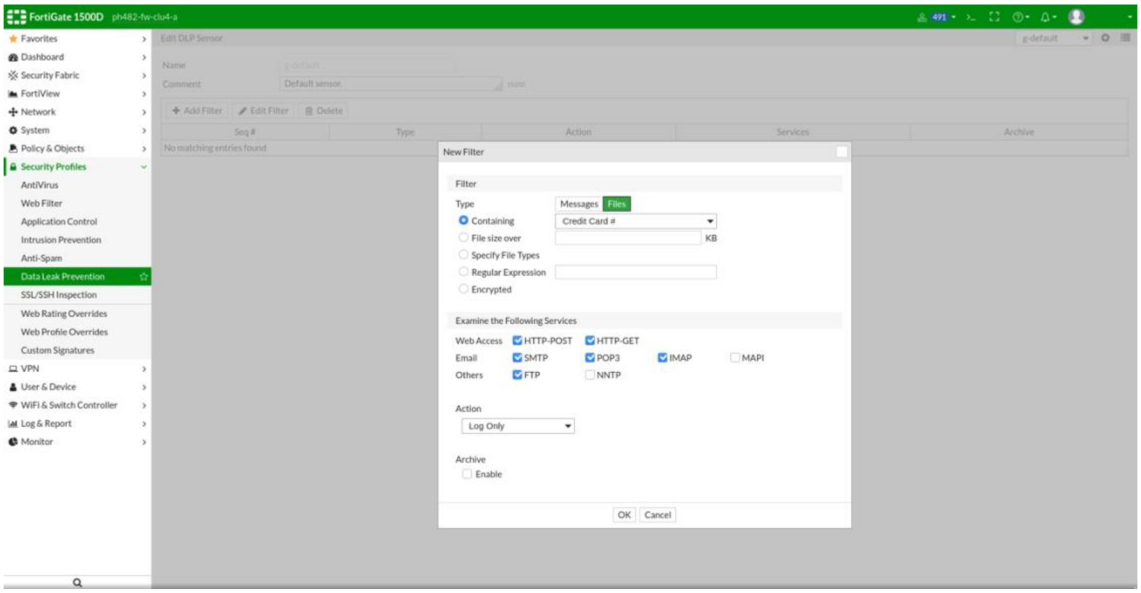
Zde popíši pravidla, jakými se DLP bude řídit. V rámci podnikatelského zaměření společnosti TGC pracují zaměstnanci backoffice s několika typy dobře specifikovatelných souborů. Pravidla platí pro odchozí, ale i příchozí soubory.

Pravidla:

- Soubory můžou mít maximální velikost 20 MB.
- Požadované typy souborů:
    - PDF,
    - Doc, docx, xls, xlsx, txt, odt,
    - Jpg, jpeg,
    - Png.
- Všechny ostatní soubory budou pro zaměstnance mající přístup k datům klientů zakázané.

3.8.2 Nastavení

Nastavení DLP probíhá velmi komfortně a jednoduše. Nastavení se skrývá v základním zobrazení FortiGatu v menu – Security Profiles – Data leak Prevention. Zde probíhá nastavení daných pravidel pomocí filtrů. Pro naše požadavky musí být nastaveno více filtrů. První filtr je nastavení omezení velikosti. Další filtry budou pro nastavení přijímaných a odesílaných souborů. Všechna nastavení se řídí dokumentací FortiGatu.



Obr. 22: Prostředí FortiGate – nový filtr DLP (vlastní zpracování)

3.9 Produkční režim

Žádoucím stavem v produkčním provozu obou opatření je, aby opatření fungovala bez nutnosti zásahů zaměstnance IT. Počítá se ovšem s případnou správou v případě nutnosti.

3.9.1 Provozní režim monitorovacího systému

Jak již bylo zmíněno v kapitole *3.3 Monitorované události*, monitorovací systém bude sledovat předem nadefinované události a v případě propuknutí hrozby bude notifikovat příslušnou osobu. Pro nastavení specifikace každé hrozby se využije prostředí nastavení monitorovacího systému Ntopng. Mnou vybrané řešení tuto možnost má a pokud zmiňované definované události nastanou, propukne hrozba, která se změní v bezpečnostní incident, nadefinované sledování zareaguje a odešle e-mail odpovědné

osobě. Každé hrozbě bude přiřazena odpovědná osoba, která bude odpovědná za její řešení. Nebude notifikovaná pouze jedna osoba, ale určí se i osoba, která bude v jejím zastoupení.

Počítá se s tím, že monitorovací systém bude v neustálém provozu. Bude tedy připravený kdykoli bude potřeba zareagovat a zamezit tak buď propuknutí hrozby, nebo napomůže snížení dopadu. Nebude tedy potřeba neustálý dohled zaměstnance. Zaměstnanec DevOps bude mít pouze předem plánovaný čas na údržbu, upřesňování metrik a vylepšení monitorovacího systému.

Díky možnosti vytvoření více účtů s různými právy, bude možné vytvořit přístup například i pro management, který bude moci kdykoliv vstoupit do grafického rozhraní monitorovacího systému a podívat se na zaznamenaná data.

3.9.2 Provozní režim ochrany proti úniku dat

V produkčním provozu bude každý filtr DLP na firewallu FortiGate blokovat odchozí i příchozí zakázané soubory dle předem stanovených podmínek. Pokud zablokuje nežádoucí soubor, uloží o této události zprávu do logu. Tato služba poběží zcela samostatně, aniž by potřebovala zásahy obsluhy. Pokud nastane problém v blokování souborů, můžou zaměstnanci IT využít zmíněný log k tomu, aby odhalili případné potíže.

3.10 Návrh udržitelnosti

Se zavedením nových technických řešení do společnosti by měla vzniknout dokumentace a zároveň vnitřní směrnice a pravidla. Dokumentací se částečně může brát i tato práce, nicméně by se dokumentace měla doplnit o další informace z následné finální implementace. Zároveň by u směrnic měly být vedené odpovědnosti.

Odpovědnost za monitoring a DLP

Odpovědnost za technické provedení, správu a údržbu bude mít DevOps tým firmy Zeus Solutions. Konkrétně zaměstanec s pozicí linux administrátor/administrátor sítě. Bude mít v měsíčním plánu vyhrazený čas pro správu. Zároveň pokud přijde incident spojený

s monitoringem a DLP, bude mít na starost jeho řešení. Tento zaměstnanec bude mít zastoupení v podobě kolegy z DevOps na pozici IT specialista.

Odpovědnost za výskyt hrozeb

Hrozby budou rozděleny dle typů a každé hrozbě bude přidělena odpovědná osoba. U hrozeb technického původu budou chodit notifikace na technickou podporu – DevOps. U ostatních hrozeb bude odpovědnou osobou, které přijde upozornění, vedoucí daného oddělení. Vedoucí bude řešit problém přímo se zaměstnancem nebo s DevOps. Přehled odpovědností je v následující tabulce.

Tabulka 12: Tabulka odpovědností (vlastní zpracování)

Hrozba	Odpovědná osoba
Krádež dat zaměstnance	Vedoucí oddělení backoffice
Poškození dat zaměstnancem	Vedoucí oddělení backoffice
Nezamknutý počítač	DevOps, Vedoucí oddělení backoffice
Chyba SW	DevOps
Chyba HW	DevOps
DDoS útok	DevOps
Krádež (vlivem viru)	DevOps, Vedoucí oddělení backoffice

Statistiky

Za každý uplynulý měsíc je vyžadováno dodávat statistické reporty managementu společnosti TGC. Reporty budou obsahovat přehledy výkonosti zaměstnanců, nejnavštěvovanější adresy, nežádoucí adresy, zatížení sítě a další reporty, které si management vyžádá dle možností monitoringu.

Přizpůsobení měření

Zároveň s měsíčními statistikami bude vyhodnocovat měření za poslední měsíc zaměstnanec DevOps, který má na starost monitoring, se svým vedoucím, aby se měření neustále zpřesňovalo. A to tak, aby stanovené metriky odpovídaly co nejvíce skutečnému dění a neohlašovaly falešné události.

3.11 Analýza rizik po implementaci opatření

Na závěr, po implementaci opatření, jsem opět provedl analýzu rizik pro porovnání. Výhodou po zavedení opatření je především včasné varování zodpovědných zaměstnanců, kteří mohou okamžitě zasáhnout, a tak hrozbu zažehnat nebo minimálně snížit její dopad. Dále došlo ke zvýšení ochrany práce s daty, čímž se snížila míra rizika u hrozeb, kde hraje roli zaměstnanec s přístupem k datům.

Tabulka 13: Porovnání hodnoty rizik po aplikaci opatření (vlastní zpracování)

Aktivum	Incident	Událost	Hrozba	Riziko	Riziko (po aplikaci opatření)
Informace	Neoprávněné získání dat	Útok počítačového viru	Zašifrování dat	2	2
			Smazání dat	1	1
			Poškození dat	2	2
			Únik dat - krádež	2	2
		Nelegální činnost	Krádež dat zaměstnancem	4	2
			Úmyslné poškození dat zaměstnancem	4	2
	Interní získání dat	Nedbalost zaměstnance	Nezamknutý počítač	4	3
		Nelegální činnost	Krádež dat zaměstnancem	5	3
			Úmyslné poškození dat zaměstnancem	5	3
	Zneužití dat	Neoprávněné vniknutí	Krádež dat	2	2
		Technické selhání	Selhání HW	3	3
			Chyba SW	4	2
	Poškozená data	Technické selhání	Selhání HW	2	2
			Chyba SW	3	3
		DDoS útok	Zkolabování firemní počítačové sítě	3	2
	Nedostupná data	Útok počítačového viru	Zašifrování dat	2	2
			Smazání dat	2	2
			Poškození dat	2	2
			Únik dat - krádež	3	2
		Technické selhání	Selhání HW	2	2
			Chyba SW	3	3
		DDoS útok	Zkolabování firemní počítačové sítě	3	3

3.12 Ekonomické zhodnocení

Jedním z požadavků investora byly minimální náklady za implementaci monitoringu. Vzhledem k tomu, že licence na kolektor vyjde na 1250 Kč, tak si myslím, že požadavek byl splněn a tato zanedbatelná částka nebude překážkou. Další položkou, se kterou se ovšem počítalo je cena za rutinní správu a operativu. Kapacity zaměstnance na DevOps se tak patrně zvýší o nízké jednotky MD za měsíc. Celkově odhaduji, že by toto řešení stálo za první rok provozu necelých 73 000 Kč.

3.13 Doporučení pro management

Z návrhu vlastního řešení mohu doporučit použití navrhovaných řešení. Hlavním cílem bylo snížení rizika a dopadu u hrozeb, kde konfiguruje zaměstnanec, což se podařilo. Navrhl jsem sledovat toky pomocí monitorovacího systému od firmy Ntop a používat ochranu proti úniku dat ve firewallu FortiGate. Obě řešení využívají stávající HW vybavení společnosti a jejich implementace bude stát opravdu minimální náklady. Řešení splnily téměř všechny požadavky investora.

Jediná patrná nevýhoda řešení je absence monitoringu na tocích vedoucí přes firewall ze sítě ven. Jedná se především o absenci monitoringu uživatelů sítě, kteří se připojují přes VPN. Pro tento případ mohu do budoucna doporučit nákup FortiClienta, upgradovat stávající balíček Managed Firewall o další stupeň, kde bude i FortiAnalyzer a sledovat s ním provoz, který jde přes firewall FortiGate. To by mělo za následek sledování provozu i na VPN. Zároveň by bylo možné i logování na koncových zařízeních. Toto řešení je ovšem značně dražší.

ZÁVĚR

Základní myšlenkou této práce bylo zvýšení zabezpečení firemní privátní sítě holdingu TGC, redukování a snížení dopadu hrozeb, především proti úniku dat klientů ze společnosti. Ve firmě se pracuje se soukromými daty klientů, které je potřeba chránit a zamezit jejich úniku mimo síť. Vzhledem k tomu, jaké bezpečnostní prvky firma již používá, bylo navržení mnou zvolených komponent na základě analýzy současného stavu, logickým krokem kupředu.

Z počátku práce jsem uvedl základní teoretická východiska nutná pro pochopení této diplomové práce. Následně jsem v analýze současného stavu představil firmu TG Community Holding, a.s., udělal analýzu ICT, znázornil práci s daty ve společnosti a především, udělal analýzu rizik informačního aktiva, což bylo stěžejním bodem této práce. Z analýzy rizik mi vzešly hrozby působící na informace ve společnost. Ve vlastním návrhu řešení jsem se zabýval výběrem opatření, které by redukovaly hrozby. Předem jsem definoval události navázané na hrozby. Tyto události byly nastaveny jako možné scénáře propuknutí hrozeb a popsal jsem jejich implementaci do opatření. Jako opatření jsem vybral monitorovací systém počítačové firemní sítě a ochranu proti úniku dat ze společnosti na firewallu. První zmíněné opatření má i mnoho dalších využití, ale především bude okamžitě informovat odpovědné osoby o stavu, kdy hrozba nastala nebo, že může potencionálně nastat. Druhé opatření bude v produkčním provozu v reálném čase filtrovat procházející soubory přes firewall. Tím se zamezí nežádoucím souborům (zakázané typy souborů a omezená velikost na soubor) v průchodu z nebo do sítě. V závěru vlastního návrhu řešení jsem udělal opětovnou analýzu rizik, kde jsem znázornil reálné snížení rizik po aplikaci opatření.

Ve vlastním návrhu řešení jsem se snažil co nejvíce vyhovět požadavkům investora. Především kvůli požadavku na minimální náklady je mnou zvolené opatření monitorovacího systému kompromisem. Lepším řešením, tak jak jsem uvedl i v doporučení pro management, by bylo rozšíření služeb od firmy Fortinet a monitorovat jak provoz na VPN, tak i na koncových zařízeních ve firemní síti. Toto řešení by mělo vyšší účinnost ve snížení rizik.

SEZNAM POUŽITÉ LITERATURY

1. JORDÁN, Vilém a Viktor ONDRÁK. *Infrastruktura komunikačních systémů III: integrovaná podniková infrastruktura*. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-214-5241-1.

2. DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. *Řízení bezpečnosti informací*. Praha: Professional Publishing, 2008. ISBN 978-80-86946-88-7.

3. POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-86898-38-5.

4. ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. ISBN isbn978-80-7204-872-4.

5. JIROVSKÝ, Václav. *Vademecum správce sítě*. Praha: Grada, 2001. ISBN 80-7169-745-1.

6. PUŽMANOVÁ, Rita. Moderní komunikační sítě od A do Z: [technologie pro datovou, hlasovou i multimediální komunikaci]. 2., aktualiz. vyd. Brno: Computer Press, 2006. ISBN 80-251-1278-0.

7. DONAHUE, Gary A. *Kompletní průvodce síťového experta*. Brno: Computer Press, 2009. ISBN 978-80-251-2247-1.

8. HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 4., aktualiz. a rozš. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2073-6.

9. KUROSE, James F. a Keith W. ROSS. *Počítačové sítě*. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

10. Topologie sítí. www.cs.vsb.cz [online]. Dostupné z: http://www.cs.vsb.cz/grygarek/PS/lect/topologie.html

11. ČSN ISO/IEC 27000:2014 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Přehled a slovník. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. 31 s. Třídící znak 369790.

12. ČSN ISO/IEC 27001:2006 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Český normalizační institut, 2006.

13. ČSN ISO/IEC 27002:2005 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2005.

14. ISO/IEC 7498-4:1989 - Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 4: Management framework. [online]. Copyright © All Rights Reserved [cit. 26.01.2020]. Dostupné z: https://www.iso.org/standard/14258.html

15. ONDRÁK, V. Management Počítačových sítí: Lekce 2 – Protokoly pro management sítí. 2013

16. sFlow vs NetFlow: Which is Better for Network Monitoring? plus Monitors. ITPRC – IT Professional's Resource Center [online]. Copyright © 2020. [cit. 26.01.2020]. Dostupné z: https://www.itprc.com/sflow-vs-netflow/

17. Data leak prevention. Fortinet Online Help [online]. Copyright © [cit. 26.01.2020]. Dostupné z: https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/DLP/dlp_chapter.htm

18. Veřejný rejstřík a Sbírka listin – Ministerstvo spravedlnosti České republiky. [online]. Copyright © 2012 [cit. 12.12.2019]. Dostupné z: https://or.justice.cz/ias/ui/rejstrik-firma.vysledky?subjektId=915313&typ=PLATNY

19. Historie firmy | Terra Home. Terra Home – Snižujeme výdaje za elektřinu a plyn [online]. Copyright © Copyright 2020 TG Community Holding, a.s. [cit. 11.01.2020]. Dostupné z: https://www.terrahome.cz/pages/historie-firmy.php

20. TG Community – TG Community Holding a.s. [online]. Copyright © Copyright 2018 [cit. 11.01.2020]. Dostupné z: https://www.tgc.cz/

21. Informace od vedení TG Community Holding a.s.

22. Osobní zkušenosti v TG Community Holding a.s.

23. SSH Protocol – Secure Remote Login and File Transfer. SSH.com [online]. Copyright ©2020 SSH Communications Security, Inc. All Rights Reserved. [cit. 23.04.2020]. Dostupné z: https://www.ssh.com/ssh/protocol/

24. Aruba | Enterprise Networking and Security Solutions. *Aruba | Enterprise Networking and Security Solutions* [online]. Copyright © Copyright 2020 Hewlett Packard Enterprise Development LP [cit. 27.04.2020]. Dostupné z: https://www.arubanetworks.com

25. ntop – High Performance Network Monitoring Solutions based on Open Source and Commodity Hardware. ntop – High Performance Network Monitoring Solutions based on Open Source and Commodity Hardware. [online]. Copyright © 1998 [cit. 03.05.2020]. Dostupné z: https://www.ntop.org/

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

TGC – TG Community Holding a.s.

ICT – Information and Communication Technologies

IT – Information Technologies

HW – Hardware

SW – Software

OS – Operační Systém

VPN – Virtual Private Network

HP – Hewlett-Packard

CRM – Customer relationship management

BM – Bussines Maker

IT OPS – Information Technology Operations

ISMS – Information Security Management Systém

MD – Man Day

DLP – Data Leak Prevention

DevOps – Development and Operations

SEZNAM OBRÁZKŮ

SEZNAM TABULEK