VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

IMPLEMENTACE ZVOLENÉ TECHNOLOGIE PRO MONITOROVÁNÍ SÍŤOVÉHO PROVOZU V REÁLNÉM PROSTŘEDÍ

IMPLEMENTATION OF SELECTED TECHNOLOGY FOR THE NETWORK TRAFIC MONITORING IN REAL ENVIRONMENT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. Diana Ujhelyiová

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Viktor Ondrák, Ph.D.

BRNO 2022

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Studentka:	**Bc. Diana Ujhelyiová**
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2021/22
Studijní program:	Informační management

Garant studijního programu 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:

Implementace zvolené technologie pro monitorování síťového provozu v reálném prostředí

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 sítě.

Základní literární prameny:

BIGELOW, S. J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. Brno: Computer Press, 2004. 990 s. ISBN 80-251-0178-9.

DONAHUE, G. A. Kompletní průvodce síťového experta. Brno: Computer Press, 2009. 528 s. ISBN 978-80-251-2247-1.

JULIAN, M. Practical Monitoring. Kalifornia, USA: O'Reilly Media, Inc., 2017. 167 s. ISBN 978-1-491-95735-6.

LIGUS, S. Effective Monitoring and Alerting. Kalifornia, USA: O'Reilly Media, Inc., 2012. 166 s. ISBN 978-1-449-33352-2.

MORRIS, S. B. Network Management, MIBs and MPLS: Principles, Design and Implementation. 1.vyd. New Jersey: Pearson, 2003. 416 s. ISBN-13: 978-0-13-101113-7.

SOSINSKY, B. Mistrovství - počítačové sítě. Brno: Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2021/22

V Brně dne 28.2.2022

L. S.

doc. Ing. Miloš Koch, CSc. garant	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Diplomová práca sa zameriava na analýzu monitoringu siete a implementáciu zvolenej technológie v reálnom prostredí. Výskum je robený vo zvolenej organizácie, ktorá nechce byť menovaná a sídli na Slovensku.

V teoretickej časti sa zaoberám základnými poznatkami – čo je to sieť, monitoring siete, aktívum a jeho klasifikácie. V praktickej časti práca bližšie špecifikuje monitorovací systém firmy – silné a slabé stránky, riziká a návrh zmien k zvýšeniu efektívnosti monitorovania a upozorňovania na budúce problémy.

Abstract

The master thesis focuses on the analysis of network traffic monitoring in a selected company and the implementation of selected technology in the real environment. The research is made in the small organization, which does not want to be named and is based in Slovakia.

In the theoretical part I deal with basic knowledge - what is information, data and information system. In the practical part, the thesis specifies the company information system - strengths and weaknesses of the organization, risks and proposal of changes to increase the efficiency of work with the company IS.

Kľúčové slová

monitoring, optimalizácia, sieťový manažment, upozorňovací systém, sieťová prevádzka, LibreNMS

Key words

monitoring, optimalization, network traffic management, alerting system, network, LibreNMS

Bibliografická citácia

UJHELYIOVÁ, Diana. *Implementace zvolené technologie pro monitorování síťového provozu v reálném prostředí* [online]. Brno, 2022 [cit. 2022-05-09]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/139469. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky.
Vedoucí práce Viktor Ondrák.

Čestné prehlásenie

Prehlasujem, že predložená diplomová práca je pôvodná a spracovala som ju samostatne. Prehlasujem, že citácia použitých prameňov je úplná a že som vo svojej práci neporušila autorské práva (v zmysle Zákona č. 121/2000 Sb., o práve autorskom a o právach súvisiacich s právom autorským).

V Brne dňa

……..

Diana Ujhelyiová

Poďakovanie

Chcela by som poďakovať môjmu vedúcemu Ing. Viktorovi Ondrákovi, Ph.D. za odbornú pomoc pri vypracovávaní diplomovej práce, predanie odborných znalostí a za ochotu pri jej vedení. V neposlednom rade patrí veľká vďaka mojim rodičom za podporu a manažérov zvolenej firmy za poskytnutie užitočných informácii, ktoré ovplyvnili túto záverečnú prácu.

OBSAH

ÚVOD **11**

CIELE PRÁCE, METÓDY A POSTUPY SPRACOVANIA **12**

1 TEORETICKÉ VÝCHODISKÁ PRÁCE **13**

1.1 Počítačová sieť 13

1.1.1 Rozdelenie sietí podľa rozsahu 13
1.1.2 Rozdelenie sietí podľa topológie 16
1.2 Protokoly 18

1.2.1 CDP – Cisco Discovery Protocol 18
1.2.2 FDP – Foundry Discovery Protocol 19
1.2.3 LLDP – Link Layer Discovery Protocol 19
1.2.4 OSPF – Open Shortest Path First 20
1.2.5 BGP – Border Gateway Protocol 20
1.2.6 SNMP – Simple Network Management Protocol 20
1.2.7 ARP – Address Resolution Protocol 22
1.2.8 STP – Spanning Tree Protocol 22
1.3 Aktívne prvky 22

1.3.1 Repeater (opakovač) 22
1.3.2 Router (smerovač) 23
1.3.3 Switch (prepínač) 23
1.4 Systém riadenia bezpečnosti informácií 23

1.4.1 Základné pojmy ISMS 23
1.5 Aktíva 24

1.5.1 Klasifikácia aktív 25
1.5.2 Zraniteľnosť aktív 26
1.5.3 Identifikácia zraniteľnosti aktív 26
1.6 Riziko 26

1.6.1 Analýza rizík 26
1.6.2 Typy analýzy rizík 26
1.6.3 Kvantifikácia rizík 28

1.6.4 Riadenie rizík 29
1.7 Lewinov model na riadenie zmien 29
1.8 Projektové riadenie 30
1.8.1 Projekt 30
1.9 SLEPTE analýza 31
2 ANALÝZA SÚČASNÉHO STAVU 32
2.1 Popis zvolenej spoločnosti 32
2.1.1 Stratégia firmy 32
2.1.2 Vývoj spoločnosti 32
2.1.3 Organizačná štruktúra 32
2.1.4 Hardvérové vybavenie 34
2.1.5 Softvérové vybavenie 34
2.2 Analýza spoločnosti 34
2.2.1 Identifikácia aktív 35
2.2.2 Identifikácia vlastníkov aktív 35
2.2.3 Klasifikácia aktív spoločnosti 35
2.2.4 Identifikácia zraniteľností aktív spoločnosti 36
2.3 Analýza hrozieb a rizík 38
2.3.1 Identifikácia hrozieb pred implementáciou nástroja LibreNMS 38
2.3.2 Skórovacia metóda pre hrozby pred implementáciou návrhu 38
2.3.3 Mapa rizík skórovacej metódy pred implementáciou návrhu 40
2.3.4 Identifikácia hrozieb pri implementácii nástroja LibreNMS 41
2.3.5 Skórovacia metóda pre hrozby pri implementácii návrhu 42
2.3.6 Mapa rizík skórovacej metódy pri implementácii návrhu 44
2.4 Analýza vonkajšieho prostredia - Analýza SLEPTE 45
2.4.1 Politické faktory 46
2.4.2 Ekologické faktory 46
2.4.3 Sociálne faktory 46
2.4.4 Technologické faktory 47
2.4.5 Legislatívne faktory 47
2.4.6 Ekonomické faktory 48
2.5 Výsledky analýz 50

3 NÁVRH RIEŠENÍ 52

3.1 Dôvody potreby nasadenia technológie 52

3.2 Implementácia navrhovanej zmeny z technického pohľadu 53

3.2.1 Dôvod výberu technológie LibreNMS a pracovnej stanice 53
3.2.2 Riešenie incidentov 54
3.2.3 Organizačné začlenenie technológie 54
3.2.4 Popis vybranej technológie 54
3.2.5 Podpora vybranej technológie 57
3.2.6 Podmienky nasadenia 57
3.2.7 Postup inštalácie v reálnom prostredí 57
3.2.8 Nastavenie jednotlivých parametrov 59
3.2.9 Systém upozorňovania (*alerting*) 63
3.2.10 Monitorovanie prevádzky 64

3.3 Implementácia navrhovanej zmeny z pohľadu projektového riadenia 66

3.3.1 Popis navrhovanej zmeny 66
3.3.2 Lewinov model 68
3.3.3 Časová analýza 72
3.3.4 Časový harmonogram implementácie projektu 72

3.4 Zhodnotenie vlastných návrhov a ich prínosy pre spoločnosť 75

3.4.1 Ekonomické zhodnotenie 75
3.4.2 Prínosy návrhov pre firmu 75
3.4.3 Kvantifikácia prínosov 76
3.4.4 Porovnanie nákladov 76

ZÁVER 78

ZOZNAM POUŽITÝCH ZDROJOV 79

ZOZNAM POUŽITÝCH SKRATIEK A SYMBOLOV 83

ZOZNAM OBRÁZKOV 84

ZOZNAM TABULIEK 85

ZOZNAM PRÍLOH 86

ÚVOD

V tejto záverečnej práci zanalyzujem monitoring siete zvolenej firmy a zároveň navrhnem riešenia pre zefektívnenie monitorovania siete so zvolenou technológiou.

Správne vypracovanie tejto problematiky bude prínosom pre firmy, ktoré majú časté problémy kvôli nedostatočnému sledovaniu siete, a tým pádom nedokážu predchádzať vzniknutým problémom včas.

V prvej kapitole sú spracované teoretické východiska práce, ktoré objasňujú základné pojmy potrebné k pochopeniu problematiky. Vdruhej analyzujem spoločnosť, systém a možné riziká spojené s implementáciou. Tretia kapitola sa zaoberá konkrétnou implementáciou a konfiguráciou vybratej technológie LibreNMS.

CIELE PRÁCE, METÓDY A POSTUPY SPRACOVANIA

Cieľom diplomovej práce je navrhnúť manažment siete v reálnom prostredí. Zvolila som si reálnu IT firmu, ktorá začína využívať technológiu Libre NMS. Vybrané prostredie analyzujem, popíšem nasadenie LibreNMS – jednotlivé kroky inštalácie, možné nastavenie parametrov a na záver zhodnotím prínosy a náklady pre firmu pri implementácii tohto systému na monitorovanie siete.

Čiastočným cieľom tejto práce je zníženie nákladov organizácie, a tým zvýšiť zisk na možný ďalší vývoj alebo na rozšírenie pôsobenia organizácie. Takisto zefektívnenie monitorovania, čo môže predísť budúcim problémom úplne alebo môžu byť vyriešené skôr, ako vôbec nastanú.

Vybranú tematiku popíšem z teoretického hľadiska, vymedzím a vysvetlím používané pojmy na pochopenie problému a neskôr sa v praktickej časti zameriam na samotnú organizáciu a jej monitorovací systému. V záverečnej časti navrhnem implementáciu konkrétneho monitorovacieho systému.

Pre túto diplomovú prácu som si vybrala anonymizovanú firmu, ktorá si prevádzku v sieti monitoruje sama s využitím systému Libre NMS a pomocou vlastného nástroju na monitoring záťaže siete podľa potrieb - na doplňujúce informácie, ktoré Libre NMS neposkytuje (monitorovanie optického pripojenie, televízie), ktorý vyvíjal interný zamestnanec firmy.

1 TEORETICKÉ VÝCHODISKÁ PRÁCE

V prvej kapitole vysvetlím dôležité pojmy a princípy pre správne pochopenie problematiky manažmentu siete. Vysvetlené sú najmä základné termíny, ako počítačová sieť, monitoring, aktívne prvky, čo sú aktíva a riziká a ako sa klasifikujú. Ďalej bližšie rozoberiem pojmy bezpečnostná udalosť, bezpečnostná hrozba a protokoly, ktoré vybraná technológia využíva. V neposlednom rade je definované riadenie rizík a riadenie zmien pomocou Lewinovho modelu a projektový manažment.

1.1 Počítačová sieť

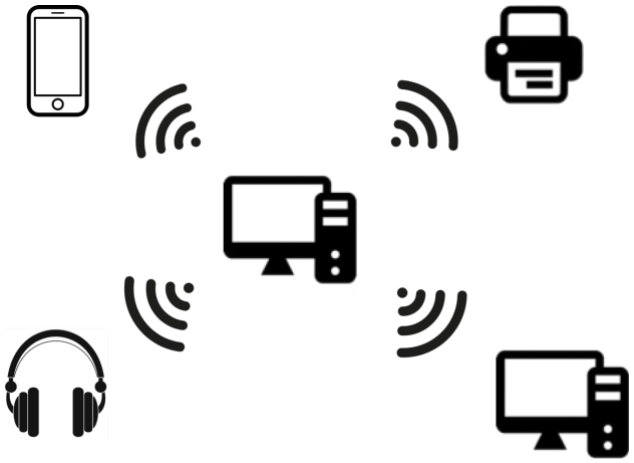
Počítačovú sieť tvorí prepojenie viacerých zariadení, teda počítačov (tzv. hosts), prepojených tak, aby mohli medzi sebou bezproblémovo komunikovať, prijímať a odosielať potrebné dáta. Sieťovými zariadeniami, ktoré pomáhajú počítačom komunikovať môžu byť napríklad router (smerovač), switch, hub alebo aj bridge. Internet je obrovskou počítačovou sieťou. Medzi základné delenia sietí patrí rozdelenie podľa rozsahu a rozdelenie podľa topológie. (2)

1.1.1 Rozdelenie sietí podľa rozsahu

Rozlišujeme 4 kategórie počítačových sietí podľa vzdialenosti dielčich prvkov.

PAN

Osobná počítačová sieť (personal area network) je tvorená viacerými počítačmi v malej vzdialenosti alebo jedným počítačom, ku ktorému sú pripojené ďalšie elektronické zariadenia (napr. tlačiareň, mobilný telefón, bezdrôtové slúchadlá) cez bezdrôtové pripojenie (napr. bluetooth). PAN sieť slúži na prenos a synchronizáciu údajov a má nízku prenosovú rýchlosť (Mb/s). (2)

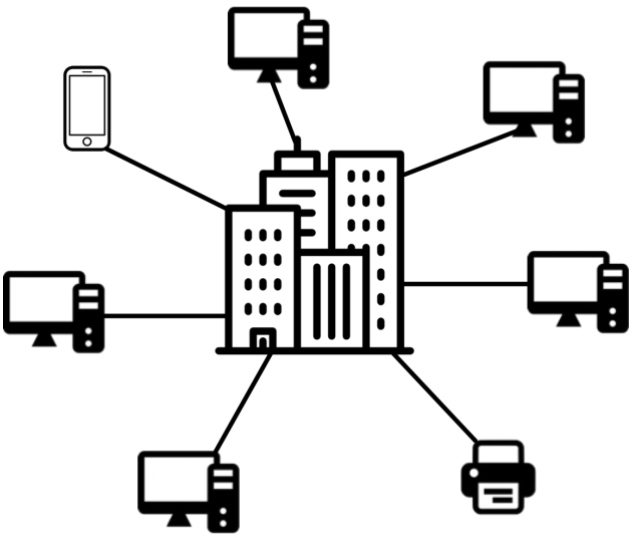


Obrázok č. 1: Sieť PAN

(Zdroj: Vlastné spracovanie podľa 21)

LAN

Lokálna počítačová sieť (local area network) je tvorená zariadeniami, ktoré sú vo vzdialenosti stovky metrov, prípadne niekoľko kilometrov. Je to sieť počítačov v jednej budove alebo v budovách k nej priľahlých, napr. firemná privátna sieť, sieť v kancelárii, byte, či na poschodí. Medzi pripojenými zariadeniami je spojenie neustále s rýchlosťou niekoľkých Gb za sekundu. Dáta sa prenášajú rýchlejšie a s väčším zabezpečením ako v rozsiahlejších sieťach. (2)

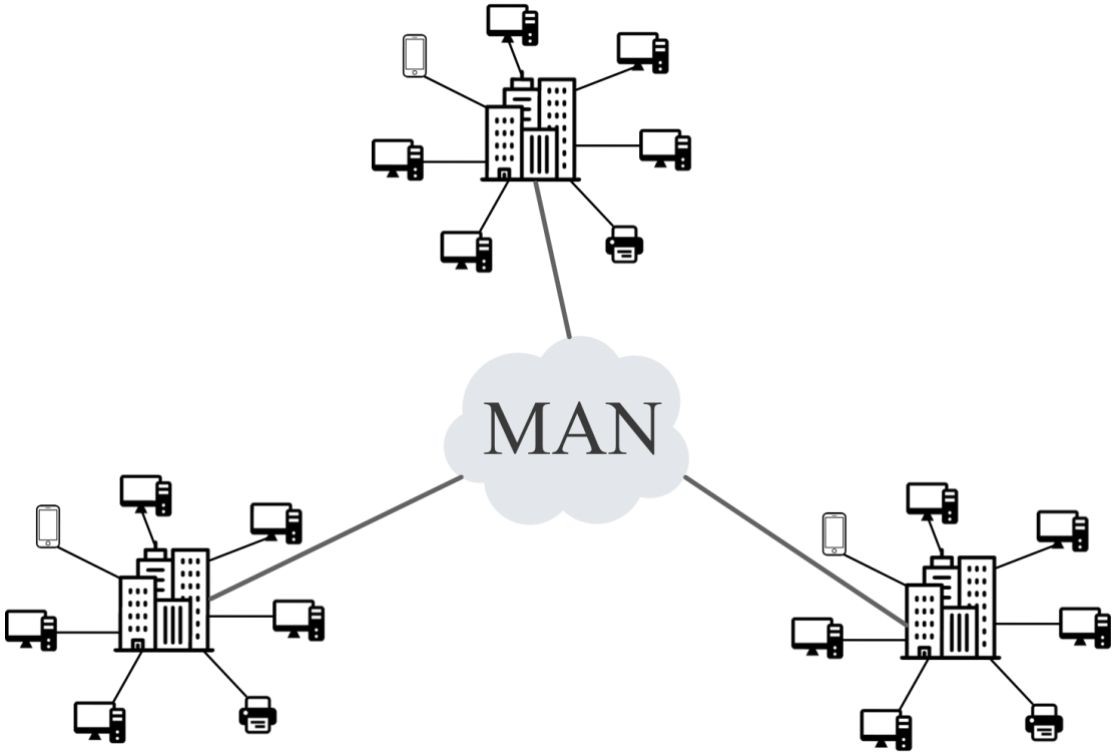


Obrázok č. 2: Sieť LAN

(Zdroj: Vlastné spracovanie podľa 21)

MAN

Mestská sieť (metropolitan area network) je rozsiahlejšia, je tvorená spojením viacerých LAN sietí dokopy pomocou optického pripojenia. Jej dosah je vyšší od LAN a môže to byť napríklad sieť firmy s viacerými budovami a pobočkami. (2)



Obrázok č. 3: Sieť MAN

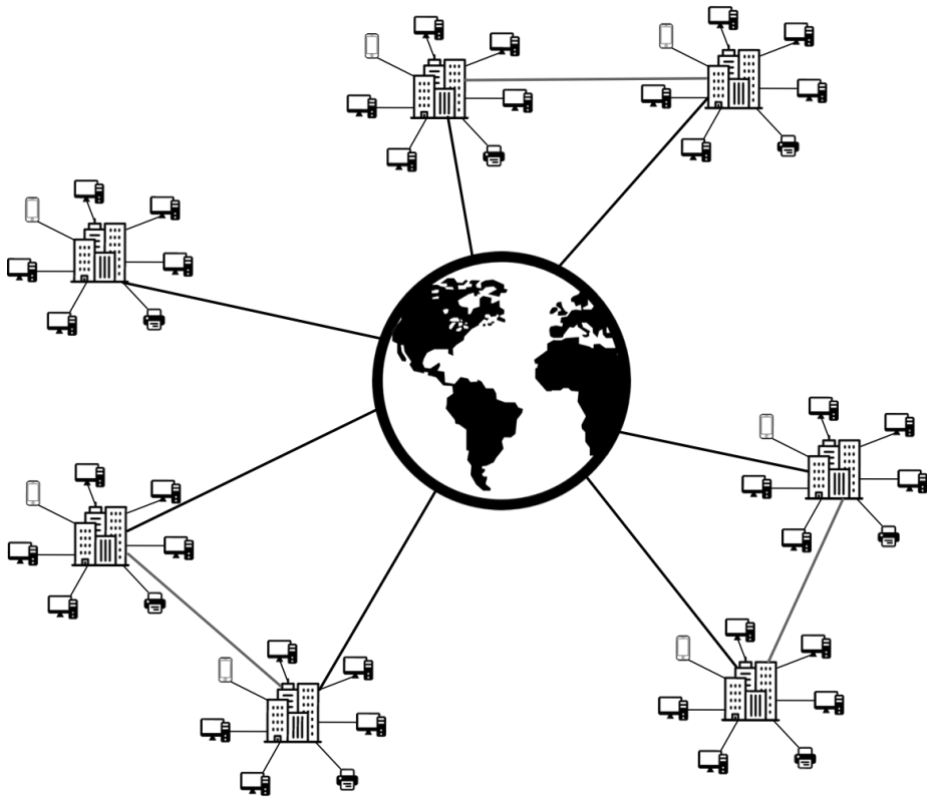
(Zdroj: Vlastné spracovanie podľa 21)

WAN

Rozloha tejto siete je neobmedzená, preto sa nazýva aj sieť rozľahlá (wide area network). Spája zariadenia na území štátu alebo kontinentu pomocou optického alebo satelitného pripojenia. / spojenia

Tento diaľkový prenos údajov je tvorený základným komunikačným kanálom (tzv. backbone) s vysokou prenosovou rýchlosťou cez optické vlákna. K tejto chrbtovej sieti (backbone) sú následne pripojené ďalšie zariadenia a siete. Rýchlosť tejto rozsiahlej siete je v rozmedzí od desiatok kb/s až po niekoľko Gb/s; záleží, či pripojenie zariadení je

trvalé alebo vytáčané. Najväčšou a najznámejšou WAN sieťou je Internet, ktorý má široké využitie v každodennom živote. (2)



Obrázok č. 4: Sieť WAN

(Zdroj: Vlastné spracovanie podľa 21)

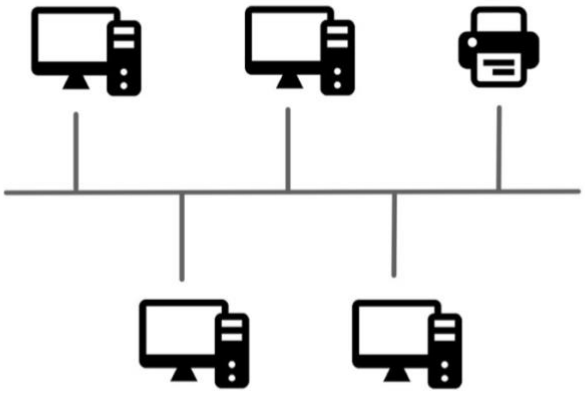
1.1.2 Rozdelenie sietí podľa topológie

Delenie sietí podľa topológie závisí od fyzického umiestnenia uzlov (počítačov a ostatných zariadení), ktoré sú spolu prepojené a komunikujú medzi sebou cez komunikačné kanály. Každá topológia má svoju schému zapojenia kabeláže. Rozpoznávame tri základné fyzické topológie. (8)

Zbernicová topológia (bus)

Topológia bus je najjednoduchšou, kedy zariadenia majú spoločné vedenie a sú prepojené pomocou odbočovacích tzv. T-konektorov. Na konci zbernice sa musí nachádzať ukončovací člen (tzv. terminátor). Výhodou tejto topológie sú nízke náklady na jej realizáciu, avšak kvôli spoločnej hlavnej ceste môžu vzniknúť kolízie v sieti, prípadne

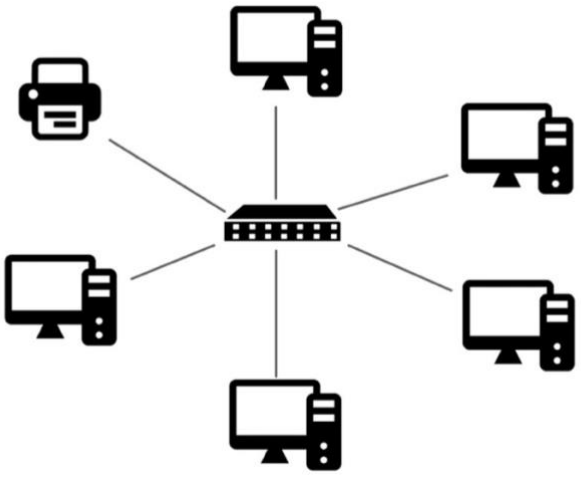
zlyhanie celej siete, ak zlyhá hlavný kábel. Preto je jej použitie dnes už ojedinelé. Proti vzniku kolíziam sa využívajú protokoly linkovej vrstvy (CSMA/CD alebo Pure Aloha). (8)



Obrázok č. 5: Zbernicová topológia
(Zdroj: Vlastné spracovanie podľa 9)

Hviezdicová topológia (star)

Všetky zariadenia topológie star sú pripojené portom k jednému centrálnemu bodu (uzlu), ktorým je switch (prepínač). Náklady na realizáciu sú vyššie ako u topológie bus. A taktiež tu hrozí riziko zrútenia sa celého systému, ak skolabuje jediný prvok – switch.



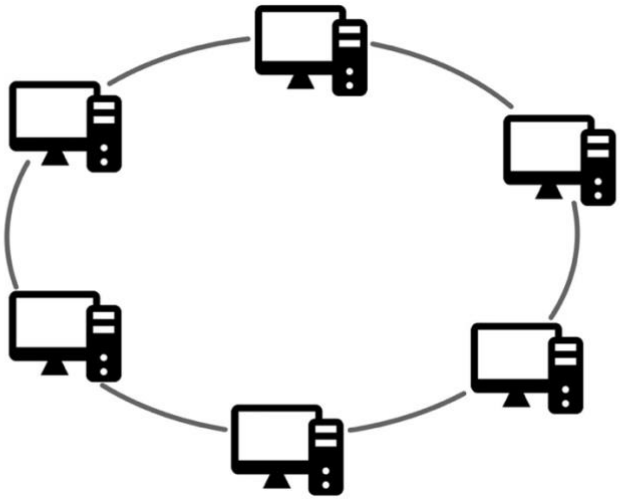
Obrázok č. 6: Hviezdicová topológia
(Zdroj: Vlastné spracovanie podľa 9)

Rozšírená hviezdicová topológia je spojenie viacerých hviezdíc dokopy pomocou switchov (prepínačov) alebo rozbočovačov. (8)

Stromová (hierarchická) – viaceré hviezdice sa prepájajú s počítačom, ktorý kontroluje premávku sietí. (8)

Kruhová topológia (ring)

V kruhovej topológii sú jednotlivé zariadenia zapojené za sebou – prvý s druhým, druhý s tretím, až kým posledný uzol nie je prepojený s prvým. Dáta sa primárne posielajú jedným smerom, ale v prípade poruchy sa využije redundantné vedenie, ktoré ide opačným smerom. Výhodou tejto topológie je lacná inštalácia. (8)



Obrázok č. 7: Kruhová topológia
(Zdroj: Vlastné spracovanie podľa 9)

1.2 Protokoly

V tejto podkapitole bližšie objasním protokoly, ktoré používa nástroj na monitorovanie siete LibreNMS na automatické vyhľadávanie siete.

1.2.1 CDP – Cisco Discovery Protocol

Protokol CDP sa používa na zhromažďovanie detailov o priamo pripojených zariadeniach (rozhraniach) – hardvér, softvér, názov zariadenia apod. Sú dve verzie – CDP v1 je schopná zhromažďovať informácie o pripojenom zariadení na druhom konci a novšia

verzia CDP v2 dokáže efektívnejšie sledovať jednotlivé zariadenia. Upozorní na nesúlad ID VLAN na kanáloch 802,1Q, či na nesúlad v duplexných stavoch medzi jednotlivými zariadeniami. (22)

Každé Cisco zariadenie periodicky posiela CDP pakety s nenulovou hodnotou time-to-live (TTL), ostatné zariadenia tieto packety prijímajú, spracovávajú a ukladajú informácie do vyrovnávacej pamäte packetu. Pri akejkoľvek zmene informácie sa nová informácia opäť uloží do vyrovnávacej pamäte a predošlé informácie sa zahodia, aj keď sa ich TTL hodnota ešte nerovná nule. (22)

Informácie sa ukladajú do tabuľky a obnovia sa vždy, keď sa príjme nové oznámenie od susedného zariadenia, a zároveň sa znovu inicializuje čas zadržania, tzv. *holdtime*, tohto záznamu. Doba zadržania určuje životnosť záznamu v tabuľke. Ak nie je prijaté žiadne hlásenie, ktoré presahuje dobu zadržania, informácie o zariadení sú z tabuľky vymazané. (22)

1.2.2 FDP – Foundry Discovery Protocol

FDP je proprietárny protokol linkovej vrstvy, ktorý bol vytvorený spoločnosťou Foundry Networks. (23)

1.2.3 LLDP – Link Layer Discovery Protocol

LLDP je protokol na druhej (linkovej) vrstve a môže byť využitý stanicou, ktorá je pripojená na špecifický LAN segment. Stanica môže zdieľať svoju identitu a schopnosti. Tento protokol bol definovaný v roku 2005 ako IEEE štandarda 802.1AB-2005 a bol vyvinutý z mnohých proprietárnych vyhľadávajúcich protokolov, ako napr. CDP (Cisco Discovery Protocol) a EDP (Extreme Discovery Protocol). (24)

Dátové jednotky LLDP sú odosielané na cieľovú MAC adresu (01:80:c2:00:00:0e), ktorá je definovaná ako LLDP_Multicast. Táto adresa sa nachádza v rozsahu adries vyhradených IEEE pre protokoly, ktoré sú obmedzené na individuálnu LAN. (24)

1.2.4 OSPF – Open Shortest Path First

OSPF je podporovací smerovací protokol vnútornej brány (IGP) založený na algoritme tzv. *Shortest Path First* (SPF). Tento *vnútrodoménový* protokol bol vytvorený pre IP siete, tzn. že sa používa vrámci jednej siete alebo oblasti. (25, 26)

Každý router (smerovač) obsahuje informácie o každej doméne a vďaka tomu dokáže určiť najkratšiu cestu. Tieto informácie zisťuje odoslaním tzv. *Link State Advertisements* (LSA), ktoré obsahujú detaily o každom routeri, podsieti a viac informácii o sieti samotnej. Informácie sa zapisujú do databázy stavu prepojenia známej aj ako *Link-State Database* (LSDB). (25, 26)

Medzi výhody protokolu OSPF určite patrí schopnosť prepočítať trasy v krátkom čase, aj pri zmene topológie siete. Tento protokol sa využíva najmä pri obsluhovaní veľkej heterogénne siete a je možné autonómny systém (AS) rozdeliť na viaceré oblasti, aby sa znížila prevádzka siete. (25, 26)

1.2.5 BGP – Border Gateway Protocol

Smerovací BGP protokol je zodpovedný za správne smerovanie dátových paketov v sieti výberom najlepšej (najefektívnejšej) cesty spomedzi viacerých možných ciest. BGP pomáha vzájomne prepojeným autonómnym systémom (AS) medzi sebou komunikovať prostredníctvom výmeny informácii o smerovaní paketov. Protokol smeruje pakety podľa informácii v IP adrese a používa tzv. *čísla autonómneho systému* (ASN), tj. jedinečné identifikátory pre každý autonómny systém, ktoré bližšie identifikujú cieľ. (27)

1.2.6 SNMP – Simple Network Management Protocol

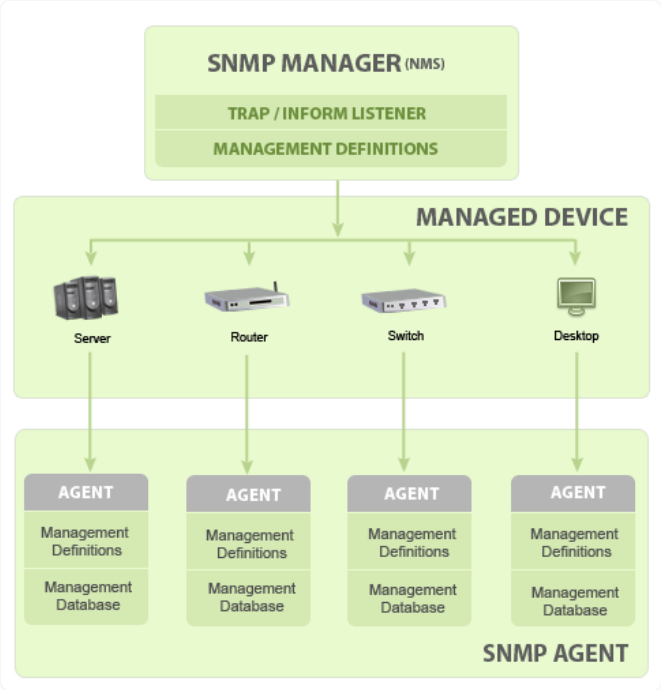
SNMP protokol aplikačnej vrstvy používa UDP port čísla 161/162. Využitie tohto protokolu spočíva najmä v oblasti monitorovania siete, zisťovania poúch v sieti alebo na konfiguráciu vzdialených zariadení. Existuje viacero používaných správ v tomto protokole, medzi ktoré patria napr. getRequest, getNextRequest, setRequest, response, trap alebo informRequest. (28)

SNMP protokol má tri komponenty:

- ***SNMP manažér*** – je centralizovaný systém, ktorý sa využíva na monitorovanie siete, tzv. Network Management Station (NMS);
- ***SNMP agent*** – je modul na správu softvéru. Medzi zariadenia, ktoré spravuje patrí napr. počítač, router (smerovač), switch (prepínač) alebo server;
- ***Manažérska informačná základňa*** (MIB) – jedná sa o hierarchické usporiadanie informácii o spravovaných zdrojoch. (28)

Rozlišujeme tri verzie protokolu SNMP, rozdiel je v spôsobe autentifikácie:

- ***SNMPv1*** – na autentifikáciu používa komunitné reťazce a UDP;
- ***SNMPv2*** – takisto používa reťazce komunity a UDP, ale môže byť nakonfigurovaný aj na TCP;
- ***SNMPv3*** – na ochranu súkromia používa napr. SHA alebo DES-56 a používa TCP. Táto verzia protokolu je najbezpečnejšia a poznáme tri úrovne zabezpečenia – *noAuthNoPriv* (žiadne overenie, žiadne súkromie), *authNopriv* (autentifikácia, žiadne súkromie) a *authPriv* (autentifikácia, súkromie). (28)



Obrázok č. 8: Diagram komunikácie protokolu SNMP

(Zdroj: 31)

1.2.7 ARP – Address Resolution Protocol

Protokol druhej (linkovej) vrstvy slúži na priradenie (mapovanie) IP adresy k MAC adrese. Hostiteľ začne broadcastovým odoslaním paketu ARP, pomocou ktorého zisťuje MAC adresu zodpovedajúcej IP adresy. Hostiteľ s danou IP adresou potom odpovedá poslaním ARP paketu so svojou MAC adresou. (29)

1.2.8 STP – Spanning Tree Protocol

Hlavnou úlohou protokolu druhej vrstvy ISO/OSI modelu je zabránenie vzniku slučkám pri redundantných trasách a zabránenie vzniku zahlteniu siete tzv. *broadcastovým smršťiam*. Špecifikácia tohto protokolu je IEEE 802.1D, pričom zo STP vznikol protokol RSTP (Rapid STP) so špecifikáciou IEEE 802.1w, ktorý má oproti STP rýchlejší čas konvergencie. Princípom protokolu je vyhľadávanie najkratšej cesty medzi uzlami (switchami) a v prípade nutnosti blokovanie alebo odblokovanie jednotlivých portov v STP topológii. (30)

Poznáme tri roly portov:

- ***Root port*** – jedná sa o koreňový port s najlepšou cenovou cestou, ktorý posiela dáta do koreňového mosta (tzv. *Root Bridge*);
- ***Designated port*** – je členom STP topológie a pripája segment. Všetky porty na *Root Bridge* sú typu *designated*;
- ***Blocked port*** – všetky ostatné porty, ktoré vedú k mostom (*bridge*) a prepínačom (*switchom*). Tieto porty sú zablokované a redundantné. (30)

1.3 Aktívne prvky

Aktívne sieťové prvky sú zariadenia umiestnené v uzloch siete, ktoré navzájom prepájajú všetky prvky počítačovej siete a aktívne pracujú so signálom, a to buď tak, že ho zosilňujú, modifikujú alebo hodnotia. (8)

1.3.1 Repeater (opakovač)

Opakovač pracuje na fyzickej vrstve, kde útlm a skreslenie negatívne ovplyvňuje kvalitu signálu, až môže prísť k jeho strate a to spôsobí prerušenie komunikácie.

Opakovač prijíma tento signál, opraví ho, zosilní a binárne rovnaký signál posiela ďalej v sieti. (1)

1.3.2 Router (smerovač)

Smerovač patrí do tretej vrstvy ISO/OSI modelu a jeho úlohou je spojenie viacerých sietí LAN. Posiela pakety, ktoré posiela podľa logickej IP adresy zariadenia. Smerovač poskytuje sieti pripojenie k internetu a využíva smerovacie protokoly, vďaka ktorým zisťuje informácie o sieťach, najznámejším je IP protokol. (2)

1.3.3 Switch (prepínač)

Prepínač (switch) je typ zariadenia, ktorý prepája jednotlivé zariadenia v počítačovej sieti (segmenty siete). Podľa adresy odosielateľa a prijímateľa, ktorá je v dátovom pakete, switch smeruje pakety len do portu určeného zariadenia. MAC adresy si zapisuje do tabuľky MAC adries, v ktorej si pri obdržaní rámca záznamy vždy kontroluje – cieľovú a už známu MAC adresu. Ak MAC adresa ešte nie je v tabuľke, rámce pošle na všetky porty a následne si MAC adresu uloží do tabuľky. Používa protokol Ethernet a najčastejšie využitie má v topológii LAN. (2, 8)

1.4 Systém riadenia bezpečnosti informácií

Systém riadenia bezpečnosi informácií (ISMS), z angličtiny Information Security Management System, podlieha rade noriem ISO/EIC 27000 a je to systém štandardov, pravidiel, doporučení, postupov a kontrol pre zabezpečenie aktív vo firme. Aktíva sú chránené pre rizikami vďaka riadeniu rizík a zavedeniu bezpečnostných opatrení. Popisuje náplň výkonu riadenia bezpečnosti. (10) Ide o neustály proces hľadania rizík, navrhovanie opatrení a ich kontrola. (20)

1.4.1 Základné pojmy ISMS

V tejto podkapitole rozoberiem základné pojmy spojené s bezpečnosťou ICT.

Informačná bezpečnosť je ochrana informačného systému pred zničením alebo odcudzením.

Informačný systém je jednoduché a logické zoradenie informácií pripravené na ďalšie procesy.

Aktívum je cenná súčasť IS, ktorá má určitú štruktúru (HW, SW, dáta, ...).

Zraniteľné miesto je nazývané aj náchylným miestom alebo slabinou, na ktoré môže bezpečnostná hrozba pôsobiť.

Bezpečnostná udalosť je pôsobenie hrozby na zraniteľné miesto aktíva.

Bezpečnostným incidentom je narušenie zraniteľnosti aktíva bezpečnostnou udalosťou a tým zmena vlastností informačného aktíva.

Dopadom označujeme dôsledok bezpečnostného incidentu.

Hrozba je vplyv, ktorý môže spôsobiť nežiadúci účinok na aktívach.

Rizikom nazývame pravdepodobnosť premeny bezpečnostnej hrozby na bezpečnostný incident. (12, 13)

1.5 Aktíva

Za aktívum pokladáme čokoľvek, čo má pre vlastníka aktíva určitú hodnotu. Podľa zákona o kybernetickej bezpečnosti delíme aktíva nasledovne: (11)

Primárne aktívum – informácie, popr. služby poskytujúce informačný alebo komunikačný systém kritickej informačnej infraštruktúry (KII). (11)

Podporné aktívum – technické aktívum a ľudia (zamestnanci, či dodávatelia), ktorí sa podieľajú na procese prevádzky, rozvoja, správe či bezpečnosti informačného, komunikačného alebo inak dôležitého systému KII. (11)

Technické aktívum – technické a programové vybavenie informačného, komunikačného alebo inak významného IS KII a objekty v ňom umiestnené. (11)

1.5.1 Klasifikácia aktív

Ohodnotenie jednotlivých aktív závisí od toho, aký má ich narušenie dopad na spoločnosť. Klasifikáciu určujeme na základe klasifikačného stupňa a klasifikačných kritérií spolu s dopadom na danú organizáciu. Najpoužívanejšie klasifikačné stupne sú znázornené nižšie v tabuľke. (12)

Tabuľka č. 1: Klasifikácia aktív podľa rizika pre organizáciu

(Zdroj: Vlastné spracovanie podľa 12)

Klasifikačný stupeň	*Kritérium*	*Riziko*
1	žiadny dopad na spoločnosť	bezvýznamné
2	zanedbateľný dopad na spoločnosť	akceptovateľné
3	problémy alebo finančné straty pre spoločnosť	nízke
4	vážne problémy alebo finančné straty	nežiadúce
5	existenčné problémy spoločnosti	neprijateľné

Klasifikačné stupne dôvernosti dát spolu s kritériom sú popísané v tabuľke č.2.

Tabuľka č. 2: Klasifikácia podľa dôvernosti dát v komerčnej sfére

(Zdroj: Vlastné spracovanie podľa 12)

Klasifikačný stupeň	*Klasifikačné kritérium*
1 - Verejné	Informácia pre širokú verejnosť (kontakt na spoločnosť, verejne dostupné účtovné výkazy)
2 - Interné	Informácia určená len pre zamestnancov spoločnosti (informácie o zákazkách)
3 - Dôverné	Únik týchto informácií môže mať negatívny dopad na spoločnosť (informácie o dodávateľoch, informácie o projektoch, vývoji cien a plánovaných zmenách)
4 - Súkromné	Únik týchto informácií môže mať negatívny dopad na spoločnosť (osobné údaje o zamestnancoch a klientoch)
5 - Prísne dôverné	Najvyšší stupeň, únik týchto informácii môže mať až zničujúci dopad na spoločnosť (zdrojové kódy, strategické plány spoločnosti)

1.5.2 Zraniteľnosť aktív

Zraniteľnosť aktíva je slabina aktíva, ktorú môže hrozba zneužiť a následne môže vzniknúť bezpečnostný incident (narušenie integrity, dôvernosti, či dostupnosti). (13)

1.5.3 Identifikácia zraniteľnosti aktív

Na základe klasifikácie aktív je určený klasifikačný stupeň, ktorý určuje do akej miery má narušenie jednotlivých aktív dopad na chod podniku. Pomocou klasifikačného stupňa identifikujeme zraniteľnosť aktív našej spoločnosti. (13)

1.6 Riziko

Riziko popisuje stav, keď existuje pravdepodobnosť vzniku určitej škody. Aby sme mohli škodám vopred predísť, musíme najskôr pomocou analýzy hrozieb identifikovať, aké riziká vôbec existujú a aký majú vplyv na jednotlivé aktíva. Vychádzame zo zoznamu obecných rizík zo Systému riadenia bezpečnosti informácii (ISMS), ktorý môžeme doplniť o tie vlastné. (13)

1.6.1 Analýza rizík

Táto podkapitola sa zaoberá analýzou rizika. V prvom rade vytýčim základné pojmy, ako napr. riziko, a následne detailnejšie popíšem samotnú analýzu rizík, jej metódy výpočtu a samotný princíp. (13)

1.6.2 Typy analýzy rizík

Analýza rizík identifikuje relevantné iniciačné udalosti a vytvorí obraz príčin a následkov. Spôsob určenia závisí od použitej metódy a od toho, ako sa majú jednotlivé výsledky použiť. Zámer všetkých analýz je vždy rovnaký, t.j. opísať dané riziko. (14)

Táto analýza je najdôležitejšou časťou ISMS a dá sa rozdeliť do niekoľko *krokov*. Najprv sa identifikujú aktíva, stanovia sa riziká, buď sa príjmu alebo sa vylúčia a na záver príjmeme určité opatrenie. Riziká hodnotíme tabuľkami, v ktorých môžeme využiť kvalitatívnu alebo kvantitatívnu schému. Hlavné metódy analýzy rizík sú v nasledujúcej tabuľke. (13)

Tabuľka č. 3: Hlavné kategórie metód analýzy rizík podľa T.Avena

(Zdroj: Vlastné spracovanie podľa 14)

Hlavná kategória	*Typ analýzy*	*Popis*
Zjednodušená analýza rizík	Kvalitatívna	*Zjednodušená (neformálna) analýza rizík tvorí obraz o rizikách pomocou brainstormingu a diskusií v skupinách. Riziko môže byť ohodnotené bez formalizovaných metód, napr. len na základe stupňov nízke, stredné a vysoké riziko.*
Štandardná analýza rizík	Kvalitatívna alebo kvantitatívna	*Využívajú sa tu už formalizované metódy, napr. analýza HAZOP (štúdia nebezpečenstva a prevádzkyschopnosti) alebo analýza hrubého rizika. Výstupom sú rizikové matice.*
Analýza rizík založená na modeli	Primárne kvantitatívna	*Táto analýza rizík na určenie rizika využíva analýzu stromu udalostí a analýzu stromu chýb.*

Kvalitatívne ohodnotenie určuje pravdepodobnosť spôsobenia bezpečnostného incidentu pôsobením bezpečnostnej hrozby. Na vyhodnotenie sa používa klasifikačná stupnica. (13)

Kvantitatívna metodika je detailnejšia a určuje pravdepodobnosti jednotlivých scénarov. Zahŕňa pravdepodobnosť výskytu bezpečnostnej hrozby, vyvolanie bezpečnostnej udalosti až vyvolanie bezpečnostného incidentu. Tieto hodnoty sa následne násobia a stanovia tak výslednú hodnotu rizika. (13)

Miera rizika nám udáva scénare, ktoré môžu nastať, ak sa riziko uskutoční. Nízky dopad rizík spôsobuje, že riziká nemusia mať žiadne opatrenie, ak je aj úroveň pravdepodobnosti jeho vzniku nízka. Rastúca hodnota dopadu znamená potrebné aplikovanie opatrení a niekedy môže znamenať až okamžité riešenie rizika. (13)

1.6.3 Kvantifikácia rizík

V analýze rizík musíme buď numericky alebo slovne ohodnotiť úroveň pravdepodobnosti, dopadu a rizika. Hodnotenie bude podľa kritérií z nasledujúcich tabuliek. Tabuľka nižšie zobrazuje hodnotenie pravdepodobnosti rizika. (13)

Tabuľka č. 4: Pravdepodobnosť rizika

(Zdroj: Vlastné spracovanie)

Hodnota	% vyjadrenie	Slovné ohodnotenie
1-2	0-19	veľmi nepravdepodobné
3-4	20-39	nepravdepodobné
5-6	40-59	pravdepodobné
7-8	60-79	viac pravdepodobné
9-10	80-100	veľmi pravdepodobné

Nasledujúca tabuľka popisuje hodnotenie dopadu určitého rizika.

Tabuľka č. 5: Dopad rizika

(Zdroj: Vlastné spracovanie)

Hodnota	Slovné ohodnotenie
1-2	bezvýznamné
3-4	málo významné
5-6	významné
7-8	veľmi významné
9-10	kritické

Hodnota jednotlivých rizík je vyhodnotená na základe stanovených kritérii popísaných v tabuľke nižšie.

Tabuľka č. 6: Hodnota rizika

(Zdroj: Vlastné spracovanie)

Hodnota rizika		Pravdepodobnosť				
		1-2	3-4	5-6	7-8	9-10
Dopad	1-2	bezvýznamná	bezvýznamná	bezvýznamná	bezvýznamná	bezvýznamná
	3-4	bezvýznamná	bežná	bežná	bežná	bežná
	5-6	bežná	bežná	významná	významná	kritická
	7-8	bežná	významná	významná	kritická	kritická
	9-10	významná	významná	kritická	kritická	kritická

1.6.4 Riadenie rizík

Risk management alebo riadenie rizík sa používa na zníženie pravdepodobnosti uskutočnenia rizika alebo aspoň zníženie jeho dopadu. Jedná sa o neustály proces kvôli zvýšeniu bezpečnosti informácii. Proces riadenia sa dá nadefinovať algoritmom, je komplexný a dohliada, aby všetky potrebné činnosti spojené s riadením rizika boli uskutočnené a riadené. (13)

Prvým krokom procesu riadenia rizík je výber metodiky a spôsob hodnotenia. Následne sa vykonáva samotná analýza rizík. Riziká sa vyhodnocujú a stanovujú sa potrebné opatrenia. V záverečnom kroku sa rozhoduje, či sa jednotlivé riziká príjmu alebo nie. V prípade, že sa riziko nepríjme, daný proces sa opäť zopakuje. Celý proces sa monitoruje a zaznamenáva. (13)

1.7 Lewinov model na riadenie zmien

Lewinov model riadenia zmien patrí medzi najznámejšie modely zmien v organizácii. Autorom tohto modelu je americký psychológ K. Lewin, podľa ktorého má zmena prebiehať v 3 fázach: (18)

1. ***Fáza rozmrazenia*** - príprava zmien. V tejto fáze prebieha presvedčovanie o nutnosti určitých zmien, existujúce pravidlá a zvyklosti sú „*rozmrazené*“.
2. ***Fáza zmeny*** – predstavuje priebeh vlastnej zmeny. V tejto fáze je typická neistota alebo zmätenosť.
3. ***Fáza zamrazenia*** - ukončenie zmeny. V poslednej fáze modelu ide o stabilizáciu systému, tzv. „*zamrazenie*“ nových pravidiel a novonadobudnutých zvykov alebo ukotvenie tohto nového stavu, prípadne školenie, či oslava úspešnej zmeny vo firemných procesoch. (18)

Obrázok č. 9: Lewinov model

(Zdroj: Vlastné spracovanie podľa 17)

1.8 Projektové riadenie

Riadenie projektov (angl. Project Management) je pomerne nový odbor, ktorý sa zaoberá viacerými aktivitami spojenými s plánovaním, organizovaním, riadením a kontrolou zdrojov podniku s určitým cieľom, ktorý sa stanovil pre dosiahnutie špecifických cieľov a stratégie spoločnosti. Takisto sa jedná aj o viaceré nástroje, schopnosti, znalosti a technológie, ktoré pomáhajú splniť požiadavky daného projektu. Jedná sa teda o kombináciu využitia dostupných metód a znalostí za účelom dosiahnutia stanovených cieľov projektu. (15)

1.8.1 Projekt

Projektom môžeme označiť sled udalostí, ktorý je stavebným prvkom projektového riadenia a spĺňa viacero požiadaviek. Každý projekt má začiatok a koniec; určité pravidlá

riadenia a regulácie; špecifický cieľ, ktorý má byť na záver projektu splnený; a stanovený limit čerpania zdrojov, ktoré sú nevyhnutné na realizáciu každého projektu. (16)

Každý projekt je jedinečný a ohraničený časom, nákladmi a zdrojmi, pomocou ktorých sú na záver vytvorené výstupy projektu v súlade s vopred stanovenými požiadavkami. (16)

1.9 SLEPTE analýza

SLEPTE analýza je analytická technika, ktorá slúži k strategickej analýze okolitého prostredia organizácie. Je konceptom viacerých marketingových princípov. Tento koncept je vhodný ako nástroj na pozorovanie okolia, v ktorom firma pôsobí alebo do ktorého chce implementovať nový produkt, či službu. Skúma šesť externých faktorov, ktorými sú: sociálne, ekonomické, politické, technologické, ekologické a legislatívne faktory. (31)

2 ANALÝZA SÚČASNÉHO STAVU

Druhá kapitola záverečnej práce sa zaoberá analýzou aktív a rizík, ktorá je potrebná pre implementáciu riešenia.

2.1 Popis zvolenej spoločnosti

V tejto práci som sa zamerala na IT spoločnosť, ktorá poskytuje telekomunikačné služby, internetové a dátové služby realizované na dátových sieťach. V súčasnosti firma ponúka televízne a internetové služby cez optické pripojenie B2B aj B2C sektoru.

Firma má svoju serverovňu a prevádzkuje niekoľko ďalších staníc s technickými zariadeniami, s dátovými rozvádzačmi a servermi. V prípade výpadkov sietí sú technici schopní problém identifikovať a opraviť v celkom malom časovom úseku.

2.1.1 Stratégia firmy

Uspokojenie zákazníkov, získanie si ich dôvery a byť spoľahlivým poskytovateľom internetových služieb je základnou víziou firmy.

2.1.2 Vývoj spoločnosti

Zvolená IT firma je na trhu už desiatky rokov a takisto, ako sa menil trh a túžby zákazníkov, vyvíjalo sa aj pôsobenie firmy na trhu a jej zámer v poskytovaní širokého spektra telekomunikačných služieb.

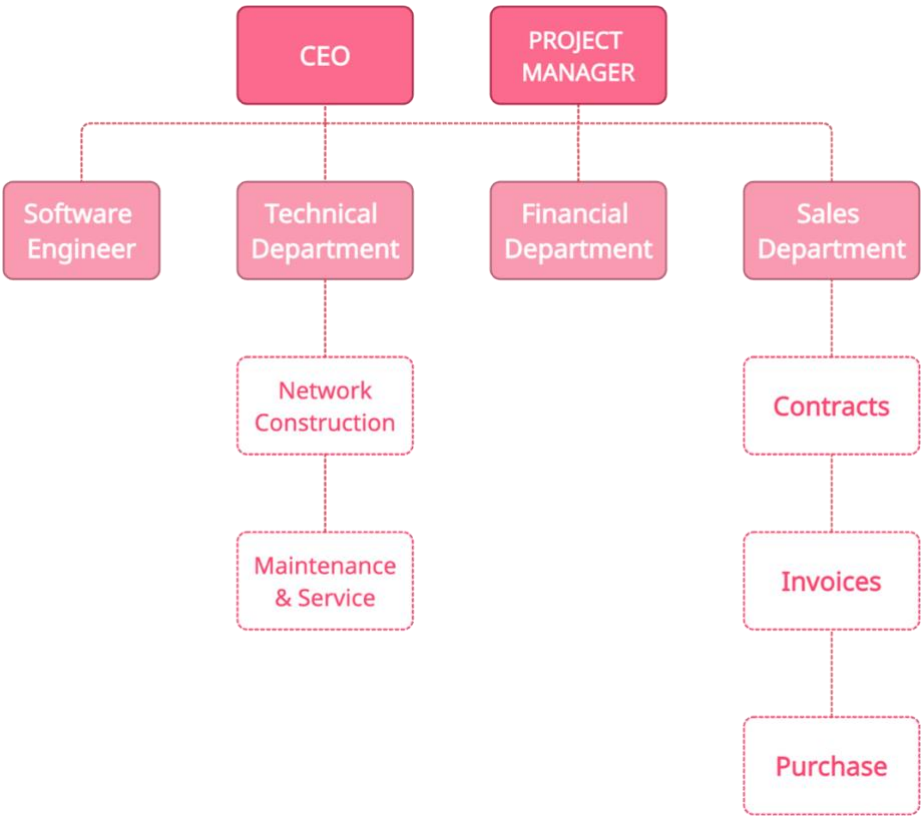
2.1.3 Organizačná štruktúra

Vybraná spoločnosť je malou spoločnosťou s počtom zamestnancov v rozmedzí 20 až 30 ľudí. CEO spoločnosti sa spolu s projektovým manažérom nachádza na najvyššej úrovni organizačnej štruktúry. Na rovnakej úrovni sa nachádza softvérový inžinier, celé technické, ekonomické a obchodné oddelenie. Hlavnou pracovnou náplňou technického oddelenia je výstavba, údržba a servis sietí. Ďalej, v obchodnom oddelení sú vyčlenení samostatní pracovníci pre fakturácie, tvorby zmluv a nákup tovaru.

Na samotné monitorovanie dátovej prevádzky nie je vyčlenený žiadny tím pracovníkov, dokonca ani jeden konkrétny zamestnanec nemá túto úlohu pridelenú ako hlavnú pracovnú náplň. Monitoringu záťaže siete sa venuje len softvérový inžinier, keď mu príde upozornenie (výstraha), že niečo nie je v poriadku a potom sa ďalšie kroky delegujú na technické oddelenie, kde sa o vyskytnutý problém postarajú už technici (fyzický zásah do infraštruktúry).

Pre bezproblémový chod siete, vyššiu spoľahlivosť a pre eliminovanie rizík výpadkov siete by bolo vhodné v budúcnosti prideliť manažment siete novému zamestnancovi, ktorý by mohol nepretržite kontrolovať stav siete a všetkých pripojených zariadení. Následne v prípade výpadkov, možných kolízií a iných problémov informovať ďalších ľudí, poprípade vopred zaujať určité postupy, aby tieto problémové situácie ani nastať nemuseli.

Organizačnú štruktúru firmy vidieť na nasledujúcom obrázku.



Obrázok č. 10: Organizačná štruktúra spoločnosti

(Zdroj: Vlastné spracovanie)

2.1.4 Hardvérové vybavenie

Firma obsluhuje serverovňu so svojimi technickými zariadeniami a prevádzkuje aj niekoľko ďalších staníc s dátovými rozvádzačmi. Vybudovanie kvalitnej infraštruktúry a serverovne je pomerne dosť finančne náročné, ale neskôr to vyžaduje veľmi malé finančné úsilie, pretože technici pri budovaní myslia na funkčnosť aj v ďalších rokoch.

V prípade, že nastane akýkoľvek problém ohľadne výpadku siete, zamestnanci z technického oddelenia sú schopní problém identifikovať a opraviť v pomerne krátkom časovom úseku.

Všetci zamestnanci majú vlastný počítač, na ktorom máajú prístup k potrebnému softvéru, najmä k internému firemnému IS, Money S3 a balíku aplikácii Microsoft Office 365. Do firemnej siete je pripojených približne 20 počítačových zariadení, spolu s ďalšími zariadeniami ako napr. telekomunikačné zariadenia, kamerový systém a televízne pripojenie. Do firemného IS je možné sa pripojiť aj vzdialene.

2.1.5 Softvérové vybavenie

Vybraná spoločnosť využíva najmä interný podnikový systém, účtovnícky systém Money S5, balík aplikácii Microsoft Office 365 a začína používať systém Libre NMS na monitorovanie sieťovej prevádzky.

2.2 Analýza spoločnosti

Prvým krokom k navrhnutiu efektívnych riešení na vylepšenie situácie vo firme je nutné najskôr vykonať dôkladnú analýzu firmy a jej okolia. V prvom rade zanalyzujem aktíva spoločnosti, identifikujem ich vlastníkov a napokon klasifikujem jednotlivé aktíva podľa stanovených kritérii. V ďalšej časti identifikujem riziká, ktoré môžu nastať implementovaním navrhovanej zmeny, pomocou skórovacej metódy ich vyhodnotím a vďaka mape graficky znázorním do štyroch kvadrantov. Na záver navrhnem vhodné opatrenia, ktoré by mali rizikám predísť alebo aspoň znížiť ich dopad na spoločnosť. V neposlednom rade vyhodnotím vonkajšie okolie pomocou analýzy SLEPTE.

2.2.1 Identifikácia aktív

Informačný systém je najdôležitejším aktívom spoločnosti. Zahŕňa jednotlivé databázy s informáciami o zákazníkoch, dodávateľoch, informácie o všetkých objednávkach, prijatých či vydaných faktúrach a dáta o výrobe. *Fyzickú časť aktív* podniku tvoria počítače spolu s potrebným vybavením a ostatné komunikačné zariadenia, ako napr. tlačiarne, tablety a telefóny, aktívne prvky počítačovej siete, kabeláž; mimo komunikačné zariadenia sem patria aj technické zariadenia ako napájacie zdroje či úložné médiá. Firma používa účtovný softvér a objednávkový softvér. Jednu z podstatnej časti aktív tvoria zamestnanci spoločnosti, ktorí pomocou kvalifikovanej práce s vyššie uvedenými aktívami vytvárajú podniku hodnotu. Potom sem patria technologické postupy a systémy pri výrobe, dobré meno firmy a iné. Všetky aktíva majú medzi sebou väzby, ktorými sú navzájom previazané a majú hodnotný význam pre podnik.

2.2.2 Identifikácia vlastníkov aktív

Aktíva sú v majetkovom vlastníctve firmy – jej majiteľa, ktorý je za ne aj zodpovedný. Zamestnanci majú právomoc používať jednotlivé aktíva a sú zodpovední za ich efektívne a bezchybné využitie pri výrobe. Zodpovednosť za bezchybnú prevádzku informačného systému má tvorca systému. Každý systém je sprístupnený iba povolaným osobám, ktoré s ním pracujú. Účtovný systém je prístupný len účtovníčke, finančnému manažérovi a majiteľovi firmy, ktorí sa naň môžu pripojiť cez vzdialenú plochu. Objednávkový systém je navyše prístupný obchodným manažérom, ktorí sa starajú o nákup a predaj tovaru a zásob. K systému monitorovania siete má prístup len obmedzený okruh ľudí, a to je technik, softvérový inžinier a majiteľ spoločnosti.

2.2.3 Klasifikácia aktív spoločnosti

V nasledujúcej tabuľke sú najdôležitejšie aktíva vybranej spoločnosti.

Tabuľka č. 7: Klasifikácia aktív spoločnosti

(Zdroj: Vlastné spracovanie)

Aktívum	***Stupeň dôvernosti***
Účtovné výkazy	1 - Verejné
Interná dokumentácia	2 - Interné
Zamestnanci	2 - Interné
Projektová dokumentácia	3 - Dôverné
Informácie o dodávateľoch	3 - Dôverné
Komunikačné zariadenia	3 - Dôverné
Počítačové vybavenie	3 - Dôverné
Programové vybavenie	3 - Dôverné
Databáza klientov	4 - Súkromné
Strategické plány organizácie	5 - Prísne dôverné

Nasledujúca tabuľka klasifikuje vybrané aktíva podľa ich dostupnosti (reakčnej doby).

Tabuľka č. 8: Klasifikácia aktív podľa dostupnosti

(Zdroj: Vlastné spracovanie)

Aktívum	***Dostupnosť***
Použitá aplikácia LibreNMS	rádovo sekundy
Zamestnanci	rádovo minúty

2.2.4 Identifikácia zraniteľností aktív spoločnosti

V tabuľke č. 9 sú slovne ohodnotené zraniteľnosti jednotlivých aktív spoločnosti spolu s odôvodnením zvolenej klasifikácie.

Tabuľka č. 9: Zraniteľnosti aktív spoločnosti

(Zdroj: Vlastné spracovanie)

Aktívum	*Stupeň zraniteľnosť*	*Zraniteľnosť*
Účtovné výkazy	Nízka	Dokumenty nie sú umiestnené na mieste, kde môže vzniknúť fyzické poškodenie alebo strata.
Interná dokumentácia	Nízka	Dokumenty nie sú umiestnené na mieste, kde môže vzniknúť fyzické poškodenie alebo strata.
Zamestnanci	Stredná	Ľudský faktor.
Projektová dokumentácia	Nízka	Dokumenty nie sú umiestnené na mieste, kde môže vzniknúť fyzické poškodenie alebo strata.
Informácie o dodávateľoch	Nízka	Dokumenty nie sú umiestnené na mieste, kde môže vzniknúť fyzické poškodenie alebo strata.
Komunikačné zariadenia	Stredná	Umiestnenie a zastaralé siete.
Počítačové vybavenie	Vysoká	Nepretržitá prevádzka, obmedzená životnosť.
Programové vybavenie	Stredná	Spôsob ukladania dát.
Databáza klientov	Vysoká	Nešifrované ukladanie dát.
Strategické plány organizácie	Nízka	Dokumenty nie sú umiestnené na mieste, kde môže vzniknúť fyzické poškodenie alebo strata.

2.3 Analýza hrozieb a rizík

Táto podkapitola práce sa venuje identifikáciou hrozieb a rizík navrhovanej zmeny a ich následnou analýzou, vďaka ktorej bude firma pripravená čeliť týmto hrozbám, znížiť možný dopad na prijateľnú úroveň a tie najkritickejšie hrozby bude môcť eliminovať vďaka vopred navrhnutým opatreniam. Analýzu som vykonala pomocou tzv. ***skórovacej metódy***, ktorá pozostáva z troch základných krokov – identifikácia hrozieb, ich kvantifikácia a následne návrhy na opatrenie.

2.3.1 Identifikácia hrozieb pred implementáciou nástroja LibreNMS

Pred implementáciou navrhnutého riešenia medzi hrozby s najväčšou mierou rizika patrí: nedostatočná kapacita siete, neidentifikovanie problému včas, nedostatočné odborné znalosti zamestnancov a zlyhanie infraštruktúry. Všetky hrozby majú veľmi vysoký (vážny) dopad na fungovanie spoločnosti.

2.3.2 Skórovacia metóda pre hrozby pred implementáciou návrhu

Stanovené hrozby som v nižšie priloženej tabuľke vyhodnotila pomocou tzv. *skórovacej metódy*. Kvantitatívne som vyjadrila mieru pravdepodobnosti, že hrozba prerastie v incident, následne možný dopad a mieru rizika (MR) pred opatrením a v stave pred implementáciou navrhovanej zmeny.

Najkritickejšie hrozby sú vyhodnotené v nasledujúcej tabuľke spolu s mierou rizika.

Tabuľka č. 10: Analýza rizík pred implementáciou navrhnutého riešenia
(Zdroj: Vlastné spracovanie)

č.	*Hrozba*	*Incident*	*Pravdepo-dobnosť vzniku*	*Dopad*	*MR*
1	***Nedostatočná kapacita siete***	Zahltenie siete = prerušenie sieťovej prevádzky	7	7	49
2	***Neidentifikovanie problému včas***	Dlhá reakčná doba = prerušenie dodávky internetového signálu	8	7	56

3	***Neodbornosť zamestnancov***	Dlhotrvajúci výpadok siete = strata zákazníkov	7	9	63
4	***Zlyhanie infraštruktúry***	Nefunkčnosť zariadení a prerušenie sieťovej prevádzky	6	8	48

V nasledujúcej tabuľke som vypísala jednotlivé hrozby a k nim dve možné opatrenia – bez využitia nástroju LibreNMS, tzv. ľudský zásah a opatrenie s využitím nástroja. Výsledná miera rizika sa zníži v oboch prípadoch, avšak z ekonomického a časového hľadiska je výrazne efektívnejším riešením využiť technológiu LibreNMS. Takisto som objasnila nápravné činnosti bez a s nástrojom v prípade, že hrozba prerastie v incident.

Opäť je ekonomicky (detailnejší rozpis nákladov sa nachádza v poslednej kapitole Ekonomické zhodnotenie) a časovo výhodnejším riešením využitie technológie LibreNMS, keďže vďaka nástroju trvá obnovenie sieťovej prevádzky len pár sekúnd, a to aj bez ľudského zásahu.

Tabuľka č. 11: Analýza hrozieb, opatrení a nápravných činností pred implementáciou návrhu
(Zdroj: Vlastné spracovanie)

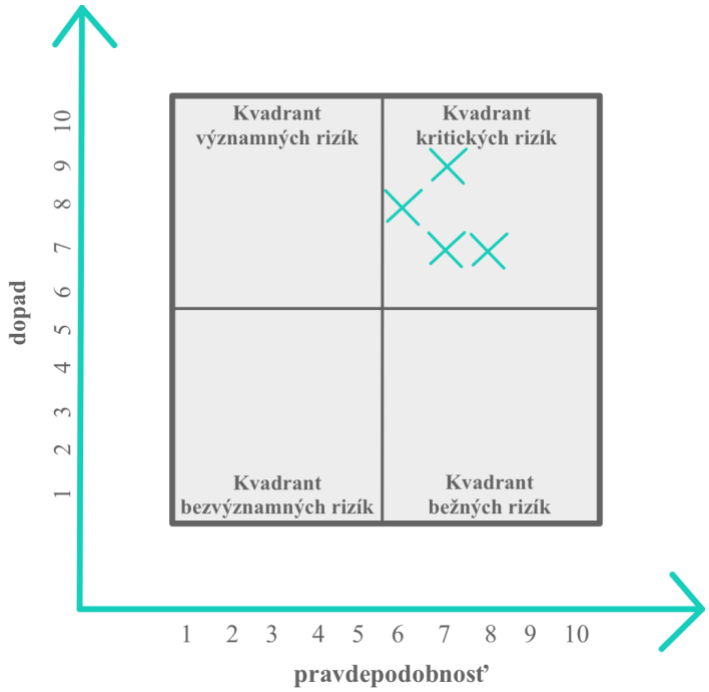
č.	***Hrozba***	***Opatrenie bez nástroja***	***Opatrenie s nástrojom***	***Nápravná činnosť bez nástroju LibreNMS***	***Nápravná činnosť s nástrojom LibreNMS***	***Výsledná MR***
1	***Nedostatočná kapacita siete***	Ručná neustála kontrola kapacity	Nastavenie kontroly kapacity	Ručné zasiahnutie (v priebehu niekoľkých minút, hodín)	Automatické presmerovanie prevádzky	12
2	***Neidentifikovanie problému včas***	Ručná neustála kontrola stavu siete	Nastavenie kontroly siete	Ručné zasiahnutie a výjazd technikov	Automatické presmerovanie prevádzky	18

3	***Neodbornosť zamestnancov v prípade výpadku***	Školenie tímu technikov	Nastavenie upozornení na detekovanie možných výpadkov	Ručné zasiahnutie (v priebehu niekoľkých hodín)	Automatické reštartovanie zariadenia (v priebehu pár sekúnd)	14
4	***Zlyhanie infraštruktúry***	Ručná neustála kontrola stavu zariadení	Nastavenie upozornení na detekovanie potreby servisu zar.	Ručné zasiahnutie a výjazd technikov (v priebehu niekoľkých hodín, dní)	Zaslanie upozornenia s možno potrebným zásahom technika	15

2.3.3 Mapa rizík skórovacej metódy pred implementáciou návrhu

Ďalším krokom v analýze rizík je vykreslenie mapy rizík skórovacej metódy pred a po zavedení patričných opatrení.

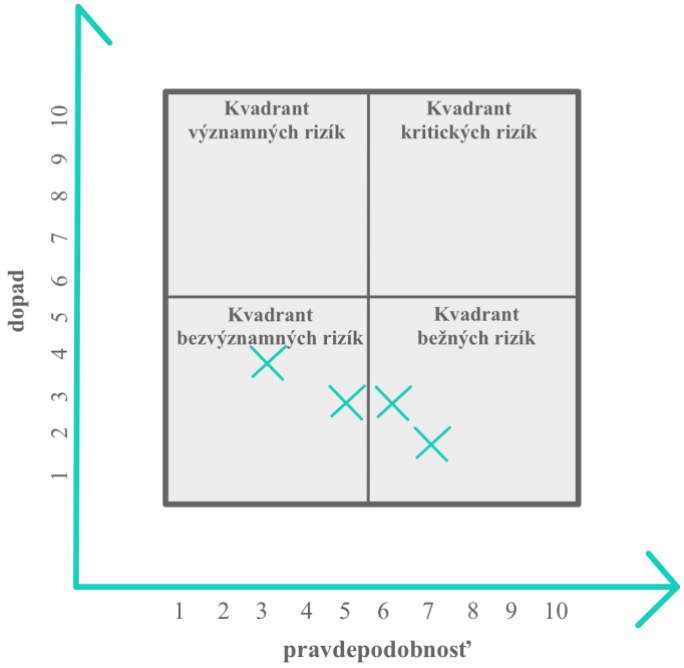
Na obrázku nižšie je vidieť mieru jednotlivých rizík rozloženú v štyroch kvadrantoch pred zavedením akýchkoľvek opatrení.



Obrázok č. 11: Mapa rizík pred implementáciou návrhu pred opatrením

(Zdroj: Vlastné spracovanie)

Obrázok nižšie zobrazuje mapu rizík pred implementáciou po zavedení opatrení.



Obrázok č. 12: Mapa rizík pred implementáciou návrhu po opatrení

(Zdroj: Vlastné spracovanie)

2.3.4 Identifikácia hrozieb pri implementácii nástroja LibreNMS

Pri implementovaní novej technológie do firmy môžu nastať nasledujúce hrozby, ktoré by mohli prerásť v incidenty:

- Presné nedefinovanie všetkých *požiadaviek* / zabudnutie na niektoré kľúčové požiadavky;
- Nesprávna *inštalácia* a *konfigurácia* nového systému;
- Vytvorenie nedostatočných *manuálov* na prácu v systéme;
- Nedostatočné *znalosti* na prácu so systémom (aj napriek absolvovaniu školenia);
- Nedostatočná *spätná väzba* od užívateľov nového systému;
- Nesprávne nastavenie *právomocí* a *bezpečnostných* prvkov;
- *Neochota* zamestnancov sa učiť pracovať s novým systémom;
- Nenájdenie dostatočne *kvalifikovaných* ľudí na pozíciu monitorovania prevádzky;

- *Prehliadnutie* kľúčových ukázateľov (nedostatočné monitorovanie stavu prevádzky) v dashboarde systému, ktoré môžu spôsobiť veľké komplikácie (zničenie infraštruktúry a iných elektrických zariadení, ai.);
- Nevčasné identifikovanie (veľkých) výpadkov siete;
- Nevčasná identifikácia potreby servisu niektorej časti infraštruktúry.

2.3.5 Skórovacia metóda pre hrozby pri implementácii návrhu

Hrozby stanovené v predchádzajúcej podkapitole som v tabuľke nižšie vyhodnotila pomocou tzv. *skórovacej metódy*. K jednotlivým hrozbám, ktoré môžu nastať pri implementácii zmeny, som numericky vyjadrila ich pravdepodobnosť uskutočnenia (P), možný dopad hrozby, mieru rizika (MR) a následne som navrhla opatrenia, pomocou ktorých sa výsledná miera rizika výrazne znížila.

Tabuľka č. 12: Analýza rizík pri implementácii návrhu

(Zdroj: Vlastné spracovanie)

č.	*Hrozba*	*Incident*	*P.vzniku incidentu*	*Dopad*	*MR*	*Opatrenie*	*Výsledná MR*
1	Presné nedefinovanie všetkých *požiadaviek* / zabudnutie na niektoré kľúčové požiadavky	Nekompletný návrh na zmenu	4	9	36	Kontrola viacerými ľuďmi	12
2	Nesprávna *inštalácia* a *konfigurácia* nového systému	Navrhovaná zmena nebude mať požadovaný výstup	5	9	45	Inštalácia odborným pracovníkom	24
3	Vytvorenie nedostatočných *manuálov* na prácu v systéme	Zlý výstup návrhu zmeny	7	6	42	Zvýšená pozornosť na správnosť materiálov	10
4	Nedostatočné *znalosti* na prácu so systémom (aj napriek absolvovaniu školenia)	Nedostatočné využitie systému	7	8	56	Záverečné overenie užívateľov (formou testu, skúšobného prostredia)	24

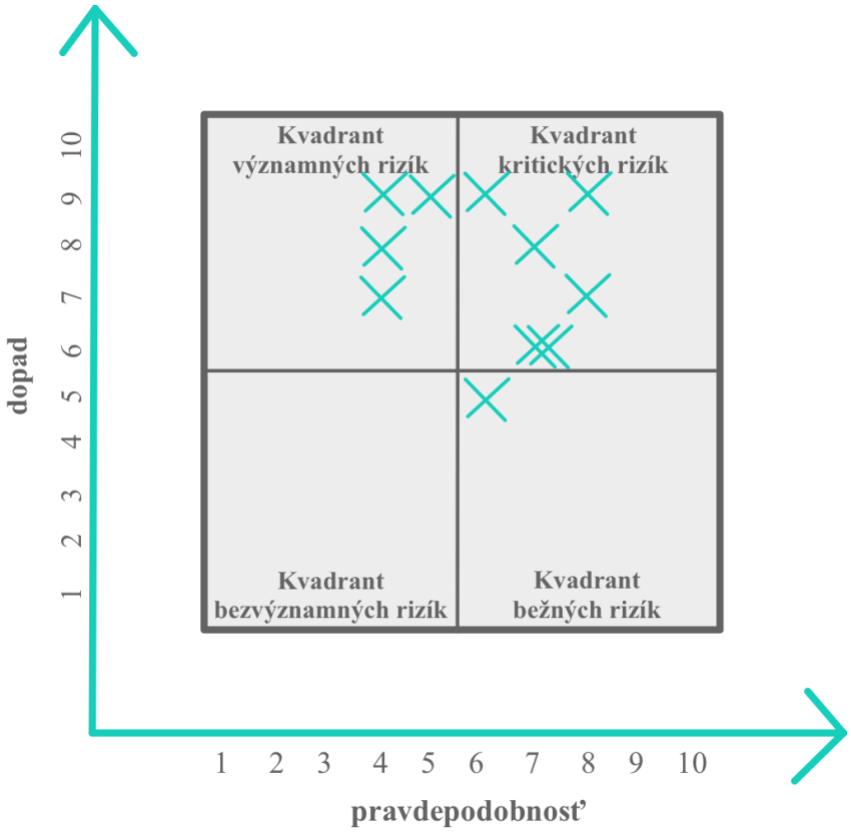
5	Nedostatočná *spätná väzba* od užívateľov nového systému	Možný vznik komplikácie	4	7	28	Motivácia na uľahčenia práce v budúcnosti	15
6	Nesprávne nastavenie *právomocí* a *bezpeč.* prvkov	Navrhovaná zmena nebude mať požadovaný výstup	4	8	32	Dôkladná záverečná kontrola (ďalšou osobou)	12
7	*Neochota* zamestnancov sa učiť pracovať s novým systémom	Spomalenie alebo problém s vykonaním zmeny	7	6	42	Predstavenie benefitov zmeny a jej využitia v budúcnosti, motivácia efektívnej práce (formou prezentácie, popr.finančnej odmeny za proaktivitu)	20
8	Nenájdenie dostatočne *kvalifikovaných* ľudí na pozíciu monitorovania prevádzky	Nedostatočný výstup zmeny	6	5	30	Vyškolenie zamestnanca vo vnútri organizácie	20
9	*Prehliadnutie* kľúčových ukázateľov (nedostatočné monitorovanie stavu prevádzky) v dashboarde systému, ktoré môžu spôsobiť veľké komplikácie (zničenie infraštruktúry a iných elektrických zariadení, ai.)	Nedostatočné využitie systému	6	9	54	Nastavenie upozornení (formou emailu, SMS) a školenie užívateľov	18

10	Nevčasné identifikovanie (veľkých) výpadkov siete	Nedostatočné využitie systému	8	9	72	Nastavenie upozornení (formou emailu, SMS)	24
11	Nevčasná identifikácia potreby servisu niektorej časti infraštruktúry	Nedostatočné využitie systému	8	7	56	Nastavenie upozornení (formou emailu, SMS)	16

2.3.6 Mapa rizík skórovacej metódy pri implementácii návrhu

Totožnú mapu som spravila aj pre hrozby, ktoré môžu nastať pri alebo po implementácii navrhovanej zmeny.

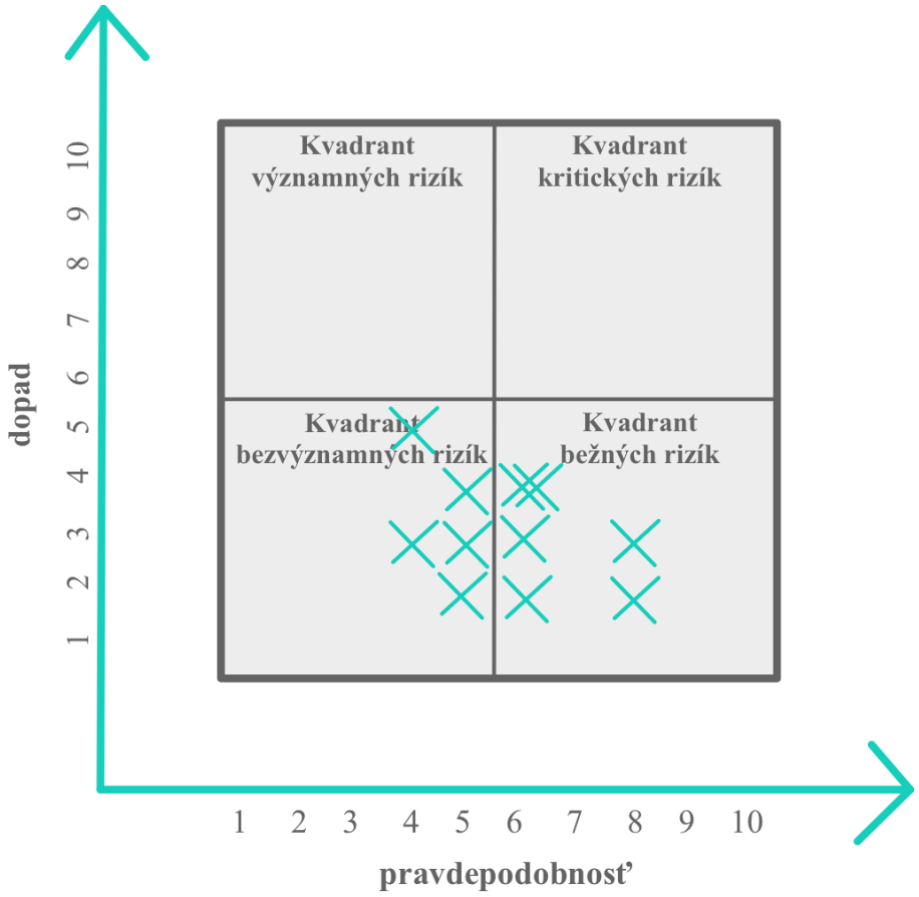
Na nasledujúcom obrázku je vidieť mieru rizík opäť rozloženú do štyroch kvadrantov pred zavedením akýchkoľvek opatrení.



Obrázok č. 13: Mapa rizík pri implementácii pred opatrením

(Zdroj: Vlastné spracovanie)

Nasledujúci obrázok znázorňuje mapu rizík po zavedení odporúčaných opatrení, ktoré výrazne znížia výslednú mieru rizík.



Obrázok č. 14: Mapa rizík pri implementácii po opatrení

(Zdroj: Vlastné spracovanie)

2.4 Analýza vonkajšieho prostredia - Analýza SLEPTE

Aby bola vybraná spoločnosť úspešná v dosahovaní svojich cieľov, je pre ňu potrebné vytvoriť súlad firemnej stratégie s jej okolím. Z tohto dôvodu je pre firmu podstatné dobre poznať jej okolie, jeho prostredie a faktory, ktoré podnik ovplyvňujú. K tomuto účelu nám poslúži analýza SLEPTE, tiež označovaná ako PESTLE.

2.4.1 Politické faktory

Firmy musia neustále monitorovať aj politickú situáciu na Slovensku. Spolu so stále meniacimi sa politickými stranami, sa menia aj zákony, podľa ktorých sa menia aj požiadavky a smernice, ktoré spoločnosti musia spĺňať.

2.4.2 Ekologické faktory

Ekologické faktory sa firmy týkajú kvôli ekologickosti prevádzky budovy, prepravy do práce alebo ku klientom, či pri vonkajších prácach (budovanie optického alebo metalického pripojenia ku zákazníkom v nových oblastiach).

V nedávnej dobe firma uzavrela zmluvu s dodávateľom služieb triedenia odpadu a likvidácie špeciálneho materiálu. Spoločnosť sa týmto krokom snaží znižovať svoju negatívnu ekologickú stopu, reaguje na aktuálne ekologické trendy a snaží sa spríjemniť pracovné prostredie. Takisto významným krokom vpred je aj elektronizácia viacerých dokumentov, najmä zmlúv s klientami, ktoré sa ešte donedávna tlačili v papierovej podobe. Elektronizácia je výhodná aj kvôli rýchlemu vyhľadávaniu a kontrole údajov a podpisových vzorov.

2.4.3 Sociálne faktory

Niektoré zo zmien v sociálnom prostredí môžu mať značný vplyv na dopyt po službách a produktoch, ktoré spoločnosť ponúka na trhu.

Vzdelanie

Jedným z kľúčových sociálnych faktorov je vzdelanosť obyvateľstva. O určité služby a produkty spoločnosti budú zrejme javiť záujem len ľudia, ktorí majú v tejto sfére aspoň priemerné poznatky o IT. Televízne a internetové služby sú dostupné pre všetkých ľudí, aj tým, ktorí nemajú dostatočné znalosti v tejto oblasti. Servisní technici spoločnosti vedia vybranú službu zapojiť každému, či už sa danej problematike rozumie alebo nie. Avšak určité produkty firmy (niektoré elektronické zariadenia, routere, switche, či iné špeciálne príslušenstvo) nebudú využívať ľudia, ktorí sa v tejto oblasti vôbec nepohybujú, pretože

nebudú vedieť s tým manipulovať a nebudú vedieť využiť toho benefity. S technologickým pokrokom všade vo svete, rastie aj vzdelanosť obyvateľstva ohľadom IT, a tým pádom sa o IT produkty zvyšuje záujem.

Vekové rozloženie

Firma ponúka svoje služby a produkty širokej skupine ľudí, ako mladším generáciám, tak aj tým starším. Nemenovaná spoločnosť svojou ponukou produktov cieli predovšetkým na mladšie generácie, ktoré môžu zaujať rôzne technologické novinky, ale zároveň so svojimi širokospektrálnymi službami cieli aj na staršie generácie, pre ktoré tvorí špeciálne televízne balíčky.

2.4.4 Technologické faktory

Vzhľadom na rýchly technologický vývoj vo svete, je na tom firma pomerne dobre, pretože sa snaží udržiavať krok s dobou a v niektorých oblastiach nemá na výber a musí ponúkať aktuálne trendy, aby si udržala svoje miesto na trhu medzi konkurentami v odvetví. Preto je nutné, aby spoločnosť neustále monitorovala aktuálnu situáciu a v prípade vývoja nových technológii musí byť ihneď pripravená na ne reagovať a aj ich implementovať, aby nezaostávala a tým nestratila svoje portfólio zákazníkov.

Avšak nejedná sa len o nákup nových technológii, ale s tým je zároveň spojené aj neustále vzdelávanie zamestnancov vo forme rôznych odborných kurzov, školení a získavaní certifikátov. Tie slúžia nielen na zvýšenie povedomia o nových trendoch, ale aj kvôli znalostiam ako nové technológie používať, ponúkať a implementovať svojim zákazníkom.

2.4.5 Legislatívne faktory

Legislatívne faktory výrazne ovplyvňujú fungovanie všetkých spoločností v krajine. Do legislatívy patrí obchodný zákonník, pracovný zákonník, zákon o bezpečnosti a ochrane zdravia pri práci, zákon o dani z pridanej hodnoty, zákon o dani z príjmov a zákon o obchodnom registri. Nie všetky legislatívne zmeny musia spoločnosť výrazne (negatívne) ovplyvniť, a preto to pre fungovanie firmy nepredstavuje až také veľké riziko.

Od roku 2018 musí anonymizovaná firma rešpektovať zákon č. 18/2018 z.z. ohľadom GDPR, teda *Zákon o ochrane osobných údajov*. Toto spoločnosť ovplyvnilo a pri každom uzatvorení *Zmluvy o poskytovaní služieb* dáva svojim zákazníkom podpísať *Súhlas so spracovaním údajov*, aby im mohla aj naďalej poskytovať svoje služby.

Ďalším dôležitým legislatívnym faktorom je výška odvodov na zamestnanca a podnikateľa, ktorá sa neustále zvyšuje, takže sa výrazne zvyšujú aj celkové náklady firmy.

2.4.6 Ekonomické faktory

Ekonomická časť analýzy spočíva v rozbore národnej a prípadne miestnej ekonomiky. Existuje viacero faktorov, ktoré fungovanie spoločnosti na trhu priamo ovplyvňujú, napr. nezamestnanosť, kúpna sila a miera inflácie.

Vybraná spoločnosť má sídlo v Slovenskej republike a preto je vhodné bližšie preskúmať ekonomické faktory najmä v tejto zemi.

Slovenská ekonomika

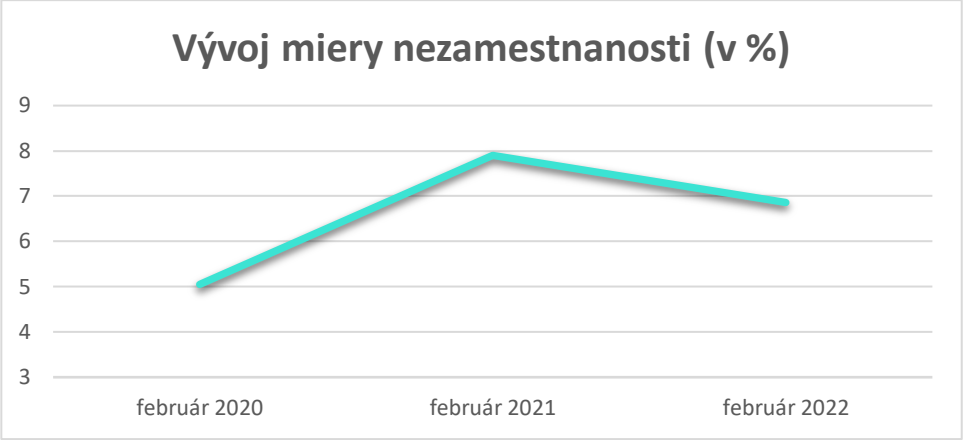
Najskôr priblížim vývoj ekonomiky v Slovenskej republike, kde zanalyzujem makroekonomické javy – mieru nezamestnanosti, minimálnu mzdu a vývoj cien energií.

Miera nezamestnanosti

Spolu so vznikom pandémie a rastom covidových prípadov ešte v roku 2020, rástla postupne aj miera nezamestnanosti. Mesiac pred vypuknutím pandémie a zasiahnutím Slovenska koronavírusom bola miera nezamestnanosti na úrovni 5,05 % ešte vo februári 2020. O rok neskôr, v roku 2021, sa miera nezamestnanosti vyšplhala až na hodnotu 7,9 % a podľa posledných štatistických údajov je tento ukázateľ na úrovni 6,86 % za mesiac február 2022.

Všeobecne vyššia hodnota nezamestnanosti môže byť pre niektoré firmy príležitosťou nabrať nových ľudí (ak to finančne utiahnu), avšak pre IT firmu, akou je mnou vybratá,

to neplatí, pretože v dopyt po kvalifikovaných pracovníkov v IT oblasti v dnešnej dobe výrazne stúpa, a tým je týchto ľudí na trhu dostupných menej.

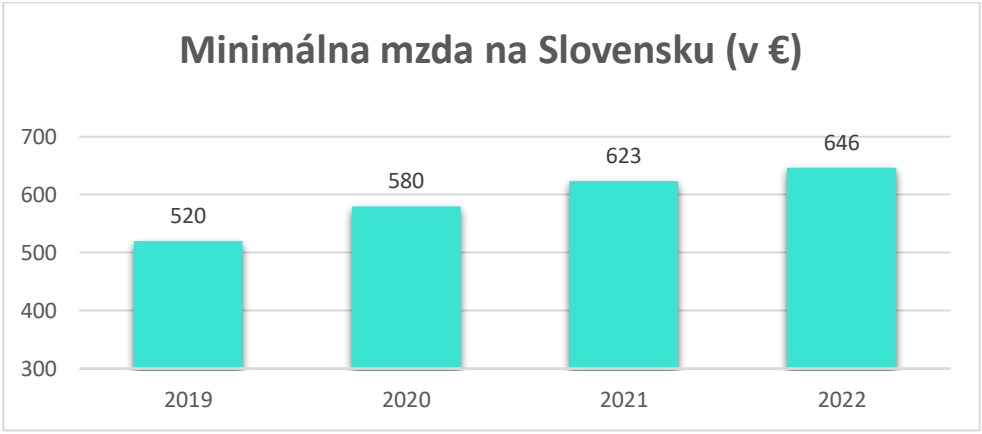


Obrázok č. 15: Vývoj miery nezamestnanosti v posledných rokoch

(Zdroj: Vlastné spracovanie)

Minimálna mzda

Podľa zákona č. 663/2007 Z. z. o minimálnej mzde a Zákonníka práce § 119 ods. 1, má každý zamestnanec nárok aspoň na minimálnu mzdu, ktorá je podľa údajov z Ministerstva práce a sociálnych vecí na úrovni 646 € za mesiac (hrubý príjem).



Obrázok č. 16: Vývoj minimálnej mzdy na Slovenku v priebehu rokov

(Zdroj: Vlastné spracovanie)

Výška minimálnej mzdy obmedzuje firmu v naberaní nových ľudí, pretože si finančne nemôže dovoliť nabrať veľké množstvo ľudí, ale len zopár kvalifikovaných. Čo je síce pre firmu výhodné, ale nie vždy je v užšom výbere (tzv. *talent poole*) dostatok kvalifikovaných ľudí na pozície, ktoré firma potrebuje.

Vývoj cien energií

Ceny energií klesali od mája roku 2020 do februára 2021 v rozmedzí od 1 do 9-tich %, avšak od marca roku 2021 začali výrazne stúpať. V novembri 2021 boli ceny na rekordnej úrovni 26 %, avšak táto hodnota bola v januári 2022 prekonaná, vyšplhala sa až na úroveň 27 %. Aj tento faktor môže výrazne ovplyvniť dopyt po internetových, či televíznych službách spoločnosti, keďže to výrazne ovplyvňuje výdaje domácnosti, a tým pádom niektoré skupiny ľudí budú mať tendenciu utrácať menej paňazí sa tieto služby, čo firme spôsobí nižší dopyt, a tým aj nižší výnos z poskytovania svojich služieb.

2.5 Výsledky analýz

Zanalyzovaním podniku a jeho vonkajšieho okolia som zistila, že firma má niekoľko príležitostí a silných stránok, na ktoré by mala klásť väčší dôraz.

Medzi ***silné stránky*** jednoznačne patrí silné postavenie firmy na trhu s poskytovaním televíznych a internetových služieb. Firma často rozširuje svoju ponuku služieb, aby zaujala čo najväčšie množstvo ľudí, ktoré môže uspokojiť spoľahlivými službami vďaka kvalitnému základu telekomunikačnej infraštruktúry a dátových sietí. Vysoko kvalifikovaní zamestnanci a špecialisti vo svojom odbore takisto pridávajú firme dobré renomé v regionálnej oblasti. V neposlednom rade, silnou stránkou firmy je flexibilita pracovníkov z technického oddelenia, transparentná komunikácia so zákazníkmi a ochota pomôcť pri riešení problémov aj mimo pracovnej doby.

Medzi ***príležitosti*** jednoznačne patrí popularita IT a záujem o prácu v tejto oblasti. Firma tak má väčší tzv. *talent pool*, z ktorého môže vyberať kandidátov, budúcich zamestnancov, ktorí by sa venovali monitorovaniu sieťovej prevádzky. Noví zamestnanci do technického tímu sa odrazia nielen na zvýšenej efektivite monitorovania a odhaľovania výpadkov siete, ale aj vo finančných ukázateľoch firmy, keďže sa

minimálna mzda každým rokom na Slovensku zvyšuje. Značnou príležitosťou je aj fakt, že ľudia trávia veľa času na internete a veľa ich pracuje z domu, čo zvyšuje dopyt po televíznych balíkoch a po kvalitnom a rýchlom internetovom pripojení.

Medzi súčasné ***hrozby*** vo firme a tie, ktoré môžu nastať pri implementovaní navrhovanej zmeny patrí ľudský faktor, resp. pochybenie človeka. Najúčinnejším opatrením je kontrola dôležitých rozhodnutí, aby sa zamedzilo vzniku problémov v budúcnosti. Ďalšou hrozbou, ktorá môže nastať je výpoveď od kvalifikovaných zamestnancov, ktorí majú vo firme dôležité postavenie, väčšinou nemajú za seba plnohodnotnú náhradu a ich práca je kľúčová pre správny chod spoločnosti.

Analyzovaná firma v súčasnej dobe začína s monitorovacím systémom, avšak tento proces neprebieha efektívne kvôli nedokončenej konfigurácii systému a infraštruktúry a aj kvôli tomu, že na sledovanie aktuálnej sieťovej prevádzky nie je vyhradený ani jeden zamestnanec, čo negatívne pôsobí na odhalenie výpadkov siete v budúcnosti. Sledovanie dátových tokov a prevádzky siete by malo byť pre spoločnosť najvyššou prioritou, pretože poskytovanie spoľahlivých a kvalitných služieb zákazníkom je pre jej existenciu kľúčové a nevyhnutné.

Aktuálny stav vo firme je nevyhovujúci a je nutné vykonať zmenu čo najskôr, v opačnom prípade to môže firme spôsobiť veľké problémy.

3 NÁVRH RIEŠENÍ

Táto kapitola práce sa zameriava na návrhy na zavedenie zmien vo firme, konkrétne ide o implementáciu nového informačného systému (zvolenej technológie) na monitorovanie sieťovej prevádzky v reálnom prostredí. Tento návrh je založený na analytickom základe, ktorý bol bližšie popísaný v predchádzajúcej kapitole tejto práce; na podmienkach nasadenia, na postupe inštalácie a na konfigurácii vybranej technológie. Na záver bude toto riešenie aj ekonomicky zhodnotené, zhodnotím výhodnosť a efektivitu tejto technológie vo firme.

3.1 Dôvody potreby nasadenia technológie

Firma, ktorá poskytuje dátové a internetové služby zákazníkom B2B a B2C potrebuje mať vybudovanú dostatočne veľkú dôveru v zákazníkoch, v ktorej jej pomôže zabezpečovanie spoľahlivého internetového pripojenia. Správne nastavenie a používanie monitorovania dátovej prevádzky zabezpečí spoľahlivé pripojenie bez dlhších výpadkov, a v takom prípade zákazník nemusí ani postrehnúť, že k nejakej chybe došlo, ak firma bude reagovať dostatočne včas. Veľké zaťaženie siete a následný dlhší výpadok môže spôsobiť stratu zákazníkov, ktorí sú pre existenciu spoločnosti kľúčovými.

Ako som už spomínala v úvode práce, na monitorovanie záťaže siete nie je pridelený konkrétny pracovník, ktorého zodpovednosť spočíva iba v kontrole dátovej prevádzky. To znamená, že zvolený pracovník sa plne nesústredí len na monitorovanie, ale reaguje iba v prípade notifikácii, výstrah, a preto je každý deň veľké riziko, že nastanú problémy s výpadkom sietí v budúcnosti.

V súčasnosti je za tieto kontroly zodpovedný pracovník v IT (technickom) oddelení spolu so softvérovým integrátorom, ktorí dostávajú upozornenia zo systému a sú zodpovední za predanie týchto informácii a následné delegovanie na príslušné oddelenie. Za vyriešenie vzniknutých problémov sú už (vo väčšine prípadov) zodpovední technici, ktorí sú vyslaní do terénu, aby situáciu vyriešili v čo najkratšom čase.

To, že na túto činnosť nie je pridelený konkrétny zamestnanec sprevádza fakt, že je to spoločnosť s relatívne malým počtom zamestnancov; a to je dôvodom, že pravidelné

kontroly záťaže siete neprebiehajú, čo môže viesť k neželaným výsledkom. Aj napriek tomu sa podarilo zamestnancom zostaviť pár pravidiel, kedy má systém vyslať upozornenie, takže v konečnom dôsledku to riziko výpadku nemusí byť také vysoké.

Avšak v budúcnosti, pri expanzii firmy (so zvyšovaním počtu zákazníkov a spravovaných sietí) by som odporúčala vyhradiť celý tím zamestnancov alebo aspoň jedného zamestnanca len na monitorovanie prevádzky, ktorý by bol zodpovedný za všetky spojené procesy a vedel by včas predvídať situáciu a zasiahnuť.

Po vypracovaní krátkeho dotazníku som zistila, že vo firme nikto nemá čas na kontrolu monitoringu, a preto sa viacmenej spoliehajú len na nastavený systém upozorňovania najkritickejších reportov. Kontrola neprebieha vôbec pravidelne, čo som pôvodne predpokladala.

3.2 Implementácia navrhovanej zmeny z technického pohľadu

Ďalšou časťou návrhovej kapitoly je implementácia navrhnutého riešenia z technického pohľadu. Popisujem podmienky pre nasadenie technológie, postup a nastavenie jednotlivých parametrov.

3.2.1 Dôvod výberu technológie LibreNMS a pracovnej stanice

Po analýze viacerých nástrojov na monitorovanie sieťovej prevádzky ako je napr. Wireshark, Zabbix, MRTG, DarkStat, Monitorix alebo Microsoft Network Monitor, organizácia zvolila nástroj LibreNMS pretože dokáže takmer ako jediný sledovať viacero procesov súčasne. V prípade zahltenia siete nástroj dokáže behom niekoľkých sekúnd presmerovať prevádzku cez inú trasu (iné zariadenie) alebo v prípade výpadku dokáže automaticky zariadenie reštartovať bez nutnosti fyzického zásahu človekom. Avšak výber konkrétnej technológie ***nie je*** predmetom tejto diplomovej práce.

Zvolený nástroj funguje na operačnom systéme Linux, ktorý je zdarma. Ako pracovnú stanicu, na ktorej je technológia nainštalovaná, spoločnosť vybrala počítač HP Z1 G8 Tower s parametrami RAM 16GB, SSD 512GB a 6 jadrový procesor Intel Core i5. (32)

Vyššia pamäť RAM umožní technológii mať spustených veľa procesov naraz, čo je veľmi efektívne na monitorovanie sieťovej prevádzky. Je nutné zvoliť počítač s dostatočne

vysokým výkonom procesora. Zvolená pracovná stanica vyhovuje požiadavkám technológie a má veľmi dobrý pomer cena a výkon.

3.2.2 Riešenie incidentov

V prípade vzniku incidentu LibreNMS spustí podprogram, ktorý opraví danú závadu - automaticky reštartuje zariadenie, presmeruje sieťovú prevádzku napr. v prípade prehltenia siete, spustí zálohovaný okruh, v prípade výpadku siete zálohuje dáta na server a upozorní pracovníkov emailom alebo SMS-kou.

Systém zvládne väčšinu incidentov vyriešiť sám, avšak ľudský dohľad je aj napriek tomu nevyhnutný. Preto by bolo vhodné mať na monitorovanie vyhradeného jedného človeka.

3.2.3 Organizačné začlenenie technológie

Vlastníkom zvolenej technológie ako u každého iného aktíva bude spoločnosť, resp. jej majiteľ, ktorý je za ňu aj zodpovedný. Zamestnanci, ktorí budú potrebovať s danou technológiou pracovať, budú mať *právomoc* k nej pristupovať.

Na obsluhovanie technológie bude vyhradený (minimálne) jeden ***zamestnanec***, ktorý bude súčasťou technického oddelenia a bude *zodpovedný* za reportovanie všetkých neštandardných stavov hlavnému technikovi, ktorí už ďalej rozdelí prácu medzi technikov, aby mohli včas zasiahnuť v prípade vzniku problému. Povinnosťou tohto zamestnanca bude aj viesť evidenciu, sledovanie štatistík a upozornení v hlavnom informačnom paneli nástroja.

3.2.4 Popis vybranej technológie

Zvolená IT spoločnosť vybrala systém Libre NMS, ktorý môže využiť na monitorovanie dátovej prevádzky. Tento systém je založený na PHP a využíva protokol SNMP (Simple Network Management Protocol) na aplikačnej vrstve. (19)

Spoločnosť nástroj Libre NMS bude môcť využiť nielen na monitorovanie záťaže siete a na správu aktívnych prvkov v sieti, ale tento nástroj poskytuje ešte veľa ďalších možností jeho využitia. Medzi ne patrí napr. automatické zisťovanie siete pomocou ARP, SNMP alebo BGP, ktorý využíva vybraná firma. Systém umožňuje automatické

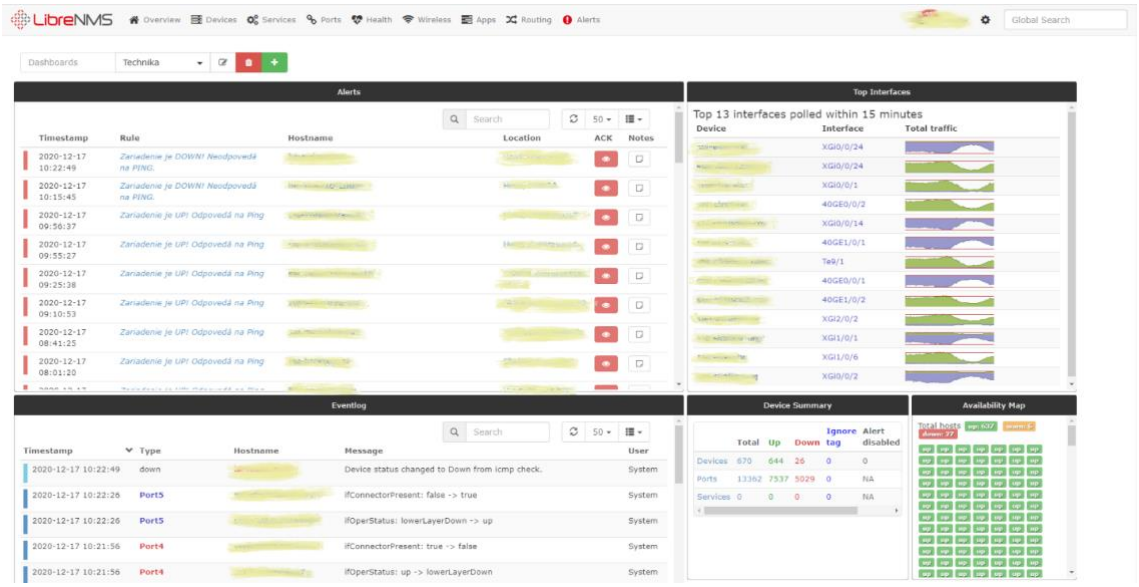
aktualizácie a správu cez úplné rozhranie API, kde možno vytvárať a editovať grafy a načítavať viaceré štatistické údaje podľa firemných požiadaviek.

Obrázok č. 17: Logo nástroja Libre NMS

(Zdroj: 19)

Monitorovanie a pozorovanie dátového toku je možné aj skrz aplikáciu na mobilných zariadeniach (prispôsobené webové UI), je vstavaná integračná podpora pre SmokePing, NFSen. Nástroj takisto poskytuje viaceré možnosti autentifikácie (cez MySQL, http alebo LDAPs).

V neposlednom rade je vhodné spomenúť prispôsobiteľný systém upozorňovania – je tu možnosť nastavenia kritickosti výstrahy a nastaviť upozornenie cez vybratý komunikačný kanál (napr. emailom, na Slack alebo pomocou SMS upozornení). (19)



Obrázok č. 18: Základný dashboard Libre NMS

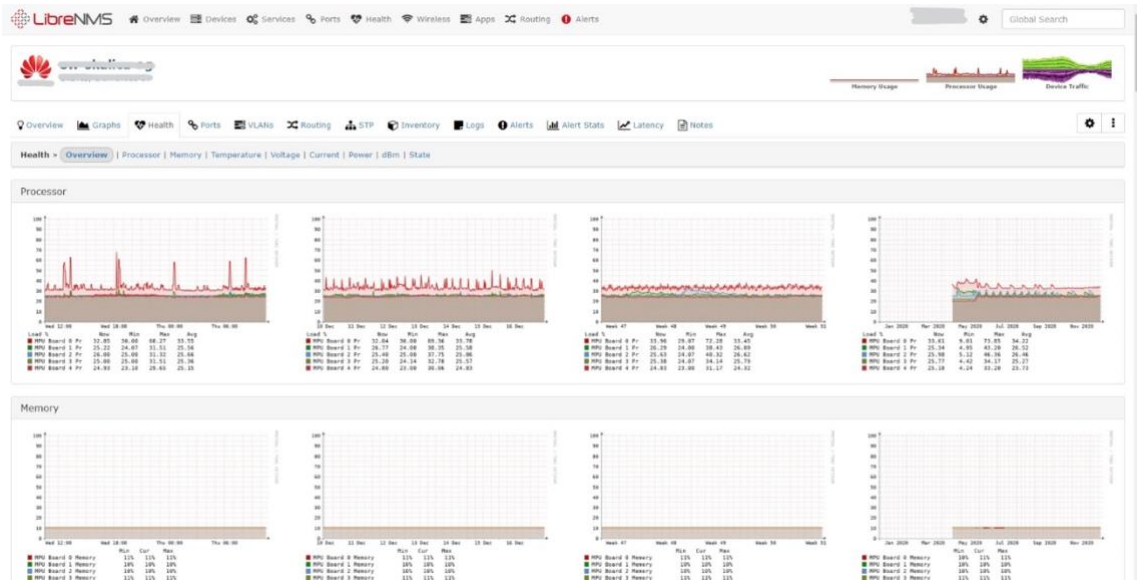
(Zdroj: 19)

Na predošlom obrázku môžeme vidieť úvodnú stránku po prihlásení sa do Libre NMS. Táto stránka nám umožňuje pohľad na monitoring celej siete – tabuľku nedávno zaslaných upozornení (výstrah), zoznam eventlogov, zoznam rozhraní, ktoré boli naposledy použité a základné informácie o našich zariadeniach, portoch a službách (či fungujú správne – identifikátor up / down). Tento prehľad nám podáva rýchle informácie o celkovej prevádzke siete (tzv.*traffic*) a je užívateľsky prispôsobivý.

Hlavný informačný panel nám ponúka detailnejšie zobrazenie služieb, zariadení, jednotlivých portov, tzv. zdravie firemných sietí, aplikácií, nastavenie smerovania a zoznam upozornení a výstrah. V pravom hornom rohu si môžeme konfigurovať všeobecné užívateľské nastavenia.

V systéme si dokážeme vyčítať podrobnejšie informácie o jednotlivých zariadeniach (switchoch) a portoch; a to aj pomocou grafického znázornenia. Z jednotlivých grafov si v okne Zdravie (*Health*) vieme vyčítať zaťaženie procesorov a pamäte, teplotu jednotlivých portov, hodnoty napätia, prúdu, napájania, útlmu a stav konkrétnych portov.

Grafy znázorňujú namerané hodnoty z dlhšieho časového hľadiska – hodinové, dňové, týždňové a mesačné zobrazenie údajov. Nasledujúci obrázok zobrazuje namerané hodnoty vo firme na vybranom switchi.



Obrázok č. 19: Okno Zdravie

(Zdroj: 19)

3.2.5 Podpora vybranej technológie

Technická podpora zvolenej technológie je online vo forme oficálnej stránky komunity, FAQ, Discord, Twitter, GitHub a takisto vo forme dostupných manuálov online.

3.2.6 Podmienky nasadenia

Na nainštalovanie nástroja Libre NMS je v prvom rade nutné mať nainštalovaný Linux server s podporovaným operačným systémom a odporúčaným webovým serverom NGINX. Ďalšou podmienkou je PHP verzie 7.3 a vyššie.

3.2.7 Postup inštalácie v reálnom prostredí

Základnou podmienkou pre správne nainštalovanie je byť adminom (tzv. *root userom*), ak to neplatí, je potrebné pred jednotlivé príkazy dávať tzv. *sudo*.

Užívateľ má na výber tri servery, na ktorých môže inštalovať LibreNMS:

- na serveri Ubuntu
- na serveri CentOS
- na serveri Debian

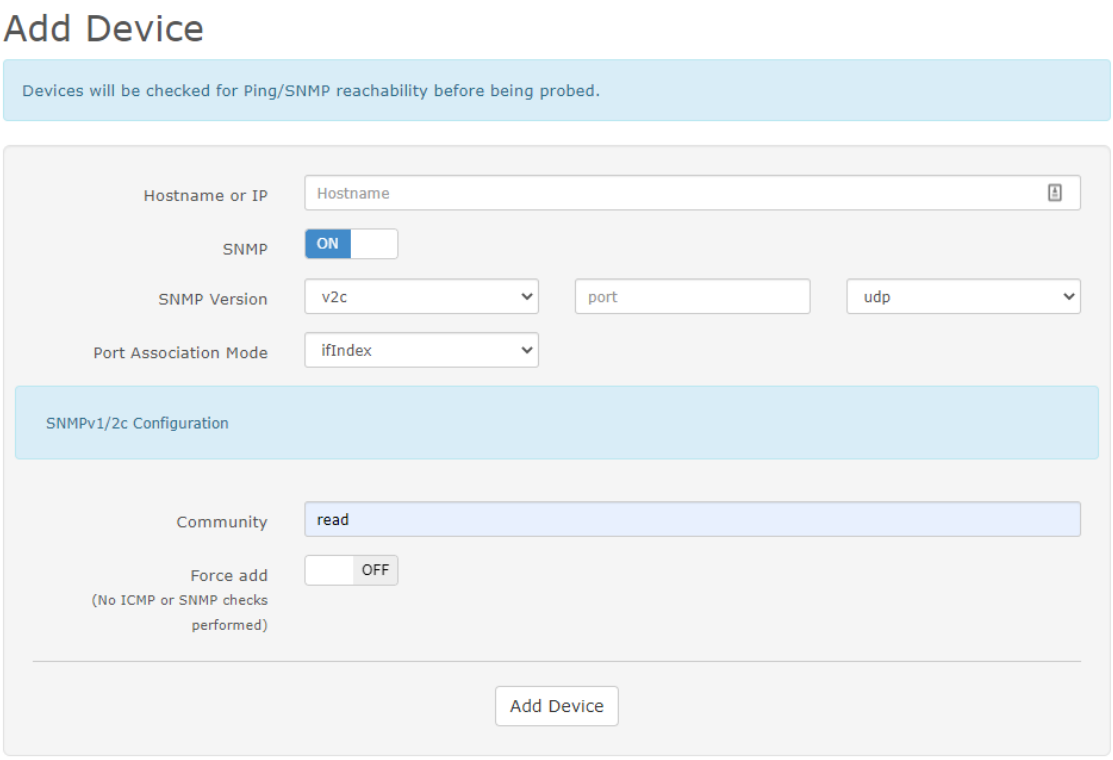
Pre konkrétne kroky inštalácie a nastavenie parametrov som si vybrala príkazy vhodné pre server Ubuntu (ostatné servery sa líšia len v malých detailoch).

Jednotlivými krokmi inštalácie sú:

- inštalovanie potrebných balíčkov (vyžaduje prihlásenie užívateľa, príkaz *apt update*),
- pridanie užívateľa LibreNMS (príkaz *useradd*)
- stiahnutie serveru LibreNMS
- nastavenie povolení
- nastavenie časových zón
- konfigurovanie databázy pomocou príkazov MySql (príkazy na vytvorenie databázy, užívateľa, nastavenie tzv.privilégií)
- konfigurácia PHP a webového servera
- povolenie prístupu cez firewall (predvolene prístup nie je povolený)

- povolenie príkazu Inms
- nakonfigurovanie snmpd (nastavenie vlastného reťazca *community string*)
- inštalácia webu (podľa zobrazených pokynov na obrazovke)
- (nakonfigurovanie zabezpečeného HTTPS, ktoré nie je predvolene nastavené)

Po úspešnej inštalácii je už možné sa prihlásiť na stránke http://librenms.example.com/ a začať pridávať svoje zariadenia cez webové rozhranie (ako prvé sa odporúča pridať localhost). Takisto je možné konfigurovať nastavenia optimalizácie výkonu, upozorňovania, editovať skupiny zariadení a nastaviť automatické zisťovanie nových zariadení.



Obrázok č. 20: Pridávanie nového zariadenia

(Zdroj: 19)

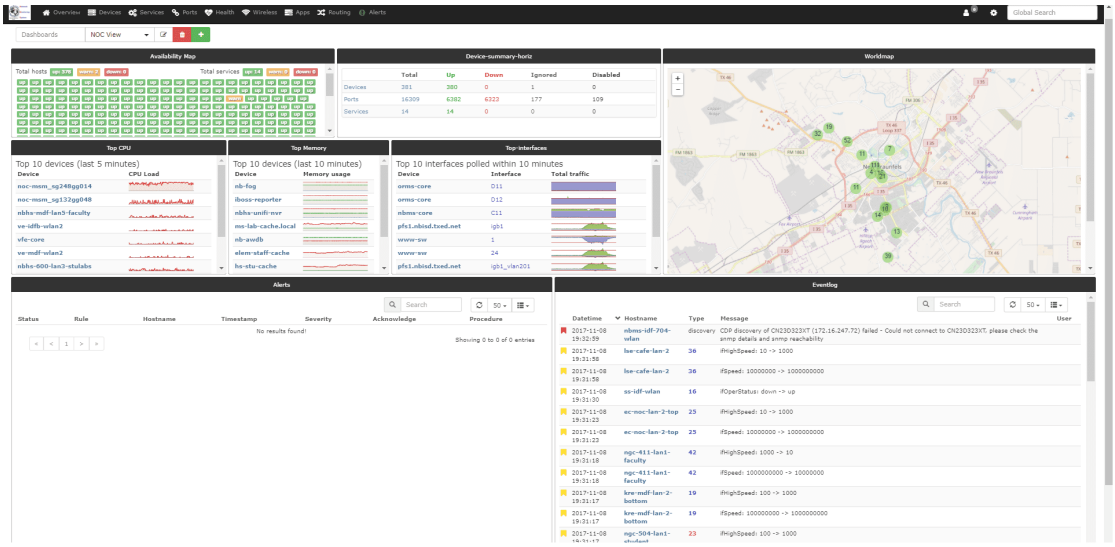
Jednotlivé zariadenia je možné pridávať do tzv. komunít, ktoré si vytvoríme podľa našich požiadaviek (napr. v našom prípade je to komunita *read*).

3.2.8 Nastavenie jednotlivých parametrov

Server Libre NMS poskytuje možnosť zmeniť nastavenia podľa vlastných požiadaviek, aby si každý mohol prispôsobiť monitoringovací systém na jeho sieťovú prevádzku.

Dashboard

Jedným zo základných parametrov, ktoré je užitočné nastaviť už hneď na začiatok je prispôsobenie si základného informačného panela (*dashboardu*), ktoré si každý užívateľ môže prispôsobiť pre seba (výhodné, ak na monitoring sú pridelení viacerí ľudia a každý je zodpovedný za inú oblasť).



Obrázok č. 21: Úvodný informačný panel

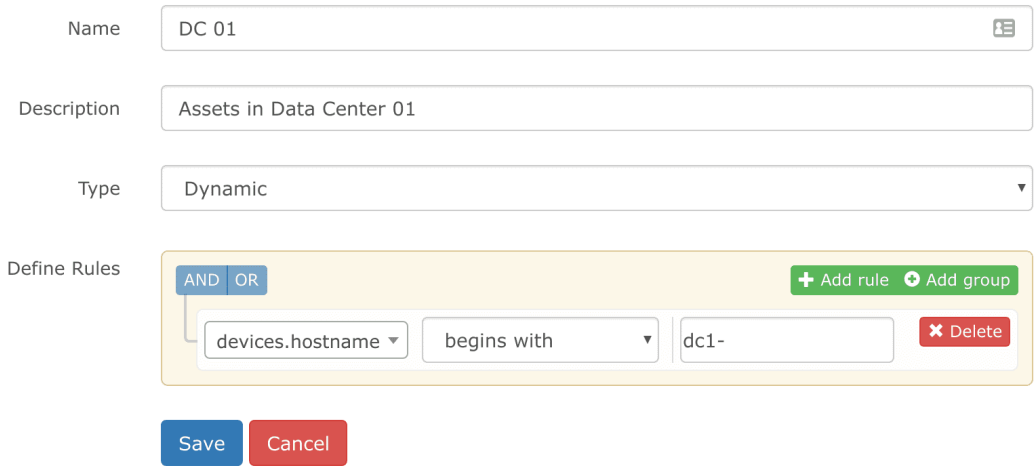
(Zdroj: 19)

Užívateľ si môže vybrať z viacerých widgetov, ktoré mu poskytnú rýchly prehľad o tých najnutnejších údajoch. Podporované sú widgety pre prehľad všetkých výstrah a upozornení, zoznam zariadení, eventlogov, základné prispôsobené grafy, poznámky, najvyťaženejšie zariadenia a rozhrania a mnoho iných.

Vytvorenie skupín zariadení

Nastavenie pravidiel je možné pomocou príkazov založených na štruktúre MySQL. Jedná sa o zobrazenie všetkých entít *show tables*, zoskupovanie na základe názvu zariadenia *device.hostname* alebo na základe typu.

Takisto si môžeme vytvoriť aj ***statické skupiny*** (a/alebo konvertovať dynamické na statické), ktoré budú obsahovať len nami vybrané zariadenia. Toto nastavíme hodnotou *Static* v poli *Type* a následne pridáme požadované zariadenia.



Obrázok č. 22: Vytvorenie skupín zariadení

(Zdroj: 19)

Automatické zisťovanie nových zariadení

Po pridaní minimálne jedného zariadenia v systéme si môžeme nastaviť automatické pridávanie ďalších zariadení do našej siete. Libre NMS poskytuje viacero spôsobov, ako sa to dá nastaviť. Základnými požiadavkami systému pre nastavenie tejto možnosti je vedieť detaily SNMP, zoznam našich sietí a podsietí (na základe IP adresného priestoru), nastavenia výnimiek zariadení, ktoré nemôžeme automaticky priradiť (príkazom *autodiscovery nets-exclude* s priradením konkrétnej IP adresy tohto zariadenia).

Automatické pridávanie nových zariadení je predvolene nastavené podľa reverzného dns mena, ale je možné to nastaviť aj podľa IP adresy.

Metódy zisťovania nových zariadení:

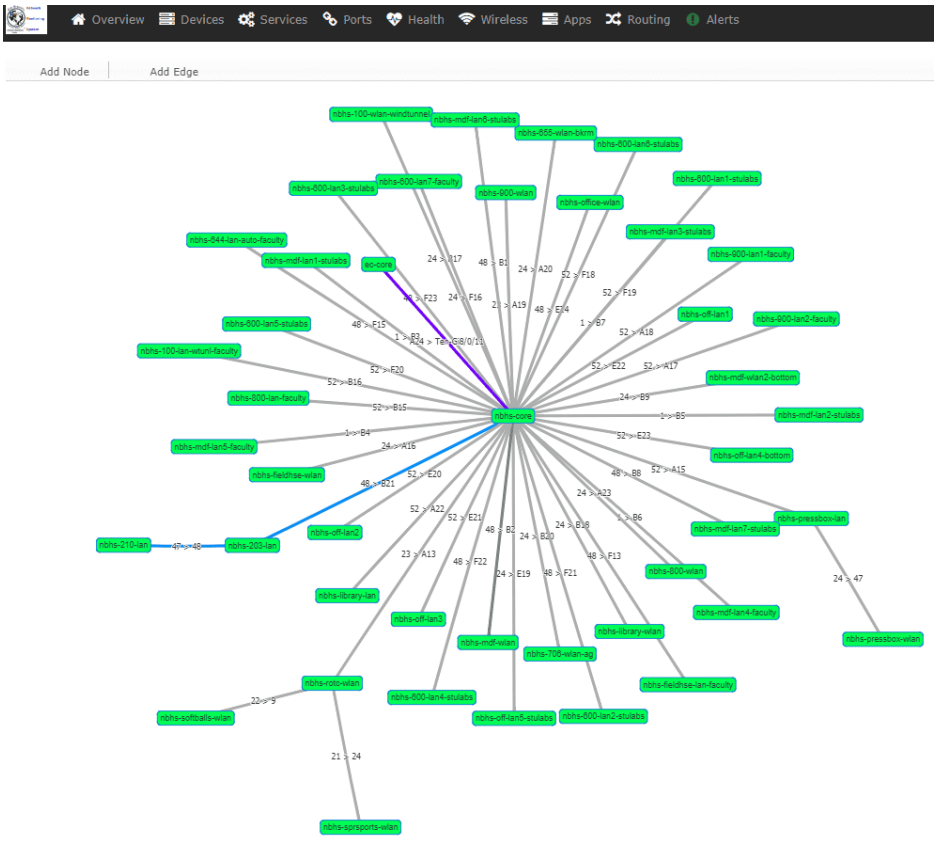
- ARP (predvolene zakázané) – pridanie nového zariadenia na základe údajov v ARP tabuľke (nutné mať povolený modul ARP tabuľky a navrátenia hodnôt)
- XDP (predvolene povolené) – podpora FDP, CDP a LLDP
- OSPF (predvolene povolené)

- BGP (predvolene povolené)
- Pomocou skenovania SNMP – pri povolení tejto možnosti je sieť skenovaná s rešpektovaním nastavených pravidiel (obmedzení) a pomocou nakonfigurovanej siete

Vybraná firma má možnosť automatického pridávania zakázanú a nové zariadenia si tam pridávajú sami manuálne, kvôli tomu, aby sa im nemiešali klientské zariadenia s tými, ktoré spravujú.

Network Map

Mapa sietí sa dá predvolene zobraziť na základe MAC adries a / alebo tzv. xDP zisťovania (založené na podpore FDP, CDP a LLDP). Zobrazenie máp je možné nakonfigurovať podľa potreby, dajú sa zobraziť vzťahy pre jednotlivé zariadenia alebo aj skupiny zariadení.



Obrázok č. 23: Network Map

(Zdroj: 19)

Optimalizácia výkonu

Na zníženie záťaže siete je viacero možností, ako toho dosiahnuť. Medzi ne patrí napríklad nakonfigurovanie RRDCached, optimalizácia MySQL (navrhnutie odporúčaní podľa našich nastavení), zakazovanie načítavania nepotrebných modulov, nastavenie maximálneho počtu SNMP opakovačov, upravenie webového rozhrania a mnoho ďalších.

Rýchla kontrola stavu (Fast up / down checking)

Nastavenie tohto parametru je celkom užitočné pre popisovanú firmu, pretože kontrola zariadení, či sú *up* alebo *down* prebieha v časovom úseku piatich minút a nastavenie *Fast checking-u* umožní rýchlejšie reagovať na možné problémy so zariadeniami a so zvýšenou záťažou siete.

Dvojfaktorová autentizácia

Odporúčaným dodatočný nastavením je napríklad povolenie ***dvojfaktorovej autentizácie*** užívateľa, ktorá prístup obmedzí len na pár vybraných užívateľov vo firme a tak zaistí zvýšenú bezpečnosť ukladaných dát. Toto sa dá nakonfigurovať dvomi možnosťami:

- ***TOTP*** – časové jednorázové heslo, je nutné poznať tajný kľúč;
- ***COTP*** - jednorázové heslo založené na synchronizovaní počítadla so serverom, je to bezpečnejší typ ako TOTP.

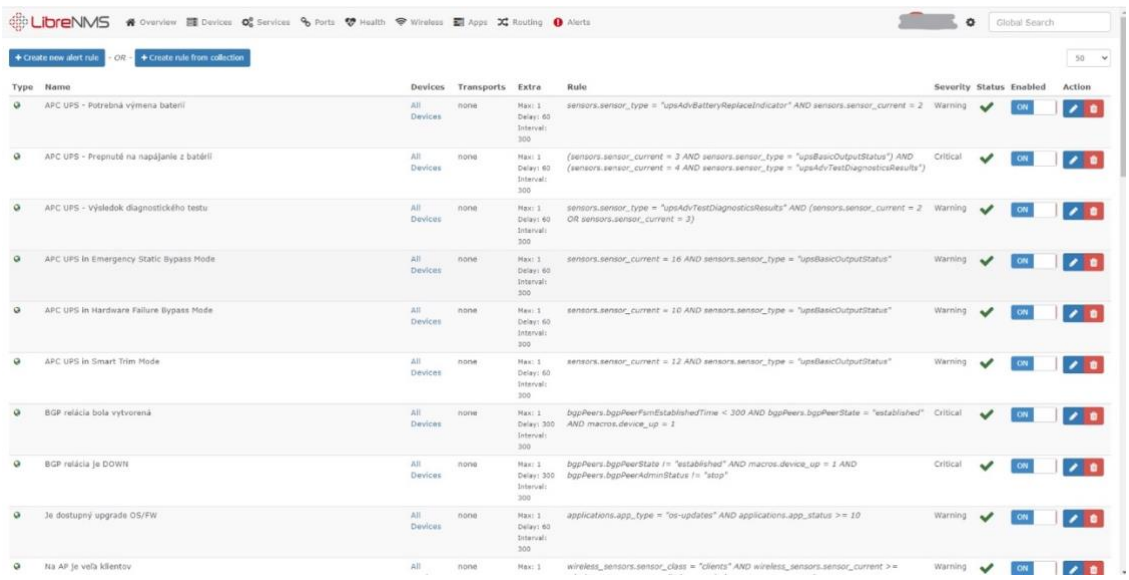
Zhrnutie parametrov

Je zrejmé, že je možné nastaviť ešte ďalšie parametre pre efektívnejšie monitorovanie, vyššiu optimalizáciu systému a vyššiu bezpečnosť, ale pre túto prácu som vybrala tie najzákladnejšie, ktoré by nemali chýbať pri úvodnej implementácii. Ďalšie nastavenia si dokáže spoločnosť nastaviť podľa používaných oblastí, kde jej to príde vhodné upraviť, vylepšiť a rôzne editovať.

3.2.9 Systém upozorňovania (*alerting*)

Užívateľ má pri nastavovaní upozorňovacieho systému veľmi rozsiahly zoznam možností. Základným nastavením je názov a obsah upozornenia (*rule*), čas (*timestamp*), názov zariadenia (*devices*) a v neposlednom rade level kritickosti (upozornenie / výstraha).

Na nasledujúcom obrázku je zopár konkrétnych ***pravidiel na zasielanie upozornení***, ktoré som s technikom spoločnosti nastavila. Po spoločnom brainstormingu sme najskôr začali tvorbou zoznamu *výstrah*, ktoré majú pre spoločnosť kritickú závažnosť (*severity*) a neskôr tými, ktoré sú označené len ako *upozornenie*. Systém bude technikom na to určeným zasielať upozornenia ohľadom potreby výmeny batérii, napájania, zlyhania hardvéru, výpadku siete, či preťaženia siete.



Obrázok č. 24: Nastavenie pravidiel upozorňovania

(Zdroj: 19)

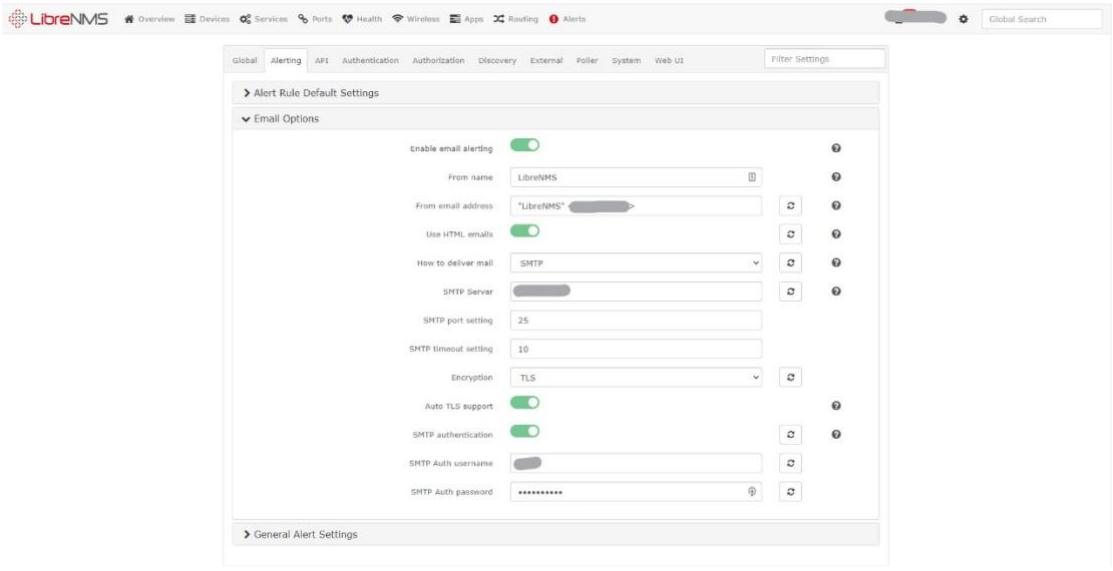
Reporty sa odosielajú každú minútu, keď nastane situácia definovaná v pravidlách (časový úsek je skrátený pre rýchlejšiu reakciu), sú primárne odosielané emailom a SMSkou dvom zamestnancom v technickom oddelení a tí to vyriešia na diaľku alebo v kritickejších prípadoch riešenie delegujú na technikov, ktorí už fyzicky zasiahnu.

Všetky upozornenia sa ukladajú v systéme LibreNMS po dobu jedného mesiaca.

Obrázok č. 25: Príklad upozornení ku zvolenému zariadeniu

(Zdroj: 19)

Jednotlivé upozornenia je možné zasielať na vybrané komunikačné kanály, napr. cez email, na Slack, na webovej stránke v systéme a dokonca je možnosť využiť aj SMS upozornenia v tých najkritickejších stavoch.



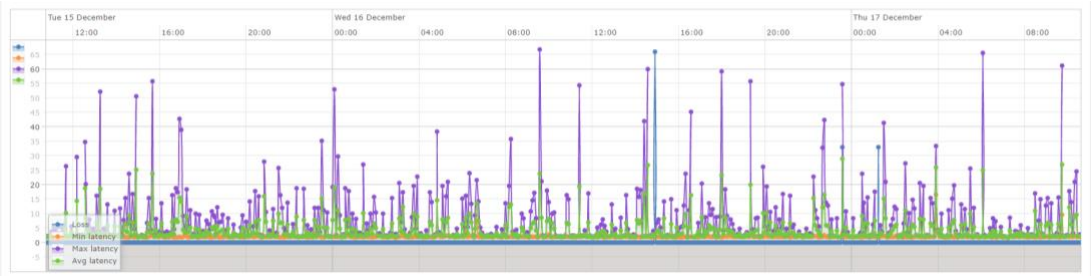
Obrázok č. 26: Nastavenie emailových upozornení

(Zdroj: 19)

3.2.10 Monitorovanie prevádzky

Do tejto oblasti som zahrnula zopár štatistík a grafov z reálneho prostredia. Zobrazenie viacerých grafov je v hodinách, dňoch, týždňoch a mesiacoch.

Na obrázku je vidieť oneskorenie na jednotlivých zariadeniach.



Obrázok č. 27: Latencia (oneskorenie) na zariadení

(Zdroj: 19)

Obrázok č. 28: Ping Response

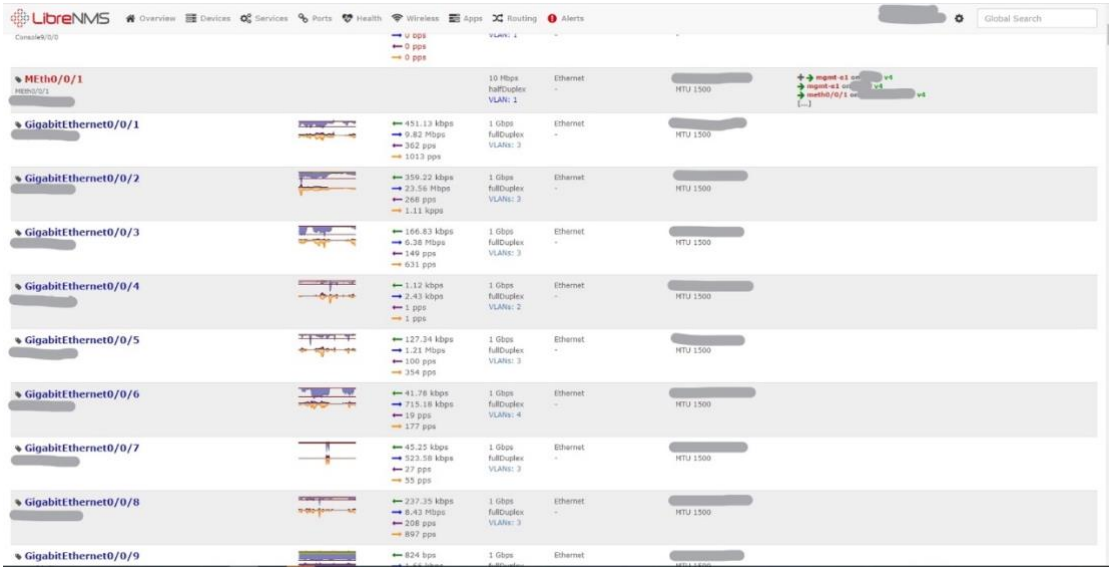
(Zdroj: 19)

Nasledujúci obrázok znázorňuje namerané teploty jednotlivých portov v zariadení.

Obrázok č. 29: Teplota jednotlivých portov v zariadení

(Zdroj: 19)

Z nasledujúceho obrázku vieme vyčítať aktuálny stav všetkých portov vybraného switchu. Vidíme tu zoznam a označenie všetkých portov, *traffic* (download a upload), rýchlosť VLAN, MAC adresu a maximálnu prenosovú jednotku (MTU).



Obrázok č. 30: Prehľad portov

(Zdroj: 19)

3.3 Implementácia navrhovanej zmeny z pohľadu projektového riadenia

V tejto podkapitole sa zaoberám implementáciou zmeny z pohľadu projektového manažmentu – určím potrebné kroky implementácie, vypracujem Lewinov model riadenia zmien, určím tri kľúčové role zmeny, intervenčné oblasti a zakončím časovou analýzou implementácie zmeny.

3.3.1 Popis navrhovanej zmeny

Spoločnosť má viacero požiadaviek, ktoré by mala implementácia vybranej technológie spĺňať. V prvom rade by firma vďaka implementácii zvolenej technológie mala byť schopná:

- efektívne monitorovať sieťovú prevádzku;
- monitorovať sieťovú prevádzku v reálnom čase a uschovávať historické dáta kvôli reportovaniu a štatistikám;

- mala by vidieť možné slabiny systému a infraštruktúry, kde sa môže firma zlepšiť a podniknúť určité kroky, aby chod siete bol bezpečnejší, plynulejší, bezproblémovejší a časovo menej nákladný aj z dlhodobého hľadiska;
- včasne predpovedať možné výpadky sietí a následne riešiť vzniknuté problémy včas, aby firma svojich zákazníkov nestratila;
- poskytovať menej vyťažené siete a tým si aj naďalej udržať spokojnosť svojich zákazníkov;
- včas detekovať potrebu servisov v rozvádzačoch v technických miestnostiach (napr. pri nefunkčnosti niektorých zariadení, switchov, routerov, či iného príslušenstva);
- pripojiť sa ku všetkým pripojeným zariadeniam v technickej miestnosti na diaľku;
- pracovať so zobrazovanými dátami rýchlejšie a produktívnejšie ako doteraz (bez možnosti monitorovania aktuálnej situácie);
- práca s novým systémom / technológiou by mala byť pomerne jednoduchá a zvládnuteľná aj pre menej kvalifikovaného zamestnanca;
- vidieť základný informačný panel (dashboard), ktorý si môže každý užívateľ prispôsobiť podľa seba. Toto nastavenie je výhodné, ak je na monitoring siete pridelených viac ľudí na rôzne jeho oblasti.
- vidieť rýchly prehľad o najnutnejších údajov vo forme widgetov – prehľad všetkých výstrah a upozornení, zoznam zariadení, eventlogov, základné prispôsobené grafy, poznámky, najvyťaženejšie zariadenia a rozhrania a mnoho iných.

Pri zvýšení požiadaviek na monitorovanie sieťovej prevádzky firma zníži riziko budúcich problémov, ktoré v súčastnosti nastávajú každý deň. Pri zavedení tejto novej technológie na monitorovanie sieťovej prevádzky bude možné sledovať aktuálnu situáciu v čase firemných zariadení. V spoločnosti bude vytvorený tím ľudí, ktorí sa budú zaoberať len oblasťou monitoringu prevádzky a jej následnou údržbou. Momentálne firma nedisponuje žiadnou takouto technológiou, vďaka ktorej by celý proces monitorovania bol oveľa efektívnejší a rýchlejší. Jednotlivé činnosti tohto riešenia (projektu) sú definované v ďalších podkapitolách tejto diplomovej práce.

3.3.2 Lewinov model

V tejto podkapitole vypracujem tri fázy *Lewinovho modelu* riadenia zmien, ktorý by mal pomôcť s implementovaním potrebnej zmeny vo vybranej spoločnosti.

A. Fáza rozmrazenia

Táto fáza sa začne konzultáciou medzi CEO spoločnosti a dvoch zamestnancov z technického oddelenia, ktorí by mohli byť na pozícii, kde sa budú starať o monitorovanie prevádzky. Jeden z nich je softvérový inžinier, ktorý bude pomáhať pri implementácii technológie a druhý bude môcť prevziať túto oblasť buď dočasne, kým si firma na to nenájde kvalifikovaných ľudí alebo natrvalo, ak zamestnanec prejaví záujem a bude dostatočne proaktívny a spoľahlivý. Výstupom konzultácie medzi jednotlivými stranami by mal byť zoznam požiadaviek a cieľov, ktoré budú vyžadovať za nevyhnutné.

Sily inicializujúce proces zmeny

Zmenou, ktorú budem popisovať v tejto časti, je zavedenie novej technológie na *monitorovanie sieťovej prevádzky* vo firme. Súčasťou implementácie je aj vznik nového tímu kvalifikovaných zamestnancov, ktorí budú mať túto oblasť vo svojej pracovnej náplni. Táto technológia poslúži na efektívne, rýchle a bezpečné sledovanie aktuálneho diania v technických miestnostiach a pri sledovaní dostupnosti siete pre klientov v reálnom čase.

Analýza silového poľa

Rozhodnutie, či požadovanú zmenu uskutočniť alebo nie, je možné určiť na základe kvantifikácie hybných a brzdných síl. Na to, aby zmenu bolo možné vykonať, je potrebné, aby celkový súčet hnacích síl bol vyšší ako súčet tých brzdných. Sily pôsobiace na zmenu som ohodnotila v intervale od 1 do 10, hybné sily kladnými hodnotami a brzdiace sily zápornými.

V nasledujúcej tabuľke vidíme znázornené sily pôsobiace **pre** (hnacie sily) a **proti** (brzdné sily) realizácii danej zmeny.

Tabuľka č. 13: Kvantifikácia síl

(Zdroj: Vlastné spracovanie)

Popis hnacích síl	*Hodnotenie (1-10)*	*Popis brzdiacich síl*	*Hodnotenie (1-10)*
Možnosť efektívne monitorovať sieťovú prevádzku	10	Finančné náklady na implementáciu technológie	- 3
Predpovedanie a eliminovanie výpadkov včas (včasný servis)	9	Nutný tréning užívateľov, aby bolo znížené riziko ľudského pochybenia a zaistené správne používanie	- 9
Dobrý prehľad o stave siete	7	Neochota zamestnancov sa naučiť pracovať s novou technológiou	- 7
Možnosť vidieť slabiny systému a infraštruktúry	5	Náklady na prilákanie a získanie nových zamestnancov do tímu monitorovania	- 10
Zníženie časových nákladov na riešenie vzniknutých problémov	6	Náklady na riadenie nového tímu	- 6
Zvýšenie tržieb	3		
Zvýšenie spokojnosti zákazníkov	8		
Poskytovanie menej vyťažených sietí	4		
Vylepšienie kvality poskytovania služieb	6		
Celkom	***58***		***35***

Z celkového súčtu oboch druhov síl je vidieť, že hybné sily prevládajú a vykonanie zmeny je teda možné, projekt je realizovateľný. Táto zmena je podporená viacerými benefitmi, ktoré daná technológia prinesie, ak sa implementuje. Takisto významnú úlohu

hrajú aj zákazníci firmy, ktorí sú pre ňu veľmi dôležití a bez ktorých by ďalej poskytovať služby nemohla.

Tri kľúčové role pre úspešnú zmenu

Agent zmeny je ten, kto *vykonáva* zmenu, takže agentom zmeny tohto projektu som ja a technik, ktorý firme pomáha implementovať monitorovací systém.

Sponzor zmeny zmenu *podporuje* zdrojmi a má *právomoc,* aby zmena prebehla. Sú to teda interní stakeholderi firmy, ktorým riešenie prospeje a požadujú ho. Primárne je to CEO vybranej spoločnosti, ktorý zároveň túto zmenu aj inicioval.

Advokát zmeny zmenu *potrebuje* a *podporuje,* preto advokátom tejto implementácie je najmä SW integrátor a technik, ktorý má na starosti monitorovanie firemných sietí a infraštruktúry.

Intervenčné oblasti

Zavedenie nového systému (technológie) na monitorovanie je implementovaná zmena, ktorá pôsobí vo viacerých intervenčných oblastiach, ovplyvní oblasti technologické, ekonomické, marketingové, ľudských zdrojov a zmení sa pri tom aj organizačná štruktúry spoločnosti.

Organizačná štruktúra sa zmení, pretože na efektívne monitorovanie prevádzky bude potrebný zamestnanec, ktorý sa bude primárne na túto oblasť špecializovať a postupne v budúcnosti sa vytvorí tím viacerých ľudí, ktorí budú mať na starosti inú podoblasť tejto tematiky.

Technologickú oblasť to ovplyvní v tom zmysle, že zavedenie novej technológie bude vyžadovať prepojenie infraštruktúry a viacerých zariadení, aby bolo vôbec možné technológiu správne využívať.

Marketingová oblasť bude ovplyvnená kvôli používaniu viacerých marketingových nástrojov na prilákanie nových kvalifikovaných ľudí a na zvyšovanie povedomia u zákazníkov o zlepšovaní kvality poskytovaných služieb.

Oblasť ľudský zdrojov bude ovplyvnená kvôli náboru nových zamestnancov a takisto kvôli prerozdeleniu súčasných tímov a pracovníkov, ktorí budú potrební pri implementovaní zmeny.

Ekonomická oblasť bude ovplyvnená kvôli celkovým nákladom na implementáciu zmeny, zakúpenie technológie a nákladmi na získanie potrebných pracovníkov a celého tímu ľudí.

B. Fáza vlastnej zmeny

V druhej fáze Lewinovho modelu prebieha implementácia na seba naväzujúcich činností. Fáza zavedenia zmeny pozostáva z nasledujúcich činností:

1. Rozhodnutie vedenia o zmene sledovania sieťovej prevádzky
2. Analýza podmienok nasadenia zmeny
3. Vyhodnotenie požiadaviek
4. Výber dodávateľa technológie
5. Konzultácia (a zmluva) s dodávateľom
6. Inštalovanie nového systému
7. Konfigurácia a prepojenie technológie
8. Nastavenie parametrov a pravidiel v systéme
9. Nastavenie bezpečnostných prvkov (dvojfaktorová autentizácia)
10. Testovanie technológie
11. Kontrola funkčnosti systému
12. Úprava prípadných nedostatkov
13. Prispôsobenie užívateľského rozhrania podľa potrieb firmy
14. Predanie finálneho riešenia systému
15. Záverečná kontrola systému (SW inžinierom)
16. Spätná väzba od SW inžiniera
17. Spracovanie požiadaviek zo spätnej väzby
18. Tvorba manuálov
19. Školenie zamestnancov
20. Spustenie novej technológie do prevádzky

C. Fáza zamrazenia

Vo fáze zamrazenia sa nový stav ukotví, resp. *zamrazí*, spolu s novo určenými pravidlami. Zavedená zmena je jednorázová, pretože ide o implementáciu vybranej technológie, ktorá sa bude dlhodobo používať po jej implementovaní viacerými užívateľmi. Pre CEO bude užitočné vedieť spätnú väzbu od užívateľov tohto systému, aby vedel, či táto investícia splnila očakávané požiadavky a priniesla želaná benefity, resp. či bola prospešná pre firmu za vynaložené náklady (finančné a časové).

3.3.3 Časová analýza

Táto podkapitola sa zaoberá časovou analýzou jednotlivých činností, ktoré sú potrebné k aplikovaniu navrhovanej zmeny pomocou využitia metódy PERT. Táto analýza firme detailnejšie zobrazí dobu trvania celého projektu až do úspešného konca, časovú náročnosť jednotlivých činností a na záver odhalím kritickú cestu s kritickými činnosťami celého projektu. Potrebné dáta slúžiace na spracovanie časovej analýzy sú vyobrazené nižšie. Doba trvania je udávaná v dňoch.

3.3.4 Časový harmonogram implementácie projektu

Legenda:

aij – optimistický odhad, koľko bude činnosť trvať

Mij – reálna doba trvania činnosti

Bij – pesimistický odhad, koľko bude činnosť trvať

$$yij = \frac{aij+4mij+bij}{6}$$

Nasledujúca tabuľka zobrazuje základné údaje, ktoré sú potrebné pre vypracovanie časovej analýzy, tzn. identifikácia jednotlivých činností navrhovanej implementácie, ich optimistická, reálna a pesimistická dĺžka trvania a bezprostredne predchádzajúca činnosť.

Tabuľka č. 14: Základné údaje pre spracovanie časovej analýzy

(Zdroj: Vlastné spracovanie)

Označenie činnosti	Činnosť	aij	mij	bij	Doba trvania (yij)	Bezprostredne predchádzajúca činnosť
A	Rozhodnutie vedenia o zmene sledovania sieťovej prevádzky	1	2	3	2	-
B	Analýza podmienok nasadenia zmeny	7	14	21	14	A
C	Vyhodnotenie požiadaviek	5	10	15	10	A
D	Výber dodávateľa technológie	4	5	12	6	B, C
E	Konzultácia (a zmluva) s dodávateľom	1	2	3	2	D
F	Inštalovanie nového systému	7	10	13	10	E
G	Konfigurácia a prepojenie technológie	4	6	14	7	F
H	Nastavenie parametrov a pravidiel v systéme	5	9	19	10	G
I	Nastavenie bezpečnostných prvkov (dvojfaktorová autentizácia)	4	6	14	7	G
J	Testovanie technológie	20	22	30	23	H, I
K	Kontrola funkčnosti systému	5	8	17	9	J
L	Úprava prípadných nedostatkov	2	4	6	4	K
M	Prispôsobenie užívateľského rozhrania podľa potrieb firmy	4	7	10	7	L
N	Predanie finálneho riešenia systému	2	4	6	4	M

O	Záverečná kontrola systému (SW inžinierom)	3	8	13	8	N
P	Spätná väzba od SW inžiniera	5	7	15	8	O
R	Spracovanie požiadaviek zo spätnej väzby	2	4	6	4	P
S	Tvorba firemných manuálov	5	10	15	10	R
T	Školenie zamestnancov	3	5	7	5	R
U	Spustenie novej technológie do prevádzky	1	2	3	2	S, T

Sieťový graf projektu sa nachádza v prílohách diplomovej práce (viď príloha č.1).

3.4 Zhodnotenie vlastných návrhov a ich prínosy pre spoločnosť

Táto podkapitola sa zaoberá ekonomickými aspektami implementácie vybranej technológie.

3.4.1 Ekonomické zhodnotenie

Cena navrhnutého riešenia je vyčíslená v nasledujúcej tabuľke č. 15 (bez DPH).

Tabuľka č. 15: Ekonomické zhodnotenie implementácie zvolenej technológie v € (bez DPH)
(Zdroj: Vlastné spracovanie)

Oblasť	***Riešenie***	***Cena***
Monitoring	Softvér LibreNMS	freeware
	Inštalácia a konfigurácia systému	400 €
	Migrácia dát (min. 5 dní)	2.000 €
Náklady na zriadenie	Pracovná stanica HP Z1 G8 Tower	915,9 €
Náklady na prevádzku	Spotreba energií	337
Celkovo	***Implementovanie navrhnutých riešení***	***~ 3.653 €***

Celkové náklady na implementáciu navrhnutého riešenia sú odhadnuté na 3.653 €, pričom monitorovací systém je sám o sebe zdarma a ročné prevádzkové náklady navrhnutého riešenia sú iba 337 €.

3.4.2 Prínosy návrhov pre firmu

Najpodstatnejším prínosom pre firmu je možnosť vidieť slabiny systému a infraštruktúry, kde sa môže firma zlepšiť a podniknúť určité kroky, aby chod siete bol plynulejší, bezproblémovejší a časovo menej nákladný aj z dlhodobého hľadiska. Menej vyťažený

systém, predpovedanie možných výpadkov a včasné riešenie problémov určite ocení podstatná väčšina zákazníkov tejto firmy, ktorej úspech je závislý na ich spokojnosti.

Pred podrobnejším nastavením tejto technológie firma zisťovala výpadky častokrát až po nahlásení sťažností od užívateľov, monitorovanie výpadkov a chýb bolo veľmi nekompletné a nastavenie spolu s kontrolou bolo nedostačujúce.

Pri vyhradení zamestnanca a zvýšení požiadaviek na monitorovanie sieťovej prevádzky firma zníži riziko budúcich problémov, ktoré pri súčasnom stave hrozia každý deň.

3.4.3 Kvantifikácia prínosov

Keby jeden pracovník testoval desať zariadení za sebou a každému zariadeniu venoval 20 sekúnd, výsledok testovania, či sú zariadenia v prevádzke, by získal približne za 200 sekúnd. Nástroj LibreNMS zvládne stovky procesov súčasne. Testovanie 10-tich zariadení by zvládol do 20-tich sekúnd.

Tabuľka č. 16: Kvantifikácia prínosov
(Zdroj: Vlastné spracovanie)

Vykonávateľ	*Počet testovaných zariadení*	*Čas obdržania výsledku testu*
Zamestnanec	10	> 200
Technológia LibreNMS	10	< 20

3.4.4 Porovnanie nákladov

Pracovník s hrubou mesačnou mzdou 1.500 € by sa monitorovaniu sieťovej prevádzky venoval iba 8 hodín denne a len v pracovné dni. Keby sme chceli 24-hodinové sledovanie prevádzky, museli by sa na to vyhradiť traja pracovníci, čo by spoločnosť vyšlo okolo 4.500 € na jeden mesiac. Zatiaľ, čo konkrétny systém pracuje nonstop za výrazne nižšie náklady na prevádzku.

Tabuľka č. 17: Porovnanie nákladov na monitorovanie s a bez nástroju

(Zdroj: Vlastné spracovanie)

Vykonávateľ	*Počet hodín*	*Cena za 1 hod (€)*	*Cena za mesiac (€)*
Zamestnanec	8	9,375	1500
	24		4500
Nástroj na monitorovanie	24	0,039	28,08

Náklady technológie sú vypočítané ako náklady prevádzky, čiže celkové náklady za spotrebované energie: 0,6 €/kWh * výkon pracovnej stanice 0,065 kW = 0,039 €/hod. Náklady za mesiac potom budú 0,6 €/kWh * 0,065 kW * 24 h * 30 dní = 28,08 €.

Pri porovnaní nákladov v predchádzajúcej tabuľke je jasne vidieť, že nástroj na monitorovanie nie je len efektívnejší, ale je to aj ekonomicky výhodnejšie riešenie.

ZÁVER

Hlavným cieľom diplomovej práce bolo navrhnúť manažment siete, analyzovať monitorovací systém zvoleného podniku a následne vďaka výsledkom analýz implementovať technológiu na zefektívnenie sledovania problémov ešte predtým než vzniknú.

Dielčím cieľom bolo navrhnúť riešenie na zníženie nákladov a na zvýšenie zisku firmy. Zisk by mohla investovať do rozvoja spoločnosti a školenie zamestnancov, a takisto do nových zariadení, ktoré jej v tejto problematike môžu výrazne pomôcť.

Zvolenú tému som detailne objasnila v prvej kapitole tejto práce, kde som základné pojmy vymedzila a následne som ich využila v ďalšej kapitole práce.

Vypracované analýzy mi pomohli nájsť možné problémy a na ich základe som v poslednej kapitole navrhla implementačné riešenia, ktoré by firme pomohli. Výsledkom návrhovej časti je postup implementácie navrhovanej zmeny v monitorovaní siete a konkrétne konfiguračné riešenie systému Libre NMS.

Stanovené ciele boli splnené a verím, že pre spoločnosť budú moje návrhy prínosné a pomôžu jej zvýšiť produktivitu a efektívnosť pri práci a prispejú k celkovému zlepšeniu súčasného stavu v spoločnosti.

ZOZNAM POUŽITÝCH ZDROJOV

1. BIGELOW, S. J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. Překlad Petr MATĚJŮ. Brno: Computer Press, 2004, 990 s.. ISBN 80-251-0178-9.

2. DONAHUE, G. A. *Kompletní průvodce síťového experta*.. Brno: Computer Press, 2009, 528 s.. ISBN 978-80-251-2247-1.
3. JULIAN, M. Practical Monitoring. Kalifornia, USA: O'Reilly Media, Inc., 2017, 167 s. ISBN 978-1-491-95735-6
4. LIGUS, S. Effective Monitoring and Alerting. Kalifornia, USA: O'Reilly Media, Inc., 2012, 166 s. ISBN 978-1-449-33352-2
5. MORRIS, S.B. Network Management, MIBs and MPLS: Principles, Design and Implementation. 1.vyd. New Jersey: Pearson, 2003, 416 s. ISBN-13: 978-0-13-101113-7
6. SOSINSKY, B. Mistrovství - počítačové sítě. Brno: Computer Press, 2010, 840 s.. ISBN 978-80-251-3363-7.
7. SUBRAMANIAN, M. Network Management: Principles and Practice. 2.vyd. New Jersey: Pearson, 2010, 724 s. ISBN-13: 978-8131734049

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. *Počítačové Siete - Fyzická Topológia, Zbernicová, Hviezdicová, Stromová a kruhová*. encyklopediapoznania.sk [online] 2.11.2013 © 2013-2022 Wesline, s.r.o. [cit. 03.03.2022]. Dostupné z: https://encyklopediapoznania.sk/clanok/406/pocitacove-siete-fyzicka-topologia-zbernicova-hviezdicova-stromova-a-kruhova

10. 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

11. *Základní Pojmy*. *KYBEZ* [online] © GORDIC spol.s r.o. 2021. [cit. 03.03.2022]. Dostupné na internete: https://www.kybez.cz/zakladni-pojmy/)

12. ONDRÁK, Viktor. 2017 *Management informační bezpečnosti* [výukové materiály]. VUT v Brně, Fakulta podnikatelská. ISBN 978-80-214-5115-5.

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

14. AVEN, Terje. *Risk analysis, 2nd Edition*. Z *O'Reilly Online Learning* [online]. September 2015 [cit. 03.03.2022]. Dostupné na internete: https://learning.oreilly.com/library/view/risk-analysis-2nd/9781119057796/

15. SVOZILOVÁ, Alena. *Projektový management: systémový přístup k řízení projektů*. 3., aktualizované a rozšířené vydání. Praha: Grada Publishing, 2016. Expert (Grada). ISBN 978-80-271-0075-0.

16. DOLEŽAL, Jan, Pavel MÁCHAL a Branislav LACKO. *Projektový management podle IPMA*. 1. vyd. Praha: Grada, 2009. Expert (Grada). ISBN 978-80-247-2848-3.

17. Lewin's Model of change [online]. SlideModel, ©2022 [cit. 2022-04-10]. Dostupné z: https://slidemodel.com/templates/lewins-change-model-powerpointtemplate/lewins-model-of-change-in-powerpoint/
18. SMEJKAL, V. a K. RAIS. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 483 s. ISBN 978-80-247-4644-9
19. Systém LibreNMS. © 2022 [prístup 2021-02-02] http://librenms.example.com/

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

21. *Počítačové Siete – Rozdelenie podľa rozlohy – PAN, LAN, MAN a WAN*. encyklopediapoznania.sk [online] 2.11.2013 © 2013-2022 Wesline, s.r.o. [cit. 03.03.2022]. Dostupné z: https://encyklopediapoznania.sk/clanok/405/pocitacove-siete-rozdelenie-podla-rozlohy-pan-lan-man-a-wan

22. BHATTARAI, Deben. *Cisco Discovery Protocol (CDP)*. Cisco Learning Network [online] [cit. 04.02.2022]. Dostupné z: https://learningnetwork.cisco.com/s/article/cisco-discovery-protocol-cdp-x

23. *Foundry Discovery Protocol overview*. Commscope Technical Content Portal [online] [cit. 01.03.2022]. Dostupné z: https://docs.commscope.com/bundle/fastiron-08090-managementguide/page/GUID-4C951D0A-F050-4DC7-96AA-FDBEC3D20C09.html

24. *Link Layer Discovery Protocol.* Wireshark [online] [cit. 02.03.2022]. Dostupné z: https://wiki.wireshark.org/LinkLayerDiscoveryProtocol

25. *Open Shortest Path First*. IBM documentation [online] 14.4.2021 © IBM [cit. 02.03.2022]. Dostupné z: https://www.ibm.com/docs/en/i/7.4?topic=routing-open-shortest-path-first

26. *OSPF protocol*. JavaTpoint [online] [cit. 02.03.2022]. Dostupné z: https://www.javatpoint.com/ospf-protocol

27. *What is BGP?* IPXO [online]. 5.11.2021 ©2022 IPXO Limited [cit. 02.03.2022]. Dostupné z: https://www.ipxo.com/tutorial/what-is-bgp/

28. *Simple Network Management Protocol (SNMP)*. GeeksforGeeks [online] 3.11.2021 © GeeksforGeeks [cit. 02.03.2022]. Dostupné z: https://www.geeksforgeeks.org/simple-network-management-protocol-snmp/

29. *Address resolution protocol (ARP)*. IBM [online] © IBM [cit. 02.03.2022]. Dostupné z: https://www.ibm.com/docs/en/zos-basic-skills?topic=layer-address-resolution-protocol-arp

30. *Spanning tree protocol (STP) overview*. Cisco Meraki [online] 22.10.2021 © 2021 Cisco Systems, Inc. [cit. 02.03.2022]. Dostupné z: https://documentation.meraki.com/MS/Port_and_VLAN_Configuration/Spanning_Tree_Protocol_(STP)_Overview

31. *Pestle Analýza*. ManagementMania.com [online] 30.7.2015 © ManagementMania.com [cit. 03.03.2022]. Dostupné z: https://managementmania.com/sk/pestle-analyza
32. *Alza*. Alza.sk [internetový obchod]. © 1994 – 2022 Alza.sk [cit. 2022-05-05] Dostupné z: https://www.alza.sk/hp-z1-g8-tower-d6622158.htm#parametry

ZOZNAM POUŽITÝCH SKRATIEK A SYMBOLOV

IS – informačný systém

IT – informačné technológie

VPN – virtuálna privátna sieť

ISMS – Information Security Management System (Systém riadenia informačnej bezpečnosti)

KII – Kritická informačná infraštruktúra

ZOZNAM OBRÁZKOV

Obrázok č. 1: Sieť PAN 14
Obrázok č. 2: Sieť LAN 14
Obrázok č. 3: Sieť MAN 15
Obrázok č. 4: Sieť WAN 16
Obrázok č. 5: Zbernicová topológia 17
Obrázok č. 6: Hviezdicová topológia 17
Obrázok č. 7: Kruhová topológia 18
Obrázok č. 8: Diagram komunikácie protokolu SNMP 21
Obrázok č. 9: Lewinov model 30
Obrázok č. 10: Organizačná štruktúra spoločnosti 33
Obrázok č. 11: Mapa rizík pred implementáciou návrhu pred opatrením 40
Obrázok č. 12: Mapa rizík pred implementáciou návrhu po opatrení 41
Obrázok č. 13: Mapa rizík pri implementácii pred opatrením 44
Obrázok č. 14: Mapa rizík pri implementácii po opatrení 45
Obrázok č. 15: Vývoj miery nezamestnanosti v posledných rokoch 49
Obrázok č. 16: Vývoj minimálnej mzdy na Slovenku v priebehu rokov 49
Obrázok č. 17: Logo nástroja Libre NMS 55
Obrázok č. 18: Základný dashboard Libre NMS 55
Obrázok č. 19: Okno Zdravie 56
Obrázok č. 20: Pridávanie nového zariadenia 58
Obrázok č. 21: Úvodný informačný panel 59
Obrázok č. 22: Vytvorenie skupín zariadení 60
Obrázok č. 23: Network Map 61
Obrázok č. 24: Nastavenie pravidiel upozorňovania 63
Obrázok č. 25: Príklad upozornení ku zvolenému zariadeniu 64
Obrázok č. 26: Nastavenie emailových upozornení 64
Obrázok č. 27: Latencia (oneskorenie) na zariadení 65
Obrázok č. 28: Ping Response 65
Obrázok č. 29: Teplota jednotlivých portov v zariadení 65
Obrázok č. 30: Prehľad portov 66

ZOZNAM TABULIEK

Tabuľka č. 1: Klasifikácia aktív podľa rizika pre organizáciu 25
Tabuľka č. 2: Klasifikácia podľa dôvernosti dát v komerčnej sfére 25
Tabuľka č. 3: Hlavné kategórie metód analýzy rizík podľa T.Avena..... 27
Tabuľka č. 4: Pravdepodobnosť rizika 28
Tabuľka č. 5: Dopad rizika 28
Tabuľka č. 6: Hodnota rizika 29
Tabuľka č. 7: Klasifikácia aktív spoločnosti 36
Tabuľka č. 8: Klasifikácia aktív podľa dostupnosti 36
Tabuľka č. 9: Zraniteľnosti aktív spoločnosti 37
Tabuľka č. 10: Analýza rizík pred implementáciou navrhnutého riešenia 38
Tabuľka č. 11: Analýza hrozieb, opatrení a nápravných činností pred implementáciou návrhu 39
Tabuľka č. 12: Analýza rizík pri implementácii návrhu 42
Tabuľka č. 13: Kvantifikácia síl 69
Tabuľka č. 14: Základné údaje pre spracovanie časovej analýzy 73
Tabuľka č. 15: Ekonomické zhodnotenie implementácie zvolenej technológie v € (bez DPH) 75
Tabuľka č. 16: Kvantifikácia prínosov 76
Tabuľka č. 17: Porovnanie nákladov na monitorovanie s a bez nástroju 77

ZOZNAM PRÍLOH

Príloha č. 1: Časová analýza – Sieťový graf I

Príloha č. 1: Časová analýza – Sieťový graf
(Zdroj: Vlastné spracovanie)