VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

NÁVRH METODIKY ŘÍZENÍ KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI

DRAFT METHODOLOGY FOR CYBER AND INFORMATION SECURITY MANAGEMENT

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Michal Gabriel

AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Sedlák

SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Michal Gabriel**
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2023/24
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:

Návrh metodiky řízení kybernetické a informační bezpečnosti

Charakteristika problematiky úkolu:

Úvod
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr

Cíle, kterých má být dosaženo:

Cílem této diplomové práce je vytvořit návrh pro společnost, která má v plánu změnu druhu svého podnikání na poskytování zpoplatněného privátního cloudového úložiště.

Základní literární prameny:

ČSN EN ISO/IEC 27001 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Systémy managementu informační bezpečnosti - Požadavky, 2023. [Praha]: Česká agentura pro standardizaci.

ČSN EN ISO/IEC 27002 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Opatření informační bezpečnosti, 2023. [Praha]: Česká agentura pro standardizaci.

DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk, 2019. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing. ISBN isbn978-80-88260-39-4.

SEDLÁK, Petr a KONEČNÝ, Martin, 2023. Přeměna ISMS v manažerské informatice. Brno: CERM, akademické nakladatelství. ISBN isbn978-80-7623-110-8.

SEDLÁK, Petr a KONEČNÝ, Martin, 2021. Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru. Brno: CERM, akademické nakladatelství. ISBN isbn978-80-7623-068-2.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2023/24

V Brně dne 4.2.2024

L. S.

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

Abstrakt

Kybernetická a informační bezpečnost je jeden z důležitých prvků zajištění bezpečnosti společnosti. Z důvodu, aby se minimalizovali možná rizika útoků na podnikovou infrastrukturu je tak rozumné vynaložit značné úsilí na její zabezpečení

Abstract

ICT security is one of many important parts for design company security. For minimalizing probability risks of attacks on company infrastructure is wise to expend considerable effort for securing it.

Klíčová slova

Proxmox, Nextcloud, Nessus, Lynis, IT Security

Key words

Proxmox, Nextcloud, Nessus, Lynis, IT Security

Bibliografická citace

GABRIEL, Michal. *Návrh metodiky řízení kybernetické a informační bezpečnosti.* Brno, 2024. Dostupné také z: https://www.vut.cz/studenti/zav-prace/detail/159577. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

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

V Brně dne 11. května 2024

……

podpis studenta

Poděkování

Tímto bych rád poděkoval jak svému vedoucímu diplomové práce za velmi cenné zkušenosti v průběhu studia na fakultě Podnikatelské VUT v Brně, tak také za vedení této diplomové práce. Věřím že zkušenosti pana Ing. Petra Sedláka mi budou v následujícím absolventském životě nápomocny v řadě případech. Další v pořadí bych rád poděkoval svému oponentovi této diplomové práce panu Ing. Martinu Kunderovi za ochotu oponentury této práce.

V poslední řadě bych rád poděkoval svým blízkým za to, že mne duševně podporovali v průběhu psaní této diplomové práce.

OBSAH

1 ÚVOD 11
2 VYMEZENÍ PROBLÉMU A CÍLE PRÁCE 13
1 TEORETICKÁ VÝCHODISKA PRÁCE 14
1.1 Proxmox 14
1.2 WHMCS 15
1.3 Nextcloud 16
1.4 HAProxy 16
1.5 OpenZFS 17
1.5.1 Snapshoty 18
1.6 DNS server 18
1.7 Zálohování 19
1.8 Replikace dat 19
1.9 Zabbix 20
1.10 OPNSense 21
1.11 Software defined network – SDN 22
1.12 TLS Certifikáty 22
1.12.1 Mutual TLS - mTLS 23
1.13 Síťové technologie 24
1.14 LAN – Local Area Network 24
1.14.1 802.1X 24
1.14.2 VLAN – Virtual LAN 25
1.14.3 WLAN – Wireless LAN 26
1.14.4 WiFi hrozby. 26
1.14.5 VPN – Virtual Private Network 26
1.14.6 Síťové hrozby 28
1.14.7 Bezpečnostní nástroje z pohledu analýzy 29
1.15 Záložní zdroj elektrické energie UPS 31
2 ANALÝZA SOUČASNÉHO STAVU 33
2.1 Představení společnosti 33
2.2 Organizační struktura podniku 34
2.3 Popis částí objektu 34
2.3.1 První podzemní podlaží – 1.PP 34
2.3.2 První nadzemní podlaží – 1.NP 35

2.4 Identifikace aktiv 36
2.4.1 Soupis časti stávajících aktiv společnosti 36
2.5 Síťová infrastruktura 36
2.6 Řízení přístupu (pozn. - fyzická bezpečnost) 37
2.7 Řízení přístupu (pozn. – datová bezpečnost) 37
2.8 Požadavky společnosti v oblasti kybernetické bezpečnosti 37
2.8.1 Kryptografie 37
2.9 Zajištění dostupnosti 38
2.10 Požadavky analyzovaného podniku pro rozšíření oboru podnikání 38
3 VLASTNÍ NÁVRHY ŘEŠENÍ 40
3.1 Navrhovaný systém 40
3.2 Navrhovaný objekt 40
3.2.1 Zabezpečení objektu 41
3.3 Hardware 42
3.3.1 HP iLO 43
3.3.2 Chlazení objektu 43
3.3.3 Redundance a SPOF 44
3.3.4 Odhadovaná spotřeba elektrické energie 44
3.3.5 Ochrana proti přepětí 45
3.3.6 Alternativní zdroje elektrické energie 45
3.3.7 Připojení k internetu 46
3.3.8 HW firewall 47
3.3.9 OpenVPN server 48
3.4 Software 48
3.4.1 SW firewall 48
3.4.2 DNS server pro správu domény 49
3.4.3 SMTP server 50
3.4.4 Reverzní proxy server 51
3.4.5 Virtualizační server se systémem Proxmox – backend 51
3.4.6 Poskytování VPS – Frontend 52
3.4.7 Replikace a zálohování dat 52
3.4.8 Nextcloud 54
3.4.9 Mutual-TLS certifikáty 55
3.4.10 Revokace přístupu 58
3.4.11 Správa certifikátů 59

3.4.12 Monitoring 59
3.4.13 Antivirus 60
3.4.14 VOIP 60
3.5 Management kybernetické bezpečnosti 61
3.5.1 Analýza rizik 63
3.5.2 Vnitrofiremní dokumentace na úseku ICT 67
3.5.3 Testování zranitelnosti systémů 67
3.5.4 Event management 70
3.5.5 Log management 70
3.5.6 Management podnikové kontinuity – BCM 71
3.5.7 Red a Blue Team testy 71
3.5.8 Řízení přístupu ke kamerovým záznamům 71
3.5.9 Elektronický zabezpečovací systém 72
3.6 Finanční zhodnocení 72
3.6.1 Investiční výdaje 73
3.6.2 Provozní výdaje 73
3.6.3 Servisní výdaje 74
3.6.4 Plánovaná ekonomická návratnost 74
3.6.5 Platební systém 74
3 ZÁVĚR 75
4 SEZNAM POUŽITÝCH ZDROJŮ 76
5 SEZNAM OBRÁZKŮ 81
6 SEZNAM TABULEK 82
7 SEZNAM POUŽITÝCH ZKRATEK 83

1 ÚVOD

Kybernetická bezpečnost je v nesmírně důležitá záležitost pro každou organizaci. S rozvojem technologií a digitalizace se však objevují také nové hrozby, které mohou potenciálně ohrozit jakýkoli systém. Proto je nezbytné rozvíjet a zlepšovat řízení kybernetické bezpečnosti, aby organizace byla schopna předcházet různým bezpečnostním incidentům a s maximálním úsilím minimalizovat rizika možných hrozeb.

Nicméně existují také určité nedostatky v řízení kybernetické bezpečnosti. Prvním nedostatkem je nedostatečné povědomí o kybernetických hrozbách a jejich potenciálních dopadech. Mnoho lidí neklade důraz na to, jak je důležité chránit informace a data před neoprávněným přístupem. Proto je nesmírně důležité zvýšit osvětu a zlepšit vzdělávání v oblasti kybernetické bezpečnosti, aby se organizace staly odolnější proti útokům.

Dalším nedostatkem je nedostatečná investice do technologií a infrastruktury, které by mohly pomoci chránit organizace před kybernetickými hrozbami. Mnoho organizací nedostatečně rozumí rizikům a nákladům spojeným s kybernetickou bezpečností a tudíž nemají dostatečné finanční prostředky vyhrazené právě pro tuto oblast. Bez adekvátních investic je však ochrana před hrozbami mnohem obtížnější a organizace jsou vystaveny většímu nebezpečí zranitelnosti.

Navazujícím nedostatkem je nedostatek specializovaných znalostí a dovedností v oblasti kybernetické bezpečnosti. Je obtížné najít dostatečně kvalifikované odborníky, kteří jsou schopni rozpoznat a odpovědět na rychle se měnící kybernetické hrozby. Navíc je poskytování odpovídajícího vzdělávání a školení v této oblasti často nepostačující.

Posledním nedostatkem, který lze identifikovat, je nedostatek komunikace a spolupráce mezi organizacemi a institucemi ve vztahu ke kybernetické bezpečnosti. Ve snaze chránit se před kybernetickými hrozbami by měly organizace spolupracovat a vyměňovat si informace o bezpečnostních incidentech a nových taktikách útoků. Nedostatek komunikace ztěžuje efektivní prevenci a reakci na kybernetické hrozby.

Závěrem lze říci, že i když se organizace snaží chránit svou infrastrukturu a data před kybernetickými hrozbami, existují stále nedostatky v oblasti řízení kybernetické bezpečnosti. Větší porozumění, adekvátní finanční prostředky, specializované znalosti a lepší spolupráce

jsou nezbytné pro zvýšení úrovně kybernetické bezpečnosti a snížení rizika pro organizace v dnešní digitální éře.

2 VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Ve velké míře společností je podle mého názoru kybernetická společnost zanedbána. Kategoricky by šlo říci, že ve společnostech o menším počtu zaměstnanců může být menší míra zabezpečení. Typickým příkladem budou dle mého názoru mikro podniky. V případě, že je společnost větší v porovnání s mikro podnikem, tak je jistá pravděpodobnost, že kybernetická bezpečnost bude lépe zajištěna mimo jiné z důvodu vyššího personálního zajištění oboru kybernetické bezpečnosti. Také ale mohou nastat případy, kdy i firma malá či střední nemusí mít zajištěnou kybernetickou bezpečnost v patřičném rozsahu.

Cílem této diplomové práce je vytvořit návrh pro společnost, která má v plánu změnu druhu svého podnikání na poskytování zpoplatněného privátního cloudového úložiště. V současné době tato společnost má jako předmět podnikání několik různých živností.

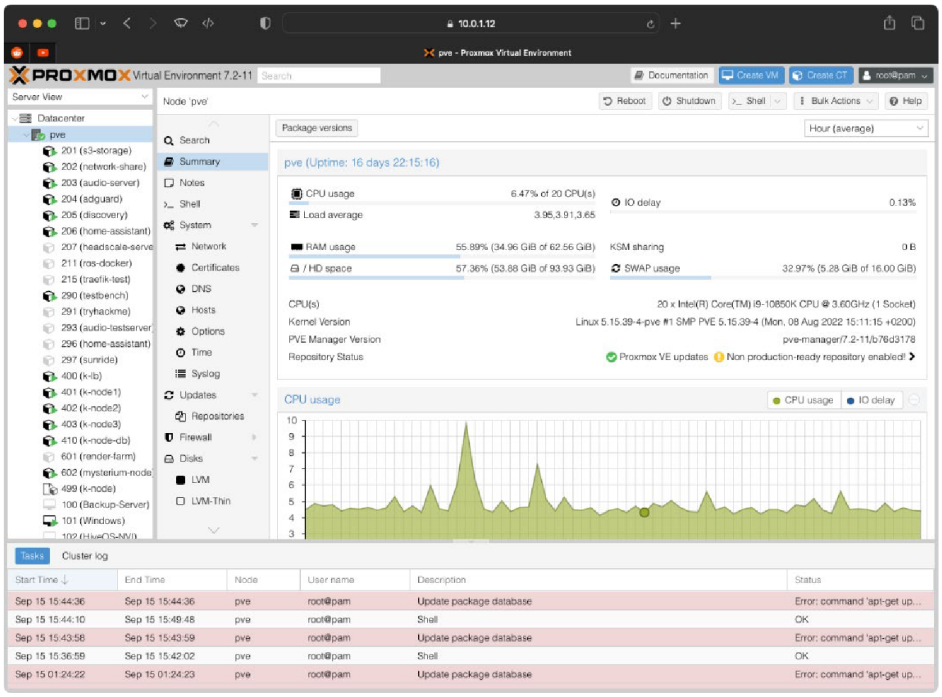
Cíle této diplomové práce je navrhnout řešení, které v případě implementace v konkrétních bodech může zlepšit kybernetickou bezpečnost pro společnost, tedy sníží míru rizik pro některé hrozby. Cílem této práce není zabránit jakémukoliv bezpečnostnímu incidentu, a to z důvodu, že obor IT/ICT se vyvíjí velmi rychle. Jednotlivec, který se zabývá kybernetickou bezpečností a také nese odpovědnost za jim navržené řešení by se měl pravidelně v tomto oboru vzdělávat, aby tak v maximální možné míře implementoval vhodné ochranné prvky pro snížení těchto rizik a tím pádem, pokud to bude možné předešel nežádoucím útokům

1 TEORETICKÁ VÝCHODISKA PRÁCE

V této kapitole sepíši pár teoretických informací, ze kterých následně vychází vlastní návrh řešení.

1.1 Proxmox

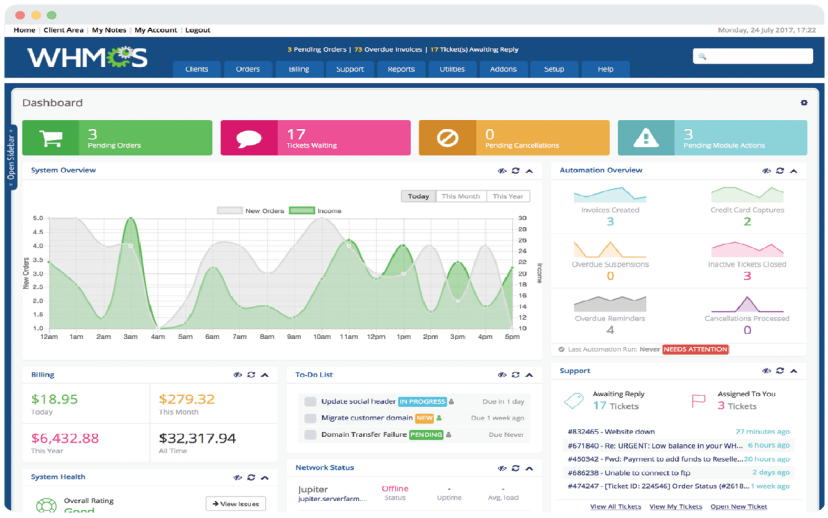
Proxmox je softwarová nástavba nad operačním systémem Linux. Jedná se o sadu nástrojů, prostřednictvím kterých tak administrátor ovládá virtualizační software QEMU a LXC. Jeho hlavní předností oproti konkurenčním softwarům je, že je licencován jako open-source což může společnosti ušetřit nemalé finanční prostředky. V případě požadavku na podporu ze strany společnosti Proxmox Server Solutions GmbH je možné se registrovat k podpoře za roční úplatu. Jako celek Proxmox tak plní funkci hypervizoru s možností vysoké dostupnosti. (1, s. 1) V tomto hypervizoru tak správce může vytvářet a spravovat jak virtuální zařízení, ale také linuxové kontejnery. Hlavním rozdílem těchto kontejnerů a virtuálních zařízení je rozdíl v přístupu k virtualizovanému prostředí. V případě LXC se jedná o oddělené prostředí, které využívá stejného systémového jádra jako hypervizor. V případě virtuálního zařízení v QEMU se tak jedná o úplnou virtualizaci systému jako celku. Z pohledu požadavků na výkon je tak rychlejší prostředí LXC než virtualizované prostředí v QEMU. (2, s. 116) Jednou z výhod pro QEMU je, že lze virtualizovat i systém s rozdílnou architekturou než je na hypervizoru, což může být nápomocné například v případě vývoje aplikací. Je tedy možné takto mít virtualizovaný systém pro architekturu ARM zatímco tak hypervizor může být například na architektuře x86. (10) Z pohledu bezpečnosti je vhodnější využití virtualizovaných zařízení QEMU z důvodu, že nelze provádět útoky na sdílené linuxové jádro hypervizoru. Linuxové kontejnery v Proxmoxu nabízí možnosti nastavení unprivileged a privileged. V případě, že by správce systému použil režim privileged, tak v tomto linuxovém kontejneru by bylo možné využít práva superuživatele root postaveného na úroveň hypervizoru čímž by došlo stavu, že tento uživatel v linuxovém kontejneru může narušit chod hypervizoru. V případě, že by podnik využíval těchto kontejnerů, tak je vhodnější použít režim untrusted. (10)



Obr. 1: Proxmox - Webové rozhraní (20)

1.2 WHMCS

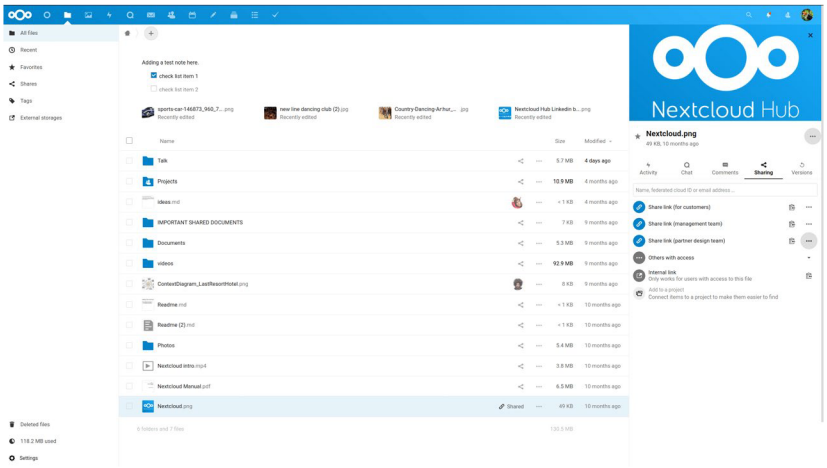
Jedná se o klientské rozhraní, prostřednictvím kterého může podnik nabízet zákazníkům přístup k virtuálním zařízením. Pomocí WHMCS tak může podnik fakturovat zákazníkům za poskytované služby, obsahuje také platformu pro podporu zákazníka. (3, s. 1-2)



Obr. 2: WHMCS - Webové rozhraní (21)

1.3 Nextcloud

Nextcloud je software, který zprostředkovává poskytování cloudového úložiště. Jako přístupové rozhraní zde slouží přístup přes webovou adresu, což je zaštítěno HTTP serverem Apache. V systému Nextcloud lze aktivovat různé moduly z různých kategorií jako řízení přístupu, kolaborativní psaní dokumentů, analytické moduly a řada dalších. V administrátorském rozhraní je možné nastavit kvóty jak pro jednotlivé uživatele nebo skupiny uživatelů, ale také globálně pro celé cloudové úložiště. V Nextcloudu je také možné aktivovat šifrování klientských dat na straně serveru. (4, s. 577)



Obr. 3: Nextcloud - Webové rozhraní (22)

1.4 HAProxy

Aby společnost mohla poskytovat více služeb na jedné veřejné IP adrese, tak může využít funkcionalit reverzního proxy serveru HAProxy. Další z funkcionalit HAProxy je možnost použití integrovaného load balancéru, kdy webová služba může být instalována ve vícero instancích nebo také na různých místech s různými veřejnými IP adresami, kdy požadavek klienta o přístup je vhodně přesměrován na jednu z instancí pro optimální vytížení systémových prostředků. HAProxy má také možnost využití web aplikačního filtru, čímž lze omezit některé nežádoucí druhy přístupů. Tento aplikační filtr spadá pod edici enterprise. Veškeré nastavení reverzního proxy serveru se provádí prostřednictvím jednoho konfiguračního souboru. Hlavní částí reverzního proxy serveru jsou frontend a backend rozhraní. Frontend je část, ke které se klient připojuje. Backend část je taková, na kterou je následně klient přesměrován. Klient tak přistupuje ke službám prostřednictvím jedné adresy a neví, na které zařízení byl přesměrován. (5, s. 85389)

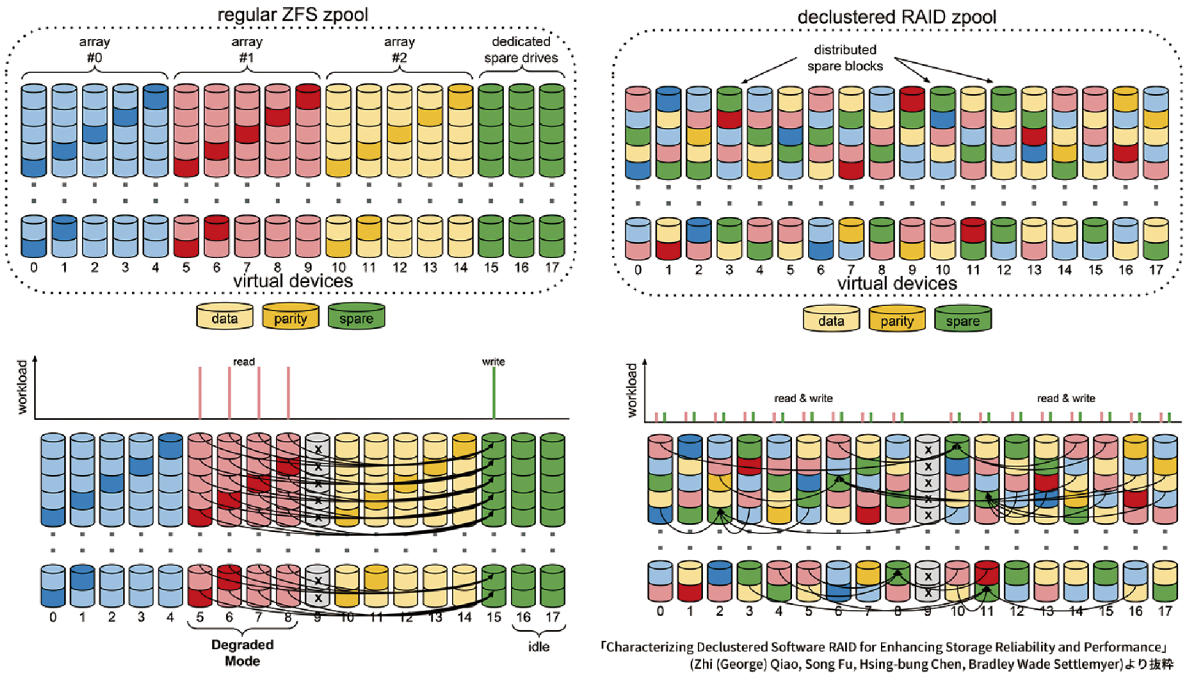
1.5 OpenZFS

OpenZFS je souborový systém s řadou funkcionalit který byl vytvořen jako náhrada za fyzický RAID. OpenZFS tak plní obdobné funkce jako RAID s tím rozdílem, že OpenZFS je softwarový. Hlavní funkcí je provoz redundantních datových polí, která tak mohou navýšit výslednou kapacitu logického pole. Tato redundantní pole jsou také provozována z důvodu snížení pravděpodobnosti ztráty dat ve formě závady na technickém vybavení. Nejpoužívanějšími konfiguracemi OpenZFS datových polí jsou obdobné režimy, které jsou z RAIDu známé jako RAID1, RAID5, RAID6 a RAID10. Jsou to tedy konfigurace zrcadlení dat na dvou a více discích. V případě obdoby RAID5 a RAID6 jsou data dle schématu vhodně distribuována napříč více disky s dopočítáním parity dat pro případnou rekonstrukci logického pole. (6, s. 1-5)

OpenZFS také využívá alokace paměťového rozsahu na fyzickém serveru, kdy tato alokovaná paměť slouží jako ARC cache pro práci s daty. Výsledkem tedy je, že při vhodné konfiguraci tento přístup k datům a práce s nimi může být výrazně rychlejší než v případě přímého přístupu na fyzické disky. V případě, že by v serveru nebyla dostatečná kapacita paměťových modulů, tak lze také použít L2ARC cache, která funguje obdobně jako ARC s tím rozdílem, že místo paměťových modulů se používá rychlých disků. Pokud by podnik potřeboval využít rychlejšího specifického druhu zápisu ve formě synchronních zápisů na logické pole, tak může také využít ZIL cache pro zápis dat, kdy tento druh cache při vhodné konfiguraci je rychlejší než přímý zápis na rotační disky. Z toho důvodu pro ZIL cache je doporučeno používat disků typu SSD. Tyto SSD disky by měly být vybírány takové, které mají vysokou odolnost v počtu zápisů. Proto v případě výběru těchto rychlých disků je vhodné hledat disky s vyšší hodnotou DWPD. OpenZFS má také možnost použití šifrování dat na datových polích. (6, s. 1-5)

Pro účely virtualizace lze využít také jedné z funkcionalit OpenZFS, a to jednotek Zvol. Jedná se o vytvoření virtuálního disku, který následně může být přiřazen jednotlivému konkrétnímu virtuálnímu zařízení. (10)

V případě požadavku je možné mít v serveru vyhrazeny rezervní disky, které plní funkci náhradních disků pro případ, kdy jeden disk v datovém poli selže. V případě, že jsou tyto náhradní disky nakonfigurované pro dané datové pole, tak souborový systém automaticky začne kopírovat data s využitím paritních dat na nový náhradní disk. Tímto se tedy sníží pravděpodobnost selhání celého diskového pole. (7)



Obr. 4: ZFS - Redistribuční schéma dat (7)

1.5.1 Snapshoty

Jednou z dalších funkcí OpenZFS jsou snapshoty, které slouží jako zachycení aktuálního stavu souborového systému do formy obrazu. Tyto snapshoty se následně již nemění. Tato funkce může být velmi užitečná pro rychlé obnovení smazaných dat na souborovém systému. Další užitečnou vlastností může být v případě testování vyvíjené aplikace nebo implementace změn na virtuálním systému, kdy tak administrátor zachytí stav ještě před změnou a v případě neplánovaného poškození virtuálního zařízení tak stačí pouze obnovit předchozí stav. (6, s. 4) Je vhodné také podotknout že snapshoty neplní funkci zálohy dat.

1.6 DNS server

DNS slouží primárně pro převod adres. V případě, že se klient chce připojit na internetovou službu, tak zadá adresu formou textu, resp. FQDN. Nicméně ve světě je používáno IP protokolu, který jako adresaci používá IP adresy. Jedním z důvodu použití je, že člověk není schopen si zapamatovat všechny IP adresy pro přístup k požadované službě. Druhým důvodem je, že na této IP adrese může být aktivních vícero webových služeb, kdy tak server neví kterou službu má tak následně klientu zobrazit. DNS pro tyto účely používá řadu různých DNS záznamů, kdy ty nejčastěji využívané mohou být A, AAA, CNAME, SRV a TXT záznamy. (8)

DNS také podporuje šifrované přenosy adres kdy jako jedna z metod je EDNS. DNS funguje na stromové architektuře, kdy se systém dotazuje postupně na části adresy až po nejnižší prvek.

1.7 Zálohování

Z důvodu zamezení nevratné ztráty dat je vhodné provádět pravidelné zálohy dat na základě automatizovaných plánů. V případě selhání datového oddílu nebo datového pole, tak prostřednictvím této zálohy může odpovědný pracovník obnovit data ze zálohy. Zálohování je velice důležitá aktivita pro zachování provozuschopnosti podnikové infrastruktury.

Zálohovací metoda 3-2-1 znamená, že zálohovaná data mají být na třech různých médiích a jedno má být umístěné na jiné lokalitě. Jiná lokalita může být chápana jak fyzická, kde bude umístěn datový nosič, nebo také virtuální formou zálohování přes internetové připojení. Jedna ze společností, která nabízí cloudové úložiště určené pro zálohy je Backblaze. V případě velkého množství dat může být přenosová kapacita internetového připojení významná pro dobu zálohy a dobu obnovy dat. (9, s. 1-2)

Proxmox Backup server je podružný systém od společnosti Proxmox GmbH, který slouží pro zálohování virtuálních zařízení, které jsou na stejnojmenném hypervizoru. Pro zálohy jsou podporovány jak zařízení běžícími pod QEMU, ale také i linuxové kontejnery LXC. Tyto zálohy mohou být komprimovány a šifrovány. (10)

1.8 Replikace dat

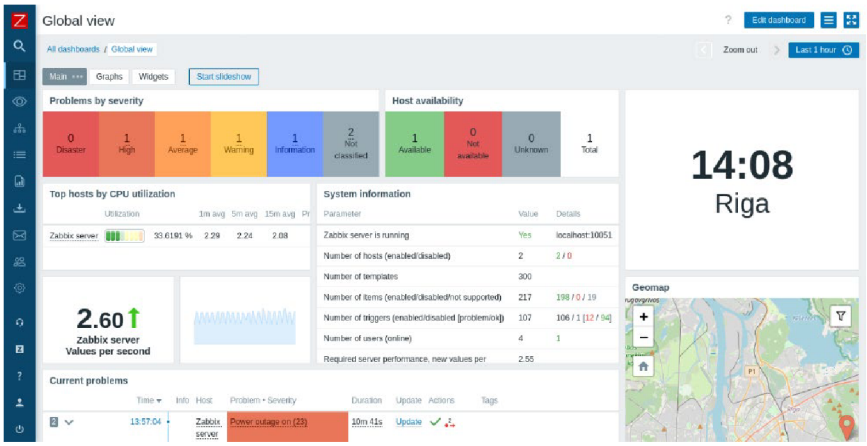
Za předpokladu, že podnik bude využívat více fyzických serverů určených pro virtualizaci, případně poskytování služeb cloudového úložiště, tak tyto servery může vložit do logického clusteru. Jakmile jsou servery vloženy do logického clusteru, tak prostřednictvím webového rozhraní je následně možné provádět migrace virtuálních zařízení mezi jednotlivými servery. Pro účely snížení výpadku virtuálního zařízení mohou být data z virtuálního zařízení v pravidelných intervalech replikována mez různými servery. Tato pravidelná replikace dat může být vhodná při situaci, kdy by tak podnik potřeboval migrovat virtuální zařízení mezi jednotlivými servery z důvodu rovnoměrného distribuování vytížení systémových prostředků. Značnou výhodou replikování dat je vysoká rychlost migrování virtuálních zařízení, kdy jelikož data jsou aktuální v závislosti na časovém plánu replikace, tak následná migrace virtuálního zařízení spočívá v podstatě v pouhém přesunu konfiguračního souboru na jiný

server v clusteru. Naopak nevýhodou replikace dat je zvýšený nárok na obsazenou kapacitu na jednotlivých serverech z důvodu vytváření téměř symetrické kopie dat.

V případě replikace virtuálních zařízení v Proxmox je možné nastavit logickou skupinu serverů s možností nastavení priorit jednotlivých serverů a také možnost parametru „restricted“, který značí, zda virtuální zařízení mohou být migrována i mimo tuto definovanou skupinu serverů například z důvodu, že všechny servery v logické skupině jsou neaktivní. (10)

1.9 Zabbix

Zabbix slouží jako platforma určená pro monitoring sledovaných stavů. Pro konfiguraci je možné využít velkou škálu existujících šablon pro monitoring. Tyto sledované stavy v závislosti na konfiguraci může ukládat do interní databáze tak, že správce monitoringu je schopen se podívat do historie na stav jaký byl v hledaný čas. V Zabbixu je také možné sledovat i logy z jednotlivých systémů, čímž ale vzroste požadavek na potřebnou kapacitu v závislosti na délce retenční smyčky. Pro inicializaci odeslání notifikace o změně stavu Zabbix využívá tzv. „triggerů“. Tento trigger je vpodstatě podmínkou, kdy sledovaná veličina dosáhne stavu nastaveného dle podmínky, tak iniciuje definovanou aktivitu, čímž zpravidla je proces notifikace. V neposlední řadě Zabbix umožňuje také zasílání notifikačních zpráv prostřednictvím řady nástrojů, kdy například e-mailová notifikace s vazbou na push notifikace mobilního telefonu může být užitečnou kombinací, jelikož odpovědný pracovník se ve velmi krátké prodlevě dozví o změně sledovaného stavu a v případě že se jedná o nežádoucí stav, tak může obratem začít provádět činnost k uvedení do žádaného stavu. (11, s. 3-4) Jednotlivé triggery mohou být nastavené o různých úrovních z důvodu členění významnosti nežádoucího stavu například z důvodu prioritizace úkolů pro nápravy vícero nežádoucích stavů.



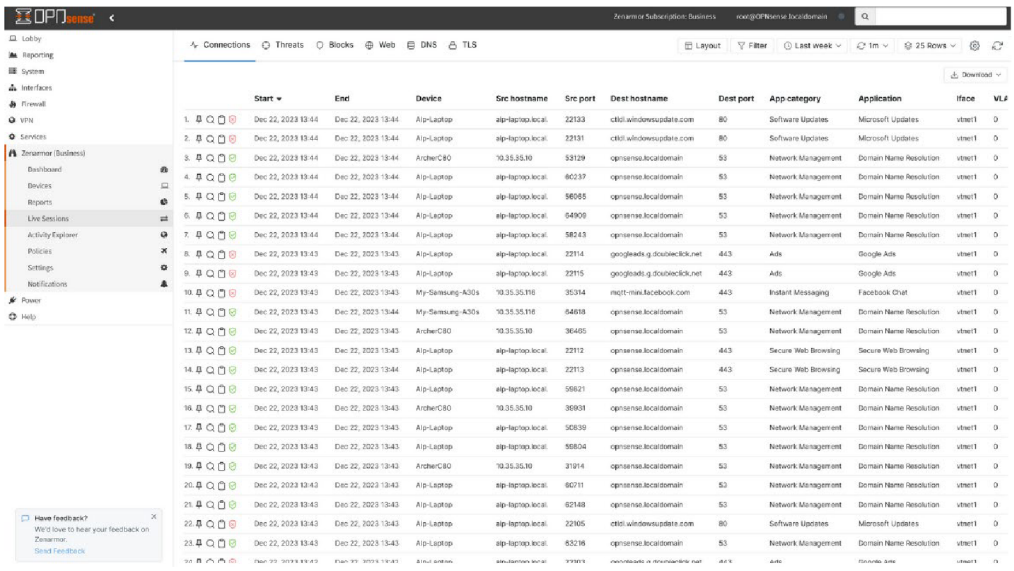
Obr. 5: Zabbix - Webové rozhraní (23)

Zabbix sbírá sledovaná data jednak protokolem SNMP, ale také i prostřednictvím Zabbix agenta, který je zapotřebí tak nainstalovat na systémy, které mají být sledovány.

1.10 OPNSense

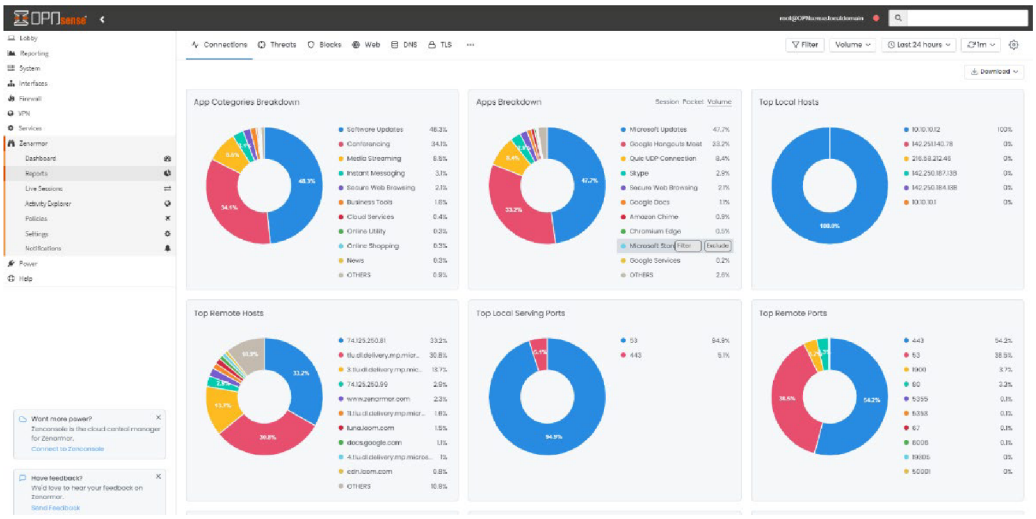
OPNSense je softwarový firewall, který vznikl na základě podobného firewallu pfSense. OPNSense je modulární tak, že si správce může doinstalovat různé balíčky které následně může aplikovat do síťového prostředí. Funkcí, které OPNSense podporuje, je mnoho. Jako krátký výčet se může jednat o omezení datového toku, proxy serveru, virtuální sítě typu VPN, detekční systém IDS, systém prevence IPS, DNS server a mnoho dalších. V případě použití virtualizace je třeba implementovat softwarový firewall, aby se zamezilo neoprávněné komunikaci na základě pravidel. (12, s. 28)

Další užitečným nástrojem je funkce ZenArmor která plní roli aplikačního firewallu. Prostřednictvím ZenArmoru je tak možné blokovat datový provoz v závislosti na definovaných zemích, umožnuje také blokovat datovou komunikaci, která obsahuje nežádoucí obsah. V případě, že je požadována analýza SSL/TLS provozu, tak po naimportování vhodných certifikátů do firewallu je možné následně prostřednictvím Zenarmoru analyzovat a blokovat šifrovanou SSL/TLS komunikaci nebo její část. (16)



Obr. 6: OPNSense ZenArmor - Live Session Explorer (24)

Live session explorer a reportovací část mohou být užitečnými nástroji v případě, že se správce systému snaží dohledat konkrétní adresy, ze kterých je pokus anebo již probíhá neoprávněná komunikace například ve formě pokusu o útok na podnikovou infrastrukturu.



Obr. 7: OPNSense ZenArmor – Reports (25)

1.11 Software defined network – SDN

Pro funkčnost virtuálních zařízení je zapotřebí vhodně nastavit virtuální síť dle požadavků společnosti. Virtualizovaná síť může být nastavena za účelem oddělení virtuálních zařízení tak, aby vzájemně nemohla komunikovat, nebo právě naopak aby vzájemně komunikovat mohla. Další možností konfigurace je vedení síťového provozu kumulativně skrze virtuální firewall z důvodu že mezi hypervizor a virtuální zařízení technicky není možné vložit firewall fyzický. (13)

1.12 TLS Certifikáty

TLS certifikáty slouží primárně jako prostředek pro šifrování komunikace prostřednictvím zabezpečeného kanálu SSL. V době, kdy ještě nebyly TLS certifikáty tak rozšířené jako nyní se využívalo nešifrovaného spojení. Toto nešifrované spojení obnášelo bezpečnostní úskalí ve formě možnosti přečtení obsahu v datové komunikaci z důvodu, že se přenášela v běžné čitelné podobě. (14, s. 1) To přinášelo řadu nebezpečných situací, kdy tak neoprávněná osoba byla schopna ze záznamu datové komunikace vyčíst například přihlašovací údaje osoby nebo také text konverzace aj. Z toho důvodu se během let přecházelo na šifrovanou komunikaci, kdy aktuálně používaná je TLS konkrétně ve verzi 1.3 Tato šifrovaná komunikace funguje na principu inicializační výměny klíčů mezi dvěma stranami, na základě kterých se následná datová komunikace šifruje. Struktura je dána hierarchickým modelem kořenem důvěry, kdy pro validní komunikaci tak vydaný certifikát musí být ověřen certifikační autoritou. Na světě existuje řada společností, které jsou uznávány jako důvěryhodné certifikační autority, jako

například Sectigo, které za poplatek jsou schopné poskytnout ověřený TLS certifikát, který si následně jeho držitel může naimportovat do zvolené aplikace. Asi nejčastějším použitím TLS certifikátů je jejich importování do webového serveru na protokolu HTTPS. V případě, že klient chce provést spojení na nějaký webový server, tak má možnost si ověřit, zda-li daná webová aplikace disponuje platným a ověřeným certifikátem ve webovém prohlížeči. V případě, že tato komunikace není zabezpečena TLS certifikátem, tak by klient měl zvážit, zda je vhodné na té konkrétní webové aplikaci pracovat z důvodu možného neoprávněného odposlechnutí informací nebo autorizačních údajů. V případě, že je zřízena vlastní certifikační autorita, která tedy nebude celosvětově uznávána, tak je zapotřebí ji vhodně zabezpečit proti útokům vedeným na certifikační autoritu z důvodu, kdy za předpokladu, že by někdo získal přístup k certifikační autoritě, by mohl tak začít vydávat certifikáty, které by sice byly ověřeny certifikační autoritou, ale byly by z pohledu oprávněného správce neoprávněné. Jedním z nástrojů pro analýzu síťového provozu a zjištění, zda-li je komunikace zabezpečena TLS spojením, je Wireshark.

TLS certifikáty také mají dobu platnosti, která když uplyne, tak se certifikát stává neplatným. Jedná se o poměrně důležitý parametr, kdy je vhodnější vystavovat certifikáty pravidelně než vystavit certifikát s relativně neomezenou dobou platnosti. (14, s. 2)

Certifikáty je také možné revokovat čímž se zruší platnost certifikátu ještě dříve, než mu vyprší platnost. Tato revokace se pak musí zanést do listu revokovaných certifikátů. (14, s. 1)

1.12.1 Mutual TLS - mTLS

mTLS komunikace je v podstatě nástavbou nad běžnou TLS komunikací. V této nástavbě je implementován ještě navíc klientský certifikát, kdy se na začátku datové komunikace tak vzájemně ověřují jak klient, tak server. Jedná se tedy o jeden z mnoha prvků, který může zvýšit bezpečnost, jak komunikace, ale také snížit perimetr možných útoků na serverovou instanci. Certifikáty určené pro mTLS komunikaci se vydávají shodně jako ostatní. Opět je zde potřebné, aby tento certifikát byl ověřen, resp. schválen certifikační autoritou. Jedním z úskalí certifikátů určených pro mTLS komunikaci je potřeba tento certifikát importovat do klientského zařízení včetně certifikační autority, což může přinášet vyšší náročnost pro některé klienty. (15, s. 31-34)

1.13 Síťové technologie

Pro účely propojení zařízení a následného přenosu dat mezi nimi je třeba zajistit vhodnou infrastrukturu. Tato infrastruktura může být drátová nebo bezdrátová. Dalšími specifickými druhy propojení jsou optická vedení a případně speciální jako laserová, rádiová, satelitní aj. V této práci budu uvažovat běžné druhy přenosu dat jako metalické, optické a bezdrátové (WiFi).

1.14 LAN – Local Area Network

LAN je síť lokálního typu. Typicky si lze tento druh představit jako propojení zařízení v rámci jedné místnosti, jednoho podlaží nebo v rámci budovy. Z pohledu fyzického zapojení dále dělíme na horizontální kabeláž a vertikální kabeláž. Hlavním důvodem je možnost nějakým způsobem přenášet data v malé a zároveň z pohledu zvenčí uzavřené sítě. (18)

Základní prvky pro vytvoření sítě LAN jsou switche (managed, unmanaged), mohou to být také bezdrátová přípojná místa, opakovače a další řada prvků. Případně pro oddělení jednotlivých podsítí v sítí LAN můžeme použít také router. Za předpokladu, že se nejedná výhradně o uzavřenou síť, která je spojena s vnějším světem tedy mimo rozsah sítě LAN, tak následně je potřeba použít router na kterém jsou nastavena další pravidla pro funkční zapojení – např. DHCP klient, NAT, Firewall pravidla, aj. (26)

1.14.1 802.1X

V sítích LAN a dalších variantách sítí je možné a občas taky moudré použít autorizaci připojení. Tedy zabezpečit, že se do jedné konkrétní zásuvky připojí konkrétní zařízení. Toto lze ošetřit například prostřednictvím MAC adresy daného zařízení formou Access-Listu na switchi. Nicméně taky může nastat situace, že tato konkrétní stanice bude přecházet mezi přístupovými body do sítě LAN. Na základě tohoto je potřeba nastavit další vhodné metody řízení přístupu například prostřednictvím autorizačních serverů. Jako další příklad poslouží zaměstnanec, který se svým laptopem přechází mezi více přípojnými body a v závislosti na kterékoliv místo se připojí, tak je potřeba zajistit práce přesně ten daný přístup, kam tento zaměstnanec přístup mít má, nikoliv méně ani více. K tomuto slouží právě ověřování standardem 802.1X (27)

Základními protokoly standardu 802.1X jsou: MD5, TLS, TTLS, EAP, PEAP, FAST, LEAP, SmartCard. (27)

Autorizace může probíhat vícero metodami. Může to být metoda přihlašovacího jména a hesla jako například Eduroam, může být také na základě MAC adresy zařízení, ale také je možnost použití certifikátu pro ověření

Pro funkčnost ověřování certifikátem je třeba na stanice rozdistribuovat certifikáty certifikačních autorit a dále následné jednotlivé vygenerované certifikáty pro jednotlivé stanice. Také je možnost využití certifikátů typu X.509 – PKCS#12, kdy daný certifikát je chráněný heslem. Varianta PKCS#12 už tvoří více-faktorovou autentizaci (*něco vím, něco mám*). Dané certifikáty by měly mít nastavenou rozumnou dobu platnosti, např. 90 dní. V případě, že zaměstnanec rozváže spolupráci se zaměstnavatelem, tak by měl být zaměstnanci v neodkladné době tento certifikát revokován pro zamezení zneužití.

Jistou nevýhodou metody 802.1X je náročnost na údržbu. Nevyplatí se zavádět ve společnosti např. o 5 zaměstnancích, kdy může být pro společnost zavedení této metody autorizace velmi komplikované, včetně následné distribuce certifikátu a následně údržby celé ověřovací infrastruktury. Nicméně technicky je možné tento protokol implementovat i v takto malé společnosti.

1.14.2 VLAN – Virtual LAN

Je další formou logické sítě. V tomto případě se jedná o virtuální LAN. Při vhodném nastavení jedna VLAN může obsahovat více LAN sítí, ale také naopak jedna LAN síť se může skládat z více VLAN podsítí. Základními parametry při nastavená sítě VLAN je VLAN ID 1-4094. Hodnoty 0 a 4095 jsou vyhrazeny. Dalšími možnými parametry je, zdali je VLAN ID značená nebo neznačená. (17)

Neznačené VLAN ID je takové, kdy se tato značka nastaví na switchi na konkrétních portech a datový provoz v dané VLAN se předává pouze do portů které obsahuji totožnou hodnotu VLAN ID. Při tomto předání se ořízne informace o hodnotě VLAN ID, takže následné další zařízení jíž neví o tom, zda-li je nebo není v nějaké konkrétní VLAN. (17)

Ve značené VLAN ID se oproti neznačené VLAN ID předává informace o konkrétním ID dále v síti na další zařízení, které náleží nastavenému portu na switchi. Tím pádem toto další zařízení

ví, že ze switche přišly datagramy obsahující konkrétní ID Vlany. Pro jeden port může být také nastaveno více VLAN ID. Tím pádem možných konfigurací virtuálních LAN na switchi je mnoho. (17)

Výhodou VLAN je, že na ně můžeme aplikovat ruzná pravidla na úrovni jak switchů, tak také pravidla založená na konkrétním rozhraní VLAN na routerech. Je možné tak například směrovat datový tok různých VLAN podle potřeby. VLAN jako takové mohou být nastaveny na jednom fyzickém rozhraní, kdy tak může probíhat nezávislá komunikace ve smyslu oddělených broadcastových sítí.

Nevýhodou VLAN je metoda útoku na VLAN ID která se nazývá VLAN Hopping. Jsou dvě metody útoku kdy první je podvržení VLAN ID tak, že se útočník dostane do jiné VLAN do které nemá mít přístup. Druhou metodou útoku je dvojité tagování. Prostřednictvím dvojitého tagování tak útočník může získat přístup do jiné sítě kdy první značka je na prvním možném switchi řádně odstraněna a na následném switchi tak může být datový tok přesměrován do nežádoucí VLAN. (28, s. 13-15)

1.14.3 WLAN – Wireless LAN

Bezdrátová lokální síť je trošku jiná forma běžné LAN. Mohou se vyskytovat případy, kdy provedení jednoduché LAN není možné. Typickým případem jsou mobilní telefony. Dalším příkladem může být omezení v délce trasy a zároveň, kdy zajištění bezdrátového přenosu dat je jednodušší a levnější. (17) Nicméně z pohledu společnosti je vhodnější pro delší trasy a případně vyšší datovou propustnost využít optických spojů, které mají parametry mnohem lepší než bezdrátový přenos.

1.14.4 WiFi hrozby.

V případě, že by podnik používal na pracovišti bezdrátových přípojných bodů, tak doporučuji aby používala zabezpečení metodou WPA3 z důvodu, že WPA2 a starší již nejsou považovány za bezpečné metody. (29, s. 271-273)

1.14.5 VPN – Virtual Private Network

Virtual Private Network slouží pro spojení mezi dvěma body, kdy toto spojení má být bezpečné. Tedy pokud důvěřujeme danému programu nebo implementaci. Spojení VPN může být na principu ověřování uživatelským jménem nebo certifikátem, případně kombinací

obojího dle standardu PKCS#12. Jestliže použijeme certifikát, tak je potřeba do VPN klienta vložit také certifikační autoritu a v případě, že máme nastavené ověřování certifikátu serveru, tak také musíme importovat certifikát serveru. Dále spojení VPN může být nastavené v režimu TCP a UDP spojení, kdy každá metoda má své výhody a nevýhody. Asi nejdůležitějším aspektem VPN je bezpečnost přenosu dat. VPN může být šifrovaná jak na vytvořeném tunelu, ale také i pro přenos autorizačních údajů. VPN je již řadu let na světě v provozu a prošlo řadou implementací jednotlivých protokolů. Proto zmíním jako příklad pouze pár druhů - PPTP, OpenVPN, Wireguard. Nicméně každý operační systém v základu může mít různou podporu jednotlivých protokolů, kdy ve většině případů by tyto protokoly měly jít do operačního systému doplnit, jestliže v nich není obsažen. (30, s. 75)

1.14.5.1 IDS/IPS – Intrusion Detection/Prevention System

IDS je detekční systém, který analyzuje síťovou komunikaci oproti uloženým pravidlům, resp. seznamům pravidel které jsou pravidelně aktualizovány. V případě, že se vyskytne nějaký paket, který je obsažen v pravidlech, tak se propíše do záznamu popis druhu komunikace případně pokusu o konkrétní kybernetický útok. IDS nebrání neoprávněné komunikaci. Naproti tomu IPS, který může fungovat ve spolupráci s IDS, tuto komunikaci zahazuje. Příkladem je aplikace Snort nebo Suricata. Nicméně v dnešní době jsou některé druhy kybernetických útoků, tak sofistikovaných, že IDS i IPS je nemusí ve 100% zachytit. (31, s. 6-7)

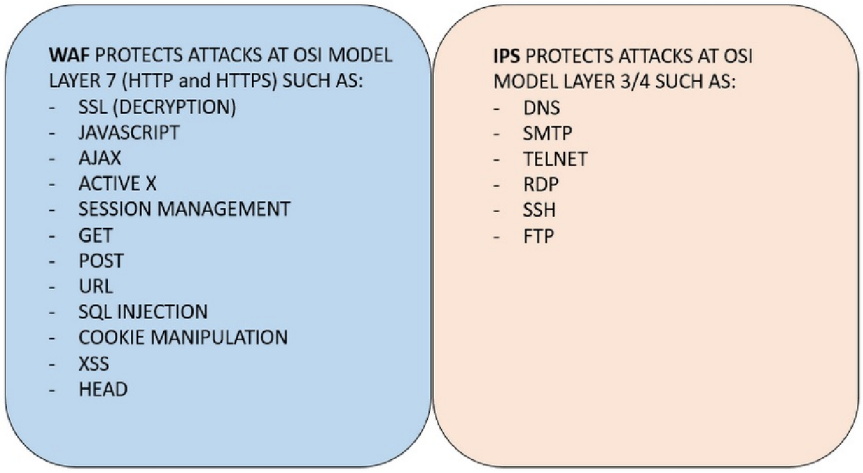
1.14.5.2 DPI – Deep Packet Inspection

Jedná se o software pro hloubkovou analýzu paketů. V závislosti na konkrétní aplikační službě je možné analyzovat obsah komunikace, případně obsah těchto paketů. V případě, že v komunikaci používáme šifrované spojení, např. TLS, tak DPI není schopen analyzovat data komunikace do doby než klientovi vnutíme použití certifikátu pro tento šifrovaný přenos, který je naimportován také v DPI. V té fázi již je schopen DPI tyto data dešifrovat. Nicméně ne vždy je vhodné použít DPI, například pro přihlašování do internetového bankovnictví. (32, s. 377-378)

1.14.5.3 WAF – Web application firewall

Chrání přístup k webovému serveru na základě pravidel na službách HTTP a HTTPS. Příkladem útoků směrovaných na webové rozhraní služby může být náhodné skenování častých souboru útočníkem, napříč internetem za účelem zjištění přístupových údajů. Některé

WAF mají již v sobě zabudované filtry takové, které ve svých pravidlech mají uložené tyto soubory a zamezí tak nežádoucímu přístupu útočníka k danému souboru. WAF tak na rozdíl od IPS chrání webovou službu, resp. aplikační vrstvu v rámci síťového provozu. (19)



Obr. 8: Srovnání rozdílných principů WAF a IPS (19)

1.14.5.4 SIEM – Security Information and Event Management

SIEM je centralizovaný server pro sběr informací o provozu v síti. Může sdružovat například datovou komunikaci a následně to graficky agregovat z důvodu přehlednosti pro správce sítě nebo pro zaměstnance zabývající se bezpečností. Další možnost použití je hromadný sběr záznamů, událostí z většího množství zařízení. Následně lze procházet tyto záznamy např. na bázi filtrů nebo fulltextového vyhledávání. V případě, že je požadavek informování události systémem SIEM odpovědným osobám, je možné nakonfigurovat odesílání oznámení e-mailem. Možnou variantou SIEM řešení je kombinace ELK Stacku a Wazuhu. (33, s. 15-24)

1.14.6 Síťové hrozby

V dnešní době se vyskytuje široká paleta nástrojů, které si útočník může zvolit. V prvé řadě si útočník provede průzkum v čem by cílový subjekt mohl být zranitelný. V závislosti na výstupu až volí nástroje. Za pomocí těchto nástrojů může následně zkoušet konkrétní útoky.

1.14.6.1 DDOS – Distributed Denial of Service

Pro DDoS útoky se používá vysoké množství stanic, které se všechny společně začnou v krátkých intervalech dotazovat serveru na službu. V případě, že serverová služba není správně dimenzovaná, tak dochází k výpadku služeb. Z tohoto důvodu se používají například

Load-balancery, které jsou schopné službu rozdělit do vícero serverů pro optimalizaci využití prostředků. Další možností je zamezení počtu aktivních spojení z jedné IP adresy. V krajním případě lze odpojovat přístup k službě jednotlivým zemím. Nicméně není stoprocentní obrana proti DDoS útokům. (34, s. 2)

1.14.6.2 Port scan

Pro skenování zranitelností sítě nebo zařízení poskytující službu, je možné provádět síťové skeny dostupných portů. Po spárování aplikačních služeb k jednotlivým otevřeným-dostupným portům z internetové databáze můžeme zjistit, jaká služba se na cílovém zařízení vyskytuje a tím pádem zvolit správný nástroj pro útok. (35, s. 27-28)

1.14.6.3 CVE – Common Vulnerabilities and Exposures

CVE je databáze zranitelností jak softwarů, tak i hardwarů. Následně na základě těchto zranitelností se provádí záplaty a vydávají se aktualizace operačních systémů nebo aplikací. (36)

1.14.7 Bezpečnostní nástroje z pohledu analýzy

Součástí návrhu této práce je také použití pár nástrojů, které tam mohou být nápomocné v oblasti skenování zranitelností jednotlivých systémů.

1.14.7.1 Shodan.io

Analytický nástroj pro skenování služeb prostřednictvím internetu. V základním volném přístupu je omezený počet skenování. Prostřednictvím tohoto nástroje je možné zjistit zda a pokud ano, tak jaké konkrétní porty, resp. služby jsou přístupné z internetu. Ve výstupu daného skenu může být obsažen krátký popis služby, který byl sken schopen získat. (38, s. 380)

Obr. 9: Sken otevřených portů DNS serveru Google. (Vlastní zpracování)

1.14.7.2 Nessus

Nessus je nástroj pro možnost automatizovaného skenování. Má přednastavenou řadu funkcionalit, ze kterých si můžeme vybrat takovou, kterou zrovna požadujeme. Výstupem je velmi přehledný report o zranitelnostech skenovaných zařízení. (38, s. 3-5) V základní free edici je limit použití na maximálně 16 IP adres, kdy pro menší kancelář tento maximální počet sledovaných zařízení může postačovat. Ve vyšších již placených edicích jsou možnosti použití širší bez omezení IP adres. Nevýhodou je však vysoký poplatek za tyto placené edice, který začíná na částce 125 tisíc Kč ročně.

1.14.7.3 Lynis

Lynis je podpůrný nástroj pod licencí GNU GPL pro skenování zabezpečení operačního systému Linux z pohledu různých kategorií. Výstupem tak může být kontrola sledovaných parametrů jak u systémových služeb, linuxového jádra, paměti a procesů, nastavení uživatelů skupin a autentifikace, nastavení linuxového shellu, souborových systémů, USB zařízení, lokální úložiště, NFS úložišť, nastavení jmenných serverů, kontrola balíčkovacího systému (apt, yum, etc.), nastavení síťových prvků, konfigurace mailového serveru, webového serveru, SSH serveru, SNMP klienta, systémových certifikátů a řadou dalších kontrolovaných prvků systému. Tento výstup může sloužit jako podpůrný nástroj pro provedení bezpečnostních záplat systému. Na konci výstupu je přímo uveden soupis daných doporučení nebo odkazů na konkrétní zranitelnosti obdobně, jak je známé z databáze CVE. (39, s. 2-3)

1.15 Záložní zdroj elektrické energie UPS

Zařízení UPS má jako primární funkci napájení elektrických spotřebičů v případě výpadku elektrické energie. Tyto výpadky by neměly nastávat, ale je nutné zohlednit i možnost, že například z důvodu závady na energetické síti distributora anebo z důvodu závady na energetických prvcích společnosti například výpadkem proudového chrániče, by tak mohla nastat situace, kdy by se podniková infrastruktura z důvodu nedostatku přísunu elektrické energie okamžitě vypnula. V lepším případě by tak pouze nebyly dostupné služby zákazníkům, které by následně mohli zákazníci reklamovat. V horším případě tímto výpadek může dojít k porušení dat v jednotlivých systémech od datových polí, databází, posledních provedených změn aj. Této situaci zabrání zařízení UPS. V případě výpadku elektrické energie tak má na jednotlivých zařízeních podniku, jako například serverů, být po definované prodlevě automaticky zahájeno korektní ukončení všech služeb a následné vypnutí serverů. Tímto procesem se zamezí ztrátě dat. V případě, že by energetická kapacita zařízení UPS byla dostatečně vysoká, tak je možné napájet servery i delší dobu, nicméně energetická účinnost UPS nebývá zpravidla vysoká, a tím pádem zálohování elektrické energie postačuje pouze k již zmíněnému vypnutí serveru. (40)

Sekundární funkcí UPS je ochrana zařízení na úseku nežádoucích hodnot některých veličin z obor elektrotechniky. Může jimi být přepětí, podpětí, různé elektrické špičky aj. Vzhledem tomu že v UPS jsou osazeny baterie, tak tato baterie dokáže v rozumné míře tyto nežádoucí vlivy absorbovat a tím tak ochrání spotřebiče, které jsou do ní připojené. (40)

UPS také může mít osazen dohledový a přístupový modul, který může mít také zabudovanou podporu protokolu SNMP, díky kterému je možné data o stavu UPS a bateriích zasílat do monitorovacího systému Zabbix.

Z pohledu vnitřního fungování se UPS dělí do několika základních kategorií (40):

- Offline
- Line-Interactive
- Online s dvojitou konverzí

Každá z těchto kategorií má své specifické výhody a nevýhody. Pro základní pochopení rozdílů principů těchto kategorii je potřebné je alespoň zkráceně popsat. Kategorie Offline, funguje na

principu dvou paralelních vedení kdy UPSkou prochází jak přímo vstupní elektrická energie na výstup, tak v druhé větvi je měnič a baterie. V případě výpadku elektrické energie dochází ke krátké prodlevě, po kterou není dodávaná elektrická energie do chráněných spotřebičů vlivem přepnutí uvnitř UPS, na dodávku elektrické energie z baterií. Line-Interactive UPS funguje na principu konstantní dodávky vstupní elektrické energie do chráněných spotřebičů s tím, že tato vstupní elektřina prochází pouze rozhraním střídavého proudu měniče. Tento měnič dále plní funci jak nabíjení baterie, tak i převádí stejnosměrnou elektřinu na střídavou v případě výpadku vstupní elektrické energie. Doba přepnutí na dodávku elektřiny z baterií je tak menší než v případě Offline UPS. Online UPS s dvojitou konverzí je nejsložitější mechanizmus, kdy v sestavě jsou umístěny dva měniče AC-DC a DC-AC, mezi kterými je umístěna baterie. Nad všemi těmito prvky je vložen bypass přepínač prostřednictvím kterého tak může technik bez výpadku chráněných zařízení provést výměnu baterií UPS. Technologie Online s dvojitou konverzí má naopak nejnižší energetickou účinnost, a to z důvodu použití dvou měničů AC-DC a DC-AC, čímž je ve výsledku nižší doba dodávky elektrické energie z baterií. Naopak ale Online UPS s dvojitou konverzí poskytuje nejvíce metod ochrany napájených spotřebičů proti nežádoucím jevům v elektrické síti. (40)

2 ANALÝZA SOUČASNÉHO STAVU

2.1 Představení společnosti

V současné době společnost Gamitech, s.r.o. má aktivní živnosti výroba, instalace a opravy elektrických, elektronických, telekomunikačních přístrojů a dále hostinská činnost, prodej kvasného lihu a lihovin a volné živnosti v oblasti IT a technických služeb.

Aktuálně jsou v podniku jsou v nejvyšší míře zastoupena data obchodního charakteru. Jedná se tedy o provozní data z pokladního systému a účetního systému. Jistá výseč těchto dat je chráněna pohledem ochrany osobních údajů, jako například zaměstnanecké smlouvy, mzdové listy, aj.

Součástí pracovní náplně zaměstnanců je průběžné pořizování obchodních dat do pokladního systému během provozní doby podniku, na základě kterých následně provádí vyúčtování se zákazníky. Ke konci pracovního dne zaměstnanec na pokladně vystaví denní uzávěrku, kterou předá nadřízenému pracovníkovi. Obchodní data jsou v současném stavu ukládána výhradně pouze na pokladním systému, který není zálohovaný záložním zdrojem elektrické energie typu UPS. V případě výpadku elektrické energie zaměstnanci za provozu ztratí informace o aktuální nevyúčtovaných položkách jednotlivých zákazníků, což jím může způsobit vysoké komplikace při rekonstrukci těchto objednávek pro vyúčtování.

Zaměstnanci kromě vedoucích pracovníků nemají přístup k historii obchodních dat. V případě, že zaměstnanec pořídí chybně položku nebo objednávku, má možnost do doby vyúčtování jednotlivé chybně namarkované položky vystornovat. Jestliže zaměstnanec objednávku již vyúčtuje, tak nemá možnost svévolně chybně pořízenou a vyúčtovanou objednávku vystornovat. Pro toto chybné vyúčtování je již zapotřebí vedoucího pracovníka, který pomocí svého přístupu může toto vadné vyúčtování opravit.

Jednotlivé denní obchodní doklady jsou ve formě papírových účtenek ukládány za účelem přepisu do účetního systému včetně denních uzávěrek.

Databáze z pokladního systému nemá nastavenou žádnou metodu zálohování, a proto by případná technická závada na pokladním systému s velkou pravděpodobností způsobila ztrátu obchodních dat. V případě odcizení by ztráta dat byla stoprocentní. V případě účetního systému

je databáze zálohována do souboru, která je uložena na externích médiích typu CD a Flash za účelem archivace a také případně za účelem obnovy dat.

2.2 Organizační struktura podniku

V aktuální situaci je podnik v utlumeném režimu od vzniku proti pandemických opatření proti SARS-COV-2. Z tohoto důvodu již po začátku platnosti vládních nařízení podnik propustil všechny zaměstnance, včetně pracovníků pracujících na dohody dle zákoníku práce. Momentálně tedy v podniku jsou pouze 2 vedoucí pracovníci, kdy jeden z nich je jednatelem společnosti, a druhý má funkci jako náhrada za hlavního vedoucího pracovníka v případě nepřítomnosti jednatele.

2.3 Popis částí objektu

V objektu v prvním nadzemním podlaží se nachází podniková provozovna. Část tohoto podlaží by šla využít pro návrh této diplomové práce. Dále objekt má jedno podzemní podlaží

2.3.1 První podzemní podlaží – 1.PP

Dané patro je stavebně členité a bez dveří. Světlá výška prostor je od 190 cm do 210 cm. Při stropu se zde vyskytují nosné prvky prvního nadzemního podlaží. Podlaha je betonová o hloubce 15 cm, kde podložím je kari-síť a pod ní již zemina. Dalším prvkem rozhodným pro návrh je, že v tomto podlaží je plynový kotel určený k vytápění. Za předpokladu, že by došlo k závadě komínu kotle, nebo by byl způsoben tah spalin jinou cestou než patřičnou komínovou vložkou a to například vzduchotechnikou pro chlazení datového rozvaděče, existuje pravděpodobnost, že by se mohl změnit tak spalin z kotle namísto do komínové vložky, tak do jiné cesty.

V tomto podlaží je také vedena domovní kanalizace v hloubce cca 1 metr pod podlahou, kdy tuto kanalizaci je možno servisovat skrze tomu určenou servisní šachtu. Existuje tedy pravděpodobnost, že touto servisní šachtou stoupá vlhkost. Z pohledu přepadu vody a případného zaplavení podzemního podlaží, společnost uvádí, že toto podlaží nebylo zaplaveno nikdy a jelikož se objekt nachází v Brně v Králově poli v 265 m.n.m., tak je téměř nulová pravděpodobnost, že by dané podlaží bylo zaplaveno vlivem rozvodnění vodních toků na území města Brna. Z pohledu větrání a obměny vzduchu jsou z tohoto podlaží skrze plášť objektu způsobeny neplánované škvíry v otvorech, které malou mírou občerstvují vzduch

vlivem proudění z jedné strany objektu na druhou. Tento proud vzduchu ale s velmi vysokou pravděpodobností nestačí pro provozování datového rozvaděče s rozvinutou technikou pro VPS a cloudové úložiště. Dalším faktorem je, že objekt je dosti členitý a má nízkou světlou výšku. Z toho důvodu by mohl být problém se zajištěním čerstvého vzduchu. Z pohledu infrastruktury zde není problém připojit senzory požární ochrany a dále pohybové senzory, kamerový systém a systém řízení přístupu. Z důvodu nízkých stropů by mohl být problém mimojiné se zajištěním ochlazeného vzduchu pro systémy a také se zřízením automatického protipožárního systému.

Společnost dále uvádí že podlaha tohoto podlaží snese statické zatížení ve výši 1500kg/m2, což odpovídá hodnotě přibližně 15kN/m2.

Dále je vedle objektu rozestavěná betonová místnost v téže rovině, která by teoreticky mohla posloužit pro návrh mé práce, a to z důvodu, že by byla vhodně stavebně oddělena od objektu za účelem minimalizace škod při případném požáru. Její stávající dispozice jsou v půdorysném pohledu 6x4metry. Teoreticky by bylo možné zde umístit datový rozvaděč se servery. Nicméně na tuto místnost se dále zaměřím v návrhu své práce.

2.3.2 První nadzemní podlaží – 1.NP

V prvním nadzemním podlaží se nachází stávající provozovna podniku formou hostince. Konkrétně se jedná o rekonstrukci bytu na hostinec v roce 1997. Toto podlaží je stavebně ve vyšší míře členité. Podlaha podlaží je betonová, světlá výška místnosti je 2,9 metru, nicméně v tomto podlaží je nainstalován umělý strop ze dřeva, který slouží jako akustická izolace do vyšších obytných prostor. Strop do dalšího podlaží je z dřevěného materiálu. Tento umělý strop je umístěn ve výši přibližně 2,4 metru od úrovně podlahy. Dle mého názoru není vhodné datový rozvaděč umístit v tomto podlaží ze dvou důvodů. Jako hlavní nedostatek pro můj návrh v tomto podlaží je relativně vysoká míra rizika vzniku požáru vlivem dřevěného umělého stropu, a to konkrétně ve formě obtížnějšího hasícího účinku v případě počátku požáru. Druhým nedostatkem je, že v případě umístění datového rozvaděče v tomto podlaží, by bylo nutné změnit dispozici části podlaží a tím pádem snížení počtu míst pro zákazníky hostince, jelikož společnost chce nadále také provozovat hostinskou činnost. Ve stávající situaci se toto podlaží dělí na přední a zadní místnost pro zákazníky s dalšími obslužnými místnostmi, jako toalety a kuchyně.

Z pohledu případného zabezpečení jak fyzické infrastruktury, tak datové, by sice bylo možné zde umístit infrastrukturu pro zamýšlené rozšíření oboru podnikání formou datového rozvaděče. Nicméně za cenu nutných stavebních úprav oddělení přístupu od veřejnosti a dále ve formě zrušení umělého stropu, ve kterém vidím riziko v případě vzniku požáru. Dřevěný strop do vyššího podlaží také nenasvědčuje optimálnímu hodnocení pro umístění výpočetní infrastruktury v tomto podlaží.

2.4 Identifikace aktiv

Provozovna neobsahuje velké množství ICT prvků. Vyskytují se zde prvky pro vykrytí potřeb pro zákazníky ve formě veřejného Wi-Fi přístupového bodu a pokladního systému pro potřeby zaměstnanců pro provozování stávající obchodní činnosti a to konkrétně pokladní systém.

2.4.1 Soupis časti stávajících aktiv společnosti

V současném stavu jsou ve společnosti tyto prvky: Router, tiskárna, pokladní systém Conto, účetní systém Pohoda, externí datové úložiště

2.5 Síťová infrastruktura

V podniku se momentálně nachází bezdrátový přípojný bod AP ve formě dvou rozdílných zařízení pro dvě různá SSID na kmitočtu 2,4GHz, které oddělují veřejný přístup k internetu, od privátního, který má také navíc možnost přístupu do interní privátní sítě podniku. Toto oddělení veřejné části od privátní je zajištěno samostatnými rozvody datové kabeláže do routeru, kde je přístup oddělen na základě pravidel pro jednotlivá rozhraní.

Z pohledu kabelového připojení je aktuálně samostatná datová linka mezi pokladním systémem a routerem a datová linka mezi samostatným serverem s účetním systémem. Pravidla řízení přístupu jsou nastavena na routeru tak, že pouze vedoucí pracovník má možnost přístupu na server s účetním systémem a pokladní systém skrze firemní datovou síť. Zaměstnanci jsou oprávněni využívat pouze WiFi síť, která je určená pro veřejnost, čímž je zabezpečen oddělený přístup rozdělený na privátní část a veřejnou část. Řadoví zaměstnanci tak nemají přístup k historii obchodních dat a na pokladně mají také omezený přístup k datům.

Do podniku není zřízená možnost dálkového přístupu do vnitrofiremní datové sítě z internetu.

2.6 Řízení přístupu (pozn. - fyzická bezpečnost)

Pokladní systém se vyskytuje v úseku, kam jsou oprávněni vstupovat pouze zaměstnanci společnosti. Mechanická zábrana možného přístupu neoprávněných osob k pokladnímu systému se zde nevyskytuje.

Účetní systém je oddělen na samostatném počítači v serverové edici s použitím dvouvrstvé architektury prostřednictvím Microsoft SQL serveru. Umístěný je v jiné místnosti s názvem administrativní místnost. Přistup k němu je zabezpečen dveřním zámkem. Přístup k němu mají pouze vedoucí pracovníci.

2.7 Řízení přístupu (pozn. – datová bezpečnost)

V rámci pohledu řízení přístupu je oddělen přístup z pohledu vnitrofiremního na oddělené přístupy zaměstnanců a vedoucích pracovníků v možnosti přístupu k vnitrofiremních datům. Druhý pohled je rozdělení přístupů prostřednictvím bezdrátového přípojného bodu, kdy přes veřejný přístupový bod mohou přistupovat jak zákazníci podniku, tak i zaměstnanci podniku. Vedoucí pracovníci mají vlastní bezdrátový přípojný bod.

2.8 Požadavky společnosti v oblasti kybernetické bezpečnosti

Z pohledu procesního řízení by společnost ráda snížila riziko bezpečnostního incidentu na ICT infrastrukturu jak ve formě fyzického útoku, tak i virtuálního útoku. Jelikož návrh mé diplomové práce spočívá v návrhu kybernetické a informační bezpečnosti se zohledněním na oblast návrhu cloudového datového úložiště a poskytování služeb VPS, tak se ve své práci budu zaměřovat výhradně na toto úzké spektrum. V aktuální době na PoS jsou zakázány aktualizace operačního systému Microsoft Windows na úrovni firewallu. Toto opatření bylo v minulosti zhotoveno pro minimalizaci situací, kdy se systém začne nezávisle na aktuálním uživateli aktualizovat a tím znemožní případně i po několik hodin obsluhu pokladního systému. Řešením by bylo tyto aktualizace provádět automaticky v předem definovaných intervalech mimo provozní dobu podniku.

2.8.1 Kryptografie

Společnost dále uvádí, že ve stávající situaci nemá zavedené šifrování datového úložiště obchodních dat, a že mnou navrhované řešení cloudového datového úložiště pro rozšíření

oboru podnikání by společnost ráda vedla šifrované. Jako podklad bych rád využil souborový systém OpenZFS. Dále pokud to bude možné, tak aby můj návrh práce obsahoval také způsob pro šifrování oddílů určených pro virtuální servery VPS.

2.9 Zajištění dostupnosti

Stávající situace podniku neobsahuje v rozumné míře redundanci infrastruktury jak fyzické, tak datové. Obchodní data na pokladním systému PoS jsou ukládána lokálně na daný počítač do serverové aplikace, nejedná se tedy o online přenos dat na nějaký vzdálený systém. Toto řešení má své výhody i nevýhody.

Výhodou je, že daný systém není závislý na výpadku lokální datové sítě, a je tak schopen plně fungovat i při výpadku elektrické energie, jelikož je zálohován systémem UPS pro případy ztráty přívodu elektrické energie. Nicméně takto již nejsou zálohovány místní switche-přepínače pro funkční rozvod datové sítě a komunikace v rámci objektu.

Nevýhodou je, že tento systém PoS tedy není chráněn proti lokální závadě v konkrétním počítači, kde tento systém běží. Za předpokladu, že by daný počítač selhal například vlivem závady na disku počítače nebo vlivem jiných vektorů útoků, tak by s vysokou pravděpodobností mohla vzniknout ztráta dat v kompletním rozsahu z tohoto konkretního systému. Proto by bylo řešením zálohovat daný systém v daných obdobích například každý rok, nebo jako celek, nebo jednotlivá data replikovat online. Nicméně jelikož pokladní systém Consulta Conto je closed-source systém a licenční podmínky neumožňují reverse-engineering systému jako celku, tak není možno v souladu s licenčními podmínkami upravit aplikační databázi na platformě Firebird tak, aby se data replikovala online na jiný systém.

Rozvody síťové infrastruktury jsou aktuálně vedeny paralelně společnou cestou jak pro veřejnou síť tak i pro privátní síť samostatnými médii. Jelikož se zde nachází přípojná zařízení typu router s dostatečným počtem volných portů, tak ve stávající moment tyto rozvody a síťové prvky vyhovují stávajícímu systému. Nicméně pro rozšíření nového předmětu podnikání již tyto prvky se stanou nevyhovujícími, jak počtem portů, tak přípravnou kapacitou do budoucna.

2.10 Požadavky analyzovaného podniku pro rozšíření oboru podnikání

Jako vstup pro návrh mé diplomové práce podnik uvádí následující požadavky. Podnik požaduje, aby datový rozvaděč byl umístěn na vhodném místě z pohledu statického zatížení

v rámci dispozic objektu, dále z pohledu požárně bezpečnostních předpisů, a také s ohledem na ochranu proti srážkovým jevům a se zajištěním bezpečnosti proti vzniku úrazů a škod na majetku a na životech vlivem elektrických nehod. Dále společnost požaduje, abych vyhotovil návrh metodiky pro budoucí zaměstnance podniku, kteří budou povinni tyto metodiky dodržovat pro minimalizaci následků a vzniklých škod. Také součástí požadavků je, abych vyhotovil návrh metodiky tak, aby zohlednila zajištění vedení pravidelné dokumentace a záznamů o jednotlivých úkonech.

Z pohledu dohledu navrhovaných systémů podnik požaduje, abych vyhotovil návrh systému, respektive metodiky pro dohled infrastruktury pro zajištění její dostupnosti.

Z pohledu zajištění alternativního monitoringu v případě výpadků, jak elektrické energie, tak i spojení k internetu, podnik si sama zařídí návrh systému pro minimalistický dohled infrastruktury prostřednictvím SMS přes telefonního operátora.

3 VLASTNÍ NÁVRHY ŘEŠENÍ

V této kapitole se zaměřím na návrh práce samotný, kdy pro účely nových nabízených služeb zákazníkům použiji virtualizační systém Proxmox a pro účely cloudového úložiště využiji software Nextcloud. Oba tyto systémy budou mít vazby na různé další aplikace. Druhou částí bude oblast bezpečnostního managementu ve vztahu k těmto navrhovaným systémům.

3.1 Navrhovaný systém

Můj návrh řešení bude obsahovat dva základní systémy, o které opírám svoji práci.

Pro můj návrh použiji jako virtualizační systém Proxmox, který pro účely této práce pokrývá všechny požadavky z pohledu podsystémů, na které se tato práce zaměřuje. Jeho hlavní výhodou je, že je z větší části opensource. Jako klientské rozhraní pro zákazníky narhuji použít systému WHMCS s module ModulesGarden, prostřednictvím kterého by tak mohli zákazníci spravovat své virtuální zařízení.

Pro kapitolu poskytování cloudového úložiště použiji systém virtualizovaný Nextcloud, který bude využívat datové úložiště sdílené z virtualizačního serveru.

Z pohledu pokrytí bezpečnosti systému na úrovní síťové infrastruktury využiji systému RouterOS-Mikrotik.

Pro účely monitoringu dostupnosti služeb a stavů jednotlivých sledovaných veličin použiji monitorovací nástroj Zabbix.

3.2 Navrhovaný objekt

Pro účely této práce navrhuji dané mikro datové centrum zprovoznit v prvním podzemním podlaží v nové přistavěné místnosti o rozměrech 6x4x3,5m.

Tato místnost je nad úrovní rozvodů odpadních vod. Pro účely odvodu případných nežádoucích kapalin bude pod místností osazena trubka o průměru 25cm. Na rozmezí místnosti a odpadní trubky bude osazen ventil, který bude napojen na detektory vodní hladiny.

3.2.1 Zabezpečení objektu

Do objektu navrhuji zprovoznit elektronický zabezpečovací systém od společnosti Jablotron, který bude disponovat PIR/Laserové senzory, a dále obsahující čtečku otisku prstů pro omezení přístupu do objektu pouze pro oprávněné osoby v kombinaci s číselnou klávesnicí pro zadání bezpečnostního kódu pro průchod do objektu. Tento zabezpečovací systém bude ukládat data o průchodech a o aktivaci a deaktivaci systému ostrahy. V případě, že vznikne neplánovaná nebo nežádoucí událost ve formě neoprávněného vniknuti do objektu, tak se z tohoto zabezpečovacího systému odešle SMS zpráva přes mobilní síť telefonního operátora oprávněným osobám a také vytočí příslušné telefonní číslo za účelem notifikace narušení bezpečnosti objektu.

Do objektu také navrhuji osadit kamerový systém CCTV s nepřetržitým záznamem s retenční smyčkou maximálně ve výši 72 hodin v souladu s doporučeními úřadu pro ochranu osobních údajů ÚOOU. Tyto kamery navrhuji napájet vzdáleně prostřednictvím datových kabelů 8P8C na protokolu 802.3af. Provedení napojení těchto datových kabelů navrhuji tak, že připojovací konektory budou umístěny pod úrovní roviny zdi a to z důvodu aby tyto konektory byly chráněny fyzickou montáží bezpečnostní kamery. Elektrické napájení těchto kamer bude oddálené od objektu sdružené do datového přepínače typu PoE s podporou protokolu 802.af a notifikačního protokolu SNMP, včetně trapových zpráv za účelem odesílání stavových zpráv na dohledový systém. Rozvody datových kabelů pro tyto bezpečnostní kamery budou umístěny pod omítkou v chráničce za účelem ochrany těchto rozvodů.

Tento kamerový záznam se bude ukládat prostřednictvím datové sítě na vzdálené fyzické úložiště a to z důvodu, aby při neoprávněném vniknutí do objektu nebylo možné odcizit tyto kamerové záznamy. Do jednotlivých kamer také navrhuji připojit komunikační kabel do vstupně výstupních portů pro připojení na elektronický zabezpečovací systém, a to za účelem notifikace pro případ odcizení bezpečnostních kamer. Na úrovni síťové komunikační vrstvy tyto kamery budou monitorovány, zda odpovídají na Ping dotazové pakety. V případě ztráty komunikace bude na dohledovém systému vyhodnocena nefunkční komunikace s jednotlivými kamerami.

Umístění jednotlivých kamer navrhuji na vstupu do objektu a další umístěné tak, aby měly v zaznamenávaném perimetru přístupnou plochu k jednotlivým datovým rozvaděčům nebo v přístupu v uličce mezi kaskádou datových rozvaděčů.

Z pohledu ochrany pro minimalizaci škod v případě požáru do objektu navrhuji zprovoznit samostatný systém EPS, kterého součástí budou senzory přítomnosti kouře v objektu přímo nad datovým rozvaděčem. Součástí EPS bude také stabilní hasící zařízení, které v případě vzniku požáru vypustí do objektu inertní plyn za účelem uhašení požáru. Z tohoto důvodu bude také nutné v objektu zprovoznit signalizační zařízení pro případ, že by se v objektu vyskytoval zaměstnanec podniku v době požáru, a to z důvodu aby měl čas objekt opustit do stanovené doby, po které se aktivuje stabilní hasící zařízení.

3.3 Hardware

Pro virtualizační server navrhuji použít více fyzických serverů. Jako minimum pro začátek považuji pět fyzických serverů z důvodu naplnění požadavků pro chod clusteru. Tento počet v případě potřeby bude možné navýšit na požadované množství.

Další dva servery navrhuji HP Proliant v konfiguraci 12LFF, které budou sloužit jako zálohovací servery typu „Warm“ v režimu master-slave. Toto nastavení volím z důvodu úspory investičních nákladů. V případě, že by podnik disponoval finančními rezervami pro tento projekt, tak bych zvolil tři zálohovací servery v online clusteru. Tyto zálohovací servery budou umístěny minimálně v jiné mistnosti a v jiném datovém rozvaděči. Tuto konfiguraci navrhuji z důvodu, že není zapotřebí vysoká datová propustnost, nýbrž jde o splnění dostačujícího zálohovacího procesu.

V rámci svého návrhu navrhuji použít rackové provedení serverů do datového rozvaděče od společnosti HP, řadu Proliant. Datový rozvaděč navrhuji použít výšku 42U jednotek s příslušnou hloubkou pro servery včetně rezervu hloubky pro kabeláž k jednotlivým serverům, a také pro odvod teplého odpadního vzduchu. Takto navržené datové rozvaděče budou poskytovat dostatečnou rezervu v podobě volných rack unit jednotek pro budoucí rozšíření.

Pro účely vyšší kapacity navrhuji použít klasické rotační disky typu HDD. Pro účely vyšších rychlostí a nižší latence systému a vnořených virtuálních systémů navrhuji použít disky typu SSD průmyslové kategorie, a to z důvodu, že použití souborového systému OpenZFS je značně náročné na omezený počet zápisů SSD disků.

Každý jednotlivý server má dle dokumentace výrobce při plném vytížení produkci odpadního tepla ve výši až 3071 BTU jednotek za hodinu provozu.

3.3.1 HP iLO

Pro účely vzdáleného přístupu je velmi užitečné webové rozhraní HP iLO, které plní funkci KVM s možností vzdáleného připojení obrazového souboru ISO pro zavedení instalace operačního systému. Jedná se o velmi užitečnou funkci, která je nápomocná technikovi pro vzdálenou správu zařízení i v případě, že k němu nemá fyzicky přístup. Další výhodou je interní monitoring stavu jednotlivých komponentů v serveru, kde je možné přehledně vyčíst hodnoty teplot, rychlosti ventilátorů, aktuální spotřeby elektrické energie a zdraví jednotlivých komponent. V případě, že se v serveru objeví nějaká závada, tak prostřednictvím iLO odpovědný pracovník zjistí poměrně snadno, jaká komponenta je vadná. Tuto vadnou komponentu následně vymění. Rozhraní iLO ze všech serverů navrhuji prostřednictvím protokolu SNMP připojit do dohledového systému Zabbix.

3.3.2 Chlazení objektu

Pro účely chlazení objektu navrhuji použít tři sety systému chlazení typu vzduch-vzduch který bude dimenzován s kapacitou přísunu chladného vzduchu o tepelné energii dvojnásobné než odpadní teplo datového rozvaděče 42U. V případě rozšíření počtu datových rozvaděčů bude investor muset pořídit výkonnější chladící systém. Tři sety volím z důvodu případné závady nebo servisních pracích na jednotlivých setech. Konkrétní provedení bude provedeno přísunem chladného vzduchu při podlaze a odvodem teplého vzduchu u stropů.

Chladící systém vzduch-vzduch má oproti jiným technologiím značně nižší účinnost ve vztahu k odebrané elektrické energii. Nicméně jej považuji za značně jednodušší na servis a údržbu než jiné technologie.

Za průmyslově nejúčinnější mně známou technologii považuji chlazení olejem. Tuto metodu využívá například společnost WEDOS.cz, s.r.o. Tato společnost tuto metodu využívá tak, že jednotlivé servery jsou trvale ponořeny v olejové lázni, která je kontinuálně přečerpávána za účelem odvádění odpadního tepla. Jako značnou nevýhodu považuji obtížnější údržbu vnitřních částí serverů, které jsou znečištěny olejem. Z důvodu vyšší složitosti chladícího systému jako celku tuto metodu nenavrhuji.

Za účelem udržení optimálních teplot datových serverů a také pro snížení rizika vzniku požáru je nutné do místnosti, kde bude umístěna datová infrastruktura, umístit průmyslové teploměry. Jako vhodný komunikační protokol pro tyto teploměry uvažuji protokol Modbus,

prostřednictvím kterého se budou přenášet stávající hodnoty do centrálního uzlu mimo tuto místnost. Tento centrální uzel bude sloužit pro získávání hodnot z měrných zařízení jako teploměry, vlhkoměry, aj. a také pro zasílání instrukcí jednotlivým akčním členům, které budou kompatibilní s protokolem Modbus. Výsledné stavy měřených hodnot budou zasílány z centrálního uzlu Modbus do dohledového systému Zabbix, který bude provozován na jiném technickém vybavení než hlídané servery, pro účely dohledu.

Z pohledu chladícího systému navrhuji do dohledového systému nastavit limity měřených hodnot, tak aby v případě dosažení teplot mimo nastavený práh byl dohledovým systémem upozorněn odpovědný pracovník na nežádoucí stav sledovaného chladícího systému ve formě nežádoucí nízké nebo vysoké teploty.

3.3.3 Redundance a SPOF

Servery navrhuji použít takové, které mají sloty pro připojení disků přímo v jednotlivých serverech, nikoliv tedy použití samostatného datového úložiště typu DAS, a to za účelem snížení míry SPOF. Z toho důvodu tyto servery budou muset obsahovat výkonné síťové karty, kdy jeden fyzický datový port bude vyhrazen výhradně pro komunikaci clusterového úložiště pro udržení minimální latence a vysoké míry datové propustnosti.

3.3.4 Odhadovaná spotřeba elektrické energie

Odhadované množství elektrické energie bude činit 500VA na 2 rack-unit. Při provozu 15ti fyzických serverů na jeden datový rozvaděč tak spotřeba elektrické energie fyzických serverů bude ve výši 7,5kVA.

V datových rozvaděčích budou osazeny dva datové přepínače pro připojení fyzických serverů do vnitropodnikové datové sítě. Tyto datové přepínače mají deklarovanou spotřebu elektrické energie v součtu ve výši 500VA.

Systém chlazení má v součtu deklarovanou spotřebu elektrické energie ve výši až 15kVA.

V této fázi by celková odhadovaná okamžitá spotřeba elektrické energie pro datový rozvaděč včetně příslušenství činila přibližně 23kVA.

Do objektu je přiveden jediná přípojka elektrické energie z distribuční soustavy. Z toho důvodu v návrhu nelze dimenzovat redundantní napájení na rozhraní předávacího místa z distribuční soustavy.

3.3.5 Ochrana proti přepětí

Na úrovni předávacího bodu do objektu z energetické distribuční sítě navrhuji nainstalovat přepěťově ochrany, které budou mít sveden vlastní svod do země pro případ přepětí. Jednotlivé fyzické prvky, které budou technicky dostupné oprávněným osobám, musí být řádně galvanicky uzemněny pro vyloučení úrazů elektrickým proudem. Pro tento účel navrhuji mj. zařízení v datovém rozvaděči galvanicky propojit s pláštěm datového rozvaděče, vhodným vodičem o barevném značení „ŽZ“, který bude elektrický uzemněný na jeden ze zemnících bodů objektu.

3.3.6 Alternativní zdroje elektrické energie

Pro účel snížení odběru elektrické energie odebírané od dodavatele energií bych doporučil v objektu nainstalovat solární panely, které by byly schopné napájet jednotlivé servery po dobu osvitu slunečními paprsky. V prvotní fázi bych doporučil systém dimenzovat na 10kWp. K solárním panelům je samozřejmě potřeba zajistit ostatní infrastrukturu jako invertor ze stejnosměrného napětí na napětí střídavé, kabeláž aj. Z důvodu použití serverů bych navrhoval třífázové napájení, a to z důvodu nižší pořizovací ceny kabelových rozvodů pro rozvod elektrické energie, a to z důvodu nižšího průřezu vodičů. Elektrická síť v objektu bude typu TN-C. Bateriový systém pro ukládání elektrické energie není potřeba, a to z důvodu, že konstantní spotřeba bude teoreticky vyšší než kapacita možné produkce elektrické energie. Nutno podotknout že fotovoltaický systém není vhodný jako jediný zdroj elektrické energie za předpokladu výpadku napájení v elektrické síti z důvodu, že tento systém nedokáže pokrýt potřebu celoročně z důvodu, že v zimním období je energetický zisk z fotovoltaických panelů velmi malý, řádově okolo 400W/h bez zohlednění energetických ztrát na celém fotovoltaickém systému z navrhovaných 10kWp.

Z důvodu provozních nákladů podniku nedoporučuji použít motorový agregát pro náhradní zdroj elektrické energie, protože lze předpokládat, že zprvu podnik nebude mít dostatečné množství zákazníků, aby mohl financovat tyto generátory. Za vhodnější považuji použít na začátku provozování živnosti podniku použít záložní systém elektrické energie typu UPS pro

pokrytí korektního vypnutí služeb a serverů a tím pádem minimalizaci rizika poškození dat nebo technického vybavení. Tato situace může nastat například v případě výpadku elektrické energie na úrovni distribuční sítě před předávacím bodem objektu.

V případě, že by podnik dokázal spolehlivě generovat obrat z poskytování VPS a cloudového úložiště tak, že by byl schopen hradit provozní náklady motorového agregátu, tak bych jednoznačně doporučil podniku zakoupit tři jednotky agregátů s tím, že jeden by byl aktivně v provozu, a další dva by sloužily jako záložní případně na jednom ze záložních agregátů by byla prováděna údržba. Vhodným elektroinstalačním materiálem lze zajistit, že v případě výpadku prvního agregátu se obratem aktivuje záložní pro nepřerušený provoz infrastruktury. V tomto případě navrhuji zachovat také systém UPS pro překlenutí doby náběhu motor agregátů a vykrytí nežádoucích vlivů na elektrické síti jako přepětí, podpětí, kmitočet napětí mimo smluvní rozsah s distributorem, aj.

3.3.7 Připojení k internetu

V případě, že by společnost měla vyšší počet zákazníků (přibližně do 500), kteří by odebírali služby, tak by bylo vhodné zajistit redundantní vysokokapacitní připojení k internetu a to ideálně dvěma samostatnými přenosovými médii. Z řad kapacity přenosu bych společnosti doporučil obě tyto datové přípojky k internetovému připojení stanovit přenosovou kapacitu vyhrazenou ve výši alespoň 10 Gbit/s. Je nepravděpodobné, že by nastala situace taková, kdy by současně všech až 500 zákazníků aktivně využívalo internetovou přípojku. Proto by bylo rozumné aby společnost aktivně sledovala pravidelné vytížení přenosové linky, a v případě, že by se v průměru dosahovalo více než 75% vytížení přenosové linky začala uvažovat o navýšení přenosové kapacity anebo v lepším případě přesunu datových serverů na jinou lokalitu, kde je vysokokapacitní přípojka k internetu o přenosové kapacitě vyšší než 10 Gbit/s. Jistým problémem, který firma sama nedokáže vyřešit, že v aktuálním stavu je v navrhovaném místě přístupné pouze připojení typu DSL nebo možnost umístění antény pro přenos skrze WiFi. V budoucnu se ale toto omezení má vyřešit a to z důvodu podporovaných a plánovaných investic do sítě CETIN, kdy stávající koaxiální kabely mají být postupně nahrazovány optickými kabely. V tento okamžik tedy nelze říci jak bude stanovena přenosová kapacitá nové datové přípojky po rekonstrukci a jaké na ni budou nabízené parametry kvality.

3.3.8 HW firewall

Pro účely této práce uvažuji platformu Mikrotik, primárně z důvodu, že ji již znám. Pro optimální konfiguraci by byl vhodný firewall typu NGFW. Nicméně bohužel k takovému zařízení nemám přístup, pokusím se jej tedy pro účely této práce v úzkém spektru nahradit softwarovým firewallem.

Předpokladem pro tuto práci je nastaven podnikový předávací bod tak, aby byla pokud možno vhodně zabezpečena vnitropodniková síť. Součástí této práce se budu tedy zabývat pouze pravidly, souvisejícími s navrhovaným systémem.

3.3.8.1 Konfigurace HW firewallu

Tato část se zaměřuje pouze velmi úzkým navrhovaným výběrem pravidel pro návrh této práce. V obecné rovině tedy lze říci, že firemní firewall musí obsahovat velkou řadu dalších pravidel nutných k zabezpečení sítě, jak vnitropodnikové sítě, tak i hlavního rozhraní na hraně předávacího bodu podniku. Pro účely vzdáleného přístupu oprávněných osob nebo administrátora z prostor mimo podnikovou síť navrhuji použít OpenVPN spojení z důvodu, že jej považuji za spolehlivý a bezpečný.

Pro účely přístupu k virtuálním zařízením zákazníků navrhuji nastavit přístupová pravidla následovně, pro přístup na webová rozhraní platforem a dále následující pravidla, kdy IP adresa x.x.x.x odpovídá hraniční veřejné IP adrese společnosti a IP adresa y.y.y.y odpovídá adrese SW firewallu:

/ip firewall nat add chain=dst-nat dst-address=x.x.x.x protocol=tcp dst-port=443 action=dst-nat to-addresses=y.y.y.y to-ports=443

Další pravidlo navrhuji limit počtu spojení z jedné zdrojové adresy na cílovou službu pro zamezení DoS útoku. V případě, že by nastal útok DDoS, tak navrhuji odstavit systém od přistupu k internetu, a to z důvodu, že podnik nebude disponovat kapitálem vhodným pro zajištění tak silné inrastruktury, která by mohla snížit riziko útoků DDoS.

Pro interní podnikovou síť, na kterou budou připojení pracovníci podniku, by bylo užitečné zprovoznit autentifikační systém 802.1X, který tak v budoucnu po rozšíření může být součástí Single-sign-on pro přístupy k oprávněným podsystémům z daných pracovních úseků.

3.3.9 OpenVPN server

Za účelem vzdáleného přístupu zaměstnanců do vnitropodnikové sítě navrhuji zřídit OpenVPN například na firewallu Mikrotik, který by byl nastaven tak, že by vyžadoval klientský certifkát pro připojení. Na základě tohoto tak bude zapotřebí aby, pro funkčnost připojení skrze VPN odpovědná osoba společnosti zřídila klientské certifikáty které by byly ověřeny certifikační autoritou. Tyto všechny certifikáty by následně bylo třeba naimportovat do klientských zařízení. Vytváření certifikátů za tímto účelem Mikrotik podporuje. Jako ideální kombinaci volím takovou, aby společnost použila certifikáty PKCS#12, které bude také chráněny uživatelským jménem a heslem, čímž se zajistí více faktorová autentizace například z důvodu odcizení klientského zařízení. Tyto klientské certifikáty jsou podporovány v klientských aplikacích OpenVPN jak pro Windows tak i pro Android. V případě, že by došlo k podezření zneužití těchto přístupových certifikátů na VPN server, tak je možné na firewallu Mikrotik tyto certifikáty zneplatnit, čímž se tak zamezí jejich dalšímu použití pro vzdálený přístup.

3.4 Software

Pro potřeby podniku a návrhu mé práce je třeba vyhotovit také programové vybavení takové, které bude funkční a pokud možno bylo zabezpečeno tak. Aby se v maximální možné míře snížil vektor možných útoků na podnikovou infrastrukturu.

3.4.1 SW firewall

V rámci zamezení neoprávněného přístupu mezi virtuálními zařízeními a hypervizorem je třeba prostřednictvím bezpečnostních pravidel třeba také oddělit komunikaci mezi nimi. Pro tyto účely se mi jako vhodná jeví platforma OPNSense, která je open-source založena na firewallu pfSense. Po prvotní instalaci shledávám grafické rozhraní jako poněkud nepřehledné. Nicméně po delším seznámení se s konfigurací OPNSense již je technik schopen využít svých obecných znalostí sítí a implementovat požadovaná pravidla.

OPNSense pro trasu komunikace z fyzického rozhraní na rozhraní frontendu virtualizace pro zákazníky a frontend Nextcloudu bude sloužit jako hraniční firewall. Hlavním účelem SW firewallu tedy bude zamezení přístupu mezi jednotlivými systémy vzájemně a také k zabránění přístupu z virtualizovaných systémů do rozhraní firewallu, hypervisoru a také do interní sítě podniku.

Pro účely zabezpečení síťového provozu k nebo od zákaznických virtuálních zařízení bych doporučil využít vlastností OPNSense, a to z důvodu, že Proxmox nenabízí v zabudovaném firewallu takové možnosti pro oddělení provou jako Vnitřní SW firewall. Na základě uvedeného bych doporučil využít oddělených sítí typu VLAN s nastavením vhodných pravidel pro zamezení neoprávněného přístupu mimo rozsah privilegií zákazníků.

3.4.2 DNS server pro správu domény

Přístup k webovým službám pro zákazníky bude zprostředkován přes FQDN webovou adresu. Doménu druhého řádu bude mít podnik zakoupenou u jakéhokoliv z dostupných registrátorů. Jako jmenné servery bude podnik používat vlastní jmenné servery, kde bude zajištěna konfigurace požadovaných přístupových sub-domén na jednotlivé služby. Za příklad lze vzít následující sub-domény: https://cloud.mujpodnik.cz/, https://vps.mujpodnik.cz/ . Vlastní jmenné servery volím z důvodu možnosti přímých změn IP adres pro domény, například formou skriptu za předpokladu, že to společnost bude potřebovat. Dále z důvodu, že dostupnost konfigurace DNS serveru nebude závislá na dostupnosti webového rozhraní pro administraci doménových záznamů u registrátora. Ke dni vydání této diplomové práce mi není známo, zda-li pro zónu .cz existuje registrátor s možností IXFR změn DNS záznamů. Pro účely této práce navrhuji použít DNS serverovou aplikaci Named nebo BIND. Konfigurace DNS serveru není součástí návrhu této diplomové práce.

V případě, že podnik bude mít vlastní DNS server pro provoz interní domény, tak je třeba zajistit pravidla taková, aby nebylo možné neoprávněně změnit jednotlivé DNS záznamy odkazující na konkrétní zařízení tak, že by nežádoucí osoba mohla dané požadavky přesměrovat na nevyžádanou stanici.

Pro základní provoz poskytovaných služeb zákazníkům je tak vhodné až potřebné, aby odpovědný pracovník v konfiguračním souboru odpovídající DNS zóny nastavil SOA, A, MX, TXT, CAA, NS a CNAME záznamy. V případě že by společnost využívala protokolu IPv6, tak by měla nastavit také AAA záznam. Jako možný příklad pro společnost níže uvádím možné nastavení těchto záznamů:

- A: 44.55.66.77
- AAA: e725:a13b:eec0:9620:de13:71e6:bce6:4ff6

- CAA: 0 issue “sectigo.com”
- CNAME: cloud.mujpodnik.cz
- CNAME: vps.mujpodnik.cz
- MX: 10 mail.mujpodnik.cz
- NS: ns1.mujpodnik.cz + ns2.mujpodnik.cz
- SOA: ns1.mujpodnik.cz
- TXT: _domainkey "v=DKIM1; h=sha256; k=rsa; p=MIIC…“
- TXT: _dmarc v=DMARC1; p=quarantine; fo=0; adkim=r; aspf=r; pct=100; rf=afrf; ri=86400; sp=quarantine

NS záznamy by měly být ideálně dva na různé nameservery, které běží na různých systémech.

3.4.3 SMTP server

Jak Proxmox, tak Nextcloud mají podporu k zasílání notifikací skrze mailový server. V případě, že by podnik chtěl tohoto využít, tak doporučuji vhodně zabezpečit mailový server proti neoprávněnému užití mailového serveru například nadměrným odesíláním nevyžádaných mailových zpráv a také nastavit pravidla, tak aby počet odchozí pošty splňoval limity, maximálně o hodnotách vyžadovaných providerem. Detailní popis a konfigurace SMTP serveru není součástí této diplomové práce z důvodu, že jej považuji za rozsáhlý a náročný pro provoz a případnou údržbu. Pro účely této diplomové práce tedy navrhuji použití SMTP serverů s omezením pouze pro účely zasílání mailových zpráv o potvrzení registrace zákaznických účtů a pro zasílání mailů jako odpovědi na žádost o obnovení přístupových údajů.

Za předpokladu, že by zaměstnanci podniku chtěli využívat vnitropodnikový mailový server pro účely vnitrofiremní komunikace, tak bych doporučil zprovoznění druhého samostatného mailového serveru, který nebude nakonfigurován vůbec na odesílání mailové pošty do internetu. Jednalo by se tedy o metodu, kdy se zaměstnanci svými klientskými zařízeními připojují lokálně nebo vzdáleně na mailový server. V případě, že by se jednalo o vzdálené připojení, tak je vhodné zvážit použití připojení prostřednictvím VPN šifrovaného tunelu. Tento druhý mailový server určený výhradně pro vnitrofiremní účely by mohl být také napojen

na monitoringový systém Zabbix za účelem zasílání notifikačních zpráv odpovědným pracovníkům.

3.4.4 Reverzní proxy server

Pro účely přesměrování z FQDN adresy na adresu virtualizačního frontendu nebo frontendu cloudu na IP adresu navrhuji použít reverzní proxy server HAProxy. Za pomocí HAProxy tak může společnost zařídit, že na jedné veřejné IP adrese bude k dispozici více různých webových domén. Tento proxy server bude mít jako primární úlohu zprostředkování vynucení mTLS certifikátů pro přístup na cloudové úložiště. Jako další benefit tohoto proxy serveru považuji budoucí možnost rozšíření na webový load-balancer za předpokladu, že by podnik byl úspěšný v rozšíření své nové živnosti v poskytování těchto služeb a potřeboval zajistit rozdělení datového toku na více vnitřních IP adres.

HAProxy umožňuje také aplikovat web aplikační filtry, které jsou součástí verze enterprise. V případě, že by společnost chtěla využít těchto filtrů pod aplikací HAProxy, tak bych společnosti doporučil použití enterprise verze.

3.4.5 Virtualizační server se systémem Proxmox – backend

Proxmox navrhuji jako hypervizor z důvodu, že s ním již mám zkušenost. Jedná se o aplikační nástavbu na operačním systému Linux. Jako nástroje které Proxmox využívá pro virtualizaci, tak je Qemu pro virtuální zařízení, a LXC pro virtualizační kontejnery.

Qemu je vhodné pro bezpečnější oddělení virtualizovaného systému od hostovaného již na úrovni oddělení načítaného jádra. V případě LXC je naopak výhodou jeho nižší nárok na výpočetní výkon. Nevýhodou LXC je jisté propojení s hostovaným systémem na úrovni namespaců a použití části systémových prostředků hostovaného systému.

Proxmox z pohledu pořizovacích nákladů je výhodný. Není zde žádná pořizovací licence na jednotlivé funkce systému a na instalaci systému. Proxmox si účtuje pouze podporu systému na roční bázi, která není povinná. Při srovnání s nejznámějším systémem VMware lze tak značně snížit tyto pořizovací náklady.

Pro účely hlavních témat této práce použiji pouze virtuální systémy prostřednictvím QEMU za účelem bezpečnějšího virtualizovaného prostředí z pohledu izolace od linuxového jádra hypervizoru.

Po prvotní instalaci systému je zapotřebí systém nakonfigurovat do podnikové sítě. Jedním ze základních předpokladů je tedy konfigurace IP adresy, DNS serverů, případně nastavení vnitrofiremní domény. Po této inicializaci je možné již začít vkládat jednotlivé servery do logického clusteru. Dále již je možné vytvářet jednotlivé virtuální zařízení dle potřeby.

Zákaznické virtuální zařízení navrhuji šifrovat a to z důvody ochrany zákaznických dat před zneužitím. Toto šifrování by bylo prováděno na straně serveru.

3.4.6 Poskytování VPS – Frontend

Provedení frontendu hypervizoru je uživatelsky nepřívětivé ve smyslu přímého použití smluvními zákazníky. Jako druhý aspekt se domnívám, že by prostřednictvím přímého webového rozhraní Proxmoxu mohly být vedeny nežádoucí útoky na infrastrukturu. Proxmox podporuje nastavení uživatelů, skupin a rolí. Jako vhodnější se mi z pohledu bezpečnosti zdá použít pro zákazníky jiné vhodné webové rozhraní, prostřednictvím kterého by mohli zákaznici přistupovat ke svým virtuálním zařízením. Na trhu je více dostupných platforem, které mohou plnit tuto funkci, jako příklad možného použití uvádím WHMCS ve spolupráci s ModulesGarden.

3.4.7 Replikace a zálohování dat

Z důvodu, že pro hlavní témata své práce používám Proxmox jako hypervizor, tak bych podniku navrhnul, aby využila řešení od stejné společnosti, které bude plnit funkci zálohovacího serveru. Jedná se o Proxmox Backup Server (PBS).

Pro podnik navrhuji použít zálohovací metodu 3-2-1. Jako souborový systém na základě svých zkušeností doporučuji použít souborový systém OpenZFS konkrétně v konfiguraci raidz-2, která funguje podobně jako klasický RAID-6. V případě, že by podnik chtěl provozovat rychlejší konfigurace souborového systému za účelem snížení doby obnovy, tak by podnik mohl použít také konfiguraci obdobné jako RAID-10. Oproti použití běžného řadiče s funkcí RAID disponuje OpenZFS řadou výhod jako například snapshoty, replikace, rozšířenější konfigurace a řada dalších.

Zálohy virtuálních systémů zákazníků budou zálohovány v intervalech smluvně dohodnutých se zákazníky. Hlavním důvodem různých zálohovacích intervalů je různá míra nákladů na provoz zálohovacích systému v závislosti na potřebné kapacitě a také v souvislosti

s požadovanou dobou obnovy. V případě požadované kratší doby obnovy by tak podnik musel vynaložit vyšší náklady na hardware v rozdílu cen a výkonových parametrů HDD, SSD a NVMe disků. Doba obnovy virtuálních systémů je přímo úměrná obsažené kapacitě.

Na začátku rozvoje nové obchodní činnosti podniku v poskytování cloudových služeb podniku nedoporučuji použít tzv. „HOT“ záloh z důvodu vyšších investičních a provozních nákladů. O těchto horkých zálohách bych navrhnul podniku uvažovat až ve fázi, kdy by měla dostatečný počet zákazníků, kteří by spolehlivě generovali dostatečný zisk pro značný rozvoj infrastruktury, nutné pro provoz horkých záloh.

Doporučuji podniku, aby zpřístupnil zákazníkům využití funkcí snapshotů, které mohou být užitečné pro verzování virtuálních systémů v případě prováděných změn zákazníky. V případě, že zákazník bude potřebovat, tak může virtuální systém vrátit do předchozího stavu formou obnovy předchozích snapshotů. Dále bych podniku doporučil, aby zákazníkům předal informaci o tom, že snapshoty nejsou zálohou systémů.

Mnou navrhované řešení využití OpenZFS souborového systému nedisponuje funkcí pro plnohodnotný clusterový souborový systém, podobně jako je znám ze systémů Ceph, GlusterFS, aj. Proto mezi jednotlivými servery, které budou mít shodné diskové konfigurace, by mohl podnik využít pravidelné replikace virtuálních systémů napříč jednotlivými servery. V případě, že by jeden server byl plánovaně nebo neplánovaně odstaven z provozu, tak obratem virtuální zařízení nastartují v ostatních ze serverů v závislosti na zvolené konfiguraci Proxmox clusteru.

Z pohledu záloh ze strany sledované společnosti navrhuji, aby také zálohovala jednotlivé systémy, které jsou potřebné pro provozování obchodní činnosti. Jako jedna z možností tak může být zálohovat jak operační systémy na serverech v souvislosti se zahrnutím základních konfigurací, dále aby podnik zálohoval konfigurace routerů, případně managovatelných switchů a dále aby zálohoval virtuální instance jako virtuální firewall, a konfigurace cloudového úložiště a virtualizačního serveru. Tyto podnikové zálohy zprvu navrhuji provádět v 3 denních intervalech. V případě, že by podnik měl potřebu zálohovat množství dat takové, které by se nestihlo zálohovat v 3 denním intervalu z důvodu kontinuální nepřetržité zálohy, tak společnosti navrhuji navýšit přenosovou kapacitu určenou pro zálohy.

Tyto podnikové zálohy navrhuji tak, aby pravidelné zálohy měly retenční smyčku ve výši 3x3 dní a dále jednu každý měsíc která by odpovídala na začátku měsíce v 1-3. kalendářní den dle

výše uvedeného harmonogramu. Tyto měsíční zálohy navrhuji použít obdobně v retenční smyčce tří měsíců. Společnost by měla také v pravidelných intervalech provádět testy obnovy záloh pro zjištění, zda jsou zálohovaná data konzistentní a proces obnovy dat funkční. V případě, že by byla napadena podniková infrastruktura, čímž by mohly být ohroženy i jednotlivé zálohy dat, tak podnik může využít druhé kopie záloh, které by byly typu „Cold“, resp. offline. Tímto společnost vhodně zabezpečí zálohovaná data proti jejím napadení.

Podnik by mohl také využít snapshotů pro své vlastní účely. Může se tak jednat o testování nových funkcí v testovacím prostředí, ale také nasazování funkcí do ostrého provozu. V případě neúmyslného nedopatření v chybných implementací tak pracovník může vrátit stav do předchozího stavu. Tyto obrazy může také použít jako prevenci proti ať záškodnému nebo neúmyslnému smazání podnikových dat, kdy touto formou tak nadřízený pracovník může dohledat předchozí stav s dohledáním potřebných dokumentů, záznamů nebo konfiguračních soborů.

3.4.8 Nextcloud

Tento software má za primární funkci ukládání dat a následnou vzdálenou manipulaci s nimi tak, jako ji známe z řady ostatních cloudových řešení. Jedná se opět o open-source řešení, které je značně modulární. Lze tak do Nextcloudu nahrát řadu modulů pro pokrytí žádaných funkcionalit. Mohou to být jak kolaborativní práce na dokumentech, chat, kalendář, kontakty, dvou faktorová autentizace, SSO & SAML autentizace, aj. Nextcloud také umožňuje sdílení dat napříč uživateli, nebo také i prostřednictvím unikátních odkazů jakékoliv osobě za předpokladu, že je to v nastavení Nextcloudu povolené. Další z funkcionalit jsou skupinové složky.

3.4.8.1 Nextcloud – konfigurace

Pro jednotlivé zákazníky bude nastavena kvóta pro úložiště, jakožto maximální možná využitelná kapacita. Za účelem ochrany dat zákazníků navrhuji aktivovat šifrování dat na straně serveru. Do podmínek použití cloudového úložiště navrhuji zakomponovat klauzuli o právní odpovědnosti zákazníků k ukládání souborů ve vztahu s právním řádem České Republiky jako právní ochrana provozovatele cloudového úložiště. V případě, že vznikne podezření na porušení legislativních podmínek ČR tak podnik předá na základě výzvy technické vybavení nebo její části oprávněné třetí osobě pro účely forenzní analýzy.

Pro účely autentizace volím dva návrhy pro společnost, ze kterých může následně vybrat variantu pro ni vhodnější. První metoda, která je jednodušší je použití metody autentizace zabudované v Nextcloudu. Druhou možností je použít správy uživatelů prostřednictvím LDAP, za pomoci kterého tak může společnost mít napojenou databázi uživatelů také do jiných systémů v případě potřeby.

Společnost Nextcloud nabízí také prostřednictvím internetové stránky jednoduchý nástroj na adrese https://scan.nextcloud.com/ prostřednictvím kterého lze otestovat zda je aplikace Nextcloud správně nastavena z pohledu zabezpečení. Výstup tohoto testu sice není tak detailní jako výstupy z jiných testovacích nástrojů, ale hlavní předností tohoto bezpečnostního skenu, je jeho jednoduchost, kdy tak stačí pouze zadat webovou adresu daného webového serveru. Jelikož mnou navrhované cloudové úložiště bude vyžadovat vynucené využití klientských certifikátů, tak tento test bude možné provádět pouze po úpravě konfiguračního souboru v HAproxy tak, aby tento testovací nástroj se mohl vzdáleně připojit na webové rozhraní Nextcloudu a provést tak zmíněný bezpečnostní sken. Za tímto účelem je možné v HAProxy konfiguraci například nastavit samostatnou virtuální doménu pro tyto účely. Jakmile test bude dokončen, tak daný správce tuto doménu může v HAProxy opět deaktivovat.

3.4.8.2 Nedostatky

Při mém testování systému Nextcloud jsem narazil na občasné chybové hlášky. Nicméně předpokládám, že podnik by měl vynaložit takové úsilí pro zprovoznění Nextcloudu bez chyb. Je ale možné, že by bylo třeba mírně vyšších požadavků správce systému na pravidelnou údržbu systému.

3.4.9 Mutual-TLS certifikáty

Pro svoji diplomovou práci jsem si zvolil konfiguraci webového rozhraní pro Nextcloud formou vynucených mTLS certifikátů. Jednou z vlastností je, že mTLS certifikáty neskryjí požadovanou doménu od klienta. Během navázání TLS spojení je v datovém paketu „Client Hello“ v nešifrované formě vidět cílová požadovaná webová adresa a to konkrétně v TLS Handshake protokolu v podpoložce Extension – Server name identification (SNI).

Pro provozování důvěryhodné webové služby pro zákazníky je zapotřebí mít certifikát vystaven certifikační autoritou po splnění důvěryhodného řetězce. Podnik si může zvolit z řady různých poskytovatelů certifikačních autorit nebo si vygenerovat vlastní certifikační autoritu,

kterou by následně distribuoval mezi zákazníky. Cloudflare nabízí vydávání klientských mTLS certifikátu s Cloudflare CA při použití vlastních jmenných serverů při měsíčním paušálu 200$,

V případě, že by se podnik i přes to chtěl rozhodnout použít vlastní self-signed certifikáty, tak po vygenerování certifikační autority může začít vytvářet jednotlivé certifikáty. V pořadí jako první se jedná o certifikát pro webové rozhraní jednotlivých služeb, který nazvu „serverový certifikát“. Tento serverový certifikát je třeba naimportovat do složky určené pro certifikáty aplikace HAProxy. Poté lze vytvářet jednotlivé klientské certifikáty, které lze distribuovat zákazníkům.

Pro vytvoření klientských certifikátů s openssl je jako první třeba vytvořit privátní klíč, kde jsem zvolil velikost 2 kilobajty, lze použít i vyšší. *openssl genrsa -out client3.key.pem 204*8

Poté za pomocí privátního klíče vytvořím žádost o podepsání certifikátu. *openssl req -new -key client3.key.pem -out client3.csr*

Následně prostřednictvím firemní vygenerované certifikační autority podepíšeme a vytvoříme certifikát, pro účely této diplomové práce jsem zvolil platnost 999 dní. V praxi je doba platnosti certifikátu na zvážení poskytovatele služeb. Ze svého pohledu bych ale doporučil dobu platnosti dvou let. *openssl x509 -req -in client3.csr -CA certs/root_ca.crt -CAkey secrets/root_ca_key -out client3.cert.pem -CAcreateserial -days 999 -sha256*

Následně zkombinujeme certifikát a privátní klíč do #PKCS12 formátu, který je možné opatřit bezpečným heslem pro účely zaslání certifikátu vzdálenou metodou.

openssl pkcs12 -export -inkey client3.key.pem -in client3.cert.pem -out client3.p12

Tento certifikát ve formátu #PKCS12 si již zákazník může naimportovat do webového prohlížeče anebo jiné klientské aplikace.

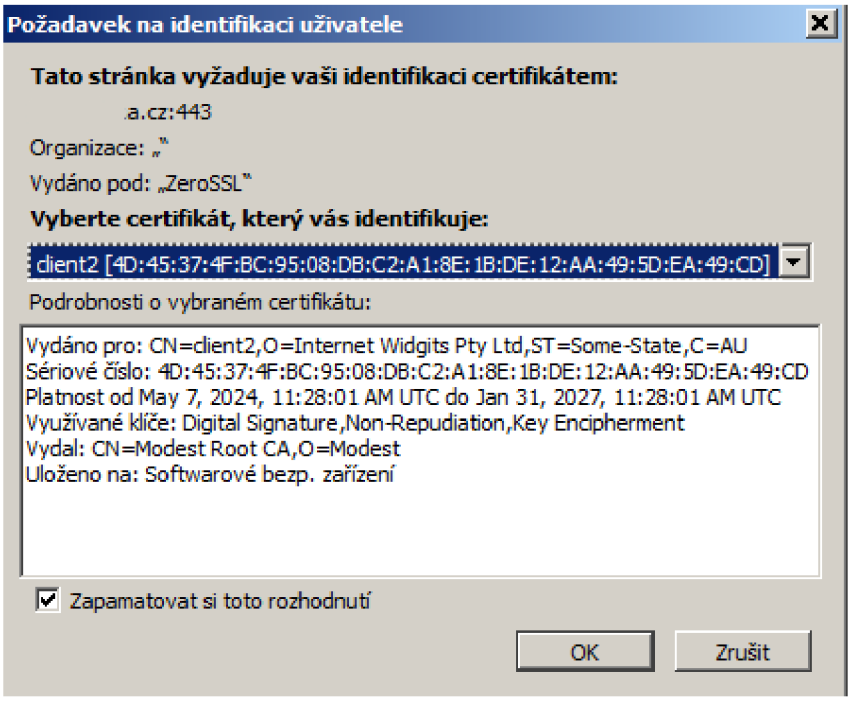
Jestliže je na straně serveru i klienta vše korektně nastaveno, tak se zákazníkovi zobrazí webové rozhraní dané služby

V případě, že klient při připojení na webovou službu nedisponuje klientským certifikátem, tak mu bude při pokusu o připojení vrácena následující odpověď.
SSL_ERROR_RX_CERTIFICATE_REQUIRED_ALERT

V případě, že bude klientský certifikát revokován, tak při pokusu o připojení na webovou službu se uživateli vrátí následující odpověď.
SSL_ERROR_REVOKED_CERT_ALERT

V případě, že společnost použije vlastní certifikační autoritu, tak je ještě navíc potřeba, aby si zákazník tuto certifikační autoritu naimportoval do svého systému nebo do patřičných klientských aplikací. Kromě toho, že se může jednat o obtížný krok pro některé zákazníky, nebo dokonce jiným může zakazovat vnitrofiremní politika importování cizích certifikačních autorit, tak může být pro mnou navrhovanou společnost jednodušší se dát cestou důvěryhodné certifikační autority prostřednictvím Cloudflare. V této své práci nicméně z důvodu možnosti výběru uvádím obě metody.

Z pohledu klienta v případě použití webového prohlížeče po pokusu o připojení na webovou službu zobrazí následující okno, kde je třeba interakce uživatele o zvolení patřičného klientského certifikátu.



Obr. 10: Volba klientského certifikátu pro mTLS připojení (Vlastní zpracování)

3.4.9.1 Výhody mTLS certifikátů

V případě použití klientských certifikátů je tak webové rozhraní plně izolováno od osob s neoprávněným přístupem. Jedná se tedy o jeden z vícero možných faktorů ochrany přístupu k webové služb, kdy jsou takto chráněna data zákazníků již na úrovni proxy serveru, a také je

chráněna webová aplikace. Bezpečnost z pohledu použití klientských certifikátu tedy stojí na bezpečnosti proxy serveru. Výsledkem, je tedy, že izolovaná webová služba tedy ani nezaujme neoprávněné uživatele ve smyslu provádění nevyžádaných operací, jako například skenování zranitelností systému.

3.4.9.2 Nevýhody mTLS certifikátů

Jako hlavní nevýhodou použití Mutual TLS certifikátů je nižší uživatelský komfort. Nelze se tedy připojit přímo na webovou službu podobně jako na řadě jiných webových stránek. To, že přístup na webovou službu je podmíněn klientským certifikátem může být pro některé osoby obtížnější ve smyslu klientské práce s certifikáty a importování do klientských aplikací nebo webového prohlížeče. Druhá nevýhoda může být také pro poskytovatele ve smyslu vyšší obtížnosti na správu těchto certifikátů. Předpokládám tak, že poskytovatel služeb je s tímto rizikem vyšší obtížnosti řádně obeznámen.

3.4.10 Revokace přístupu

V případě že zákazník pobyde práv k přístupu na cloudové úložiště, například z důvodu konce platnosti zákaznického přístupu, tak po vyzvání zákazníka ke stažení dat z cloudového úložiště budou tato data vymazána. Uživatelský účet (prázdný) bude ze systému odstraněn s tím, že bude revokován klientský certifikát. Tímto se zamezí možnosti přístupu zákazníka k webovému rozhraní cloudového úložiště. V případě, že by zákazník chtěl znovu obnovit datové služby, tak bude vystaven nový platný klientský certifikát, prostřednictvím kterého se již zákazník na webové rozhraní bude moci opět připojit.

Samotná revokace certifikátu bude prováděna následovně.

openssl ca -revoke client3.cert.pem -cert root_ca.crt -keyfile root_ca_key

Jako další krok je vygenerování nového listu neplatných certifikátů ve formě souboru CRL, což bude provedeno následovně.

openssl ca -cert root_ca.crt -keyfile root_ca_key -gencrl -out ca.crl

Tento aktualizovaný „ca.crl“ již lze vložit do systémové složky haproxy a znovu načíst, resp. restartovat službu HAProxy.

V tento okamžik již je zákazníkovi omezen přístup na webové rozhraní poskytovaných služeb.

3.4.11 Správa certifikátů

Z důvodu, že generování a revokování certifikátů potažmo importování patřičných údajů pro proxy server se děje na úrovni linuxového terminálu, tak toto generování a revokování by šlo automatizovat prostřednictvím pro to vhodných aplikací, jako například Ansible. Mnou navrhované řešení správy certifikátu tak nenabízí žádné grafické rozhraní pro administrátora, který by přehledně viděl stav jednotlivých certifikátů. Tento nedostatek přehledu stavu certifikátů by šel řešit samostatnou webovou aplikací s použitím databáze, kde by tak administrátor mohl přehledně vidět stav jednotlivých certifikátů nebo je pouhým kliknutím na příslušná tlačítka mohl generovat nebo revokovat.

Systém který bude spravovat certifikáty by měl být vhodně zabezpečen proti neoprávněnému zneužití.

3.4.12 Monitoring

Za účelem monitorování dostupnosti služeb a stavu systémů použiji software Zabbix. Jednotlivé sledované systémy budou logicky děleny dle kategorií.

- Síťové prvky fyzické
- Síťové prvky virtuální
- Monitoring hardware (servery, HDD S.M.A.R.T., aj.)
- Záložní zdroje elektrické energie UPS, motorgenerátory
- Proxmox a VPS (virtualizace)
- Nextcloud
- Vzduchotechnika
- Zabezpečovací systém (EZS + CCTV)
- Protipožární systém
- Stav virtuálních zařízení

Po napojení na vnitropodnikový SMTP server navrhuji tak aby byly zasílány notifikační zprávy zaměstnancům společnosti tak, aby byla využita metoda push notifikací a tedy odpovědný pracovník byl obratem seznámen se změnou stavu sledovaných prvků infrastruktury.

3.4.13 Antivirus

Za účelem ochrany aktiv společnosti navrhuji, aby společnost používala antivirus, který tak bude střežit infrastrukturu podniku proti nevyžádanému spuštění závadných skriptů, zdrojových kódů a aplikací. Jelikož zákaznická data budou šifrována, tak kontrola antivirem těchto dat nebude mít požadovaný účinek. Použití antiviru je zamýšleno primárně na částech systémů, která šifrována nebudou anebo taková, která budou v aktivním režimu odšifrována. Jedná se tedy primárně o ochranu infrastruktury proti ať úmyslnému nebo neúmyslnému zavedení škodlivého kódu ze strany zaměstnanců společnosti.

3.4.14 VOIP

Pro účely jak vnitropodnikové komunikace, tak i komunikace se zákazníky by bylo vhodné, aby si společnost zřídila telefonní systém, který by mohl být provozován na systému Asterisk nebo FreePBX. Nastavení tohoto VOIP serveru bych doporučil tak, aby ideálně používala lokální telefony s podporou protokolu SIP z důvodu jednodušší implementace. V případě, že by se podnik rozhodl použít linky analogové nebo ISDN tak bych doporučil, aby podnik využil vhodnou telefonní ústřednu, která by tak dělala převodník mezi touto telefonní technologií a Asteriskem. Jako jedna z možností hardwarové telefonní ústředny jsou tak zařízení od společnosti 2N. Za předpokladu, že by společnost používala telefonní zařízení fungujících na protokolu H.323, tak aby k Asterisku použila ještě vhodný Gatekeeper, například GNU Gatekeeper, prostřednictvím kterého by se tyto telefony tak plynule připojily k telefonnímu serveru Asterisk.

Z pohledu šifrování telefonních hovorů, tak tam kde to bude možné, tedy především pro vnitrofiremní komunikaci, tak by společnost mohla využít šifrování ZRTP, které je typu end-to-end. Toto šifrování může být užitečné například v případě, že jednotliví pracovníci společnosti by vzájemně komunikovali mimo vnitropodnikovou síť.

Pro připojení telefonní linky do internetu společnosti doporučují použít služeb některých poskytovatelů telefonního přípojení.

Firmě bych doporučil stanovit zákaznickou podporu v rozsahu pracovního dne společnosti typicky 8h – 16h pro pondělí až pátek. Pro tyto účely buďto společnost využije samostatného pracovníka, který ale tak zvýší mzdové náklady společnosti, nebo může tuto podporu zákazníků zkombinovat do jiné pracovní pozice.

3.5 Management kybernetické bezpečnosti

Z pohledu podniku bude třeba zajistit jak kontinuitu nabízených služeb, tak bezpečnost a integritu dat, která budou na serverech. Z toho důvodu je třeba zařídit přístup tak, aby pouze oprávněné osoby měly možnost fyzicky manipulovat se servery například z důvodu údržby.

V rovině ICT bude třeba zajistit obdobný princip s tím, že se zde může vyskytovat řada složitostí, které se týkají společnosti. Pro provoz infrastruktury podnik nejenom, že bude muset zaměstnat předem neurčený počet zaměstnanců pro provozování této činnosti, ale také bude muset vyhotovit takové bezpečnostní zásady, kde bude stanoveno, která osoba bude mít k jakému prvku přístup a za který ponese také odpovědnost v rozsahu pracovní pozice. Privilegia pracovníků, tak budou nastavena jako minimální nutná práva pro správu jim přidělených úseků. Dle těchto bezpečnostních zásad tak bude odpovídat, že pracovníci, kteří mají k jednotlivým aktivům odpovědnost, budou také vlastníky těchto aktiv ve smyslu kybernetické bezpečnosti. Jako návrh tak lze říci, že ICT prvky je možné rozdělit do základních kapitol, podle kterých následně podnik přidělí jednotlivým zaměstnancům jejich pracovní úsek. Jelikož společnost je v rozšíření oboru podnikání navrhovaná s minimem nových pracovníků, tak garantem aktiv by tak byl ředitel společnosti. Provoz fyzické infrastruktury včetně údržby, správa sítě jak fyzické, tak virtuální, správa virtualizace a cloudového úložiště a dohledový pracovník. V minimalistickém složení tak bude potřeba 4 pracovníků, kteří budou spravovat své úseky. V případě nedostatku finančních zdrojů by mohla společnost tyto úseky kombinovat do jedné pozice, s tím že naroste pracovní vytížení daných pracovníků. Další úseky jako instalace a údržba vzduchotechniky a případných elektrocentrál jako posledního prvku záložního zdroje by společnost prováděla out-sourcingem.

Z pohledu kybernetické bezpečnosti bych společnosti dále doporučil, aby jednotliví pracovníci měli různá hesla o vhodně zvolené délce a použití možných znaků, tak aby v případě úniku jednoho přístupového hesla nebyly ohroženy ostatní přístupové rozhraní na jiné podsystémy z pracovních úseků. Aby se zamezilo častému nešvaru psaní hesel na papírky na pracovišti, které jsou schované pod klávesnicí apod., tak bych doporučil, aby ve společnosti byla nějakým pracovníkem prováděna pravidelná kontrola těchto pracovišť zda takovouto nežádoucí situaci objeví. V případě, že by tak nastala výše zmíněná situace, tak by měl být tento konkrétní pracovník patřičně poučen o vnitrofiremních normách a předpisech ve smyslu, aby tato situace již znovu nenastala. Z tohoto důvodu může být užitečné, kdyby společnost používala nějaké bezpečně centrální úložiště hesel, kde by jednotliví pracovníci měli tato hesla uložena.

Nicméně já osobně na toto uvažované centrální úložiště hesel nahlížím s mírnou nedůvěrou a pocitem potenciálního úniku těchto hesel.

3.5.1 Audity kybernetické bezpečnosti

V případě, že by společnost chtěla, tak bych ji doporučil prostřednictvím třetích stran zajistit provádění nezávislého auditu, zda je vnitropodniková infrastruktura vhodně zabezpečena podle doporučení.

Součástí auditu by tak mohla být kontrola jaké osoby mají k jakému vybavení přístup, zda jsou nastaveny vhodně vnitrofiremní politiky z pohledu bezpečnosti dat, zda podnik disponuje vhodnými postupy jak má v daných situacích konat. Případně zda existují kontrolní mechanismy za předpokladu, kdy jeden z pracovníků udělá nějakou úmyslnou činnost v neprospěch společnosti. V případě že pracovník provede nějakou činnost v neprospěch společnosti, tak zda budou postupy na to aby se o tom ředitel společnosti nebo odpovědná osoba společnost vůbec dozvěděla. Z jednotlivých systému by tak měli být exportovány záznamy o jednotlivých zásazích a úkonech pracovníků, aby bylo možné v případě potřeby rekonstruovat co potažmo který pracovník udělal.

Součástí auditu by také mohlo být zda jsou vhodně umístěny kamerové systémy, jak je nakládáno s kamerovými záznamy a zároveň které osoby k těmto datům tak mohou mít přístup. Na úrovni elektronického zabezpečovacího systému by bylo možné kontrolovat, zda je systém zařízen tak, aby neumožnoval mazání historických dat například z důvodu zahlazení neoprávněných vstupů. Další kapitolou by se tak audity mohli zaměřovat zda-li jsou data zákazníků opravdu šifrovány a případně pokud, tak jak je s těmito daty manipulováno. Dalším prvkem by mohli být kontroly vnitrofiremních postupů, jak je společnost připravena provádět obnovy dat v případě ztráty nebo porušení dat, resp. datových polí.

3.5.2 Analýza rizik

Pro analýzu rizik volím metodu bodovací, kdy pro každé riziko bude vyjádřena hodnota rizika na stupnici 1-10. Pro výpočet analýzy rizik je tak třeba definovat hodnoty pravděpodobnosti rizika a hodnot dopadu.

Hodnoty bodovací metody:

Pravděpodobnost:

1–2	Minimální
3–4	Nízká
4–5	Průměrná
7–8	Pravděpodobná
9–10	Velice pravděpodobná

Dopad:

1–2	Minimální
3–4	Zanedbatelný
4–5	Významný
7–8	Velmi významný
9–10	Kritický

V následující tabulce je hodnota rizika vypočtena, jako součin pravděpodobnosti a dopadu.

Tabulka 1: Analýza rizik – hrozby (Vlastní zpracování)

Zn. rizika	Hrozba	Scénář	Pravděpodobnost	Dopad	Hodnota rizika
R1	Zaplavení fyzické infrastruktury	Povětrnostní vlivy, havárie vodovodního potrubí v objektu	1,5	10	15
R2	Nevhodně nastavená kaskáda záložních zdrojů	Hromadné starty serverů mohou způsobit rozkolísání napětí elektrické energie; v případě startu elektrocentrál až po vypnutí záložních zdrojů UPS, dojde k nežádoucímu vypnutí serverů a služeb.	4	5	20
R3	Útok na infrastrukturu zvenčí	Hackerský útok, DDoS,	6	5	30
R4	Útok na infrastrukturu zevnitř	Vloupání za účelem poškození infrastruktury, krádeže datových nosičů nebo fyzických serverů	2	10	20
R5	Nedostatečné financování projektu	Dlouhotrvající rozběh nového oboru podnikání a možná nespokojenost na straně pracovníků	4	7	28
R6	Neochota zaměstnanců	S rostoucím zatížením pracovníků může růst jejich neochota pracovat pro podnik.	3	5	15
R7	Odliv zaměstnanců	V případě extrémního přetížení pracovníků nebo podhodnocení finanční odměny, mohou pracovníci přecházet ke konkurenčním společnostem.	2	9	18
R8	Špatně zvolená cena nabízených služeb	Nedostatečný průzkum trhu, neprovádění kontinuálních kontrolních šetření konkurenčních nabídek	5	7	35

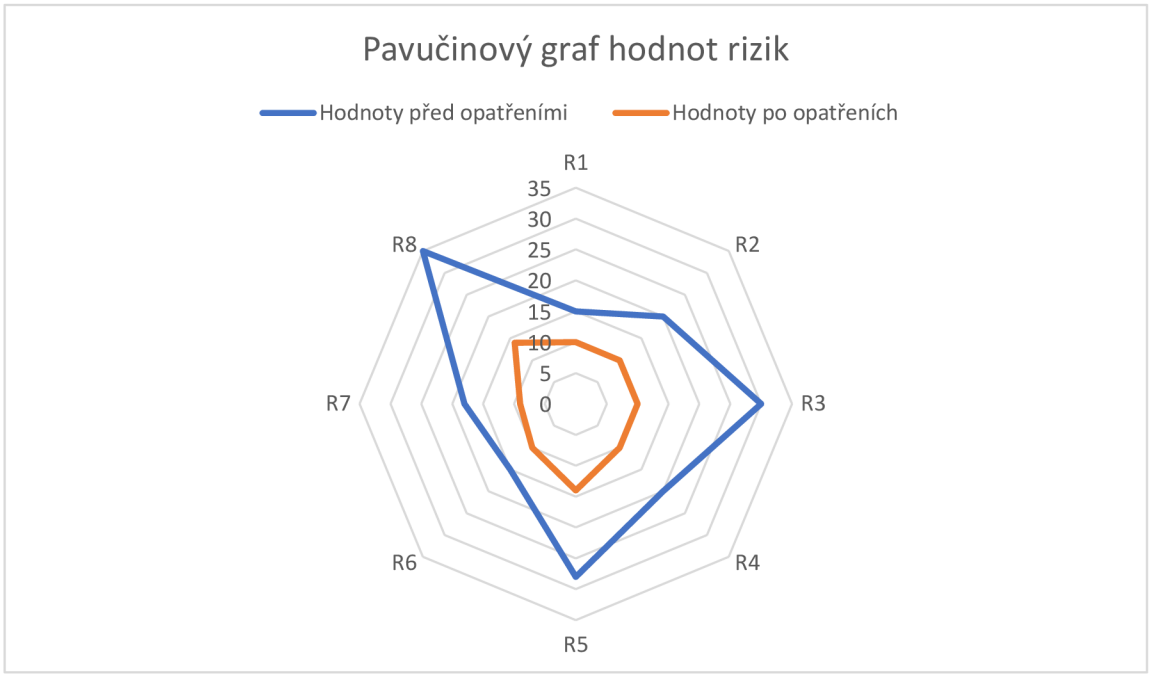
Tabulka 2: Analýza rizik - návrh opatření (Vlastní zpracování)

Zn. rizika	Opatření	Pravděpodobnost	Dopad	Hodnota rizika
R1	Osazení hladinových čidel a senzorů vlhkosti nebo umístění do samostatného objektu v jiné lokalitě	1	10	10
R2	Nastavení energetické kaskády tak, aby splňovala podmínky provozu nutné infrastruktury společnosti	2	5	10
R3	Pravidelná revize jednotlivých ochranných prvků, použití honeypotů a následné analýzy logů	2	5	10
R4	Pravidelné testy bezpečnostních prvků společnosti, uzamykání datových rozvaděčů	1	10	10
R5	V případě nedostatku finančních zdrojů zvážit úvěr nebo vstup strategického partnera do společnosti	2	7	14
R6	Provádění benefitních aktivit, ochota jednorázových zásluhových ohodnocení.	2	5	10
R7	Analýza konkurenčních pracovních nabídek pro udržení konkurenční mzdy a nastavení komunikačních metod pro zaměstnance k vedení a naopak	1	9	9
R8	Analýza konkurenčních cenových tarifů, slevové akce	2	7	14

Stav po opatřeních

Tabulka 3: Tabulka hodnot rizik (Vlastní zpracování)

Zn. rizika	Hodnoty před opatřeními	Hodnoty po opatřeních
R1	15	10
R2	20	10
R3	30	10
R4	20	10
R5	28	14
R6	15	10
R7	18	9
R8	35	14



Obr. 11: Analýza rizik pavučinový graf (Vlastní zpracování)

3.5.3 Vnitrofiremní dokumentace na úseku ICT

Pro podnik navrhuji pravidelné psaní podnikové dokumentace o systémech v podniku. Hlavním účelem je, aby při případné výměně pracovníků na jednotlivých úsecích nový pracovník měl informace ucelené na jednom místě o systému, se kterým bude pracovat. Dokumentace by měla obsahovat popis účelu systému, metodiky pro práci s jednotlivými nástroji s popisem, k čemu slouží. Dále by v dokumentaci mělo být obsaženo, jak se případně vyměňují data mezi jednotlivými podsystémy a kde je lze najít v případě potřeby. Do dokumentace také doporučuji zřizovat záznamy o významných změnách na systémech podniku a popis včetně inventarizace jednotlivých fyzických serverů například ve formě, jaké disky s jakými sériovými čísly se nachází ve kterém serveru v jakém slotu.

3.5.4 Testování zranitelnosti systémů

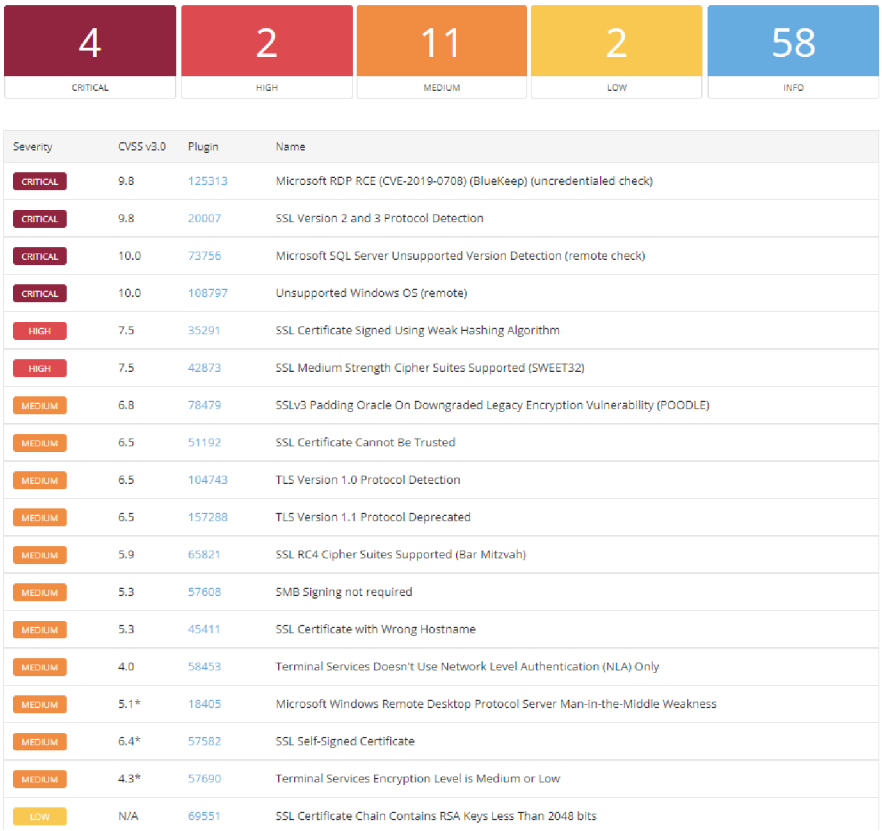
V pravidelných intervalech by měl podnik testovat podnikové systémy jak z vnitřního rozhraní, tak i z vnějšího. Tyto testy zranitelnosti by měly být založené jak na databázi CVE, tak i v případě, že to bude možné, tak také na vlastní kreativitě testera. Z důvodu objektivity výsledků testů, by tak tyto testy zranitelnosti měly provádět osoby, které nemají ve své gesci správu jednotlivých podsystémů. Může se tedy tak jednat o jiné pracovníky podniku, pokud budou mít vhodné zkušenosti pro testy zranitelnosti. Druhou možností pro podnik, tak by bylo si tyto testy nechat provádět nezávislým externím subjektem, čímž by objektivita těchto testů byla nejvýznamnější. Výstupy těchto testů budou zakládány do archivu podniku. Jednotlivé zranitelnosti budou pracovníci společnosti záplatovat tak, aby nebyly jednotlivé systémy zranitelné v těchto konkrétních oblastech. V případě, že v daný okamžik nebude existující záplata na daný systém, tak odpovědný pracovník o tomto zanese poznámku do vnitropodnikového notifikačního systému za účelem její pozdější nápravy. Předpokladem také je, že podnik bude provádět automatické aktualizace systémů, které budou prvně prováděny na testovacím systému tak, aby se zajistilo, že daná aktualizace nevyřadí z provozu služby, které budou poskytovány zákazníkům anebo zásadní vnitropodnikové zařízení významné pro provoz této obchodní činnosti. Společnost by taky měla být připravena na situaci, kdy se zákazníkem v dobré víře uzavře smlouvu o poskytování služeb ať cloudového úložiště, tak případně VPS, s tím že tento zákazník se bude pokoušet prolomit ochranné prvky jednotlivých systémů nebo platforem. Z tohoto důvodu bych společnosti dále doporučil aby testy zranitelnosti prováděla také z prostředí, které bude přístupné zákazníkům. V případě provozování virtuálních instancí

na virtualizačním serveru navrhuji, aby podnik nabízel zákazníkům výhradně virtualizované prostředí výhradně skrze aplikaci QEMU, která na rozdíl od LXC virtualizuje také systémové prostředky, jako například systémové jádro. Naproti tomu LXC kontejnery využívají sdíleného jádra s virtualizačním serverem.

Při provádění pravidelných testů zranitelnosti je tak možné zvýšit možné zabezpečení podnikových aktiv. Útokům tak ale zabránit neumí. Jedná se tedy o sadu nástrojů pro snížení rizika a zároveň o sadu postupů jak má podnik v dané situaci postupovat.

3.5.4.1 Nessus

Na následujícím obrázku je patrný výčet jednotlivých konkrétních zranitelností systému na základě kterých, by následně odpovědný pracovník měl provést implementaci záplat tak, aby systém již nebyl v těchto výstupních bodech zranitelný. Tyto reporty tak zastávají roli velmi užitečných podpůrných prvků pro eliminaci konkrétních útoků. Pro společnost by bylo vhodné, aby testy zranitelnosti programem Nessus prováděla jak z vnitřní části sítě – intranetu, ale také prostřednictvím veřejné IP adresy z internetu.



4	2	11	2	58
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	Plugin	Name
CRITICAL	9.8	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	73756	Microsoft SQL Server Unsupported Version Detection (remote check)
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	7.5	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.8	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.9	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	57608	SMB Signing not required
MEDIUM	5.3	45411	SSL Certificate with Wrong Hostname
MEDIUM	4.0	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	5.1*	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	6.4*	57582	SSL Self-Signed Certificate
MEDIUM	4.3*	57690	Terminal Services Encryption Level is Medium or Low
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Obr. 12: Nessus - Report zranitelností (Vlastní zpracování)

3.5.4.2 Lynis

Navrhuji společnosti, aby za účelem testování zranitelností Linuxových operačních systémů využívala nástroje Lynis. Jedním z důvodů je, že použití tohoto nástroje není zpoplatněno a druhým, že výstup z tohoto nástroje může být nápomocen odpovědnému pracovníkovi k uvedení zranitelného stavu do stavu bezpečnějšího. Jako příklad níže na obrázku uvádím část z výstupu, jak takový výstup z testu může vypadat.

```
[+] File systems
------------------------------------
  - Checking mount points
    - Checking /home mount point                                  [ SUGGESTION ]
    - Checking /tmp mount point                                   [ SUGGESTION ]
    - Checking /var mount point                                   [ SUGGESTION ]
  - Query swap partitions (fstab)                                 [ NONE ]
  - Testing swap partitions                                       [ OK ]
  - Testing /proc mount (hidepid)                                 [ SUGGESTION ]
  - Checking for old files in /tmp                                [ OK ]
  - Checking /tmp sticky bit                                      [ OK ]
  - Checking /var/tmp sticky bit                                  [ OK ]
  - ACL support root file system                                  [ ENABLED ]
  - Mount options of /boot                                        [ DEFAULT ]
  - Mount options of /dev                                         [ PARTIALLY HARDENED ]
  - Mount options of /dev/shm                                     [ PARTIALLY HARDENED ]
  - Mount options of /run                                         [ HARDENED ]
  - Total without nodev:44 noexec:44 nosuid:42 ro or noexec (W^X): 44 of total 62
  - Checking Locate database                                      [ FOUND ]
  - Disable kernel support of some filesystems

[+] USB Devices
------------------------------------
  - Checking usb-storage driver (modprobe config)                 [ NOT DISABLED ]
  - Checking USB devices authorization                            [ ENABLED ]
  - Checking USBGuard                                             [ NOT FOUND ]

[+] Storage
------------------------------------
  - Checking firewire ohci driver (modprobe config)               [ NOT DISABLED ]
```

Obr. 13: Lynis - report skenu zranitelnosti systému Linux (Vlastní zpracování)

3.5.4.3 SIEM

V případě, že by společnost chtěla pro účely monitorování síťového provozu v detailnějším rozsahu než umožňuje ZenArmor pod systémem OPNSense, tak bych doporučil použití ELK Stacku v kombinace s aplikací Wazuh jako jednu z možností. Výhodou tak je, že poté může podnik kromě analýzy síťového provozu také instalovat agenty do jednotlivých pracovních stanic, které by tak v reálném čase mohli monitorovat stav zabezpečení těchto klientský stanic a případné nedostatky tak přenášet na patřičnou serverovou část. Za pomocí těchto nástrojů tak může mít společnost centralizovaný přehled o všech zařízeních společnosti ne jednom místě. Další užitečnou vlastností tak je, že touto metodou může navrhovaný systém také sbírat jednotlivé záznamy ze všech sledovaných zařízení na kterých je nainstalován Wazuh agent. Tyto záznamy tak můžou být společnosti nápomocné v případě závady na daném zařízení, kdy

může nastat situace, že ze zařízení v závadě nebude možné v té době vyčíst záznamy ať z důvodu výpadku elektrické energie, nebo pouhého restartování zařízení. Z těchto záznamů tak společnost by mohla vyčíst o jakou závadu se jednalo a následně ji v ideálním případě napravit.

3.5.4.4 Shodan.io

Další nástroj který navrhuji použít je nástroj Shodan.io, který napomůže zjistit, které porty, resp. služby jsou na daných portech otevřené. Tato informace může být užitečná z pohledu následné analýzy těchto otevřených portů, zda se na nich nevyskytuje zranitelná služba. Jelikož se jedná o jeden z nástrojů, který také mohou využít útočníci pro plánování útoku na infrastrukturu společnosti, tak je dobré být seznámen s tímto výstupem také z pohledu podnikové informační bezpečnosti.

3.5.5 Event management

V případě, že nastane v podniku nežádoucí událost jako například bezpečnostní incident, tak podnik po zřízení nápravy případných škod by měl o tomto incidentu sepsat dokumentaci z důvodu zlepšení mechanizmů ochrany do budoucna a také jako případný vzdělávací materiál pro nové pracovníky.

3.5.6 Log management

Pro účely provozu navrhuji, aby podnik implementoval ukládání záznamů z jednotlivých zařízení a systémů případně podsystémů. Primárním účelem tak je, aby v případě výpadku služeb tak pracovníci podniku byli informováni, který prvek selhal a na základě toho mohli zjednat nápravu. V obecné rovině lze říci, že čím je více záznamů, tak tím je více možných informací, se kterými tak pracovníci mohou pracovat. Doporučuji tak společnosti v rámci log managementu sledovat stavy a jednotlivé požadované parametry fyzických prvků jako servery, routery, switche, elektrocentrály, záložní zdroje energie a dále virtuálních prvků jako jednotlivé operační systémy, software určený pro virtualizaci, cloudové úložiště a virtuální firewall. Veškeré tyto záznamy může společnost ukládat jak na samostatnou centralizovanou platformu nebo využít virtuálního zařízení rozprostřeného napříč clusterem, které bude sloužit výhradně pro tyto záznamy. Jako ideální považuji použít jako kombinaci samostatnou platformu s replikací záznamových dat do virtuálního zařízení z důvodu teoretického neplánovaného

výpadku jednotlivých prvků. Pro účely log managementu tak je možné využít nástrojů jako Zabbix, nebo ELK Stack v kombinaci s Wazuhem.

3.5.7 Management podnikové kontinuity – BCM

Podnik by si měl sestavit vhodné postupy pro řešení jednotlivých situací. Může se tak jednat například o postup obnovy dat nebo postup pro řešení probíhajícího bezpečnostního incidentu. V těchto postupech by měla být stanovena sestava činností pro zajištění chodu podnikové infrastruktury do původního stavu, resp. do klidového stavu. V těchto postupech by mělo být zřetelně a jasně stanoveno, kdo, kdy a jakým způsobem bude provádět jednotlivé činnosti pro návrat k žádanému stavu a definován proces reportingu nadřízeným osobám o změnách stavů jednotlivých dílčích částí podnikové infrastruktury.

3.5.8 Red a Blue Team testy

V případě, že by společnost disponovala dostatečnou kapacitou lidských zdrojů, tak by bylo vhodné pravidelně v předem definovaném času provádět vlastní bezpečnostní testy, kdy jistá část pracovníků by tak tvořila útočníky, kteří by se snažili prolomit zabezpečení infrastruktury, a druhá část pracovníků, která by jím v tomto aktivně bránila. Z důvodu efektivity těchto testů by bylo vhodné, aby volba těchto pracovníků pro tyto testy byla stanovena tak, aby útok neprováděly osoby, které znají konfigurace jednotlivých ochranných prvků podnikové infrastruktury. V případě, že by podnik nedisponoval vhodným počtem volných pracovních zdrojů pro tyto testy tak je možné, aby si společnost nechala od smluvního partnera provádět externí nezávislé pokusy o prolomení perimetru vnitropodnikové infrastruktury. Pro druhou uvažovanou variantu by tak zaměstnanci podniku tvořili Blue team a smluvní partner by tvořil Red team. V případě úspěšného prolomení ochranných prvků společnosti by měl být sepsán záznam o použitých metodách nástrojích a prvcích vnitropodnikové infrastruktury, které jsou tímto útokem ohroženy za účelem, aby pracovníci společnosti mohl nasadit vhodné protiopatření, které by tomuto útoku zamezilo.

3.5.9 Řízení přístupu ke kamerovým záznamům

Jelikož návrh řešení této práce uvažuje malý počet pracovníků společnosti, tak navrhuji, aby přístup ke kamerovým záznamům měl pouze výhradně ředitel společnosti bez zastoupení. Tato problematika je založena primárně na zabezpečení odcizení vizuálních dat neoprávněnou osobou, jimž v tomto směru jsou také ostatní pracovníci společnosti. Pro tyto účely by bylo

rozumné šifrovat úložiště pro bezpečnostní kamery, tak aby bezpečnostní klíč pro přístup k těmto datům znal jedině ředitel společnosti. V případě, že by ředitel onemocněl, zemřel anebo byl jinak indisponován, tak by společnost musela stávající sadu vizuálních dat smazat a vytvořit nové úložiště, v souladu s pokyny nového řídícího orgánu společnosti.

3.5.10 Elektronický zabezpečovací systém

Pro účely střežení aktiv podniku je vhodné, aby společnost použila EZS s vhodně rozmístěnými detektory. Formou doporučení bych si dovolil navrhnout, aby společnost stanovila střežení tak, aby pracovníci měli přístup pouze ke svým prvkům podnikové infrastruktury, které jsou potřebné pro jejich pracovní činnost, aby se snížila pravděpodobnost neoprávněného vstupu do prostor nebo neoprávněná manipulace s technickým vybavení společnosti. V případě, že bude mít společnost implementován EZS v kombinaci s kamerovým systémem, tak se v případě výstupů z těchto dvou systému může jednat o významný důkazní materiál v případě, že by společnost vyhodnotila neoprávněný zásah pracovníka k aktivům společnosti.

Podružnou funkcí, kterou může plnit EZS, je tak systém evidence docházky jednotlivých pracovníků, kteří prostřednictvím bezpečnostního kódu nebo přístupové karty si mohou tímto systémem potvrdit příchod na pracoviště, resp. odchod z pracoviště.

Funkce EZS je tak nedílnou součástí ochrany podnikového perimetru, kdy se jedná o aktivní ochranu, kdy v případě narušení prostoru tak mohou být obratem upozorněni odpovědní pracovníci nebo dohledový systém smluvních subjektů třetích stran.

3.6 Finanční zhodnocení

Vlastní návrh této diplomové práce obsahuje velké množství různého vybavení. Jedná se tak o systémy energetického charakteru, podpůrné systémy, ale také systémy přímo související s provozováním nabízených služeb. Jednotlivé podkapitoly finančního hodnocení jsou definovány jako plánované výdaje různých druhů. Výsledné částky se tak mohou lišit v závislosti na zvolených značkách, formách instalace jednotlivých zařízení a také volby konkrétních dodavatelů. Výpočet částky u harddisků je stanovena v rozmezí z důvodu možných různých kapacit, kdy si podnik zvolí vhodnou kapacitu harddisků. Částka u serverů je závislá na konkrétní zvolené konfiguraci u prodejce. Výsledná částka, která je pravidelná tak je vypočtena jako měsíční souhrnná částka.

3.6.1 Investiční výdaje

- Datový rozvaděč s příslušenstvím 25 tisíc Kč
- 7ks Servery HP Proliant – 7 x 90 tisíc Kč
- Harddisky typu HDD se sběrnicí SAS od 2 tisíc Kč do 10 tisíc Kč – 60 kusů
- Harddisky typu SSD a NVMe od 5tis. Kč 10 tisíc Kč – 48 kusů
- Síťové prvky – 75 tisíc Kč
- Záložní zdroj elektrické energie UPS – 60 tisíc Kč – 2 kusy
- Baterie do UPS – 20 tisíc Kč – 2 kusy
- Fotovoltaický systém včetně montáže – 439 tisíc Kč
- Kamerový systém (8ks kamer, PoE Switch, lokální úložiště) – 50 tisíc Kč
- EPS, EZS – 25 tisíc Kč
- Stabilní hasící zařízení – cena neznámá
- Klimatizace – 100 tisíc Kč – 3 kusy
- Záložní agregát – 30 tisíc Kč – 3 kusy
- Odhadované výdaje na instalaci – 75 tisíc Kč

Celkem od 2,2 milionů Kč do 3 milionů Kč

3.6.2 Provozní výdaje

Pohonné hmoty jsou závislé na konstantní dodávce elektrické energie. V případě, že by byla dodávána kontinuálně elektrická energie, tak ve výpočtu uvažuji pouze 5 motohodin měsíčně jako test provozuschopnosti. V nejhorší variantě je zahrnut konstantní provoz na záložní agregát po celý měsíc s tím, že je málo pravděpodobné, že by tato varianta nastala. Pro provoz záložního agregátu je také zapotřebí provádět pravidelnou údržbu včetně výměn provozních kapalin. Tyto náklady na údržbu ve výpočtu neuvažuji.

- Elektrická energie (10kVA) - 45 tisíc Kč
- Pohonné hmoty (5 motohodin měsíčně) – 500 Kč
- Pohonné hmoty (kontinuální provoz) - 67 tisíc Kč
- Mzdové výdaje (min. 4 pracovníci) – 280 tisíc Kč
- Přípojka internetového připojení – cena neznámá

Celkem od 326 tisíc Kč do 347 tisíc Kč

3.6.3 Servisní výdaje

Vzhledem k tomu, že nelze bezpečně říci, kdy dojde k selhání jednotlivých prvků infrastruktury, tak není možné jednoznačně definovat částky rozhodné pro výpočet servisu těchto prvků. V případě, že by daný prvek musel být nahrazen novým, tak se tento výdaj pohybuje přibližně ve výši pořizovací ceny prvku bez zohlednění inflace. V rámci údržby prvků jako energetický, hasící systém a systém vzduchotechniky, je částka závislá na dohodnutém smluvním partneru pro údržbu těchto prvků. Doba životnosti prvků, které přímo souvisejí s provozováním nabízených služeb jako servery a harddisky, které by se tak promítly do výpočtu servisních výdajů by mohla být stanovena jako doba záruky těchto prvků. Tím by se ale navýšily podnikové výdaje pro provoz infrastruktury. Z toho důvodu servisní výdaje neuvažuji do celkového výpočtu výdajů a životnost technického vybavení předpokládám nedefinovatelnou vzhledem k neznámé reálné životnosti.

3.6.4 Plánovaná ekonomická návratnost

Celkové plánované výdaje je v rozmezí od 2526 tisíc Kč do 3347 tisíc Kč. Za předpokladu, že by na vzorku všech zákazníků byla průměrná platba od jednoho zákazníka ve výši 300Kč měsíčně s požadovanou dobou návratnosti 2 let, tak by podnik potřeboval mít trvale alespoň 351 nebo 465 platících zákazníků v závislosti na konkrétní skladbě výdajů.

3.6.5 Platební systém

Poskytované služby zákazníkům by byly fakturovány za každý měsíc zpětně s možnosti platby bankovním převodem, nebo v hotovosti proti příjmovému pokladnímu dokladu.

3 ZÁVĚR

V této diplomové práci jsem se zaměřil na návrh nového předmětu podnikání společnosti. Po analýze současného stavu, kdy tak společnost má minimální množství technických prvků, jsem ve svém návrhu práce navrhnul řešení takové, které rozšíří obor podnikání ve smyslu poskytování virtuálních zařízení zákazníkům a také služby cloudového úložiště. Pro účely zvýšení bezpečnosti datové komunikace mezi serverem a klientem jsem zvolil vynucené použití klientských certifikátů, které tak tvoří jeden z více článků bezpečnosti infrastruktury jako celku. Závěrem svého návrhu jsem rozepsal svůj pohled na management kybernetické a informační bezpečnosti pro tuto společnost a odhadované plánované výdaje celého navrhovaného řešení.

4 SEZNAM POUŽITÝCH ZDROJŮ

1. ARIYANTO, Yuri. Single server-side and multiple virtual server-side architectures: Performance analysis on Proxmox VE for e-learning systems. Online. *ITEGAM-JETIA*. 2023, roč. 9, č. 44. Dostupné z: https://doi.org/10.5935/jetia.v9i44.903. [cit. 2024-05-12].

2. ZHUMA MERA, Emilio; BRITO CASANOVA, Orlando Jesús; TUBAY VERGARA, José a OVIEDO BAYAS, Byron. Análisis dinámico de malware en ambiente de red virtualizado. *Revista Conrado*. 2021/03/02, roč. 17, č. 78, s. 113-120.

3. *OnApp and WHMCS Help Service Providers Enter the Cloud Market with a Complete Turnkey Cloud Hosting and Client Management Platform.* New York: , Jan 21, 2014 ProQuest Central.

4. MO, Qiubo; DUAN, Shishi; HUANG, Wenhai; LAI, Yuhai a XU, Yong. Research and Design of a Personal Data Management System. In: . IEEE, 2022, s. 574-579. Dostupné z: https://doi.org/10.1109/ICISCAE55891.2022.9927545.

5. MALHOTRA, Antra; ELSAYED, Amr; TORRES, Randolph a VENKATRAMAN, Srinivas. Evaluate Solutions for Achieving High Availability or Near Zero Downtime for Cloud Native Enterprise Applications. *IEEE access*. 2023, roč. 11, s. 1-1. ISSN 2169-3536. Dostupné z: https://doi.org/10.1109/ACCESS.2023.3303430.

6. HRISTOZOV, Daniel. Properties and application of OpenZFS file system for secure data storage. *AIP conference proceedings*. 2024, roč. 3078, č. 1. ISSN 0094-243X. Dostupné z: https://doi.org/10.1063/5.0208253.

7. QIAO, Zhi; LIANG, Shuwen; CHEN, Hsing-Bung; FU, Song a SETTLEMYER, Bradley. Exploring Declustered Software RAID for Enhanced Reliability and Recovery Performance in HPC Storage Systems. In: . IEEE, 2019, s. 285-28509. ISSN 1060-9857. Dostupné z: https://doi.org/10.1109/SRDS47363.2019.00041.

8. JI, Hong. Research on Design and Security Strategy of DNS. Online. *Applied Mechanics and Materials*. 2013, roč. 378, s. 510-513. ISBN 3037857951. ISSN 1660-9336. Dostupné z: https://doi.org/10.4028/www.scientific.net/AMM.378.510. [cit. 2024-05-12].

9. W CURTIS PRESTON. For secure data backup, here's how to do the 3-2-1 rule right: The venerable 3-2-1 rule for backing up data remains a tried-and-true method for insuring the integrity of copied data that is essential to disaster recovery efforts, but it has to be done properly. Online. *Network World (Online)*. 2020. [cit. 2024-05-12].

10. PROXMOX SERVER SOLUTIONS GMBH. Online. Proxmox VE - Administration guide. 2024. Dostupné z: https://pve.proxmox.com/pve-docs/pve-admin-guide.html. [cit. 2024-05-12].

11. NGUYỄN, Ngọc; VÕ, Quang; TRẦN, Minh a TRẦN, Thu. Giới Thiệu Về Zabbix, Hệ Thống Giám Sát Thường Xuyên Tài Nguyên Của Máy Chủ. *Journal of Technical Education Science*. 2022/04/28, s. 1-7. Dostupné z: https://doi.org/10.54644/jte.69.2022.1148.

12. HAMA AMIN, Rebeen a AHMED, Dana. Comparative Analysis of Flexiwan, OPNSense, and pfSense Cybersecurity Mechanisms in MPLS / SD-WAN Architectures. *Passer Journal of Basic and Applied Sciences*. 2023/12/11, roč. 6, s. 27-32. Dostupné z: https://doi.org/10.24271/psr.2023.390989.1295.

13. NADEAU, Thomas D. a GRAY, Ken. *SDN: Software Defined Networks: Software Defined Networks*. Sebastopol, UNITED STATES: O'Reilly Media, Incorporated, 2013//. ISBN 9781449342456. Dostupné z: http://ebookcentral.proquest.com/lib/vutbrno/detail.action?docID=1343462.

14. FARHAN, Syed Muhammad a CHUNG, Taejoong. Exploring the Evolution of TLS Certificates. In: *Passive and Active Measurement*. Cham: Springer Nature Switzerland, s. 71-84. ISBN 3031284852. ISSN 0302-9743. Dostupné z: https://doi.org/10.1007/978-3-031-28486-1_4.

15. YANG, Wei; LI, Xiaohong; FENG, Zhiyong a HAO, Jianye. TLSsem: A TLS Security-Enhanced Mechanism against MITM Attacks in Public WiFis: A TLS Security-Enhanced Mechanism against MITM Attacks in Public WiFis. In: . IEEE, 2017, s. 30-39. Dostupné z: https://doi.org/10.1109/ICECCS.2017.24.

16. DECISO. *ZenArmor - Overview*. Online. OPNSense Documentation. 2024. Dostupné z: https://docs.opnsense.org/vendor/sunnyvalley/zenarmor.html. [cit. 2024-05-13].

17. BOUŠKA, Petr. VLAN - Virtual Local Area Network. Online. 2007. Dostupné z: https://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/. [cit. 2024-05-13].

18. BOUŠKA, Petr. Počítačové sítě a jejich typy. Online. 2007. Dostupné z: https://www.samuraj-cz.com/clanek/pocitacove-site-a-jejich-typy/. [cit. 2024-05-13].

19. *WAF vs IPS: What's The Difference*. Online. In: LANNER ELECTRONICS INC. Dostupné z: https://www.lanner-america.com/blog/waf-vs-ips-whats-difference/. [cit. 2023-11-04].

20. ABAYOMI185. *Proxmox WebGUI*. Online. In: . 15 Sep 2022n. l. Dostupné z: https://orionfeedback.org/assets/files/2022-09-15/1663257691-731395-screenshot-2022-09-15-at-170124.png. [cit. 2024-05-12].

21. *WHMCS - Webové rozhraní*. Online. In: WHMCS. Dostupné z: https://www.whmcs.com/assets/images/screenshots/whmcs-admin-home.png. [cit. 2024-05-12].

22. *Nextcloud - webové rozhraní*. Online. In: NEXTCLOUD GMBH. Dostupné z: https://nextcloud.com/media/multiple_share_links.png. [cit. 2024-05-12].

23. *Zabbix - webové rozhraní*. Online. In: . Dostupné z: https://www.zabbix.com/documentation/current/assets/en/manual/config/visualization/dashboard.png. [cit. 2024-05-12].

24. *ZenArmor - Live Session Explorer*. Online. In: DECISO. Dostupné z: https://www.zenarmor.com/docs/assets/images/viewing-live-session-explorer-91bab8a7783d33aa8cd4758036ee762b.webp. [cit. 2024-05-12].

25. *ZenArmor - Reports*. Online. In: DECISO. Dostupné z: https://www.zenarmor.com/docs/assets/images/zenarmor-reports-e2df2cf5eaab8f29806464cea083d3f8.png. [cit. 2024-05-12].

26. BOUŠKA, Petr. TCP/IP a ethernet - cesta v síti, aktivní síťové prvky. Online. 2007. Dostupné z: https://www.samuraj-cz.com/clanek/tcpip-a-ethernet-cesta-v-siti-aktivni-sitove-prvky/. [cit. 2024-05-13].

27. BOUŠKA, Petr. Cisco IOS 11 - IEEE 802.1x, autentizace k portu, MS IAS. Online. 2007. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-ios-11-ieee-802-1x-autentizace-k-portu-ms-ias/. [cit. 2024-05-13].

28. BULL, Ronny L. *A critical analysis of Layer 2 network security in virtualized environments*. United States -- New York, 2016. ISBN 978-1-369-34422-6. Dostupné také z: https://www.proquest.com/dissertations-theses/critical-analysis-layer-2-network-security/docview/1841228787/se-2.

29. RENAULT, Éric; BOUMERDASSI, Selma a BOUZEFRANE, Samia. Use of KRACK Attack to Obtain Sensitive Information. In: *Mobile, Secure, and Programmable Networking. 11005*. Switzerland: Springer International Publishing, 2019, s. 270-276. ISBN 9783030031008. ISSN 0302-9743. Dostupné z: https://doi.org/10.1007/978-3-030-03101-5_22.

30. KAKLAUSKAS, Liudvikas a PUGAČIUS, Dominykas. Secure remote client connection to higher education institution internal computer network through VPN. Online. *Taikomieji Moksliniai Tyrimai*. 2023, roč. 2, č. 1, s. 74-81. Dostupné z: https://doi.org/10.56131/tmt.2023.2.1.111. [cit. 2024-05-13].

31. BACEVIČIUS, Mantas. IDS/IPS technologijomis grįsto mobiliųjų įrenginių atakų prevencijos metodo sukūrimas ir tyrimas. Online. *Vilnius University open series (Online)*. 2022, s. 5-14. ISSN 2669-0535. Dostupné z: https://doi.org/10.15388/LMITT.2022.1. [cit. 2024-05-13].

32. PORCEDDA, Maria Grazia. Lessons from PRISM and Tempora: the self-contradictory nature of the fight against cyberspace crimes. Deep packet inspection as a case study. Online. *Neue Kriminalpolitik*. 2013, roč. 25, č. 4, s. 373-389. ISSN 0934-9200. Dostupné z: https://doi.org/10.5771/0934-9200-2013-4-373. [cit. 2024-05-13].

33. ΣΑΡΗΚΙΟΣΈΣ, Κωνσταντίνος. *Χρήση του Siem (Elk Wazuh Use Case)*. 2021. ISBN 9798845720900. Dostupné z: https://doi.org/10.26267/unipi_dione/969.

34. KUMAR, Anmol; SOMANI, Gaurav a AGARWAL, Mayank. Comparing HAProxy Scheduling Algorithms During the DDoS Attacks. Online. *IEEE networking letters*. 2024, s. 1-1. Dostupné z: https://doi.org/10.1109/LNET.2024.3383601. [cit. 2024-05-13].

35. DESHPANDE, Prachi; AGGARWAL, Aditi; SHARMA, S. C.; KUMAR, P. Sateesh a ABRAHAM, Ajith. Distributed port-scan attack in cloud environment. Online. In: *2013 Fifth International Conference on Computational Aspects of Social Networks*. IEEE, 2013, s. 27-31. Dostupné z: https://doi.org/10.1109/CASoN.2013.6622595. [cit. 2024-05-13].

36. THE MITRE CORPORATION. *Common Vulnerablities and Exposures*. Online. Dostupné z: https://www.cve.org/About/Overview. [cit. 2024-05-13].

37. RAE, Jacob S.; CHOWDHURY, MD Minhaz a JOCHEN, Mike. Internet of Things Device Hardening Using Shodan.io and ShoVAT: A Survey. Online. In: *2019 IEEE International Conference on Electro Information Technology (EIT)*. IEEE, 2019, s. 379-385. Dostupné z: https://doi.org/10.1109/EIT.2019.8834072. [cit. 2024-05-13].

38. DANIELYAN, Edgar. Introducing Nessus network security scanner. Online. *Inside Solaris*. 2001, roč. 7, č. 6, s. 3. ISSN 1081-3314. [cit. 2024-05-13].

39. SARDIÑAS GONZÁLEZ, Gerard. *Lynis web: una herramienta basada en la web para la generación de informes de auditoría de seguridad y la automatización de vulnerabilidades*. 2017.

40. FS.COM GMBH. *Comparison of UPS Topologies: Line-interactive vs Online vs Offline*. Online. 2021. Dostupné z: https://community.fs.com/article/line-interactive-vs-online-vs-offline-ups.html. [cit. 2024-05-13].

5 SEZNAM OBRÁZKŮ

Obr. 1: Proxmox - Webové rozhraní (20) 15
Obr. 2: WHMCS - Webové rozhraní (21) 15
Obr. 3: Nextcloud - Webové rozhraní (22) 16
Obr. 4: ZFS - Redistribuční schéma dat (7) 18
Obr. 5: Zabbix - Webové rozhraní (23) 20
Obr. 6: OPNSense ZenArmor - Live Session Explorer (24) 21
Obr. 7: OPNSense ZenArmor – Reports (25) 22
Obr. 8: Srovnání rozdílných principů WAF a IPS (19) 28
Obr. 9: Sken otevřených portů DNS serveru Google. (Vlastní zpracování) 30
Obr. 10: Volba klientského certifikátu pro mTLS připojení (Vlastní zpracování) 57
Obr. 11: Analýza rizik pavučinový graf (Vlastní zpracování) 66
Obr. 12: Nessus - Report zranitelností (Vlastní zpracování) 68
Obr. 13: Lynis - report skenu zranitelnosti systému Linux (Vlastní zpracování) 69

6 SEZNAM TABULEK

Tabulka 1: Analýza rizik – hrozby (Vlastní zpracování) 64
Tabulka 2: Analýza rizik - návrh opatření (Vlastní zpracování) 65
Tabulka 3: Tabulka hodnot rizik (Vlastní zpracování) 66

7 SEZNAM POUŽITÝCH ZKRATEK

IT	Informační technologie
ICT	Informační a komunikační technologie
RAID	Redundant Array of Inexpensive Disks
ARC	Adaptive Replacement Cache
L2ARC	Layer 2 Adaptive Replacement Cache
DWPD	Data Written Per Day
DNS	Domain Name System
SNMP	Simple Network Management Protocol
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VPN	Virtual Private Network
SDN	Software Defined Network
HTTPS	HyperText Transfer Procotol Secure
mTLS	Mutual Transport Layer Security
LAN	Local Area Network
VLAN	Virtual Local Area Network
WLAN	Wireless Local Area Network
DPI	Depp Packet Inspection
WAF	Web application filter
SIEM	Security Information and Event Management
DoS	Denial of Service
DDoS	Distributed Denial of Service
CVE	Common Vulnerabilities and Exposures
IP	Internet Protocol
GPL	General Public Licens

NFS	Network File System
SSH	Secure Shell
UPS	Uninterruptible power supply
AC	Alternating Current
DC	Direct Current
VPS	Virtual Private Server
SQL	Structured Query Language
PoS	Point of Sale
PIR	Passive Infrared
CCTV	Closed circuit television
ÚOOU	Úřad pro ochranu osobních údajů
EPS	Elektronický protipožární systém
EZS	Elektronický zabezpečovací systém
LFF	Large Form Factor
BTU	British Thermal Unit
SPOF	Single Point of Failure
DAS	Direct attached storage
VA	Volt-Ampér
ŽZ	Žlutozelený
DSL	Digital Subscribe Line
NGFW	Next Generation Firewall
SW	Software
HW	Hardware
FQDN	Fully Qualified Domain Name
SMTP	Simple Mail Transfer Protocol
PBS	Proxmox Backup Server
NVMe	Non Volatile Memory Express
SSO	Single Sign On
SAML	Security Assertion Markup Language

LDAP	Lightweigh Directory Access Protocol
SNI	Server Name Identification
CA	Certification Authority
VoIP	Voice over Internet Protocol
BCM	Business Continuity management
HDD	Hard Disk Drive
SSD	Sold State Drive