Česká zemědělská univerzita v Praze
Technická fakulta

Kybernetická bezpečnost malé podnikové IT infrastruktury

diplomová práce

Vedoucí práce: Ing. Jan Lešetický, Ph.D.
Autor práce: Ladislav – Matyáš Turek

PRAHA 2022

Česká zemědělská univerzita v Praze
Technická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Autor práce:	Ladislav – Matyáš Turek
Studijní program:	Zemědělské inženýrství
Obor:	Informační a řídicí technika v agropotravinářském komplexu
Vedoucí práce:	Ing. Jan Lešetický, Ph.D.
Garantující pracoviště:	Katedra technologických zařízení staveb
Jazyk práce:	Čeština
Název práce:	**Kybernetická bezpečnost malé podnikové IT infrastruktury**
Název anglicky:	**Cybersecurity of a small enterprise IT infrastructure**
Cíle práce:	Cílem práce bude navrhnout zabezpečení sítě pro malé společnosti s omezeným rozpočtem. Návrh bude obsahovat implementaci detekčního systému, který bude posléze podroben testování pomocí nejčastějších kybernetických útoků (např. ramsomware). Řešitel ve své práci navrhne technické a organizační zásady IT zabezpečení vybrané organizace s tím, že navržené řešení (metodiku) ověří jak v běžném provozu, tak dle platných norem (viz. doporučená literatura) a legislativy.
Metodika:	1. Úvod 2. Cíl práce 3. Metodika 4. Kybernetická bezpečnost 5. Bezpečnost na síťové a aplikační vrstvě OSI modelu 6. Legislativní a normativní zásady bezpečného provozu IT systémů 7. Detekční systémy 8. Návrh zabezpečení a implementace detekčního systému 9. Testování navrženého řešení 10. Diskuse výsledků a jejich hodnocení 11. Návrhy pro další zabezpečení 12. Zhodnocení a cenová kalkulace
Doporučený rozsah práce:	50-60 stránek včetně obrázků a grafů
Klíčová slova:	IDS,IPS, Tier model, monitoring, bezpečnost

Doporučené zdroje informací:
1. Bayuk, Jennifer L.; Healey, Jason; Rohmeyer, Paul; Sachs, Marcus H.; Schmidt, Jeffrey a Weiss, Joseph. 2012. Cyber security policy guidebook. Hoboken, N.J.: John Wiley. ISBN 978-1-118-02780-6.
2. ČSN ISO/IEC 27001, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2014.
3. ČSN ISO/IEC 27002, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Soubor postupů. Praha: Český normalizační institut, 2014.
4. Jirásek, Petr; Novák, Luděk a Požár, Josef. 2015. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze. ISBN 978-80-7251-436-6
5. SELECKÝ, Matúš. Penetrační testy a exploitace. 1. vyd. Brno: Computer Press, 2012. 303 s. ISBN 978-80-251- 3752-9.
6. TAYLOR, Andy. Information security management principles. Second edition. Swindon, UK: BCS, the Chartered Institute for IT, [2013]. ISBN 978-1780171753.
7. WHITMAN, Michael E. a Herbert J. MATTFORD. Management of information security. Sixth edition. Boston, Massachusetts: Cengage Learning, [2019]. ISBN 978-1337405713.
8. WITTKOP, JEREMY. Building a Comprehensive IT Security Program: Practical Guidelines and Best Practices. Boulder, Colorado: Apress, [2016]. ISBN 14-842-2052-8.

Předběžný termín obhajoby: 2021/22 LS - TF

Elektronicky schváleno: 3. 2. 2021
doc. Ing. Jan Malaťák, Ph.D.
Vedoucí katedry

Elektronicky schváleno: 10. 2. 2021
doc. Ing. Jiří Mašek, Ph.D.
Děkan

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci na téma: Kybernetická bezpečnost malé podnikové IT infrastruktury vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů. Jsem si vědom, že odevzdáním diplomové práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby. Jsem si vědom, že moje bakalářská práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí. Jsem si vědom, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.

V Praze dne: …….. ……..

Ladislav – Matyáš Turek

Poděkování

Děkuji Ing. Janu Lešetickému, Ph.D., vedoucímu diplomové práce, za odborné vedení a cenné rady, čímž přispěl k vypracování této diplomové práce.

Kybernetická bezpečnost malé podnikové IT infrastruktury

Abstrakt: Diplomová práce na téma „Kybernetická bezpečnost malé podnikové IT infrastruktury“ se zabývá zvýšením kybernetické bezpečnosti vybrané společnosti. Teoretická část je věnována souhrnu poznatků z tuzemské a zahraniční vědecké literatury zaměřujících se na téma kybernetické bezpečnosti a etického hackingu. V této části práce jsou popsány útoky využívající síťové a aplikační protokoly a dále možné techniky obrany nebo detekce. Praktická část se zaměřuje na návrh bezpečnostních opatření vycházejících z analýzy rizik. Analýza rizik je vytvořena na základě provedených testů, které spočívají v testování uživatelů a lokální infrastruktury. Tyto testy spočívají v reálných kybernetických útocích na danou společnost. Z výsledků jednotlivých testů je dále vyvozena míra kritičnosti dopadů jednotlivých kybernetických útoků. Významnou částí práce je sestavení nápravných opatření a jejich realizace k odstranění zjištěných nedostatků. Vlivem čehož je docíleno snížení kritičnosti interního prostředí. Cílem diplomové práce je zabezpečit počítačovou síť z pohledu kybernetické bezpečnosti s co nejmenším finančním dopadem.

Klíčová slova: Tier model, OSI, síťové útoky, aplikační útoky

Cybersecurity of a small enterprise IT infrastructure

Summary: The master thesis on "Cyber security of a small enterprise IT infrastructure" deals with increasing the cyber security of a selected company. The theoretical part is devoted to a summary of findings from domestic and foreign scientific literature focusing on the topic of cyber security and ethical hacking. This part of the thesis describes attacks using network and application protocols as well as possible defense or detection techniques. The practical part focuses on the design of security measures based on risk analysis. The risk analysis is based on the tests performed, which consist of testing users and local infrastructure. These tests consist of real cyber attacks on the company. The level of criticality of the impact of each cyber attack is further derived from the results of individual tests. An important part of the work is the compilation of corrective measures and their implementation to eliminate the identified deficiencies. As a result of which the criticality of the internal environment is reduced. The aim of the thesis is to secure the computer network from a cyber security perspective with the least financial impact.

Key words: Tier model , OSI, Network attack, applications attack

Obsah

Seznam obrázků:

Seznam tabulek:

Seznam použitých zkratek:

ACL – Access-control list

ARP – Address Resolution Protocol

CIS – Commonwealth of Independent States

DAI – Dynamic ARP Inspection

DHCP – Dynamic Host Configuration Protocol

DLL – Dynamic-link library

DNS – Domain Name System

EAP – Extensible Authentication Protocol

GDPR – General Data Protection Regulationmessage-digest algorithm

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secure

ICMP – Internet Control Message Protocol

ICMP – Internet Control Message Protocol

IDS – Intrusion Detection Systems

IP – Internet Protocol

IPS – Intrusion Prevention Systems

L1-7 – Layer 1-7

LM – Lan Manager

MAC – Media Access Control

MD5 – Message-digest algorithm

NTLM – New Technology Lan Manager

NTP – Network Time Protocol

NUKIB – Národní úřad pro kybernetickou a informační bezpečnost

OSI – Open Systems Interconnection

PEAP – Protected Extensible Authentication Protocol

RST – Reset Národní úřad pro kybernetickou a informační bezpečnost

SAM – Security Account Manager

SIEM – Security Information and Event Management

SNMP – Simple Network Management Protocol

SSH – Secure Shell Protocol

SYN – Synchronization

TCP – Transmission Control Protocol

TLS – Transport Layer Security

TPM – Trusted Platform Module

UDP – User Datagram Protocol

VLAN – Virtual Local Area Network

1. Úvod

Tématem diplomové práce je Kybernetická bezpečnost malé podnikové IT infrastruktury. Zejména vlivem onemocnění Covid-19 se více přechází do online formy a z toho důvodu jsou kladeny neustále větší nároky na kybernetickou bezpečnost. Bezpečnost se nezaměřuje pouze na ochranu výpočetní techniky, ale také samotných lidí. V dnešní době jsou technologie všude kolem nás a mají tedy přímý dopad na naše životy. Nejedná se pouze o telefony, ale celé systémy, které jsou digitálně ovládány v důležitých infrastrukturách. Příkladem jsou nemocnice, kde správná funkčnost systému může mít dopad na lidské životy.

Kybernetická bezpečnost již je a i do budoucna bude zcela zásadním tématem. Jedná se o finančně velmi náročnou oblast informačních technologií, přesto velké množství společností nesplňuje základy bezpečnostních praktik, které umožňují jejich produkty. Jednou z mnoha příčin je, že se stále toto odvětví přehlíží a firmy mu nevěnují dostatek času a financí. Z dnešního pohledu každá veřejně dostupná informace může být zneužita vůči fyzické osobě nebo společnosti. I přes tento fakt se stále neklade velký důraz na integritu dat, kde vše začíná. Na počátku většiny cílených útoků jsou řadoví zaměstnanci dané společnosti. Dochází ke sledování jejich návyků a uveřejněných interních informací. Následně veškerá tato data slouží útočníkům k obelhání uživatele a získaní požadovaných údajů.

Diplomová práce se zabývá základní úrovní kybernetické bezpečnosti, která nemusí pro společnosti představovat finanční zátěž. V teoretické části jsou popsány možné typy útoků z pohledu vnitřního a vnějšího prostředí. Dále možnosti vylepšení zabezpečení, detekce a zvýšení úrovně obdržených informací pro správce. Jednotlivé části jsou komplexně rozebrány, aby sloužily pro pochopení využitých principů.

Praktická část práce se zaměřuje na analýzu bezpečnostních rizik z pohledu kybernetické bezpečnosti, která vychází z infrastruktury dané společnosti. Analýza identifikuje míru kritičnosti, která představuje součin hodnot dopadu, hrozby a zranitelnosti lokální sítě. Tyto hodnoty jsou získávány provedením útoku z vnitřního a vnějšího prostředí na uživatele a výpočetní techniku. Cílem bezpečností analýzy rizik je zjištění kritických částí infrastruktury a poté navržení konkrétních nápravných opatření, které povedou k jejich eliminaci. V závěru práce jsou navržená opatření aplikována.

2. Cíl práce

Cílem práce je zabezpečit počítačovou síť z pohledu kybernetické bezpečnosti s co nejmenším finančním dopadem. Dílčím cílem práce je identifikovat a ohodnotit rizika spojená s možným dopadem kybernetických útoků na společnost. V rámci práce je tedy provedena analýza rizik, která slouží ke zjištění úrovně nedostatků bezpečnosti sítě. Analýza vychází z nejfrekventovanějších reálných kybernetických útoků z vnějšího a následně vnitřního prostředí. Předmětem tohoto rozboru je posouzení zavedených standardů a celé bezpečnostní architektury jako celku. Bezpečnostní analýza rizik vychází z pravidel hodnocení rizik NIST. Výstupem diplomové práce jsou nápravná opatření, která slouží k odstranění zjištěných nedostatků a jejich aplikace ve společnosti. Navržená nápravná opatření je možno využít pro zvýšení bezpečnosti sítí v libovolné IT infrastruktuře. Výsledné řešení zahrnuje bezpečnostní potřeby technologické i aplikační infrastruktury.

3. Metodika

Diplomová práce je zaměřena na kybernetickou bezpečnost a vychází z analýzy rizik. Pro její zhotovení je vytvořena osnova, která se skládá ze tří částí, a to sběr informací, testování a vyhodnocení. Sběr informací je založený na získání zranitelností v interním prostředí. Pro tento úkon je využit nástroj OpenVas. V části testování jsou definovány tři rozdílné scénáře, které společnost testují z interního a externího prostředí. Jedná se o testy, jež jsou nejčastěji využívané útočníky. Jedná se o útok hrubou silou, který reprezentuje testování v rámci interního prostředí a zjišťování zranitelností. Z pohledu externího se jedná o vektor útoku nepochází ze subjektu, který je v interní infrastruktuře. Tento útok je založený na podvržené e-mailové komunikaci skrze nástroj Gophish. Část vyhodnocení vychází ze získaných dat, která jsou aplikována do vzorce pro výpočet rizika společnosti. Výsledná hodnota stanovuje rámcové zařazení kritičnosti prostředí jako celku. Tato hodnota určuje prioritu, s jakou se má přistupovat k řešení nápravných opatření, které vznikají jako výstup analýzy rizik. Nápravná bezpečnostní opatření shrnují celé prostředí jako celek a zároveň vyhodnocují samotné testy. Pro zajištění snížení hodnoty získané ze vzorce pro výpočet rizika společnosti je navrženo zabezpečení, jenž vychází z dokumentací od výrobců aplikací nebo zařízení. Pomocí čehož se zvyšuje zabezpečení jednotlivých bodů s důrazem na minimální cenu.

4. Teoretická část

Teoretická část je rozdělena na 5 dílčích oblastí. V úvodu jsou popsány statistiky dopadu kybernetických hrozeb, kde jsou vypsány typy šíření, procentní zastoupení jednotlivých útoků, jenž vychází například z ročních zpráv NÚKIB. Další části jsou věnovány útokům, které jsou rozděleny do dvou kapitol, a to síťové a aplikační útoky. Jednotlivé útoky jsou využitelné k proniknutí do sítě, zamezení nebo omezení dostupnosti daného zařízení nebo služby a čerpání informací skrze získaná data. Tyto možné bezpečnostní incidenty jsou v teoretické rovině detailně vylíčeny, aby bylo patrné, jaká slabá místa v protokolech využívají. V následující části jsou popsány body, které přímo nebo nepřímo zvyšují kybernetickou bezpečnost v rámci lokálního prostředí. Jedná se o dostupné nástroje s přímým dopadem, nebo nástroje s vedlejším dopadem. Nástroje s přímým dopadem detekují a upozorňují na podezřelou aktivitu, zatímco nástroje s nepřímým dopadem na bezpečnost mají přímý vliv na řešení případného bezpečnostního incidentu. V poslední kapitole teoretické části je rozepsaná metodika od společnosti NIST, kdy její poznatky jsou využity pro tvoření analýzy rizik.

4.1 Kybernetická Bezpečnost

Kybernetická bezpečnost je odvětví informačních technologií, které se vztahuje do všech segmentů tohoto oboru. Cílem informační bezpečnosti je ochrana informací a majetku, přičemž informace a majetek musí zůstat bez omezení přístupné jeho předpokládaným uživatelům. Termínem Bezpečnost informačních systémů se rozumí kolektivní postupy a mechanismy, jejichž citlivé a cenné informace jsou chráněny před zveřejněním, poškozením, neoprávněnou činností nedůvěryhodných osob. Výhradním cílem této oblasti je zabránit zneužití samotných počítačů nebo sítě. (1)

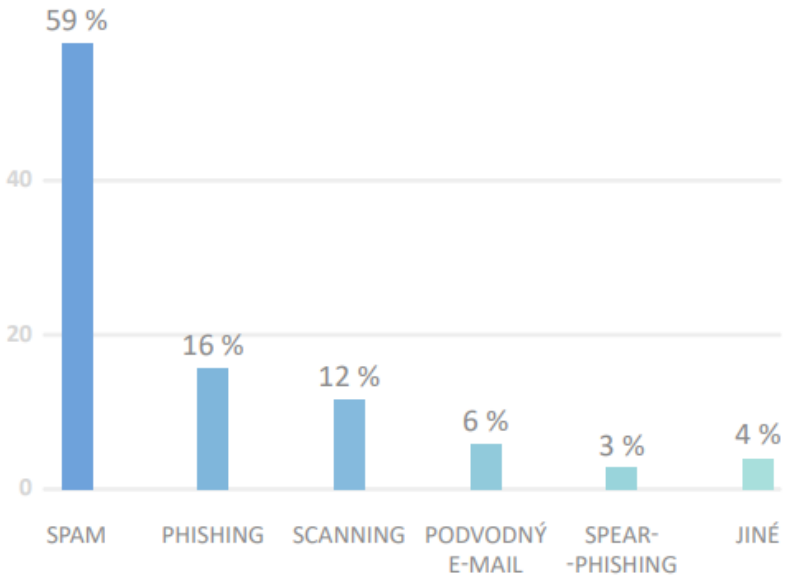
Dle studií společnosti Accenture z roku 2021 je 43 % útoků zaměřeno na malé podniky, ale pouze 14 % z nich je připraveno se bránit. Ze zprávy kybernetické bezpečnosti Ponemon Institute vychází, že 45 % malých a středních společností uvádí, že jejich procesy jsou při kybernetickém útoku neúčinné. Samotná frekvence útoků se zvýšila za posledních 12 měsíců o 66 %.

V rámci celosvětových statistik za poslední rok 2021:

- kybernetický útok je z 95 % způsoben lidskou chybou;
- na celém světě 88 % organizací zažilo pokus o spearphishing;
- z útoků bylo finančně motivováno 86 % a 10 % špionážní povahy;
- nejčastějšími škodlivými typy příloh e-mailů jsou .doc a .dot, které tvoří 37 %, další nejvyšší je .exe s 19,5 %;
- úniky dat odhalily v první polovině roku 2020 36 miliard záznamů. (2)

Dle zprávy kybernetické bezpečnosti, kterou vytvořil Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) za rok 2020 se řešilo nejvíce incidentů za poslední 4 roky, kdy druhým nejčastějším sektorem bylo zdravotnictví, kde se počet meziročních útoků zvýšil o 267 %. Dle dostupných dat pochází nejčastější kybernetické útoky přes e-mailovou komunikaci viz obrázek 1. (3)

Obrázek 1 - Nejčastější typy kybernetických útoků v roce 2020



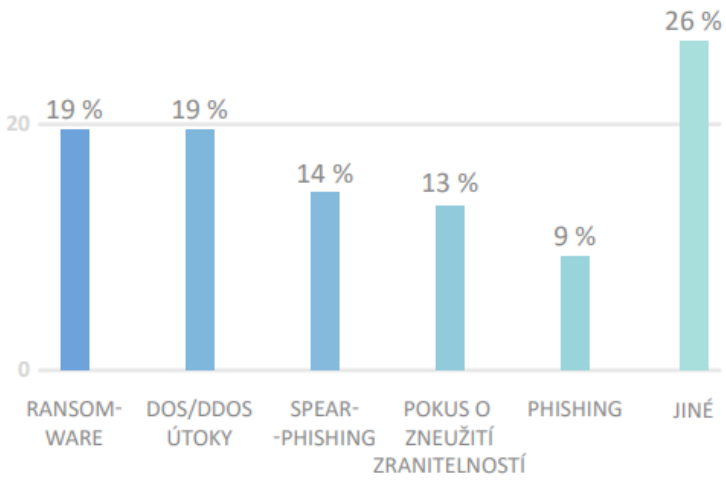
Zdroj:
https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf

Při pohledu na oblast nejzávažnějších typů kybernetických útoků, je nejčastěji zastoupený Ransomware a DoS/DDoS viz obrázek 2, které mají stejný podíl na všech typech útoků se zastoupením 19 %. Ransomware je typ malwaru navržený k šifrování souborů na zařízení, ke kterému má přístup. Soubory představují jakýkoliv soubor v rámci operačního systému. Útočníci následně vyžadují výkupné za dešifrovací klíče. (4)

DoS/DDoS je útok, který se snaží narušit normální provoz cíleného serveru, služby nebo sítě za pomoci zahlcení. Tento typ útoku využívá více kompromitovaných systémů, kdy se může jednat nejen o počítače, ale také IoT zařízení. Enormní provoz následně brání požadované komunikaci. (5)

Phishing je typ útoku, který spadá do technik sociálního inženýrství, kdy se útočník vydává za důvěryhodnou autoritu. Cílem tohoto útoku je získat citlivé informace o dané společnosti. Primárním bodem je tedy získat přihlašovací údaje, které mohou být využity pro zneužití a získání přístupu do interní sítě. (6)

Obrázek 2 - nejzávažnějších typů kybernetických útoků v roce 2020



Zdroj: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf

Firmy nemají vlastní odborné kapacity, a tak více než 28 % z nich se snaží hledat pomoc u třetích stran. Díky nárůstu všech útoků se udává, že minimálně 54 % zaměstnanců se alespoň jednou do roka odborně školí v oblasti kybernetické bezpečnosti. (3)

4.2 Síťové útoky

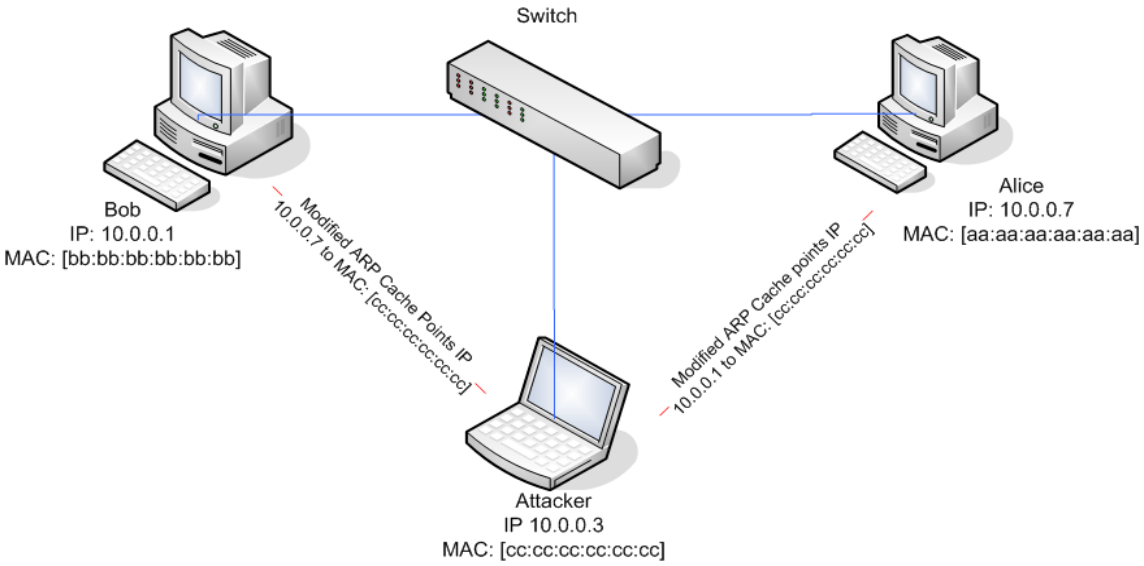
Síťové útoky mají za primární cíl získání neoprávněného přístupu do sítě dané organizace s cílem ukrást data, nebo provést jinou škodlivou činnost. Základní dělení útoků na 3 vrstvy síťového ISO/OSI modelu jsou aktivní a pasivní. Aktivní útoky nejen získávají neoprávněný přístup, ale také proaktivně upravují data. Zatímco pasivní útoky pouze poslouchají a z dostupných informací sbírají požadovaná data. (7)

4.2.1 ARP útoky

Protokol ARP se využívá pro překlad mezi linkovou a síťovou vrstvou v rámci ISO/OSI modelu, tedy překlad z IP adres na MAC adresu. Protokol si vytváří vlastní lokální tabulku N:1 vlivem čehož snižuje zatížení lokální sítě. Jedním ze základních síťových útoků, je tento protokol zneužít. Útok tohoto typu se nazývá ARP Spoofing, neboli ARP Poisoning. Tento útok umožňuje útočníkovi zneužít slabin v rámci protokolu. Vzhledem k jeho stáří, při jeho tvorbě nebyl kladen tak velký důraz na bezpečnost. Jakékoliv zařízení v síti může odpovídat na požadavky ARP, nebo je bude vysílat bez předchozího dotazu. Čehož se snaží využít útočník, který se vydává v rámci lokální sítě za jiný počítač. (8)

ARP Spoofing je využit v počítačových sítích s protokolem IP verze 4, kdy při komunikaci v rámci počítačové sítě je příjemce paketů adresován pomocí IP adres. Na každém směrovači v rámci cesty musí být paket zabalen do rámce, který obsahuje záznam o MAC adrese. Tyto informace se doplňují pomocí ARP tabulky. Princip ARP spoofingu spočívá v podvržení MAC adresy, skrze neustálé zasílání odpovědí s podvrženou MAC adresou. Směrovač si zaznamenanou falešnou linkovou adresu poznamená do ARP tabulky a následné pakety zasílá na ni. Na obrázku 3 jsou vyobrazena 3 koncová zařízení a jeden switch. Útočník s MAC adresou CC:CC:CC:CC:CC:CC posílá ARP odpovědi na směrovací prvek, ve kterých jsou obsaženy 2 základní informace, jako požadovaná IP adresa cíle a MAC adresa útočníka. Těmito odpověďmi má switch v rámci své interní ARP tabulky zaznamenáno, že informace z PC A, které by při normální komunikaci přicházeli na PC B budou odeslány na PC útočníka. (9)

Obrázek 3 - ARP Spoofing



Zdroj: https://github.com/SRJanel/arp_poisoning

4.2.2 DHCP útoky

DHCP (Dynamic Host Configutation Protocol) je využit pro automatickou konfiguraci počítačového připojení do sítě. DHCP dynamicky přiděluje počítačům IP adresu, masku sítě, výchozí bránu, DNS server, NTP server. Při zapojení počítače do sítě, dochází DORA, tato výměna informací je znázorněna na obrázku 4. DHCP klient vyšle do sítě broadcast požadavek (jelikož nemá IP), neboli DHCP Discover na port 67. V případě, že DHCP server tuto zprávu zachytí. Pošle klientovi zpět nabídku IP adresy, pod kterou se může připojit a její dobu propůjčení skrze DHCP Offer na port 68. Klient si vybere IP adresu a pošle DHCP Request, v tento moment stále není vyplněna klientská IP adresa. Tento požadavek server potvrdí DHCP Acknowledge a zároveň přidá doplňující informace, které se předávají v rámci tohoto protokolu. (10)

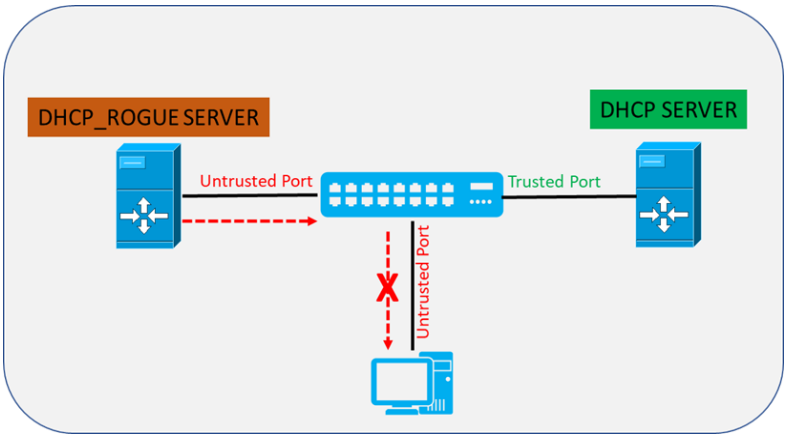
Obrázek 4 - DHCP DORA

Zdroj: https://medium.com/liveonnetwork/tagged/dhcp-dora

Útokem na DHCP server se snaží útočník dosáhnout, aby zařízením v síti nemohl primární ověřený DHCP server odpovídat, jelikož bude zahlcený. V tento moment útočník začne odpovídat na DHCP dotazy svým vlastním DHCP serverem. V případě, že je tohoto cíle dosaženo, tak útočník může měnit informace, které protokol předává klientům, jako například neautorizovaný DNS server, na který mohou klienti komunikovat.

V principu se útočník ze svého zařízení snaží zaslat velké množství DHCP Request na DHCP server a v každém jednotlivém požadavku je falešná MAC adresa. Pakliže začne DHCP server na všechny tyto dotazy reagovat, tak během chvíle budou vyčerpané dostupné IP adresy v daném rozsahu DHCP serveru. Jakmile je vyčerpaný dostupný počet adres na serveru, tak nedokáže pravým klientům odpovídat a přiřazovat IP adresy. V tento moment útočník může začít reagovat a odpovídat ze svého podvrženého DHCP serveru na dotazy klientů v síti viz obrázek 5. Jakmile podvržený server bude potvrzovat IP adresy klientům, tak v tento moment může měnit výchozí bránu do internetu, nebo svůj vlastní DNS, NTP server.

Obrázek 5 - DHCP Snooping

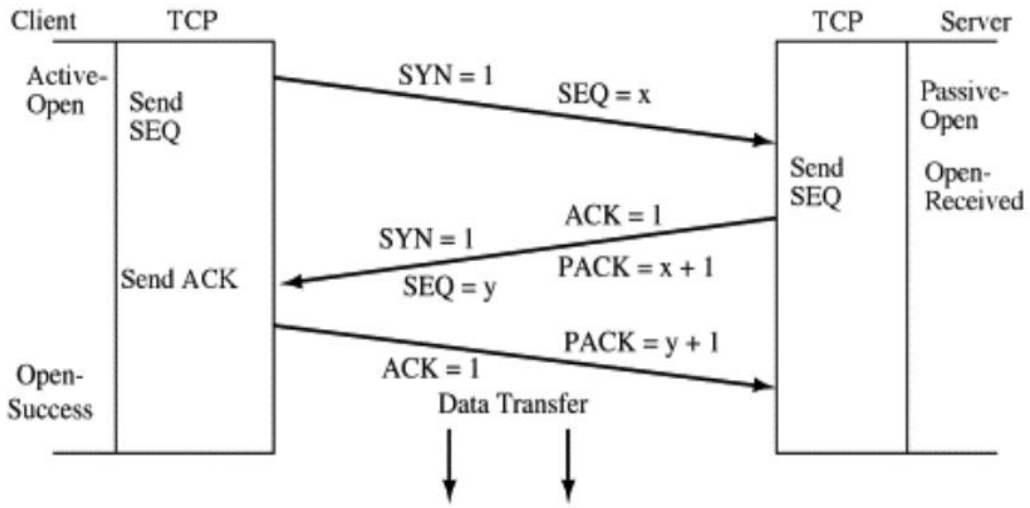


Zdroj:https://forum.huawei.com/enterprise/en/understanding-dhcp-snooping/thread/666139-861

4.2.3 TCP útoky

Samotný protokol TCP lze využít pro získání informací o daném zařízení. Tento protokol lze označovat za stavový, který je součástí transportní vrstvy v rámci ISO/OSI modelu. Jedná se o jeden ze základních protokolů, jehož účelem je vytvořit mezi dvěma body spolehlivý přenos dat. Jelikož se jedná o stavový protokol, tak obě strany znají aktuální stav spojení. Při navázání spojení se musí provést TCP handshake viz obrázek 6. V případě, že chce klient navázat spojení s protější stranou, tak nejdříve musí zaslat paket s příznakem SYN a pořadovým číslem X. Cílová strana následně zpracuje příchozí požadavek, nastaví si pořadové číslo a odešle zpět paket s příznakem SYN a ACK s nastaveným pořadovým číslem Y a potvrzovacím číslem X+1. Následně klient potvrdí synchronizační paket ze strany serveru a potvrzovacím číslem Y+1. (11)

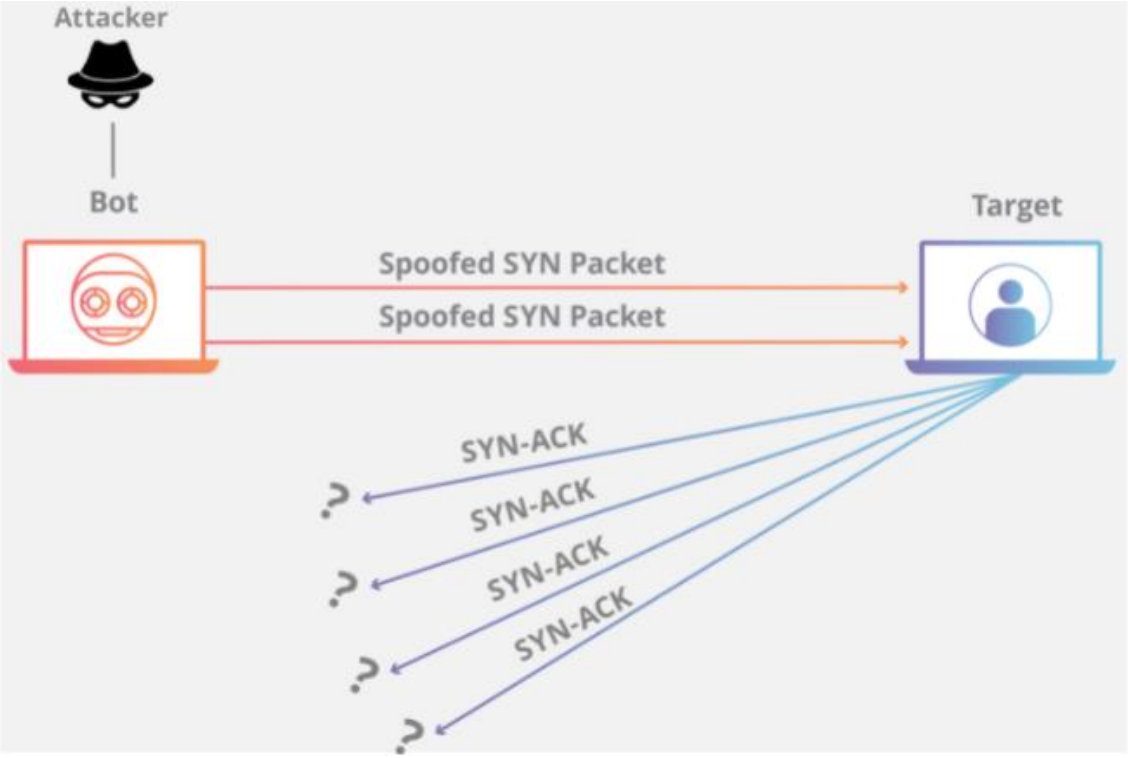
Obrázek 6 - TCP Three-Way Handshake



Zdroj: https://www.sciencedirect.com/topics/computer-science/three-way-handshake

Protokol TCP se dá zneužít v rámci síťové komunikace pomocí příznaků SYN, RST a dalších parametrů. TCP SYN útok využívá zmíněného TCP tří krokovou výměnu informací, pro navázání spojení, avšak toto spojení není nikdy dokončeno. Zařízení útočníka odešle TCP SYN paket na server, který si pro danou komunikaci otevře port, který drží otevřený, aby na něj klient mohl dále komunikovat a potvrdit spojení. Zatímco cílový bod čeká na posední krok navázání spojení, tak útočník posílá další TCP SYN pakety viz obrázek 7. Jedná se o jednu z forem Denial-of-service (Dále už jen DDOS) útoků. Pakliže je perioda posílání TCP SYN paketů větší než uvolňování portů již nenavázaných spojení, tak dochází k zahlcení a cílové zařízení nemůže odpovídat. (12)

Obrázek 7 - TCP SYN flood attack



Zdroj: https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

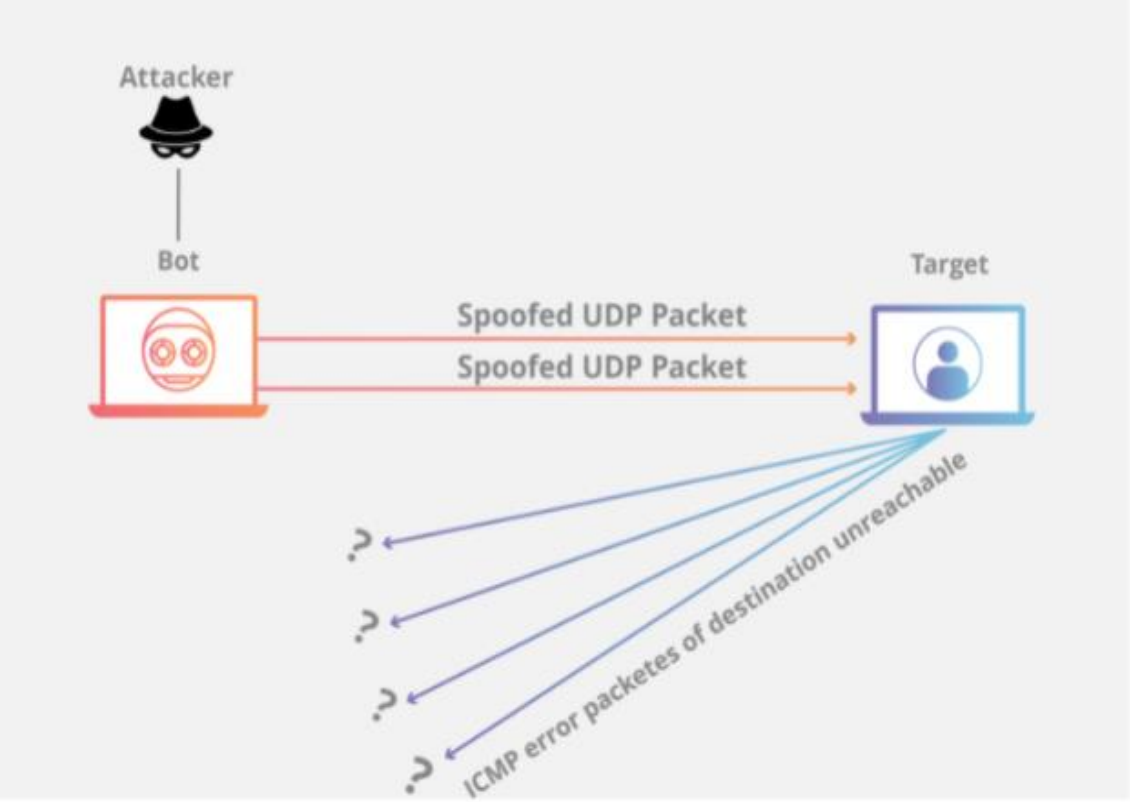
TCP SYN paket útočník může využít různými způsoby. Přímý útok, kdy útočník využívá pro odesílání pouze jednu a tu samou IP adresu. Další možností je podvrhovat IP adresu do jednotlivých synchronizačních paketů. Posledním je DDoS útok, který je vytvořen pomocí botnetu.

Myšlenkou TCP RST je, že pokud jedna strana obdrží paket s příznakem RST, tak okamžitě ukončí spojení. Tento příznak se tedy dá využít pro ukončení jakéhokoliv spojení. Například se může jednat o připojení mezi 2 zařízeními, kdy se útočník snaží jejich připojení ukončit tím, že podvrhne TCP hlavičku s příznakem RST. Pro správné vykonání tohoto útoku je třeba zasílat TCP RST paket se správným pořadovým číslem, aby byl akceptován ze strany serveru. V opačném případě je tato komunikace ignorována. (12)

4.2.4 UDP útoky

UDP je nestavovým protokolem a je jedním ze základních přenosových protokolů, který je význačný tím, že ani jedna strana nezná aktuální stav. Na rozdíl od TCP tento protokol neobsahuje žádné potvrzovací čísla. Z tohoto důvodu lze UDP protokol využít k zahlcení určitých služeb, nebo jako DDOS. Při běžné komunikaci, když server příjme UDP paket, tak zkontroluje, zda jsou spuštěny programy, které naslouchají na daném portu, kam paket přišel. Pokud na tomto portu není spuštěn žádný program, tak server odpoví pomocí ICMP zprávy, že dané místo je nedostupné. Útočník předpokládá, že server bude odpovídat na každý UDP paket, což znamená, že každý jednotlivý paket musí zpracovat. Což může vést k zahlcení daného zařízení a omezit jeho dostupnost. (13)

Obrázek 8 - UDP flood attack



Zdroj: https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/

Moderní nástroje pro zvýšení bezpečnosti, jako SIEM, který využívají společnosti ke sběru dat. Využívá pro svůj přenos protokol Syslog na portu 514, nebo šifrovaný na 6514. Tento protokol může komunikovat také přes UDP. Zařízení zasílající auditní záznamy skrze výše zmíněný protokol, jenž využívá pro přenos nestavový protokol. Vlivem toho, že protokol neprovádí navázání spojení, tak lze podvrhovat tyto auditní zprávy a zasílat je na tento nástroj. Pomocí čehož lze SIEM přehltit, nebo podvrhovat samotné informace.

4.2.5 MAC útoky

MAC je identifikátorem všech zařízení, kdy každé zařízení má svou adresu. Zapisuje se v hexadecimálním tvaru o velikosti 48 bitů. Při síťové komunikaci se nachází v rámci, tedy na 2 vrstvě referenčního ISO/OSI modelu. Útočníci se mohou snažit vystupovat do sítě pod jinou MAC adresou, aby mohli obcházet určité typy zabezpečení a zároveň se skrývat. Při připojení zařízení do sítě, by mělo být nastaveno ověření například přes 802.1x, kde je řada možností ověření. Může se jednat například o ověření na fyzickou adresu zařízení. V případě, že si útočník změní svou MAC adresu, tak dané zabezpečení obejde a následně je zařízení ovládané útočníkem v lokální síti, kde může dále vykonávat důvod své činnosti. Lze také využít změnu MAC adresy k přepisu údajů v rámci CAM (Content Addressable Memory) tabulky, která obsahuje informace o MAC adresách, portech, VLAN a časových razítkách. Samotný záznam vzniká při příchodu rámce a buď se daný záznam vytvoří, nebo se objeví jeho časová známka, a pokud již informace existuje s jinými daty, tak se smaže. (14)

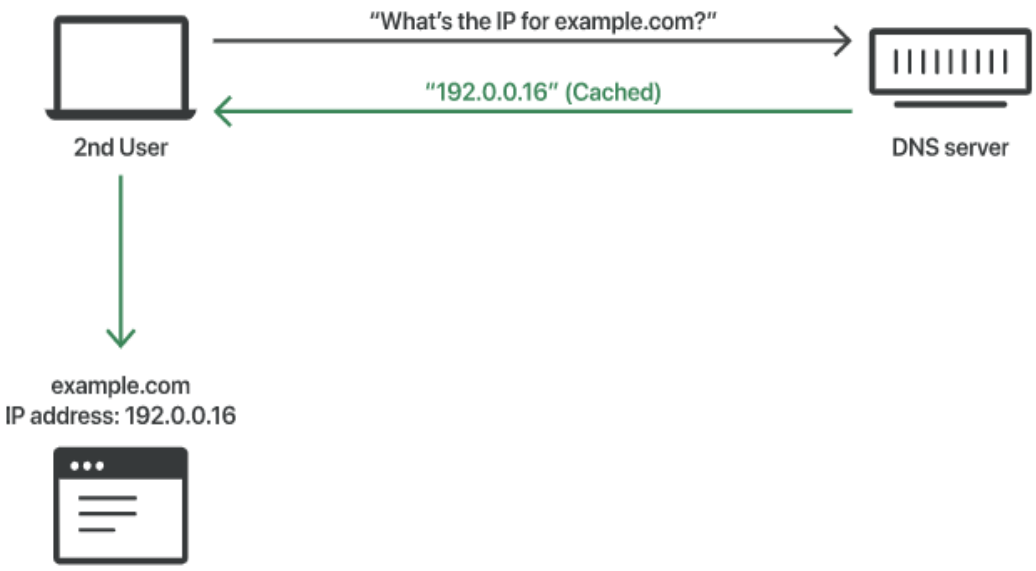
Útok na CAM tabulku – jedná se o útok, kdy útočník posílá velké množství rámců s různými podvrženými zdrojovými MAC adresami. Síťové zařízení na L2 se je snaží zpracovat a zaznamenávat do své CAM tabulky, avšak tato tabulka má omezenou velikost. Tudíž lze dosáhnout toho, že danému zařízení je zahlcena tabulka CAM informacemi o podvržených MAC adresách. V tento moment se zařízení přepne do režimu otevření při selhání a začne se chovat jako rozbočovač. Rámce jsou zasílány do všech portů. Čímž útočník, může sbírat data, nebo je posílat na všechna zařízení. (14)

4.2.6 DNS útoky

DNS protokol ležící na 7 vrstvě v rámci ISO/OSI modelu, který slouží k překladu IP adres na doménové jméno. Tento protokol se dá zneužít několika způsoby, jako typ DDOS útoky, nebo infiltrace do prostředí. DNS komunikuje na portu 53 a tento port nebývá blokován na perimetru sítě, aby uživatelé mohli využívat jeho úlohu a nemuseli zapisovat do prohlížečů IP adresy. Jedním z možných DNS je zeroday, kdy útočník využívá neznámou chybu zabezpečení DNS protokolu. (15)

DNS Cache poisoning – každý DNS server si musí ukládat svou interní databázi překladu IP a doménová jména, aby jeho překlad byl co nejrychlejší. Tento postup je vyobrazen na obrázku 9, kde daný DNS server zná překlad domény na IP.

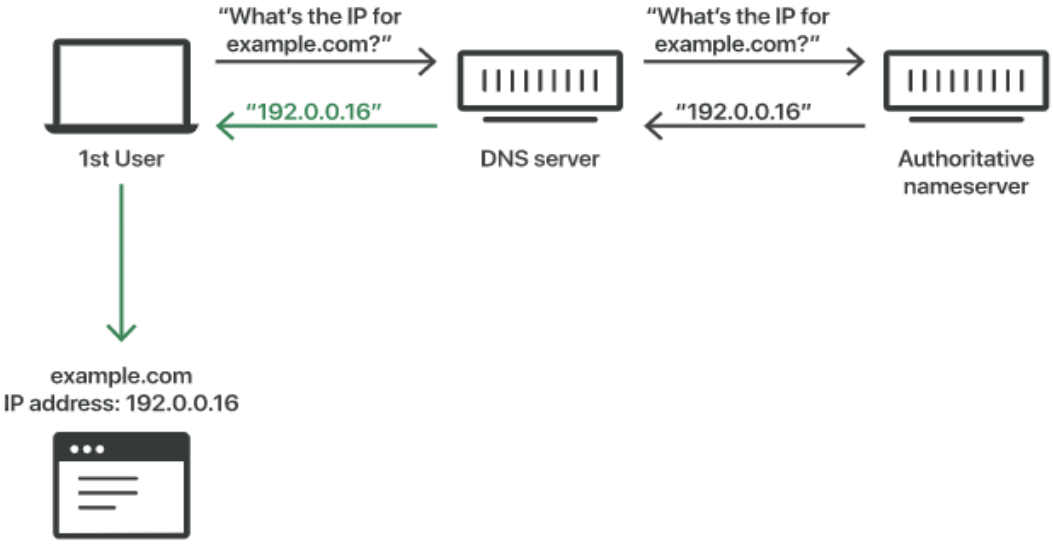
Obrázek 9 - DNS cached response



Zdroj: https://www.cloudflare.com/learning/dns/dns-cache-poisoning/

V opačném případě, pakliže danou informaci nezná, tak se zeptá nadřazené domény a daný záznam si poté uloží. Tento postup je zobrazen na obrázku 10, kde se DNS server musí doptávat na překlad nadřazeného serveru.

Obrázek 10 - DNS uncached response

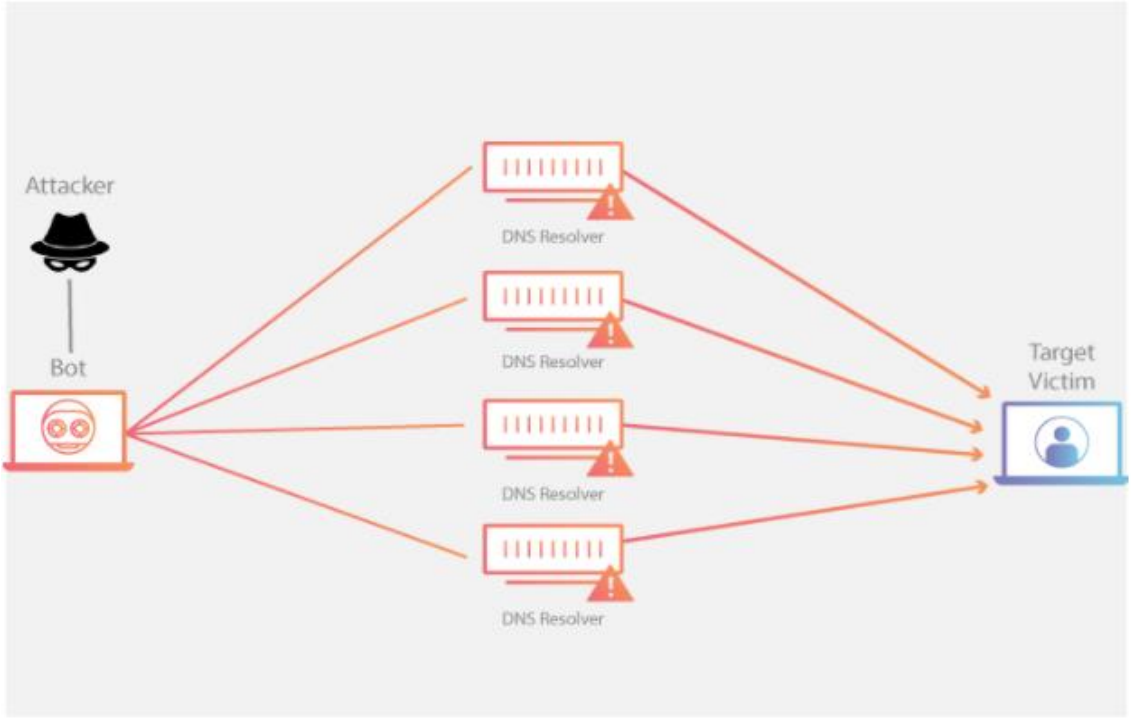


zdroj: https://www.cloudflare.com/learning/dns/dns-cache-poisoning/

Útočník se může snažit zasahovat do záznamů DNS serveru, aby dosáhl toho, že stránky, které bude vyžadovat libovolný uživatel z daného segmentu sítě ze kterého je dotazováno na tento server bude přesměrován na stránky útočníka. Protokol UDP nemusí provádět handshake pro navázání spojení, tedy nelze zajistit, že příjemce je ten, za koho se vydává. Samotný DNS protokol využívá TCP, tak UDP pro svou komunikaci. V případě, že se lokální DNS server dotazuje na překlad daného doménového jména, tak v tento okamžik posílá útočník UDP pakety na DNS server, kdy musí znát nebo uhodnout informace jako DNS ID požadavku (obsaženo v DNS hlavičce), port pro překlad a na jaký dotaz se uživatel ptal. Pakliže DNS server obdrží padělané odpovědi na jeho překlady, tak si je uloží do své mezipaměti. Nejedná o snadný realizovatelný útok, jelikož DNS servery se dotazují autorizovaných serverů, takže útočník má několik milisekund na odeslání podvržené odpovědi. (16)

DNS amplification je útok, kdy se útočník snaží skrze DNS protokol vygenerovat velké množství odpovědí s co největší velikostí. Pomocí čehož se snaží zahltit daný server, aby jej vyřadil z provozu. Útok je znázorněn na obrázku 11, kdy útočník vygeneruje DNS požadavek na libovolný DNS server kdy se doptá obecným požadavkem na informace o dané stránce. Například se může jednat o typ dotazu kdy v DNS hlavičce její časti dotazu je typ „ANY“. Tento dotaz vrací všechny údaje zaznamenané v DNS. Může se jednat o IPv4, IPv6, alias, mail server, název serveru, rezervované zóny, jméno primárního serveru a další. Tato odpověď obsahuje mnohem větší množství dat než samotný požadavek. Zároveň útočník podvrhuje svojí zdrojovou adresu a nahrazuje jí adresou, kam chce útočit. DNS server tento požadavek zpracuje a vyhodnocuje informace jako: zdroj a dotaz. Následně zpracuje dotaz a odešle zpět odpověď na zdroj. Pokud je tedy podvržená zdrojová adresa útočníka za adresu útoku, tak bude dostávat tyto odpovědi. (16)

Obrázek 11 - DNS Amplification Attack



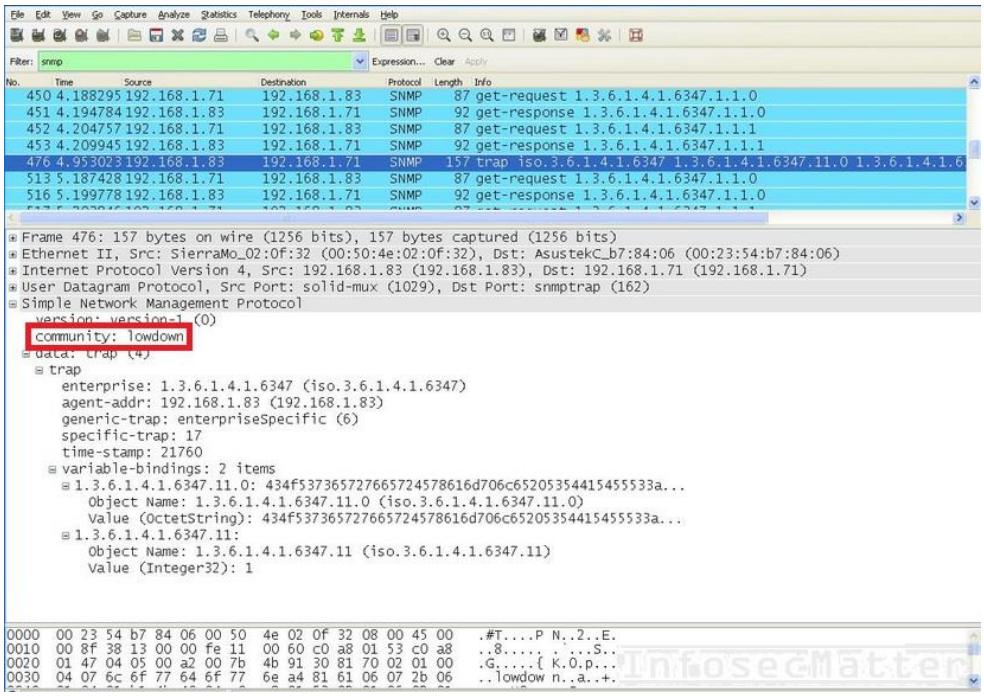
Zdroj: https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/

DNS protokol lze využít k exfiltraci, nebo infiltraci dat přes DNS. Jedná se o často využívanou možnost útočníka, jelikož nebývá blokován na perimetru sítě. Zařízení mohou komunikovat s jiným než interním DNS serverem. Exfiltrace dat může být provedena skrze DNS dotazy a odpovědí, které mohou chodit z interní infrastruktury ze společnosti ven. Infiltraci využívají útočníci při zasílání příkazů škodlivým programům v interní síti, které jsou vykonávány na straně oběti.

4.2.7 SNMP útoky

Protokol SNMP se využívá pro monitorování a nastavování síťových prvků. Tento protokol má 3 verze a hned první dvě verze jsou považovány jako nebezpečné, a to z důvodu, že jejich komunikace je v čitelném textu. SNMP verze tři je šifrovaná. Nicméně dnes se používají napříč celým světem všechny verze. Samotný protokol komunikuje na portu 161. Útočník může získat podrobné informace o vzdáleném systému. Pomocí kterých lze připravovat další možné útoky. Tento řídící protokol umožňuje skrze komunikaci upravovat konfiguraci na vzdáleném zařízení. Nástrojem jako Wireshark lze tyto komunikační řetězce zachytávat viz obrázek 12. (17)

Obrázek 12 - Wireshark SNMP



Zdroj: https://www.infosecmatter.com/capture-passwords-using-wireshark/

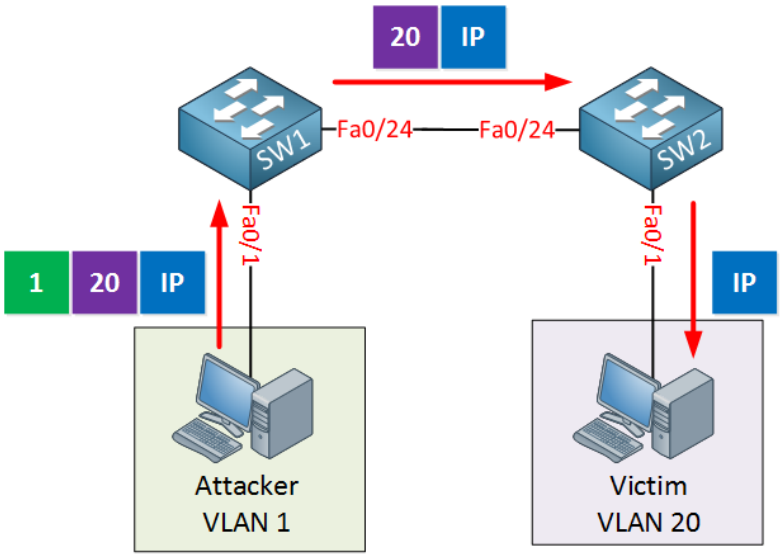
4.2.8 VLAN útoky

VLAN jsou virtuální LAN sítě sloužící k logickému rozdělení sítě, a to nezávisle na fyzickém uspořádání. Pomocí VLAN lze segmentovat síť na menší podsítě uvnitř fyzické struktury původní sítě. Samotné VLAN vycházejí ze standardu 802.1Q a využívají si na 2 vrstvě ISO/OSI modelu a informace jsou uchovávány v rámci rámce. Nejčastějším sítovým prvkem, kde jsou využity a zpracovány VLAN jsou switche, kde jejich porty mohou být nastaveny do 3 druhů. Nativní VLAN je výchozí virtuální síť, která má v základním nastavení hodnotu jedna a je využita, pakliže není nakonfigurovaná jiná než výchozí hodnota VLAN. Druhým nastavením je Acces, která přiřazuje danému rámci označení (tag) dané VLAN. Třetím nastavením je Trunk, skrze který lze propojit 2 switche a posílat mezi nimi více VLAN. (18)

Jednosměrný útok, který se snaží využití nativních VLAN pro přeskakování mezi jinými VLAN je zobrazen na obrázku 13. V principu, pakliže je Acces port na switchi nastaven tak, že přidává označení stejné jako je nativní VLAN, tak lze využít tuto možnou zranitelnost sítě. Při komunikaci zařízení útočníka pošle rámec na switch, ve kterém na místo jednoho tagu jsou za sebou dva (tzv. double tagging). Switch s označením SW1 na obrázku 13, který rámec zpracovává sleduje informace zdrojové MAC, cílové MAC a danou VLAN. Následně odebere vstupní VLAN (nativní VLAN)

a směrovač kontroluje na jakém dalším svém portu je nastavena stejná hodnota, jelikož Trunk port musí mít obsaženou i nativní VLANu, aby věděl, jak zpracovat rámce bez označení, tak tento rámec mu bude přidělen. Zároveň si na daném Trunk portu směrovač SW1 zkontroluje hlavičku rámce a zpracuje tag (druhou hodnotu VLAN), kterou útočník vložil. V tomto okamžiku je rámec posílán skrze port, jenž je propojený s protější stranou Trunkem. Směrovač SW2 příjme na portu rámec s informací, že data tečou na již jiný než nativní označení. Pomocí čehož se útočník může dostat do VLAN jiného subjektu. Tento útok je jednosměrný, jelikož nemůže dostat odpověď zpátky. (19)

Obrázek 13 - VLAN Hopping



Zdroj: https://networklessons.com/cisco/ccnp-switch/vlan-hopping

4.3 Aplikační útoky

Útoky tohoto typu spočívají v tom, že útočníci získají přístup do nepovolených čísti lokální prostředí. Nejčastěji útočníci začínají pohledem na aplikační vrstvu a hledají zranitelnosti aplikací zapsaných v kódu, nebo jejich nastavení. Samotné chyby zabezpečení se nacházejí nejen v rámci kódu, ale také ve využitých knihovnách. Vývojáři v technologických společnostech uvádějí, že průměrná aplikace má více než 10 zranitelností. Například aplikace vystavené do internetu za poslední rok podstupují každý měsíc v průměru přes 13 tisíc útoků. (20)

4.3.1 Ověření ve Windows

Autentizace v rámci operačního systému Windows jsou přímé a nepřímé. Přímým ověřením se rozumí ověření v rámci lokálního systému modelem challenge-response. V druhém případě v nepřímém ověření musí uživatel vznést požadavek na vzdálený server, který mu vrací výzvu k ověření na kterou klient odpovídá. Pro tento typ ověření lze využít protokoly typu LM, NTLMv1, NTLMv2 a Kerberos.

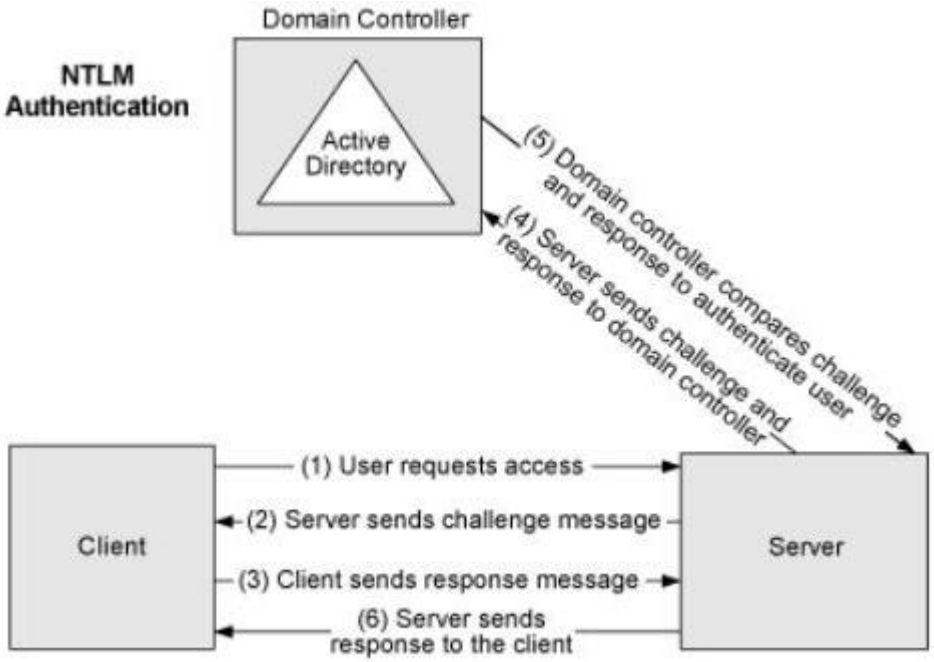
LM neboli Lan Manager je jednou z nejstarších možností pro ukládání/ověření hesel v rámci systému Windows. Jedná se z dnešního pohledu o již nedostatečný protokol pro zabezpečení hesel, a to z důvodu malé znakové sady a samotné funkčnosti. Využívá se jednoduchý typ algoritmu, který podle předdefinovaných pravidel udělá z hesla hash. Samotný hash vzniká pomocí těchto 6 bodů: (21)

1. Převeďte všechna malá písmena na velká písmena
2. Heslo má fixní velikost 14 znaků, pakliže je kratší je doplněno nulami.
3. Heslo se rozděluje na dva 7 znakové bloky
4. Vytvoří se dva klíče DES z každého 7 znakového bloku plus jeden doplňkový znak nula.
5. Tímto klíčem je zašifrován přímo tento řetězec „*KGS!@ #$%*"
6. Výsledná podoba je spojení 2 šifrovaných klíčů a společné velikosti 16 znaků a takto vznikne LM hash.

Pomocí protokolu NTLM se lze ověřovat v rámci dnešních systémech Windows. Tento protokol navazuje na LM. Jehož cílem bylo dosažení vetší bezpečnosti v rámci autentizaci. I přes to, že toto ověření je v rámci dnešních systémů, tak není považován za bezpečný. NTLM má dvě verze NTLMv1 a NTLMv2. Protokol využívá hashovací funkce, které lze definovat jako jednosměrné algoritmy po jejichž použití vzniká otisk hesla a z otisku by neměla být možnost obnovit heslo. V principu tedy systém nemusí znát heslo uživatele, ale pouze jeho otisk. NTLMv1 využívá jednosměrný překlad algoritmu MD4, který je dnes již nevyužívaný, protože byl prolomený. Druhá verze protokolu NTLM obsahuje již více bezpečnostních bodů jako časové známky, digitální podpis algoritmus MD5. I přes snahu využití novější verze algoritmu MD5 se z dnešního pohledu zdá jako nedostačující, jelikož tento algoritmus měl výsledné duplicity a zároveň byl i prolomený.

Pro vyšší zabezpečení by dnešní systéme měli využívat Protokol Kerberos a však v systému je nastaveno, že pokud Kerberos selže bude použit NTLM. Samotný postup ověření NTLM je vidět na obrázku 14. (22)

Obrázek 14 - NTLM



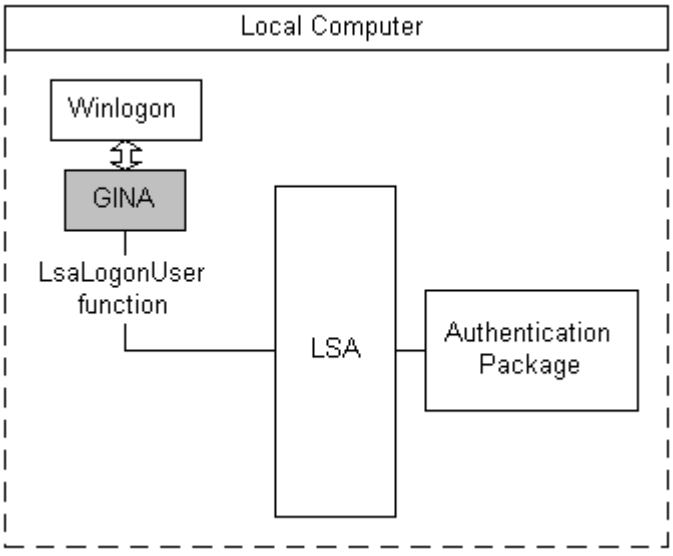
Zdroj: https://answers.microsoft.com/en-us/msoffice/forum/all/ntlm-vs-kerberos/d8b139bf-6b5a-4a53-9a00-bb75d4e219eb

1. Uživatel, který se přihlašuje do zařízení, které je v doméně, tak poskytuje informace o doménovém jméně zařízení, heslo a uživatelské jméno. Klient vypočítá podle algoritmu otisk hesla, se kterým nadále bude pracovat na místo hesla. Klient odešle své uživatelské jméno serveru v čitelné podobě.
2. Server vygeneruje 16 bytové náhodné číslo (Challenge) a pošle ho zpět klientovi.
3. Klient zašifruje tuto challenge s hashem z uživatelského hesla a vrátí jí serveru. (Response)
4. Server pošle na doménový řadič (DC) tři informace – uživatelské jméno, Challenge a Response.
5. DC používá uživatelské jméno k načtení hashe z hesla, který má uložený ve své paměti. Následně rozšifruje pomocí Challenge vrácenou Response od klienta, čímž dostane původní hash, který si v prvním kroku vytvořil klient. Pokud hash z databáze DC a nově získaného jsou identické, tak je ověření úspěšné.
6. Server pošle zpět odpověď klientovy.

Interaktivní ověření uživatele. Proces, který nastane v případě, že je uživatel vyzván k zadání přihlašovacích údajů je popsaný na obrázku 15. V rámci lokálního prostředí je spuštěn proces Winlogon což je spustitelný soubor, který je zodpovědný za správu zabezpečených interakcí uživatelů. Tento proces zahajuje proces přihlášení. Winlogon volá GINA – modul DLL (MSGINA.dll), který pracuje v rámci zabezpečení Winlogon, kdy si jej načte na začátku procesu zavádění. Samotný GINA je zodpovědný za zpracování události SAS (Secure Attention Sequence) a obsahuje rozhraní pro přihlášení. Winlogon a LSA ke zpracování přihlašovacích údajů využívají LSA, je chráněný podsystém, který napomáhá pro vytvoření zabezpečených interakcí uživatelů v systému. LSA musí vyhodnotit jaký autentizační balíček využít pro přihlášení, kdy se může jednat o NTLM, Kerberos a v rámci lokálního ověření o knihovnu MSV1_0.dll. Tato knihovna si porovnává ověřovací údaje s SAM databází. SAM ukládá informace o lokálních uživatelích účtech do registrů Windows. Hesla jsou ověřována balíčkem NTLM, jenž se stará o šifrování hesla. (23) (24)

Z popisu obrázku 15 je jasné že přihlášení uživatele na zařízení probíhá skrze několik procesů. Útočník nemusí cílit pouze na jeden proces, nebo na místo uložení pro získání přihlašovacích dat.

Obrázek 15 - Ověření v rámci lokálního počítače



Zdroj:https://docs.microsoft.com/en-us/windows/win32/secauthn/interactive-authentication

SAM databáze je uložena v rámci registru systému v části „HKEY_LOCAL_MACHINE\SAM\SAM“. Záznamy v tomto podadresáři obsahují uživatelská jména a jejich hesla ve formě jejich otisku, který vzniká pomocí NTLM. Z důvodu bezpečnosti k této databázi mohou přistupovat pouze systémové procesy. Windows v novějších systémech od verze 2000 funkci SYSKEY, která umožnuje danou databázi zašifrovat. V rámci výchozího nastavení operačního systému se databáze nachází ve složce adresáře „%WINDIR%\System32\Config\,“, kde první část v procentech označuje složku, ve které je systém Windows nainstalován. Winlogon využívá proces lsass.exe, do kterého spadá LSA s voláním na SAM databázi. Jelikož se jedná o proces pracující s otiskem hesla, tak dochází k bodu, že je tato informace uložena v paměti daného procesu, na které může útočník cílit. Samotná hesla, která jsou vázány k automatickému přihlašování na internetové stránky, nebo jiné počítače v rámci lokální sítě využívají pro správu Credential Managera ve složce „vault“ cesty: „C:\users\%username%\appdata\local\micorsoft\credentials“. K tomuto souboru mohou přistupovat pouze programy nebo služby, které hesla poskytnou serveru. Samotný LSA může mít hesla pro účty služeb, automatické přihlašování a ta jsou ložena v registrech „HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets“. (25)

Jedním z možných postupů útočníka k získání přístupu do systému může být útok pass the hash. Útočník se snaží získat hash uživatelského hesla a znovu je využít k oklamání ověřovacího systému. K samotnému provedení je tedy nejprve získat hash z cílového systému, kdy lze využít například systém Mimikatz. A následně je tento hash vložen do služby LSASS. V Rámci síťového ověření útočník získaný hash využívá v rámci kroku 3 v obrázku 14, kde na místo svého hash využije odcizený otisk hesla pro zašifrování. Zároveň, jak již bylo zmíněno, tak protokoly MD4 a následně MD5 byli prolomeny a lze z nich získávat hesla. (25)

4.3.2 Útoky hrubou silou

Útočník může využívat obecnějších technik na prolomení ověření jako je brute force. Jedná se o slovníkový útok. I tento typ se dělí na metody typu Hybrid bruet force, reverse bruet force a credential stuffing. Hybridní typ útoku je založený na seznamu potencionálně známých shod. V rámci úplně nejzákladnějších technik tohoto typu se zařízení zkouší ověřit všemi možnými kombinacemi. Tato metoda je však velmi

pomalá. Z toho důvodu vznikly listy nejpoužívanějších hesel, nebo později také programy pro vytvoření sady přihlašovacích údajů přímo pro daného uživatele. Ke slovníkům mířených na jednu osobu je zapotřebí znát blízké informace typu mazlíček, datum narození, oblíbené věci a další. Z těchto informací jsou vytvořeny různé kombinace. Reversní typ útoku se snaží využít k získání přístupu k účtu společné heslo pro více uživatelů. Credential stuffing vychází z předpokladu, že uživatelé používají stejná hesla napříč všemi aplikacemi, nebo jejich částečnou modifikaci. Samotná rychlost prolomení hesla je vypočítávaná z průměrné výpočetní techniky a zároveň je závislá na bitové délce hesla a sady znaků viz obrázek 16. (26) (27)

Obrázek 16 - Brute force

JAK DLOUHO TRVÁ HACKEROVI PROLOMIT VAŠE HESLO POMOCÍ HRUBÉ SÍLY (BRUTE FORCE)?					
Počet znaků v hesle	Pouze čísla	Malá písmena	Velká a malá písmena	Čísla, velká a malá písmena	Čísla, velká a malá písmena, speciální znaky
4	Okamžitě	Okamžitě	Okamžitě	Okamžitě	Okamžitě
5	Okamžitě	Okamžitě	Okamžitě	Okamžitě	Okamžitě
6	Okamžitě	Okamžitě	Okamžitě	1 sek	5 sek
7	Okamžitě	Okamžitě	25 sek	1 min	6 min
8	Okamžitě	5 s	22 min	1 hod	8 hod
9	Okamžitě	2 min	19 hod	3 dny	3 týdny
10	Okamžitě	58 min	1 měsíc	7 měsíců	5 let
11	2 sek	1 den	5 let	41 let	400 let
12	25 sek	3 týdny	300 let	2 000 let	34 tisíc let
13	4 min	1 rok	16 tisíc let	100 tisíc let	2 mil. let
14	41 min	51 let	800 tisíc let	9 mil. let	200 mil. let
15	6 hod	1 000 let	43 mil. let	600 mil. let	15 mld. let
16	2 dny	34 tisíc let	2 mld. let	37 mld. let	1 bilión let
17	4 týdny	800 tisíc let	100 mld. let	2 bilióny let	93 biliónů let
18	9 měsíců	23 mil. let	6 biliónů let	100 biliónů let	73 biliard let
JE VAŠE HESLO V **ZELENÉ ZÓNĚ**?					

Zdroj: Vlastní zpracování na (27)

4.3.3 Ransomware

Ransomware pochází ze spojení slov „ransom“ neboli výkupné a software. Jedná se o škodlivý program, který se vyznačuje šifrování, nebo blokací veškerých souborů v rámci operačního systému. Tento úkon znemožní využívat zařízení. Po dosažení tohoto bodu může útočník vyžadovat výkupné za dešifrovací klíč, nebo nezveřejnění informací které mohou být v rozporu například s GDPR. Samotný Ransomware se dá rozdělit podle toho, na jaký operační systém je směřovány. Dále se může dělit podle toho, jakým způsobem vstupuje do interní sítě, kdy vstupní cesty mohou být za pomocí elektronické pošty, nebo infikované stránky na internetu nebo chybou v zabezpečení.

Patrně nejdůležitějším bodem je, jak se ransomware šíří v rámci lokální sítě a jaké zranitelnosti využívá, aby mohl vykonávat svůj úkol. Při úspěšném zašifrování daného zařízení nebo celé sítě. V tento moment se postupy mohou rozlišovat na základní dva scénáře. Prvním základním přístupem k ransomwaru je pouze dosažení zamezení přístupu vlastníkům k jejich datům. V tomto případě útočník vytváří časový nátlak na získání finančního obnosu, kdy se může jednat o omezenou dobu pro zaplacení požadované částky za kterou obdrží vlastník klíč pro dešifraci. Pomocí čehož se napadené osoby dostane ke svým souborům. Druhou variantou je nejen zamezení přístupu k souborům, ale veškeré odcizení těchto dat. V tento moment útočník může klást nátlak nejen k odkoupení dešifračního klíče, ale také k zaplacení, aby odcizená data nebyla zveřejněná. I přes rozdílné metody šíření, nebo přístupu k datům má většina Ransomware stejný cíl – vynutit oběť k zaplacení výkupného. Existují však případy, kdy skrze slabé zabezpečení v jednom ze zmíněných bodu výše pronikne tzv. „botnet“ (síť infikovaných počítačů), do sítě a podaří se mu jí celou zašifrovat. V tomto případě už je pouhá závislost na tom, jak byl program připraven a na co cílí. Samotný útočník ani nemusí v době zahájení útoku tušit, že je prováděn jeho útok. V důsledku nemusí mít zájem o vymáhání peněz například při zjištění, že byl proveden útok na nemocnici. Některé skupiny útočníků propagují, že se vyhýbají útokům na tyto subjekty. (28)

Historické útoky ransomware, kde bylo požadované výkupné zaplaceno. (29)

- V červnu 2019 zaplatilo město na Floridě výkupné 600 000 dolarů za obnovení zašifrovaných souborů.
- Kalifornská univerzita v San Franciscu zaplatila za obnovu souborů zašifrovaných ransomwarem výkupné ve výši 1.14 milionu dolarů.
- Po ransomwarovem útoku zaplatila Travelex – londýnská směnárna, která podniká ve 26 zemích, 2.3 milionu dolarů, aby znovu získala přístup ke svým záznamům. Tato událost ochromila společnost na týdny.
- V květnu 2021 se severoamerická divize distributora chemikálií Brenntag stala obětí ransomwarového útoku DarkSide. I když byla škoda omezena pouze na jeden segment společnosti, v důsledku incidentu bylo odcizeno celkem 150 GB dat. Útočník požadoval nejprve 7.6 milionu dolarů, ale po vyjednávání se cena snížila na 4.4 milionu dolaru.

- Podle záznamu o vyjednávání o výkupném, Americká společnost cestovních služeb CWT zaplatila 4.5 milionu dolarů útočníkům, kteří ukradli obrovské množství jejich důvěrných obchodních souborů.

4.4 Síťová bezpečnost

Bezpečnost je jakákoli činnost, která má dopad na zachování, použitelnost a integritu sítě a dat. Tento segment zahrnuje hardwarové i softwarové technologie. Samotnou efektivitu sítě je řízena i přístupem do ní. Cílem samotné síťové bezpečnosti je zahrnout široké spektrum hrozeb a blokování jejich průniků, nebo šíření v síti. Kombinují se zde několik vrstev obrany na okraji a vnitřní síti. Každá tato vrstva by měla uplatňovat pravidla a provádět kontroly. Oprávnění uživatelé získávají přístup k interním zdrojům, ale škodlivé entity jsou blokovány. (30)

4.4.1 Zabezpečení sítě

Trafic Storm Control je metoda, která zabraňuje zahlcení sítě při nadměrném využití broadcastové, multicastové nebo neznámé unicastové komunikaci v síti, která vede k snížení síťového výkonu. Pro jednotlivý interface, nebo portchannel na síťovém zařízení se nastavují limitní hranice, které při jejich překročení začne zprávy zahazovat, nebo vypne port. Pokud bude tato hranice překročena je o ní vytvoření záznam. (31)

Port Security je metoda pro zvýšení zabezpečení portu, která má zařízení ochraňovat před podvrhování MAC adres a útokům využívajícím jejich podvrhu nebo snahu o zahlcení MAC tabulky. Tato metoda funguje na principu kontroly na druhé vrstvě ISO/OSI modelu, kde se v rámci kontroluje zdrojová MAC adresa a pakliže je jinačí než povolená, tak je daný rámec zahozen, nebo vypne port. Samostatné nastavení se dělá vůči jednomu portu, kde se nastavuje kolik MAC adres může komunikovat. Ve výchozím nastavení se jedná o hodnotu jedna, tedy na jednom portu může být jedno zařízení. (31)

DHCP Snooping, který zabraňuje nepravému DHCP serveru v rámci lokální sítě. Po samotném zapnutí bere všechny porty jako nedůvěryhodné a v rámci nastavení se musí specifikovat jako důvěryhodný. Tímto portem je označen ten, na kterém je připojený DHCP server. Tato metoda funguje tak, že DHCP pro navázání a přidělování využívá 4 druhy paketů DORA (Discovery, Offer, Request, Acknowlage). Pakety, které procházejí přes síťový prvek, kde je tato metoda zapnutá je propouští pouze na důvěryhodné porty. Jelikož zařízení zpracovává všechny DHCP zprávy si může vytvářet DHCP Snooping Binding Database. Tato databáze obsahuje záznamy o IP,

VLAN, Interface a dobu pronájmu. Záznam databáze je uložený v paměti a může mít maximálně 8192 záznamů. (31)

IP source Guard jedná se o bezpečnostní funkci, která využívá informace z databáze DHCP Snooping Binding. V případě, že je tato funkce nastavená, tak jsou kontrolovaný zdroj komunikace vůči aplikujícím se ACL, které filtrují provoz. Metoda povoluje pouze pakety, ve kterých je zdrojová IP adresa zaznamenána v rámci DHCP databázi pro daný port. Tím se zabraňuje komunikace podvrhování IP adres. Tato nastavení se provádějí vůči jednotlivému portu. Nemusí se sledovat pouze zdrojová IP, ale i MAC adresa. (31)

DAI neboli Dynamic ARP Inspection je ochrana proti útokům využívající ARP protokol. I tato metoda využívá DHCP Snooping Binding Database. DAI monitoruje ARP provoz, zda jsou ARP dotazy validní oproti DHCP DB. Nevalidní dotazy zahazuje. Lze v rámci této kontroly nastavovat důvěryhodné porty, kde se kontrola neprovádí. DAI je taky součásti při ochraně DOS útoků, jelikož omezuje množství ARP dotazů za vteřinu. Ve výchozím nastavení se jedná o 15 dotazů. Metoda se zapíná vůči VLAN. (31)

Samotné zabezpečení zařízení začíná u přihlašování. Přístup do přihlašovací konzole daného rozhraní zařízení, by neměla být přístupná uživateli. Zároveň by se měli monitorovat veškeré pokusy o možný přístup, a to především o neúspěšné pokusy. Při úspěšném ověření by mělo docházet k jednoznačnému párování 1:1 – účet: uživatel. Jeho změny v systému by též měli být auditovány. Pakliže se jedná o lokální ověření, tak by hesla neměla být uložena v čitelné podobě, ale v zašifrované. Zároveň by měla být vynucována komplexnost hesla. Každé zařízení umožňuje přihlášení do zařízení skrze několik cest typu HTTP, HTTPS, SSH, nebo Telnet. V rámci bezpečnosti se plně vylučují přihlašování pomocí protokolů http nebo telnet. Obecně vylučuje veškeré nešifrované protokoly komplexně v celé síti. Pro vyšší úroveň zabezpečení by nemělo být využito přihlášení přes uživatelské rozhraní skrze prohlížeč. Každé zařízení může mít zranitelnosti webových aplikaci, což zvyšuje riziko možného zneužití. Jednou z nejstandardnějších využití přístupu k síťovým prvkům je skrze protokol SSH. V základu při nastavování zařízení by se mělo vycházet ze stavu, kde jsou veškeré funkce a možnosti vypnutí a využijí se pro produkční provoz pouze ty, které jsou nezbytné pro provoz. Nejčastěji se může jednat o vypnutí ověřovacích možností, vypnutí nevyužitých portu, zapnutí bezpečnostních funkcí, vynucení silnějších kryptografií, nebo vypnutí Wi-Fi pakliže není využívána. Každý výrobce může podle typu modelu zařízení využívat jiné typy služeb, které nejsou nutné pro provoz.

Segmentace sítě se provádí pomocí virtuálních logických částí neboli VLAN. Síť se rozděluji na 2 vrstvě ISO/OSI modelu, kdy je informace zanesena v rámci. Tato technologie se využívá pro logické členění v rámci fyzického zapojení, které pro rozdělení může být ponecháno. Maximální počet VLAN je 4096, ale první ani poslední se nevyužívají, jsou rezervované. Mezi hlavní výhody rozložení výkonu mezi logické části, čímž se omezuje omezení broadcastových zpráv. Zvýšení bezpečnosti, kdy jsou zařízení zařazení do vlastních VLAN a nemohou skrze ně komunikovat, případná nákaza se nemůže šířit sítí mimo svou VLAN. Existují dvě metody vytváření sítí, a to statické a dynamické. Statické VLAN se přiřazují k danému portu a nastavují se ručně. Při zapojení zařízení se přepne do virtuální sítě na daném portu. Dynamické pojetí je založeno na klientovi, VLAN nejsou pevně svázány k určitému portu, ale ke klientovi. Po zapojení zařízení je přidělena na daný port síťového zařízení VLAN podle předefinovaných politik, jako záznam MAC adresa a VLAN. Sítě by měly být děleny podle logických prvků. Pro malé sítě se doporučuje nastavovat pro jednotlivé zařízení privátní VLAN.

4.4.2 IEEE 802.1x

IEEE 802.1x je standard, který je využíván pro zabezpečený přístup klienta do interní sítě. Hlavní myšlenkou tohoto standardu bylo, aby neautorizovanému zařízení v síti nebylo umožněno komunikovat. Pro připojení je vždy vyžadováno určitý typ ověření, jako může být heslo, nebo certifikát. 802.1x je na druhé vrstvě ISO/OSI modelu. Vychází z architektury AAA, neboli Authentication, Authorization a Accountig. Obecně se tato architektura snaží rozpoznat vstupní zařízení, které se snaží dle předdefinovaných parametrů ověřit a následně mu umožnit komunikaci, nebo jej zablokovat. Standard obsahuje 3 role, Supplicant je zařízení, které je připojeno do sítě a snaží se v ní ověřit. Authenticator je prostředník mezi klientem (Supplicantem) a ověřovacím prvkem. Samotný authenticator je síťový prvek například switch. Authentication Server je hlavním bodem tohoto procesu. Vyhodnocuje požadavky, které obdrží od Authenticatora a vrací na ně bud potvrzení, nebo odmítnutí. V rámci samotného ověření se využívají takzvané EAP neboli Extensible Authentication Protocol. Poskytuje řadu metod pro ověření. Níže jsou popsány nejznámější, nebo nejvyužívanější. (32)

EAP-MD5 – Tato metoda využívá pro své ověření v síti přihlašovací údaje, které jsou pomocí algoritmu MD5 převedeny do hash, aby přihlašovací údaje nebyly posílány v čitelné podobě. Díky tomuto postupu přihlašovací údaje nemusí být uloženy

na ověřovacím serveru, ale stačí pouze jejich otisk. Tato metoda nemá vzájemný mechanismus ověření, což znamená, že server ověřuje klienta, ale klient neověřuje server. (33)

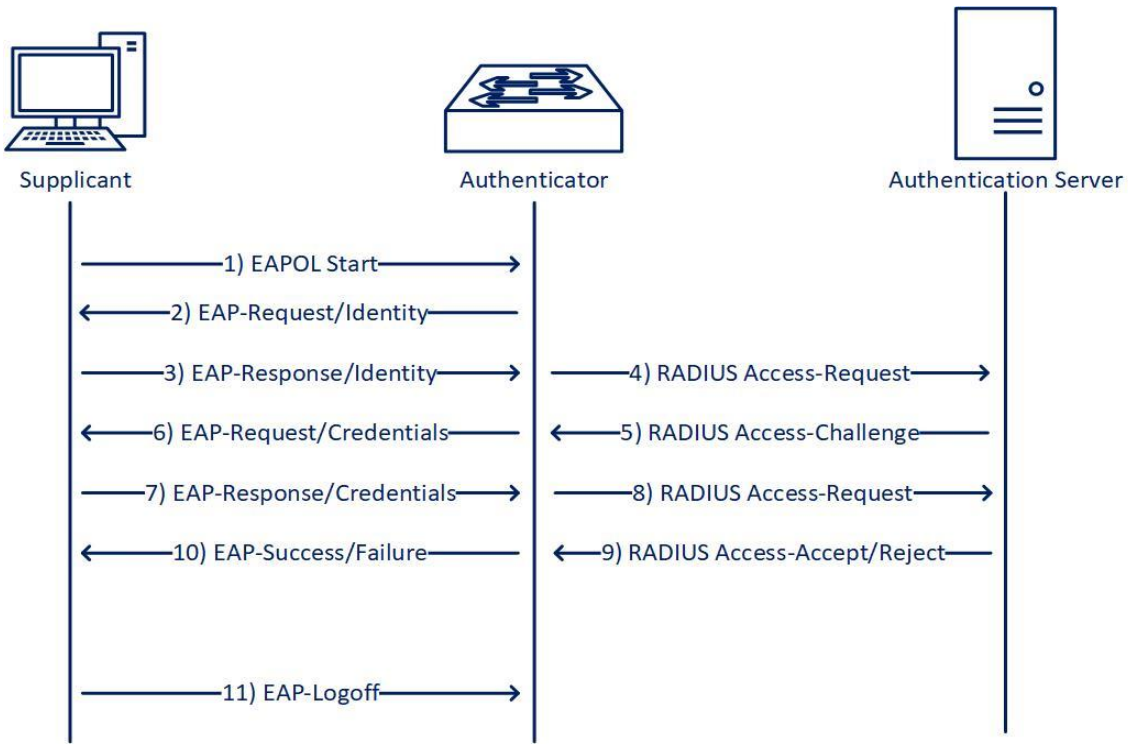
PEAP – Metoda vyžaduje certifikát na straně serveru. Před tím, než jsou předána jakákoli ověřovací data, je nastaven TLS tunel. To umožnuje klientovi nejprve ověřit server a poté mu předat přihlašovací údaje v zašifrované podobě. PEAP umožnuje provádět ověření za pomocí tokenu, nebo certifikátu, anebo přihlašovací údaje. (33)

EAP-TLS – V rámci této metody je využit pro zabezpečení komunikace TLS protokol. Pro větší bezpečnost je vyžadováno ověření certifikátu na straně serveru a klienta. Je tedy zapotřebí, aby každé zařízení mělo svůj platný certifikát. (33)

EAP – IKEv2 – Metoda je založena na protokolu Internet Key Exchange druhé verze. Poskytuje vzájemné ověřování a vytváření klíčů relace mezi klientem a serverem v reálném čase. Podporuje asymetrické, symetrické šifrovací klíče, nebo heslo a každá strana může využít jinou metodu. Po připojení zařízení je zaslán multicastovou adresou informace o Zdrojové MAC adrese. (34)

Přesné vyjádření postupu ověření zařízení v síti znázorňuje obrázek 17. V prvních krocích po zapojení Supplicanta do sítě ho vyzve Authenticator, může se jednat o switch, nebo AP k zaslání identifikačních údajů. Vstupní zařízení zašle informaci, kdo je neboli svou MAC adresu. Následně authenticator vezme tuto informaci a zašle jí se svou MAC a IP na Authentication Server, například Radius. V tento moment zná ověřovací server informace o klientovi a místu připojení. Radius server vyzve klienta, aby komunikoval po dané šifrované komunikaci, kterou bude znát a umět. Zároveň posílá OTP. Klient přijme dočasné heslo a pomocí něhož zašle na Radius zašifrované přihlašovací údaje. Po jejíž zpracování obdrží akceptační zprávu, která musí být potvrzena od klienta. Následně může dojít k předání certifikátu pro komunikaci.

Obrázek 17 - Radius ověřovací proces

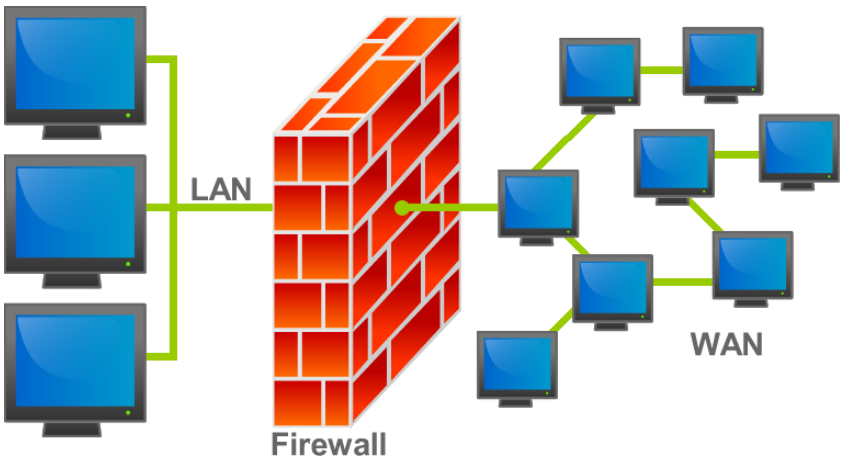


Zdroj: https://mikeguy.co.uk/posts/2018/06/understanding-nac-802.1x-and-mab/

4.4.3 Firewall

Firewall je jednou z nejstarších částí počítačových sítí, která slouží k zajištění větší bezpečnosti. Může se jednat o hardwarové zařízení, nebo softwarové programy. Obě se snaží dosáhnout stejného výsledku, tedy filtrovat a řídit datový provoz. Princip viz obrázek 18 je takový, že firewall má jasně nadefinovaná pravidla, pomocí kterých mají zařízení v síti WAN omezenou možnost komunikace na interní zařízení. Firewall se svou funkčností nemusí řadit v rámci ISO/OSI modelu do jedné vrstvy. Nejprve se jednalo o čistě síťové zařízení, ale vlivem technologického pokroku se začalo zabývat i aplikační částí. Firewall při zpracování dat vyhodnocuje dle daných pravidel bezpečnostních politik zamítnutí, nebo povolení průchodu. Primárním využitím a myšlenkou firewallu je zabránit neoprávněným přístupům do interní sítě, nebe nechtěné komunikace z ní. (35)

Obrázek 18 - Firewall



Zdroj: https://cs.wikipedia.org/wiki/Firewall#/media/Soubor:Firewall.png

Jak již bylo zmíněno výše tento typ zařízení nelze zařadit do specifické vrstvy v rámci ISO/OSI modelu. Jeho rozdělení lze dělit podle mnoha kritérií, se kterými typy dat pracuje, jak s nimi pracuje a jak je zpracovává.

Rozdělení podle funkce:

Paketový firewall jedná se o nejstarší, nejjednoduší typ firewallu. Jeho princim je založen na definování pravidel, které říkají z jaké a na jakou adresu a port je možné komunikovat. V případě že zařízení této funkce obdrží paket, který neodpovídá zmíněnému pravidlu, bude zahozen. Jedním z jeho velkých benefitů je jeho rychlost zpracování dat při vysoce objemové komunikaci. (35)

Stavový firewall se považuje jako síťový filtr druhé generace. V podstatě se jedná o zařízení, které vykonává stejnou práci jako jeho předchůdce s tím rozdílem, že dokáže pakety udržovat v paměti. Jejich uložení závisí na množství informací, které stavový firewall potřebuje k rozhodnutí o jejich zařazení. Zaznamenává všechna spojení a dokáže rozeznávat, jestli se jedná o nové nebo stávající spojení. Jednou z výhod využití tohoto firewallu je možnost nastavovat pravidla průchodu na směr toku dat. (35)

Aplikační brána lze také označovat jako proxy brány. Zcela odděluje sítě mezi které je postavena. Aplikační brány provádí analýzu na aplikační vrstvě. Pro realizaci takové úrovně ochrany musí firewall aktivně naslouchat v rámci probíhající komunikace, jako prostředník. Žádné zařízení tedy na přímo nekomunikuje se požadovaným cílem, ale s aplikační bránou. V rámci tohoto řešení tedy vznikají dvě nezávazná spojení klient-proxy a klient-cíl. Samotná komunikace může byt odmítnuta podle předem definovaných pravidel, jako například v rámci http, nebo https protokolu URL. (35)

Next-Geneneration Firewall (NGFW) jedná se o třetí generací technologie tohoto typu. Kombinuje klasické funkce předchozích generací s jinými síťovými zařízeními, jako je hloubková inspekce paketů (DPI), kontrola šifrování TLS/SSL, správa identit třetích stran LDAP a další. Tato generace zařízení přistupuje k informacím, jako k datům nad kterými jsou tvořeny statistiky a jejich odchylky jsou považovány jako potenciální hrozba. (35)

4.5 Aplikační bezpečnost

Jedná se o segment procesů, nástrojů a postupů, jejichž cílem je chránit aplikaci před kybernetickým útokem po celou dobu životního cyklu aplikace. Útočníci jsou organizovaní a motivovaní k tomu, aby našli a využili zranitelnosti podnikových aplikací ke krádeži dat, duševního vlastnictví a citlivých informací. Zabezpečení aplikací může organizaci chránit všechny druhy aplikací od mikro služby, webové aplikace a samotné programy. Velké množství úspěšných narušení interního prostředí se zaměřuje na zneužití nacházejících se v aplikační vrstvě. V této části je rozebrána čistě aplikační vrstva. Některá témata lze ve společnosti aplikovat na globální nastavení bezpečnosti. (36)

4.5.1 Tier model

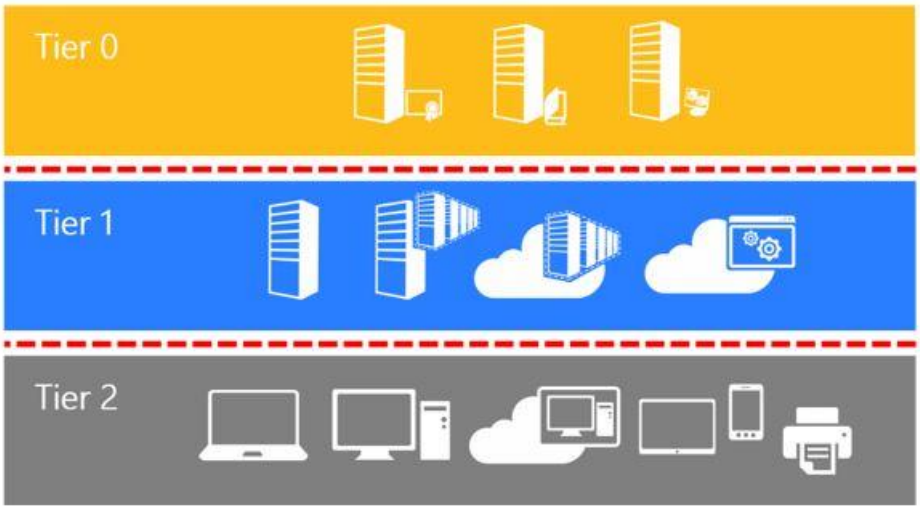
Využívají se za účelem pro zvýšení bezpečnosti rozdělení kritických zařízení. Model se definuje pomocí 3 úrovní. Zařazení jednotlivých zařízení vychází z posouzení bezpečnostního dopadu při kompromitaci objektů v jednotlivé vrstvě. Pro každou jednotlivou vrstvu by měl být vytvořen jedinečný účet pro administraci konkrétní vrstvy. Hlavní snahou je zabránit vertikálního pohybu šíření kompromitace neboli zabránit kompromitaci zařízení nebo uživatelských účtů ve vyšších vrstvách Tier modelu. Znázornění dělení Tier modelu je zobrazeno na obrázku 19

Tier 0 – je nejvyšší úroveň, která obsahuje vysoce senzitivní servery, jejichž kompromitací dojde automaticky ke kompromitaci celé domény. Dále obsahují administrativní účty a skupiny, které mají přímé nebo nepřímé administrativní řízení AD. Administrátor Tier 0 může kontrolovat log ve všech úrovní, ale může se přihlásit jen ve svém úrovni.

Tier 1 – je určen pro servery a aplikace členů domény, jako FileShare, tiskové řešení, centrální správa koncových zařízení, nebo cloudové služby. Tyto účty mají přístup k citlivým datům. Může kontrolovat aktiva v Tier 1 a 2. Mohou sledovat log (síťový log) na Tier 0 a 1, ale může se přihlásit pouze na Tier 1.

Tier 2 – řízení uživatelských stanic. Zařízení v Tier 2 mají administrativní kontrolu nad významnou část obchodních hodnot na pracovní stanici (př. Helpdesk a admin PC). Mohou ovlivnit integritu uživatelských dat. Mohou sledovat aktivity a přihlásit se pouze na své úrovni. (37)

Obrázek 19 - Tier model



Zdroj: https://docs.microsoft.com/cs-cz/security/compass/privileged-access-access-model

Podle Tier modelu mohou být rozděleny také systémy, ke kterým je přistupováno přes Jump servery, které spadají do specifické úrovně jako daný systém. Samotný Jump server má poté omezenou síťovou komunikaci pouze na zařízení v daném Tieru a zároveň by měl být vyčleněn do definované podsítě ve které mohou být jen zařízení stejné úrovně.

4.6 Zabezpečení aplikací

Jedno z možností vstupu do interního prostředí jsou koncové zařízení, které využívají především běžní uživatelé. Z tohoto pohledu se jedná o vysoce rizikový bod pro každou společnost, jelikož ne všichni mají stejné znalosti v rámci bezpečnosti, a tudíž schopnost rozeznávání rizik je rozdílná. Z toho důvodu se jedná o jeden z nejdůležitějších bodů co nejvíce eliminovat lidský faktor, který by mohl jakkoli ovlivnit lokální prostředí.

Samotné zabezpečení koncových stanic lze testovat podle tzv. „bezpečnostní benchmark“. Jedná se o porovnání globálně známých bezpečnostních standardů, která lze implementovat v téměř každém standardním prostředí. Jedním z tvůrců těchto „benchmarků“ je Centrum pro Internetovou Bezpečnost (CIS). Tato společnost se zabývá propagací spolehlivých postupů v rámci kybernetické bezpečnosti. Pomocí tohoto nástroje jsou porovnány nasazené politiky v rámci lokálního prostředí a zároveň jsou zhodnoceny třetí stranou. (38)

Windows hardening by se měl zabývat:

- Vstupními politikami – Týkajících se účtů, jako délka hesla a jeho komplexnost, perioda jeho změny, nebo samotná blokace účtu.
- Zásady auditních systémů – Všechny politiky vztahující se k zaznamenávání a zapisování událostí. Jaké informace se mají ukládat, kde mají byt uloženy, jak dlouho a kdo k nim má přístup.
- Možnosti zabezpečení – jedná se o obecnou část kde jsou definovány veškeré změny pro zvýšení bezpečnosti jako blokace účtu „Guest“, omezení určitých protokolů a další.
- Uživatelská práva – definují možnosti uživatele, co všechno vidí, ke kterým souborům, zařízením má přístup.
- Lokálního Windows Firewall – v rámci systému lze zablokovat veškerou příchozí komunikaci, nebo definovat které obecně známe protokoly, budou moc skrze něj komunikovat.

Při zabezpečování by se nemělo jednat pouze o operační systém, ale o veškeré aplikace a systémy, které jsou součástí koncového zařízení. Většina z těchto částí umožňují definovat zásady bezpečnosti. Proto je velice důležité počáteční zaměření na segmenty, které využívá většina uživatelů jako je již zmíněný OS, ale také i prohlížeč internetu. (39)

Internetový prohlížeč umožňuje aplikačnímu správci zasahovat do obecného nastavení, ale také do bezpečnostních politik. V rámci internetových prohlížečů jako Google Chrome lze definovat velké množství těchto politik. Je možné vycházet z bezpečnostních standardů, které poskytuje CIS. Pro prohlížeče je možné definovat politiky pomocí zápisů do registrů, kde se mohou určovat body.

Níže je pouze část možných bodů nastavení.

- Z jakých domén lze spustit audio, nebo video
- Umožnovat vyskakování pop-up
- Z jakých stránek je možné stahovat JavaScript
- Jakým stránkám povolovat ukládání cookies
- Jaké šifrovací protokoly používat
- Zdali uživatel může ukládat heslo, nebo PIN do prohlížeče

4.6.1 Systémové nástroje

Sysmon je systémová služba a ovladač zařízení Windows a lze jej využít v omezeném rozsahu pro Linux. Tento monitorovací systém po instalaci je neustálou součástí systému i po jeho restartu. Vlivem čehož je schopný monitorovat a zaznamenávat aktivitu systému do protokolu událostí v rámci OS. Může nabídnout informace o vytvořených procesech, síťových připojení, změnách a časech prací se soubory. Tento nástroj slouží pro rozšíření standardního sběru informací pro zvýšení dostupnosti informací při forenzní analýze. Sysmon může zaznamenávat procesy, záznam hash z otisků souborů, záznamy načítání ovladačů, knihoven DLL s jejich popisem a hash, volitelně zaznamenává síťová připojení a další možnosti nastavení. Samotný nástroj netvoří žádné analýzy události a ani není nijak skrytý v systému. Jedná se pouze o rozšíření pro běžné zaznamenávání informací. Jednotlivé události mají své identifikátory od 1 do 26 a jedno dodatkové číslo 255 označující chybu, kdy každá znamená jinou událost.

Značení Identifikátorů:

- Event ID 1 – Vytvoření procesu
- Event ID 2 – Proces změnil časové razítko souboru
- Event ID 3 – Šítové připojení
- Event ID 4,5 – Změna služby Sysmon
- Event ID 6 – Ovladač načten
- Event ID 7 – Načtení obrazu
- Event ID 8 – Vytvoření vlákna v jiném procesu

- Event ID 9 – Proces provádí operaci čtení z jednotky pomocí označení \\.\.
- Event ID 10 – Pokud proces otevře jiný proces
- Event ID 11 – Událost vytvoření
- Event ID 12,13,14 – Tyto ID soubisejí s událostmi v registrech OS
- Event ID 15 – vytvoření hash souborového strému
- Event ID 16 – Změna konfigurace systému
- Event ID 17,18 – Události s Pipe
- Event ID 19,20,21 – Události vztahující se k WMI
- Event ID 22 – DNS záznamy
- Event ID 23 – Soubor smazán
- Event ID 24 – Clicboard změny
- Event ID 25 – Manipulace s procesem
- Event ID 255 – Chyba

Nástroj ve výchozím nastavení zaznamenává úplně veškeré informace, které operační systém vygeneruje. Z toho důvodu se může stát nepřehledným nástrojem, a proto je dobré upravovat samotné nastavení, ve kterém se specifikuje co se má sledovat. Lze sledovat všechny spuštěné procesy, které lze omezit o specifické systémové procesy. Zároveň lze zaznamenávat komunikaci na určité síťové porty a IP adresy. Každý identifikátor lze nastavit specifický filtr, který bude Sysmon sledovat, nebo jej úplně vynechat pro zatížení výkonu zařízení. Samotná konfigurace je zaváděná pomocí souboru XML, který má definovanou strukturu viz obrázek 20. (40)

Obrázek 20 - Sysmon konfigurační soubor

```
<Sysmon  schemaversion="3.2">
  <!-- Capture all the hashes -->
  <HashAlgorithms>*</HashAlgorithms>
  <EventFiltering>
    <!-- Log all drivers except if the signature -->
    <!-- contains Microsoft or Windows -->
    <DriverLoad onmatch="exclude">
      <Signature condititon="contains">microsoft</Signature>
      <Signature condititon="contains">windows</Signature>
    </DriverLoad>
    <!-- Do not log process termination -->
    <ProcessTerminate onmatch="include"/>
    <!-- Log network connection if the destination port equals 443 -->
    <!-- or 80, and the process isn't InternetExplorer -->
    <NetworkConnect onmatch="include">
      <DestinationPort>443</DestinationPort>
      <DestinationPort>80</DestinationPort>
    </NetworkConnect>
    <NetworkConnect onmatch="exclude">
      <Image condition="end with">iexplore.exe</Image>
    </NetworkConnect>
  </EventFiltering>
</Sysmon>
```

Zdroj: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

AppLocker je systémový nástroj od společnosti Microsoft, který je součástí operačních systému od verze 7. Tento nástroj je dostupný pro systémy od systému Windows Pro. Samotný nástroj slouží ke správě aplikaci. AppLocker napomáhá definovat pravidla na základě atributů, která přetrvávají napříč aktualizacemi. Pravidla mohou být tvořena na základě produktu, verze souboru, názvu, nebo cestě v adresáři. Tento nástroj aktivně může zasahovat do nastavení systému a z toho důvodu se nejdříve vychází s možností audit, ze které je patrné, jaký bude mít vliv na celý systém. AppLocker řeší zabezpečení aplikací

- Inventuru aplikací – v rámci režimu audit, kde je veškerá aktivita využití aplikací zaznamenávána do registru aplikací. Z těchto dat lze dělat sumarizace systémových aplikací.
- Ochranu před nechráněnou aplikací – Skrze tento systém lze zabránit spouštění aplikací, které nespadají do seznamu povolených aplikací.
- Licenční shody – pomocí pravidla, lze zamezovat spuštění nelicencovaných softwaru.
- Standardizaci softwaru –Nástroj lze nastavit tak aby umožnoval spouštění pouze podporovaných nebo schválených aplikací.

Pro tento nástroj je velice důležité, aby měla společnost připravený tzv. „Whitelist aplikací“, který definuje přesnou sadu aplikací, který daný uživatel může používat. Tento list se následně aplikuje v AppLockeru a je zamezeno instalaci a spuštění programů třetích stran, které by mohli ohrozit chod počítače. I tento nástroj lze obcházet, podle typu jeho nastavení. Pakliže jsou výjimky nastavovány pouze na název programu, tak stačí útočníkovy přejmenovat svůj soubor. (41)

Bitlocker je funkce ochrany dat, která je integrovaná s operačním systémem Windows již od verze Vista. Především je využívána jako prevence ztráty dat při krádeži zařízení, nebo proti získávání hesel z disku po jejich odpojení. Pro větší bezpečnost se doporučuje použití s modulem TPM (Trusted Platform Module) s minimální verzí 1.2, ale u posledního vydání operačního systému Windows 11 je vyžadována verze 2.0. Samotný TPM čip je hardwarová součástka na základní desce počítače, která chrání uživatelská data při vypnutém stavu. Bitlocker umožnuje více faktorové ověření, které může být v kombinaci s pinem anebo klíčem na USB disku. (42)

Auditd je démon s jehož pomocí, lze rozšířit množství informací, které lze ukládat v rámci operačního systému Linux. Pomocí tohoto systému lze definovat pravidla pro sledování nejen administrátorských kroků v rámci systému. Tento auditní démon nezvyšuje bezpečnost zařízení, ale zvyšuje vizibilitu v rámci systému ke sledování jakéhokoli porušení bezpečnostních rizik. Auditd funguje na úrovni jádra, takže má přístup ke všem službám. Zároveň je k dispozici pro většinu distribucí Linuxu. Veškeré změny v rámci nastavení auditingu se upravují v souboru cesty „/etc/audit/audit.conf“. Auditd se zaznamenává události podle předem definovaných pravidel tato pravidla jsou upravována v cestě „/etc/audit/audit.rules“. Pravidla mají syntaxi následující.

-a akce,seznam -S systémové volání -F pole=hodnota -k název klíče

Přepínač „-a“ sděluje jádru, že chce přidat pravidlo na konec seznamu pravidel. Následuje akce, ve které je informovaný démon, jestli chceme vytvořit, nebo nevytvářet událost při sepnutí daného pravidla. Akce a seznam jsou odděleny čárkou. Platné údaje seznamu jsou úkol, záznam, ukončení, odebrání a uživatel. Dalším přepínačem „-S“ definuje systémové volání. Toto volání může být buď jméno nebo číslo, která se hlídají na úrovni jádra. Přepínačem „-F“, jenž definuje, proti čemu se má porovnávat. Na závěr přepínač „-k“ definuje přístup. (43)

4.7 Systémy pro zvýšení bezpečnosti

Komplexnost zabezpečení pomáhá organizaci přidávat nová zařízení, aplikace a služby, aniž by došlo k poškození interní infrastruktury. I když se zabezpečení nespoléhá na jedinou metodu a využívá řadu bodů k ochraně citlivých informací, stále má určité mezery, které zabraňují detekci pokročilých útoků. Organizace se proto nemohou při ochraně svých důležitých interních informací spoléhat pouze na neduplicitní prvky zajišťující určitý stupeň bezpečnosti. Systémy zvyšující bezpečnost se částečně překrývají čímž vzniká kaskáda nezávislých systému, které při selhání jedné části mohou chránit kritická data před širokou škálou útoků. (44)

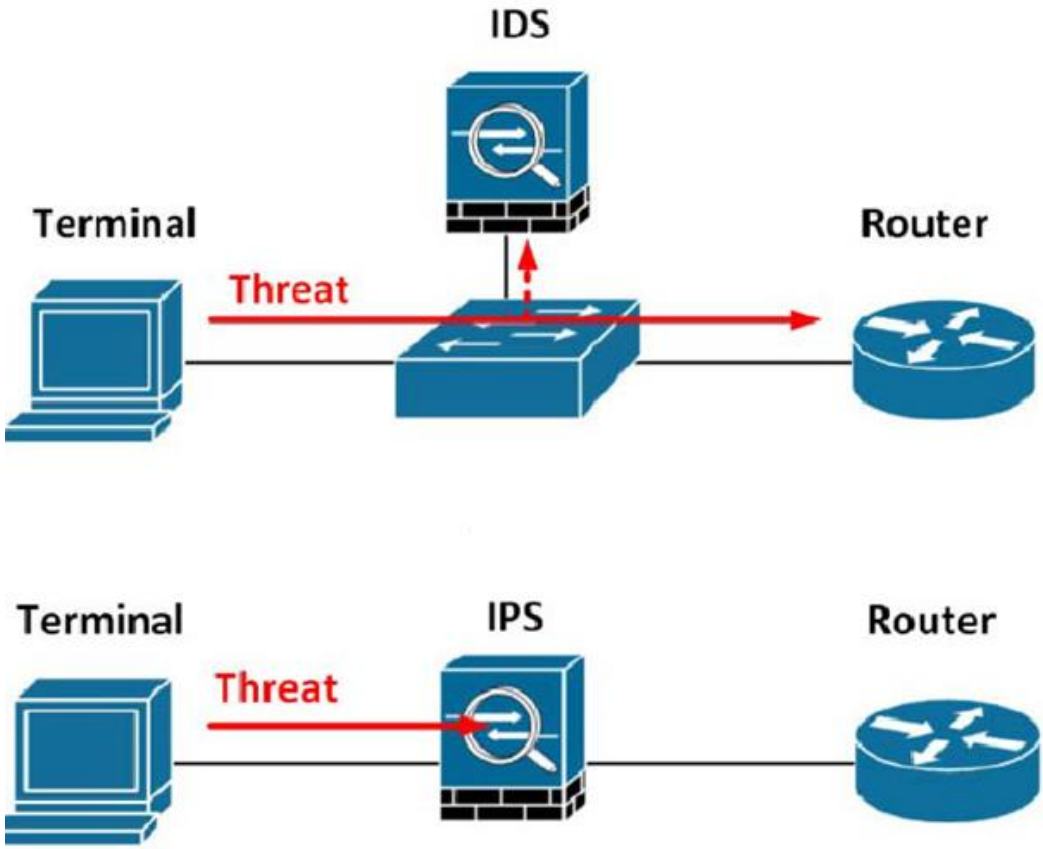
4.7.1 Detekční nástroje

Intrusion Detection System, jedná se o obraný sytém, který monitoruje síťový provoz a snaží se odhalit podezřelé aktivity podle předem definovaných signatur. Hlavní činností IDS systému je pasivní naslouchání síťové komunikace, kdy tyto záznamy procházejí analýzou, ze kterých mohou být vyvozeny neobvyklé aktivity. Detekované

případy mohou vést k narušení bezpečnosti v operačním systému, nebo počítačových sítí. Tento systém nemusí zjišťovat pouze daný typ útoku, ale i detekci akcí, které jim předcházejí, jako je skenování portů. Tento typ zařízení bývá uložen na přechodovém uzlu dané sítě, kde sbírá data pomocí tzv. port mirroringu, neboli zrcadlení provozu. Což znamená, že veškerá komunikace, která projde přes dané zařízení prochází bez omezení přes daný prvek a zároveň se stejná data posílají na IDS. Z tohoto vyplývá, že se jedná o pasivní systém, který nijak nezasahuje do provozu. (45)

Intrusion Prevention System je forma zabezpečení sítě, která slouží k detekci a prevenci hrozeb. IPS nepřetržitě monitoruje síťový provoz a na rozdíl od IDS, data procházejí přímo přes dané zařízení, což znamená, že může fyzicky zasahovat do provozu. Zároveň se zvyšuje riziko ztráty dat, jelikož se jedná o systém, přes který musí data procházet. Tudíž se využívá duplicita IPS. IDS/IPS mají stejné vyhodnocovací metody, jediným rozdílem je že IDS nemohou nijak zasahovat do provozu viz obrázek 21. Systémy pro prevenci a detekci možných bezpečnostních hrozeb je mnoho jako Fidelis, Flowmon, z open-source Snort, Suricata. (45)

Obrázek 21 - IDS/IPS systémy



Zdroj: https://www.semanticscholar.org/paper/The-security-of-RFID-readers-with-IDS%2FIPS-solution-Zitta-Neruda/ad48f02230257a5a8e344ceae576e4c549e3b8a3

Detekce mohou být prováděny na základě anomálií, kdy si systém zaznamenává nejrůznější data, ze kterých využívá statistické údaje, se kterými dále může pracovat v samotném prostoru. Tento typ detekcí, tedy nelze využívat od počátečního spuštění systému, jelikož systém musí nejprve nasbírat dostatečné množství dat, aby následně mohl vyhledávat odchylky v provozu. Pravidla na anomální chování mohou sledovat využití jednotlivých síťových protokolů, jako DNS, SMTP, kde mohou vyhodnocovat množství dat odeslaných skrze tento protokol, využití daného protokolu ke komunikaci na jiný zdroj. Dále lze vyhodnocovat obecný přenos dat, zatížení jednotlivých portu a další.

Detekce probíhá na základě pravidel. IDS i IPS systémy obsahují svá integrovaná pravidla, která sledují obecné hrozby po síťové komunikaci, nebo pro operační systémy koncových zařízeních. Dále mohou sledovat specifické zranitelnosti, které mají signifikantní ukazatel svého chování. Tento typ vyhodnocování je založený na analýze dat s databází známých vzorů hrozeb. V rámci tohoto se klade velký důraz na aktuálnost těchto zdrojů. Zároveň tyto systémy umožnují tvorbu vlastních pravidel, která mohou být specifická pro určité prostředí. (45)

Suricata byl vyvinut OISF, kdy první beta verze vyšla roku 2009. Může být nastavena do modu prevence IPS, tak i detekce IDS. Systémově jí lze využívat s grafickou i bez grafické nadstavby. Samotná Suricata je dostupná napříč platformami Windows OS, MacOS a Linux. Systém dokáže zpracovávat aplikační protokoly typu TLS, SSL, SMB, SMTP, FTP, SSH nebo DNS a další. Na nižších vrstvách se může jednat o IP verze 4 a 6, TCP, UDP, ICMP a další. Detekce samotných protokolů nevychází z obecně známých portů, ale ze samotného provozu. Detekční část rozezná provoz přes HTTP i přes to, že komunikace nebude na port 80. Pro generaci bezpečnostních upozornění Suricata potřebuje mít definovaná pravidla. Pravidlo se skládá ze 3 částí:

- **Akce** – co se stane, když popis odpovídá. Může se jedna podle o alert, zahození, odmítnutí a další. Proaktivní akce jako zahození a odmítnutí lze využívat pouze u IPS.
- **Hlavička** – definuje protokol, IP adresy, porty a směr komunikace.
- **Options** – definuje specifikace co přesně v dané komunikaci hledáme. V této části mohou být obsaženy informace o popisu, identifikátoru bezpečnostní hrozby a v jaké části dat se mají hledat signifikantní prvky.

Může se jednat například o takovýto tvar pravidla:

```
alert http any any -> any any (http_response_line; content:"403 Forbidden"; sid:1;)
```

Popis: Vygeneruj alert, který je z http provozu a nemá síťové omezení. V těchto datech hledej odpověď na dotaz „403 Forbiden“. Toto pravidlo má identifikátor 1. (46)

4.7.2 SIEM

Security Information and Event Management je přístup ke správě zabezpečení, které kombinuje funkce bezpečnostních informací a událostí. Základním principem každého podobného nástroje je agregovat data z více zdrojů, identifikovat odchylky od normy. Na nejzákladnějších úrovních může být SIEM založený na pravidlech, nebo může použít statistiky korelační model. Pokročilé systémy, nebo jejich doplňky se vyvinuly tak, aby zahrnovaly analýzu chování uživatelů UEBA.

Prakticky se může jednat o zařízení, které přijímá logy ze všech zařízení, jako firewall, switch, OS a další. Tyto záznamy jsou odesílány na takzvané kolektory, které si informace rozdělují, indexu a ukládají. Nad těmito všemi daty mohou být prováděny korelace, které hledají znaky chování, jež by mohli vést k porušení bezpečnostních předpisu daného podniku. Při takovémto vyhodnocení jsou vygenerovány upozornění, aby daný užívat, nebo správce mohli danou událost zkontrolovat. (47)

4.8 Bezpečnostní standard NIST

Národní institut standardů a technologií (dále jen NIST) je vládní agentura vyvíjející technologie, metriky a standardy pro podporu inovací hospodářské konkurenceschopnosti v organizacích. NIST vytváří standardy a směrnice, které pomáhají splnit požadavky federálního zákona o řízení bezpečností informací (FISMA). Pokyny od této společnosti poskytují doporučení bezpečnostní kontroly pro informační systémy. Tyto doporučení jsou navržena pro přísná bezpečnostní opatření, které jsou publikovány s názvem SP-800. NIST poskytuje framework pro kybernetickou bezpečnost. Jedná se o soubor pokynů a osvědčených postupů. Rámec těchto doporučení kategorizuje veškeré činnosti v oblasti kybernetické bezpečnosti do 5 základních funkcí.

- **Identifikace** – tento bod pomáhá společnostem v rámci řízení rizik, pro stanovení hrozeb a následné stanovení priorit v souladu se strategií řízení rizik. Mezi zásadní činnosti v této skupině patří identifikace fyzických a softwarových aktiv, identifikace zranitelností, stanovení strategie řízení a identifikace právních a regulačních požadavků.
- **Obrana** – popisuje vhodná ochranná opatření v závislosti typu poskytovaných služeb a podporuje omezení dopadu potenciální události. Do této skupiny se vztahuje správa identit, řízení nejen fyzického přístupu v rámci organizace, zavádění ochrany dat pro obranu důvěry integrity a dostupnosti, procesy týkající se správy ochrany informačních systémů.
- **Detekce** – popisuje detekci potenciálních kybernetických incidentů s včasnou dobou zachycení. Činnosti v této části zahrnují detekce anomálií, plán navrhující možnosti nepřetržitého monitorování událostí vztahující se ke kybernetické bezpečnosti.
- **Reakce** – tato část se zaobírá vhodnou aktivitou v případě přijetí opatření na základě zjištění bezpečnostního incidentu. Tímto bodem se omezuje možný dopad daného incidentu na celé prostředí. Reakční část se zaměřuje na procesy během a po kybernetickém incidentu, řízení komunikace, analýza incidentů pro zajištění efektivní reakce, nastavení minimální doby reakce.
- **Obnova** – jsou plány zaměřující se na částečnou nebo plnou obnovu jakýchkoli schopností nebo služeb, které byli narušeny v důsledku kybernetického bezpečnostního incidentu. Zde je kladen velký důraz na včasné obnovení normální provozu, aby se snížil dopad na organizaci. Body zahrnuté v posledním bodu se částečně překrývají s reakčním bodem. Jsou zde obsaženy procesy a postupy plánování obnovy systémů, zavádění vylepšení na základě zjištěných poznatků z testování obnovovacích procesů a samotná interní a externí komunikace bezpečnostního incidentu.

Rámec těchto bodů slouží k hodnocení vyspělosti dané společnosti, kdy daná organizace může dosahovat určitých úrovní, které NIST definuje od nejhoršího po nejlepší. První úroveň je nazvána jako „částečný“, kdy daná společnost nemá plnou viditelnost v síti. Druhou úrovní je informovaný, která je stanovena komplexní viditelností v reálnem čase. Předposledním variantou je opakovatelná úroveň vychází z předchozí úrovně a zároveň zpracovaná její data, jenž následně integruje do pracovních postupů. Nejvyšší bodem je úroveň adaptivní, což znamená, že společnost je na nejlepší možné úrovni zabezpečení. (48)

5. Praktická část

V rámci praktické části je pospán v kapitole 5.1 – popis společnosti stav před touto diplomovou prací. Z popisu je patrné, že se jedná o síťovou infrastrukturu ve velmi špatném stavu.

Praktická část je rozdělena do dvou hlavních částí. Prvním bodem je popis společnosti, druhá část se zaměřuje na téma bezpečnostní analýzy rizik a posledním bodem je návrh zabezpečení a jejich implementace.

1. Popis společnosti
2. Analýza bezpečnostních rizik
    - Sběr informací
    - Testování
    - Vyhodnocení
3. Návrh zabezpečení a implementace
    - Návrh zabezpečení
    - Implementace

Základní postup hodnocení rizik standardně zpracovává odborný zaměstnanec, jenž se danou problematikou zabývá. Hodnocení vychází z důvěryhodnosti, integrity a dostupnosti. Pro stupeň rizika je využita dopadová tabulku 1, která se skládá ze čtyř úrovní. Jednotlivé hodnoty jsou zastoupeny maximálním rozsahem 1 až 5, kdy nejmenší číslo znamená nejnižší stupeň ohrožení. Výsledná hodnota rizika může nabývat hodnoty od 1 do 125, kdy nejvyšší hodnota je označena jako kritická. Pro analýzu rizik je využit následující vzorec na základě: (48)

$$Riziko = Hrozba \cdot \frac{Zranitelnost}{2} \cdot Dopad \qquad (1)$$

,kde: *Dopad* – tato hodnota určuje, jaký je dopad na provoz při částečném nebo úplném omezené dané služby, nebo zařízení. Zároveň také hodnotí důvěryhodnost, integritu a samotnou dostupnost. Hodnocené parametry se mohou upravovat v případě specifičnosti hodnoceného. Standardně hodnotu dopadu určuje správce dané aplikace, nebo zařízení.

Hrozba – je skutečnost, událost, síla nebo osoba, jejichž působení může vést k poškození, zničení. Hrozby se rozdělují podle úmyslu, zdroje a aktivity. Úmyslné hrozby mohou být náhodné, nebo neúmyslné. Náhodné hrozby nelze predikovat. V případě že se jedná o naplánovanou aktivitu, je označena jako úmyslná hrozba. Hrozby dělené podle zdroje jsou vnitřní a vnější dle jejich působení. Posledním parametr vychází z aktivity, kdy se zohledňuje, zdali se jedná o aktivní, nebo pasivní hrozbu vedoucí ke změně stavu systému v důsledku narušení integrity a dostupnosti. Hodnotu hrozby standardně určuje z dostupných informací architekt sítě s bezpečnostním pracovníkem.

Zranitelnost – je slabé místo, které může být zneužito skrze veřejně publikované zranitelnosti. Jednotlivé zranitelnosti se hodnotí dle CVSS, jenž může nabývat hodnot 0 až 10. Výsledná hodnota je stanovena nejvýše ohodnocenou zranitelností ze všech prvků, na kterých byl prováděn test.

Návrh a analýza zabezpečení pracuje se zprávou z předchozí části útoku. Hlavním motivem je zabezpečit prostředí před replikací typově podobného fyzického útoku. Při návrhu se bude pracovat i s částí, kde jsou popsány teoretické možnosti vniku do sítě. Po zhotovení návrhu budou tyto části implementovány do prostředí. Jejich správnou funkčnost ověří simulace tohoto útoku. Čímž by mělo dojít ke zvýšení zabezpečení interního prostředí.

Tabulka 1 - Hodnocení rizik

Úroveň	**Stupnice**	**Popis**
Nízké	0 až 5	Akceptovatelné riziko.
Střední	6 až 29	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.
Vysoké	30 až 65	Riziko je z dlouhodobého pohledu neakceptovatelné. Musí být stanoven plán systematického odstranění. Případnou akceptaci rizika schvaluje vedení společnosti.
Kritické	66 až 125	Jedná se o neakceptovatelné riziko. Musí vést k okamžitému postupu odstranění, nebo jeho ukončení služby/zařízení.

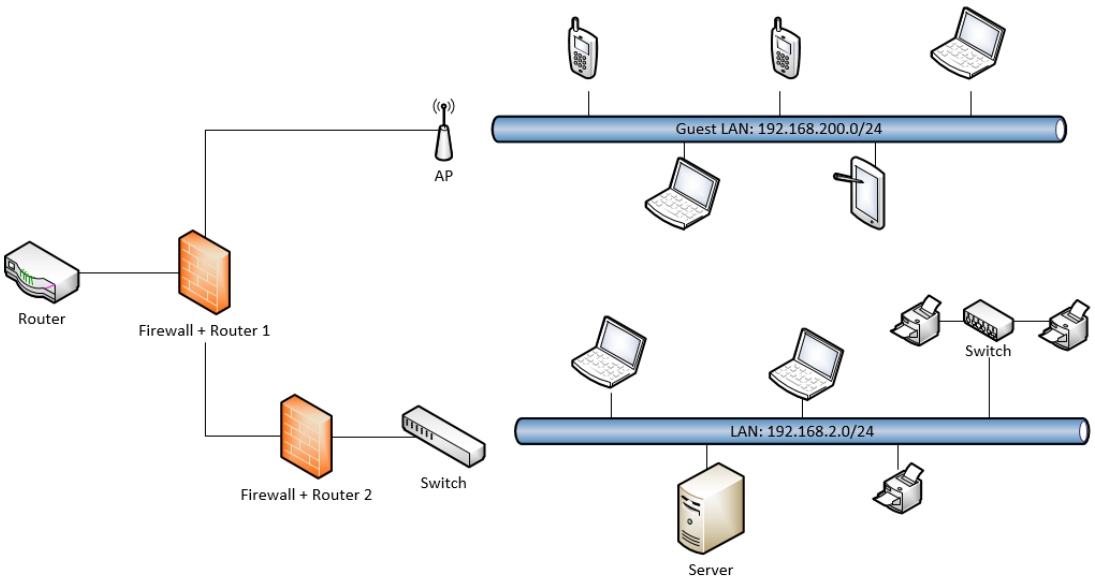
Zdroj: Vlastní zpracování na základě (48)

5.1 Popis společnosti

Společnost, pro kterou byl vytvořen tento test lze označit, jako malou neziskovou organizaci z pohledu fyzických zařízení, ale střední z pohledu počtu zaměstnanců, která má ve svém pronájmu dvoupatrovou budovu, kdy přízemí je využito pro sklad. V druhém patře jsou kanceláře, které jsou rozděleny podle jednotlivých oddělení a podle pracovního využití. V každé z těchto místností jsou obsaženy IT zařízení spadající pod správu místního správce sítě. Samotná pozice IT správce je v této společnosti brána, jako osoba, která se stará o všechny technické záležitosti vztahující se nejen k informačním technologiím. Do pracovní náplně spadají části fyzické bezpečnosti, udržovaní provozuschopnosti všech zařízení a běžná správa všech prvků. V samotné společnosti je zaměstnáno přibližně 25 lidí, kteří navštěvují z velké části v rámci svého pracovního výkonu fyzicky společnost a dalších 20 lidí, kteří nepotřebují, nemusí nebo nemohou vykonávat svou práci z budovy.

Základní popis sítě a zabezpečení je vyobrazen na obrázku 22. Síť je rozdělená na veřejnou a interní. Kdy na veřejnou síť se mohou připojovat hosté, ale také zaměstnanci s vlastním i firemním zařízením.

Obrázek 22 - Topologie sítě



Zdroj: Vlastní zpracování

V rámci lokální sítě se vyskytují síťové směrovací prvky. Jedná se o tří zařízení, kdy každé z nich je vyrobeno odlišným výrobce. Router ZTE H267A je nastaven ve výchozím nastavení, kdy byly upraveny pouze části DNS, DHCP, LAN síť. Samotné nastavování se může zprostředkovat skrze jakoukoli stanici v rámci interní sítě

přes libovolné webové rozhraní na protokolu HTTP. Lokální síť má nastavenou masku sítě pouze pro 2 zařízení. Veškeré fyzické porty jsou v provozu, ale aktivně je využit pouze jeden. Druhý routerem v kaskádě je směrovač od společnosti TP-Link TL-R600VPN, ke kterému je připojen Mikrotik a Cisco router, který je využíván pouze jako AP, jenž je využito pro připojení hostů na Wi-Fi a 3 koncová zařízení v místnostech pro konzultace. Tento prvek je nastaven jako DHCP server a Firewall. V rámci Firewallu jsou blokace na základní typy útoků, jako UDP-FLOOD, UDP-FLOOD, TCP-SYN-FLOOD, SPI Firewall a nejsou zde nastaveny žádné interní politiky. Veškeré nastavení bylo ponecháno ve výchozím nastavení, samotná správa zařízení je dostupná ze všech zařízení skrze webový prohlížeč na portu 80, který je využit protokolem HTTP. Tento prvek má obsazeno všech 5 svých portů. Posledním směrovačem je Mikrotik RB750Gr3, kde je velice podobné nastavení jako u předchozích zařízení, kdy jeho správa je dostupná přes HTTP ze všech stanic. V rámci nastavení jsou povoleny všechny možnosti připojení telnet, SSH, WinBox a HTTP. K routeru je napojen switch a tiskárny. Bezdrátový přístup pro hosty obstarává Wi-Fi, kterou zajišťuje AP od společnosti Cisco RV215W. Samotná Wi-Fi je nastavená jako veřejně viditelná s automatickým přidělováním kanálu a jedním SSID, byla nastavena verze zabezpečení WPA2-PSK s šifrováním AES. Bezdrátový přístupový bod neobsahuje filtr, který by umožnoval spravovat přístupy připojených zařízení. Všechny fyzické porty na tomto zařízení nejsou obsazeny, ale i přesto jsou všechny zapnuté. Aby klienti obdrželi IP adresu, tak má AP nastaveno vlastní DHCP, zároveň je zde zapnut firewall ve výchozím nastavení. Samotná administrativní správa je dostupná klientům přes HTTP. Pro celou budovu je využit pouze jeden AP. Veškeré L2 síťové prvky jsou switche bez možnosti správy, jenž zprostředkovávají připojení tiskáren a zařízení.

Ve společnosti se nachází 24 počítačů (z toho polovina desktop a druhá polovina notebook) a 3 tiskárny. Počítače jsou rovnoměrně rozděleny po kancelářích. Část z těchto zařízení neobsahují minimální hardwarové požadavky pro případné povýšení licence z Windows 10 na 11, a to například TPM verze 2. Aktuálně dochází k postupné inovaci celého prostředí čímž se eliminuje tento problém. V rámci celého prostředí je využit operační systém od společnosti Microsoft a to Windows 10 ve verzi Profesionál. Samotný BIOS na všech zařízeních je volně přístupný bez hesla. Systém obsahuje pouze 2 účty, a to pro administrátora a uživatele. Jelikož se nerozlišuje mezi uživateli, tak pro celé prostředí je pouze jeden uživatelský účet se stejným heslem, a to samé platí i pro administrátorské oprávnění. Uživatelé využívají základní sadu aplikací MS office,

prohlížeče, Adobe, 7-zip, Keepass a někteří uživatelé využívají 3 specifické programy pro neziskové organizace, kdy některé z nich využívají Javu. Jeden z těchto programů je tvořen přímo pro danou společnost. Aplikace jsou všechny ve výchozím nastavení a nejsou nijak upravované. Na každé stanici je součástí antivirový program od společnosti Eset Endpoint Antivirus 8.0.2039.3. Přes počítače lze využívat všechna externí zařízení skrze USB porty. Samotný operační systém má zapnuté automatické aktualizace, a to samé platí i pro antivirový systém. Tiskárny mají administrátorské prostředí dostupné ze všech lokálních stanic a přístup je přes HTTP. Tiskárny jsou chráněny heslem. Jedna z tiskáren má přístup na server pro ukládání dat ze scanneru.

Aktuálně je využit server běžící na zařízení, které bylo odebráno z provozu jako nedostačující. Jedná se o notebook s operačním systémem Linux distribuci CentOS. Souborový server je založený na Samba serveru, který dle základních politik rozděluje kořenový adresář na IT a Provoz. Běžní uživatelé mají přístup na všechny adresáře v části provoz.

Fyzickou bezpečnost v rámci budovy zajišťuje zabezpečovací systém od společnosti Jablotron. Páteřním bodem celého zabezpečení je ústředna, na kterou jsou napojeny prvky jak bezdrátové a metalické vedení, které mají zvyšovat bezpečnost budovy. K ústředně jsou připojeny pomocí kroucené dvoulinky magnetické spínací kontakty pro sledování otevření oken. V každé místnosti a průchodové chodbě jsou pohybové senzory, které jsou napojeny bezdrátově. Stejným způsobem jsou zapojeny senzory, které detekují zvuk možného tříštění skel. Zabezpečovací systém uživatelé spouští pomocí pinu, který znají všichni a má pouze jednu variantu.

Místnost sloužící pro uchování nejen všech síťových prvků a serveru, slouží také pro uchování části skladových věcí pro provoz. Lokalita této místnosti je uprostřed budovy v místnosti bez oken s jedním přístupem. Tímto vstupním bodem jsou myšlené běžné vstupní dveře zabezpečené běžným zámkem. V této části objektu není umístěn samotný server, který společnost využívá. Server je alokován v uživatelské kanceláři jednoho oddělení v rackové skříni.

5.2 Analýza bezpečnostních rizik

Pro získání hodnoty zranitelnosti do vzorce 1, je důležité ověřit v prostředí obsahující zranitelnosti. Získání hodnot hrozby a dopadu je v takto komplexním případě velice náročné. Z toho důvodu budou vytvořeny 3 testovací scénáře, ze kterých bude posuzován dopad na celé prostředí a zároveň z toho budou vyvozeny možné hrozby pro společnost. První variantou bylo zaslání podvodných zpráv k získání přihlašovacích údajů. Jedná se tedy o testování z vnějšího prostředí přímo na uživatele což je dle statistik NÚKIB nejčastější vektor útoku. (3) Zde bude sledováno, jak se uživatelé chovají. Kolik příjemců přistoupilo na stránku útočníka a kolik z těchto uživatelů zadalo přihlašovací údaje. Následující 2 testy jsou vázány na interní prostředí. V rámci druhého testu bude zapotřebí získat přístup do interní sítě s následnou detekcí zařízení v ní. Závěrečnou fází tohoto testu bude pokus o získání přihlašovacích údajů administrátorského účtu na jednom ze zjištěných koncových zařízení. Tato část bude realizována skrze útok hrubou silou. V tomto případě bude výsledkem chování samotné síťové infrastruktury a počítačů v ní. Posledním testem bude zajištění zranitelností na těchto zařízeních. Pakliže byl předchozí test úspěšný a bylo dosaženo přístupu do interní sítě, tak je možné realizovat tuto část. V opačném případě bude umožněno přístupu pro pokračování testů. Pro dosažení informací o zranitelnostech bude využit open source nástroj OpenVas, který slouží k reportování informací o zranitelnostech daných zařízení. Pro skenování sítě je po dohodě ze společnosti vyloučen server, který by nemusel vzhledem ke svému stáří přežít náročnost nástroje. Z toho důvodu bude zjišťování zranitelností zaměřeno na síťový prvek Mikrotik, jenž se stará o rozdělení sítě a zároveň zprostředkovává interní firewall. Skrze tento bod, je sdružena veškerá síťová komunikace z lokální sítě. Druhá část skenování je zaměřena na koncové stanice. V obou případech těchto testů se jedná o neautorizované zjišťování zranitelností neboli získávání informací pomocí dat z odpovědí navrácených ze zařízení.

5.2.1 Phishing

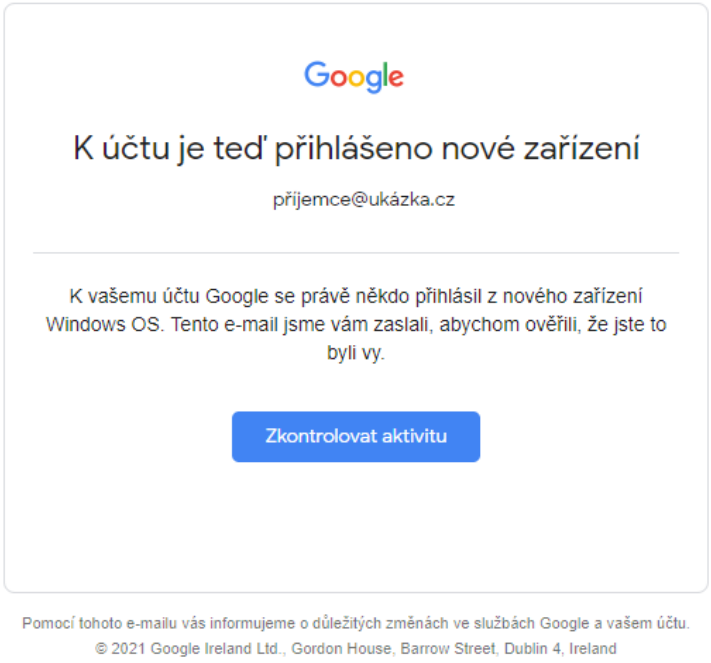
Pro vytvoření phishingu je zapotřebí připravit prostředí, ze kterého bude tato komunikace pocházet. Cest k vytvoření útoků tohoto typu je mnoho. V tomto případě byli zajištěny následující body:

- Registrace domény, na kterou se útočník bude připojovat.
- Zařízení s veřejnou IP adresou, ze kterého budou odesílány podvodné zprávy.
- Instalace operačního systému Ubuntu.
- Instalace Gophish.
- SSL certifikát pro doménu.
- DNS záznamy sloužící pro překlad domény na IP adresu.

Samotný server běží u poskytovatele hostingových služeb, který umožnuje využít server s veřejnou IP adresou, aby byl přístupny z internetu. Pro správnou funkčnost útoku je zapotřebí zasílat v rámci e-mailu podvrženou URL s odkaz na stránku útočníka. Tato doména musí být také zaregistrovaná u poskytovatele. Pro návaznost 1:1 přístupu IP adresy vůči URL adrese se musí vytvořit DNS záznam pro oboustranný překlad. Na samotném zařízení, které poskytuje poskytovatel, byl nainstalován operační systém Ubuntu do kterého byl nainstalován volně dostupný nástroj pro zasílání phishingu a to Gophish. Z něhož byly odesílány podvodné zprávy k získání přihlašovacích údajů. Pro přístup na stránku je vyžadován SSL certifikát, který byl zdarma vytvořen u certifikační autority Let’s Encrypt.

Testem prošli všichni zaměstnanci společnosti. Hlavní cíl samotné komunikace bylo získání přihlašovacích údajů do e-mailových schránek. Případná odcizená hesla byla také ozkoušena v rámci uživatelských účtů v systémech koncových zařízení. Níže je zobrazen samotný e-mail v obrázku 23, jenž obdrželi uživatelé. Tato zpráva byla odeslána 45 zaměstnancům ve stejný čas. Z e-mailu je patrné, že upozorňuje na podezřelou aktivitu v rámci přihlašování do schránky uživatele.

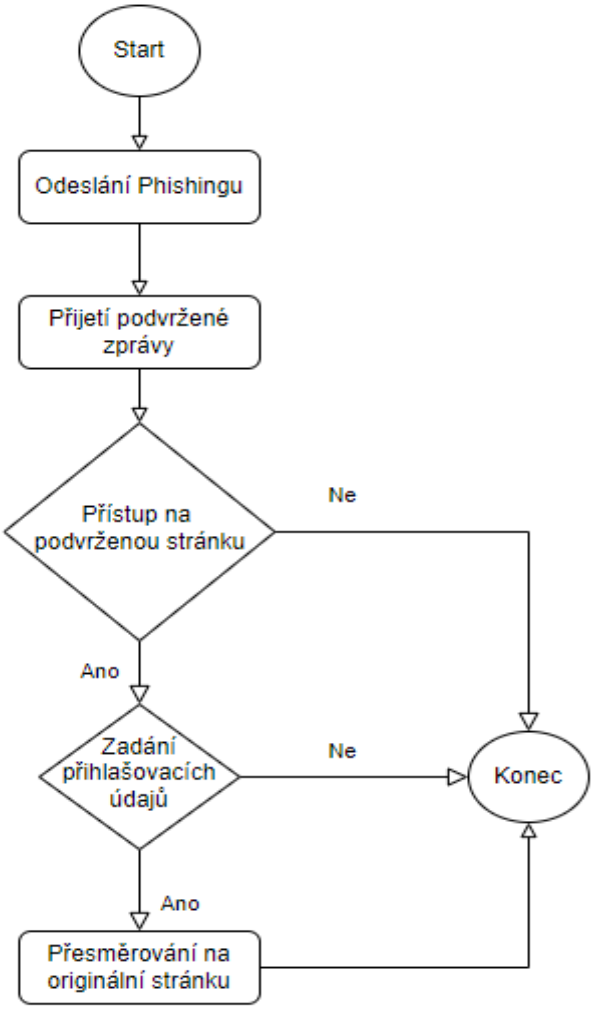
Obrázek 23 - Podvržená zpráva



Zdroj: Vlastní zpracování na základě Google komunikace

Tento e-mail se snaží přimět uživatele, aby zkontroloval veškerá zařízení, jež jsou připojena ke schránce. V případě, že uživatel bude chtít tuto podezřelou aktivitu zkontrolovat skrze odkaz skrývajících se pod „Zkontrolovat aktivitu“. Bude uživatel přesměrován na podvrženou stránku, která vyžaduje oprávnění k dané schránce. Po zadání přihlašovacích údajů je uživatel přesměrován na oficiální přihlašovací stránky poskytovatele viz vývojový diagram zobrazený na obrázku 24.

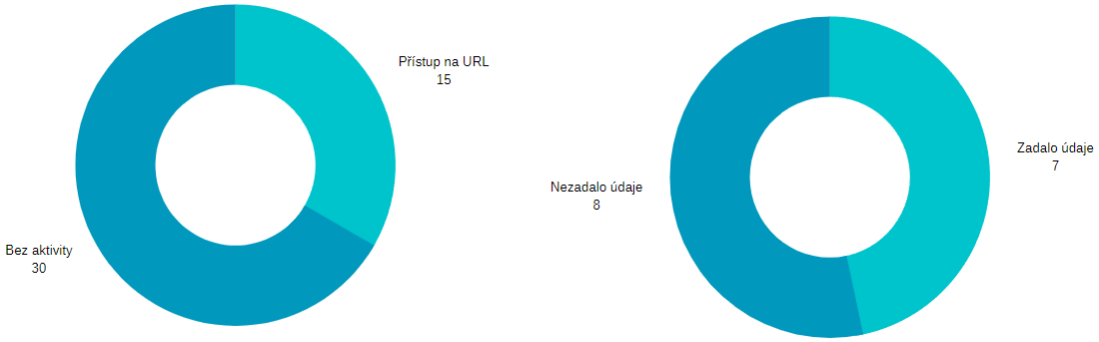
Obrázek 24 - Vývojový diagram phishing



Zdroj: Vlastní zpracování

Výsledky testování uživatelů jsou zobrazeny níže na obrázku 25. Z 45 účastníků kampaně pro získání přihlašovacích údajů bylo aktivních pouze 15 uživatelů. Důvodem menší, než poloviční aktivity mohlo být zapříčiněno několika body. Kampaň je nejefektivnější pouze z počátku, pakliže přišla totožná komunikace všem uživatelům, tak se tento fakt skrze společnost velice rychle rozšířil. Zároveň ne každý uživatel byl při spuštění kampaně aktivně u svého pracovního zařízení, kde mohl zmíněnou komunikaci postřehnout. V pozdějším čase již o rozšíření zprávy se stejným vizuálním obsahem mohl znát od svých spolupracovníků. Z 15 uživatelů, kteří přistoupili na podvrženou stránku zadalo své přihlašovací údaje k účtu 7 uživatelů, tedy téměř polovina. Vlivem chybějícího dvoufázového ověření bylo možné přistoupit ke schránkám uživatelů.

Obrázek 25 - Statistiky phishingu



Zdroj: Vlastní zpracování

5.2.2 Brute-force

Druhým testovaný scénář byl zaměřený na fyzické napadení sítě hrubou silou. V rámci testu bylo zapotřebí se dostat do interní sítě a pokusit se získat přihlašovací údaje lokálních administrátorských účtů skrze bruteforce. V první části získání přístupu do lokální sítě nevznikl žádný problém, jelikož po zapojení síťového kabelu do počítače bylo zařízení připojeno do interní sítě. Následně si pomocí klasického systémového příkazu „ping“ v konečném cyklu dotázal na všechna zařízení v dané adresním rozsahu, čímž získal povědomí o všech zařízeních v dané síti.

```
1.  for ($i=0;$i -lt 255;$i++){
2.      $i
3.      $ping = ping 192.168.2.$i -n 1
4.      if($ping -like "*TTL=64*"){
5.          $device =  "Pod IP 192.168.0."+$i+" je zařízení Linux/Unix"
6.          echo $device
7.      }elseif($ping -like "*TTL=128*"){
8.          $device =  "Pod IP 192.168.2."+$i+" je zařízení Windows"
9.          echo $device
10.     }elseif($ping -like "*TTL*"){
11.         $device =  "Pod IP 192.168.2."+$i+" je jiné zařízení"
12.         echo $device
13.     }
14. }
```

Test pomocí příkazu „ping“ byl zvolen z důvodu, že data podobného typu se vyskytují ve všech sítích. Protokol ICMP nebývá blokován v podnikových sítích. Detekce vychází z odpovědi TTL, který svou hodnotou poukazuje, o jaké operační systémy by se mělo jednat. Vlivem toho, že samotná síť není nijak segmentována, tak lze komunikovat se všemi prvky.

Pro získání přístupu do koncového zařízení byl využit nástroj od společnosti Microsoft s názvem PsExec, který spadá do sady Sysinternals. PsExec byl zvolen pro svou univerzálnost a velkou rozšířenost u správců Windows prostředí. Pomocí tohoto

nástroje byla navazována spojení na lokální Administrátorský účet. Z důvodu neznalosti hesla byla zvolena metoda útoku Bruteforce, čímž se ověřilo, jestli dané účty mají politiky na zamykání účtů, nebo zdali je v síti aktivní sledování technik typově stejných útoků. Pro ilustraci je níže uvedena pouze část kódu, kterou lze využít na testování hesla o velikosti 3 znaků. Jedná se pouze o část, aby tento kód nebylo možné zneužít.

```
1.  Function Get-Password{
2.      $char_1 = 33
3.      $char_2 = 33
4.      $char_3 = 33
5.      while(($char_3 -le 125) –or ($valid –eq $true)){
6.          if($char_1 -eq 125){
7.              $char_2++
8.              if($char_2 -eq 125){
9.                  $char_3++
10.             }
11.
12.         }
13.         $password = [char]$char_1 + [char]$char_2 + [char]$char_3
14.         Try{
15.            Psexec \\IP –u Administrator –p $password
16.         }catch{
17.            $valid = $false
18.         }
19.         $char_1++
20.         if($char_1 -eq 126){
21.             $char_1 = 33
22.             if($char_2 -eq 126){
23.                 $char_2 = 33
24.             }
25.         }
26.     }
27. }
```

Po dokončení testu bylo odhaleno heslo. Z čehož lze vyvést úsudek, že samotný účet nemá nastavenou politiku hesel. Jelikož při délce hesla 6 znaků by se hrubou silou muselo otestovat 606 355 001 344 hesel při využití všech velkých a malých písmen, čísel a speciálních symbolů. I přes tak velké množství pokusů žádný ze systému neupozornil správce k obezřetnosti. V tomto případě se vychází z předpokladu, že zařízení je stále aktivní. V případě cizího útoku by mohl být zvolen útok stejného typu na SSH přístup na server, který je spuštěný celý den. Vzhledem k plošné hiararchii sítě, lze komunikovat na všechna zařízení. Při prolomení administrátorského hesla lze přes nástroj PSexe přistupovat na všechna zařízení v lokální síti.

5.2.3 Zranitelnosti v síti

Získané informace o zranitelnostech síťového prvku Mikrotik zařazeného do L3 jsou vyobrazeny v tabulce 2. Na zařízení bylo spuštěno skenování, které mělo odhalit všechny veřejně publikované zranitelnosti. V OpenVAS byl nastaven typ testování jako „plné“ a to z důvodu aplikování všech testů, které poskytuje nástroj. Samotný proces trvá přibližně 10 minut. Jsou zde vydefinovány IP adresy, nebo případné IP rozsahy. Jednotlivé zranitelnosti jsou rozděleny dle CVSS do 3 kategorií a to vysoká, střední a nízká. Toto rozdělení je podle závažnosti zranitelností, kdy každý z nich může mít jiný dopad na zařízení. I v rámci těchto kategorií je dělení jednotlivých závažnosti dle CVSS. Níže je vyobrazena tabulka zranitelností z routeru. Jedná se pouze o zranitelnosti hodnoceny kategorií vysoká. Jednotlivé zranitelnosti umožňují útočníkovi omezit plnou funkčnost zařízení, nebo získávání informací. Zároveň bylo zjištěno, o jaké zařízení se jedná a typ operačního systému.

Tabulka 2 - Zranitelnosti L3 prvku

ID	Kategorie	CVSS	CVE	Název
1	Vysoká	8,8	CVE-2018-1156	Přetečení zásobníku licence
2	Vysoká	8,8	CVE-2018-1157	Vyčerpání paměti
3	Vysoká	8,8	CVE-2018-1158	Vyčerpání zásobníku
4	Vysoká	8,8	CVE-2018-1159	Poškození paměti
5	Vysoká	8,1	CVE-2019-3943	Přístup k souboru skrze adresářovou cestu
6	Vysoká	7,5	CVE-2019-3924	Prostřednictvím SW obcházení FW
7	Vysoká	7,5	CVE-2019-3976-9	Nedostateční ověření aktualizací, Ochrana DNS
8	Vysoká	7,5	CVE-2019-16160	DoS zranitelnost na přetečení SMB serveru
9	Vysoká	7,5	CVE-2020-11881	Umožnění vzdálené neověřené ovládání SMB

Zdroj: Vlastní zpracování

Pro získání stejných informací z koncové stanice bylo zvoleno stejné nastavení jako u předchozího skenování. V tabulce 3 jsou zobrazeny pouze kritické zranitelnosti. Z testu je patrné, že všechny mají hodnocení CVSS 10, tedy nejvyšší možnou hodnotu. Skrze tyto zranitelnosti lze spouštět například reverzní spojení, skrze kterou se útočník může připojit na zařízení a následně v příkazovém řádku operovat.

Tabulka 3 - Zranitelnosti koncové stanice

ID	Kategorie	CVSS	CVE	Název
1	Vysoká	10	CVE-2009-2526	SMB2 vzdálené spuštění kódu
2	Vysoká	10	CVE-2009-2532	SMB2 vzdálené spuštění kódu
3	Vysoká	10	CVE-2009-3103	SMB2 vzdálené spuštění kódu
4	Vysoká	10	CVE-2010-0020	Přetečení vyrovnávací paměti
5	Vysoká	10	CVE-2010-0021	Možnost způsobení poškození paměti
6	Vysoká	10	CVE-2010-0022	Odmítnutí služby
7	Vysoká	10	CVE-2010-0231	Obcházení ověření

Zdroj: Vlastní zpracování

5.2.4 Výpočet hodnocení rizik

Pro finální kategorizace kritičnosti rizik společnosti je zapotřebí spočítat vzorec (1). Všechny získané hodnoty budou vycházet z provedených testů a zároveň z poznatků z části zabezpečení sítě, kdy tyto informace mohou přímě nebo nepřímě napomáhat k šíření kybernetických útoků v případě reálných kybernetických útoků.

Hodnota hrozeb je první částí výpočtu rizika. Z provedených testů je patrné, že kritický vektor útoků může být interního a externího charakteru. První testem bylo odhaleno, že při pokusu o získání přihlašovacích údajů bylo 15,5 % úspěšnost získání přihlašovacích uživatelských údajů. V případě, že by se namísto získání přihlašovacích údajů jednalo pouze o vstoupení na infikovanou stránku, tak se procento přístupů zvýšilo na 33 %. Z výsledků testu z interního prostředí je patrné, že útok byl provedený úspěšně a žádné ze zařízení síťových nebo koncových tento bezpečnostní incident nezablokovalo nebo proaktivně neinformovalo. Tento stejný scénář za využití jiných nástrojů lze aplikovat i na síťové prvky, které mají dostupnou správu ze všech zařízení přes prohlížeč. Samotnému testu však předcházel bod vstupu do sítě, který nebyl nijak zabezpečený a zároveň vlivem nepřítomné segmentace sítě bylo umožněno komunikovat na všechna zařízení. Z těchto získaných dat s různými závažnostmi je vyvozena hodnota celku jako téměř kritická, a proto je části vzorce hrozeb přidělena hodnota 4.

Hodnocení zranitelností vychází především z posledního provedeného testu, pomocí něhož byli zjišťovány zranitelnosti v rámci lokální infrastruktury. Dle získaných zranitelností na páteřním směrovači a koncovém zařízení v tabulkách 2 a 3 je patrné, že tato výpočetní technika obsahuje zranitelnosti kategorizované jako vysoké. CVSS všech těchto zranitelností je na stupnici od 0-10 vždy vyšší než 7,5. Pomocí těchto zranitelností je možné získat plnou nebo částečnou kontrolu nad zařízením. Umožnují

získávání neautorizovaných informací, které mohou napomáhat kybernetickým útokům. Nejvýše hodnocené zranitelnosti mají nejvyšší stupeň dle CVSS a to 10. Jedná se o zranitelnosti vztažené k protokolu SMB, jenž je využit pro přenos souborů. Pomocí těchto zranitelností lze vzdáleně spouštět kód na cíleném zařízení. Vzhledem ke kritičnosti těchto zranitelností je zranitelnosti přidána hodnota 10, jenž je reflektována dle CVSS.

Hodnocení dopadu je poslední potřebnou částí k získání hodnoty rizik. Samotný dopad vychází z výsledků samotných testů, kdy výslednou hodnotou je vyvozeno z největšího možného dopadu, jenž mohli způsobit provedené testy při reálném útoku. Zároveň je zde bráno v potaz obecná část rozboru zabezpečení společnosti rozebraná v úvodu praktické části. Po získání přihlašovacích údajů do e-mailových schránek uživatelů získaných za pomocí externího testování. Vzniká pro společnost dopad vysoký, který se může promítat do odcizení interních nebo osobních dat, čímž může dojít k porušení GDPR. Zároveň mohou být schránky využity k poškození jména společnosti. Z pohledu interních testů vychází hodnota dopadu jako kritická, a to z důvodu, že při získání administrátorských údajů může dojít k úplnému vyřazení zařízení, získání interních nebo osobních údajů. Skrze provedené testy bylo zjištěno, že existuje více cest k získání plné kontroly nad zařízením. Vlivem neomezené komunikace a stejným přihlašovacím údajům se jedná o celoplošný dopad. Z tohoto důvodu je hodnota dopadu označena 5.

Výpočet rizika společnosti z rovnice (1), která je složena z hrozby, zranitelnosti a dopadu po dosazení získaných hodnot vychází, že výsledná hodnota analýzy rizik je 100. Tato hodnota dle tabulky hodnocení rizik je v rozmezí úrovně kritické. Což znamená, že se jedná o neakceptovatelné riziko pro společnost. Samotná rizika musí být v co nejkratší době odstraněna.

5.2.5 Nápravná opatření

Výsledná hodnota analýzy kybernetických rizik pro bezpečnost IT jako celku je kritická. Nápravná opatření reflektují zjištěné informace skrze body dopadu, hrozeb a zranitelnosti, jež vycházeli z provedených testů. Z této části budou vycházet provedené úpravy v rámci lokální infrastruktury, jak po fyzické stránce, tak procesní.

Nápravná opatření v bodech jsou:

- **Z pohledu síťové vrstvy**
    - **Segmentace sítě** – Pomocí čehož dojde ke snížení dopadu možného útoku. Při nákaze zařízení se samotná nákaza nemůže šířit na ostatní zařízení, jelikož dojde k jejich separaci.
    - **Ověření nových zařízení v síti** – Každé nové zařízení v síti bude ověřeno vůči serveru, aby bylo zamezeno připojení neoprávněným zařízením, jako v případě druhého testu počáteční fázi přístupu do sítě.
    - **Hardening síťových prvků** – Vlivem čehož dojde k eliminaci zranitelností a samotné zvýšení bezpečnosti.
    - **Zavedení IDS** – Systém bude detekovat možné další kybernetické útoky.
- **Z pohledu aplikační vrstvy**
    - **Hardening OS a aplikací třetích stran** – V rámci aplikací dojde k stejnému zabezpečení jako u síťových prvků. Tímto krokem dojde k omezení možností odcizení hesel z prohlížeče v případě vstupu na podvodnou stránku, nebo blokování účtů při pokusu o útoky hrubou silou.
    - **Aplikační architektura** – Vlivem tohoto bodu a vytvořením PAW dojde ke zvýšení bezpečnosti v rámci aplikační vrstvy. Pomocí této nápravy je zamezeno zneužití administrátorského účtů napříč organizací.
    - **Vytvoření PAW** – Definováno zařízení, ze kterého se mohou spravovat zařízení.
- **Ostatní**
    - **Zvýšení auditního režimu na všech zařízení** – slouží pro zvýšení auditování zařízení, a to z důvodu případného prolomení stávajících opatření musí existovat dostatečné množství záznamů, které by napovídali k příčině vzniku kybernetického útoku.

5.3 Návrh zabezpečení a implementace

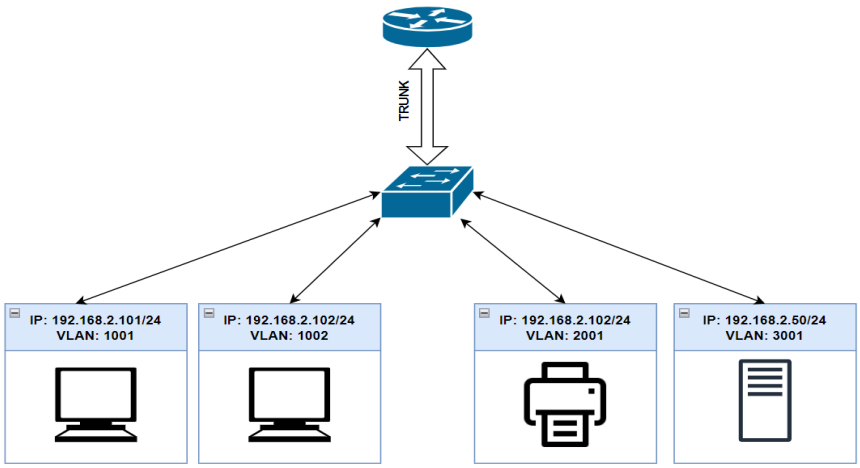
Z výsledku analýzy rizik jsou vyvozena nápravná opatření, které v této části budou rozebrána a popsána jejich plná nebo částečná úprava na jednotlivé zařízení pro využití společnosti. Výsledkem čehož by mělo dojít k částečnému nebo úplnému odstranění chyb objevených pomocí testování. Vlivem čehož dojde ke snížení hodnoty rizika ve společnosti.

Nasazení aplikací pro zvýšení bezpečnosti za účelem zajištění většího množství informací pro případné forenzní řešení nejen kybernetických útoků, ale i operačních problémů. Základním bodem celé bezpečnosti je architektura celé sítě, jak po fyzické, tak logické stránce. Dále jsou v této části definovány bezpečnostní politiky pro jednotlivé aplikace a systémy. Jednotlivé body mají účel úplného zamezení, nebo částečného omezení útočníka. Těmito opatřeními se prodlužuje potřebná doba k realizaci úspěšného útoku, čímž se úměrně zvyšuje doba pro možné odhalení útočníka. Vlivem čehož se zmenšuje riziko možností získání a odcizení interních informací.

5.3.1 Segmentace sítě

Segmentace sítě je zavedena především z důvodu možného šíření nákazy. Pakliže se vyskytuje v rámci nesegmentované lokální sítě infikované zařízení, tak zároveň toto zařízení může komunikovat s veškerou výpočetní technikou, která je v totožné síti. Což umožnuje zdroji rozšiřovat nákazu po všech bodech. Segmentace sítě má za úkol tomuto zabránit. Pro rozdělení jsou využity VLAN. Každé zařízení má dynamicky přidělovanou jednu VLAN, jenž přísluší pouze jemu. Využité VLAN začínají od 1000. Pro koncová zřízení je definovaný rozsah 1000-1999, kdy každé zařízení má dynamicky přidělovanou svou VLAN. Tiskárny mají rozsah 2000-2999 a servery 3000-3999. První číslo tedy naznačuje typ využité VLAN. Veškerá zařízení jsou zapojeny do L2 směrovače, který má nastavený Trunk na router, čímž je toto spojení rozděleno podle využitých zařízení. V rámci tohoto zapojení na sebe nemohou jednotlivá zařízení komunikovat. L3 prvek se v rámci tohoto spojení bere jako kořenový uzel, kde se tvoří pravidla pro komunikace mezi VLAN pro specifické porty, která se především využijí pro umožnění koncových počítačů komunikovat jednosměrně na tiskárny a další potřebná zařízení.

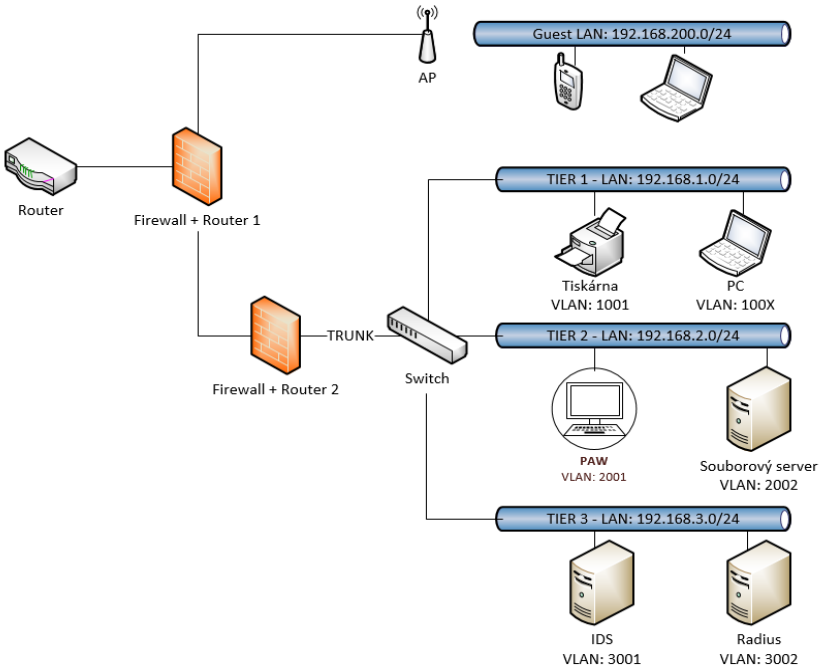
Obrázek 26 - Dělení VLAN



Zdroj: Vlastní zpracování

Upravená topologie sítě byla rozdělena fyzicky podle Tier modelu, kdy každý Tier má svou podsíť. V těchto částí sítě se vyskytují jiná zařízení, která jsou rozdělena virtuálně dle VLAN viz obrázek 26. Samotná zařízení byla rozdělena podle kritičnosti pro provoz. Zařízení, jež byla označena jako kritická neboli s přímým dopadem na provoz, nebo sdružují velké množství bezpečnostních informací, tak byla zařazena do nejvyšší vrstvy. Fyzické dělení sítě je vidět na obrázku 27, který rozřazuje systémy do jednotlivých subnetů podle Tier.

Obrázek 27 - Nová segmentace sítě



Zdroj: Vlastní zpracování

Aby vše správně fungovalo musí se definovat prostupy na obou směrovačích, kde je spuštěn Firewall. Samotný výpis pravidel je uveden v tabulce 4, která popisuje jednotlivé prostupy. Tabulka popisuje prostupy ze směrovače 2. Výpis specifikuje jednotlivé prostupy, která VLAN může přistupovat do jaké VLAN a zároveň na které porty. Veškerá ostatní komunikace je zahazována. Jednotlivé záznamy jsou označeny identifikátorem. Níže jsou povoleny pouze protokoly nezbytné pro funkčnosti. Kdy objekty „Trust“ označují veškerý lokální provoz, kterému lze důvěřovat a „Untrust“ je definovaný pro internet. V části zdrojové cílové komunikace se může vyskytovat libovolná IP adresa, pakliže má označení „Any“. V pravidlech označených indexem 10 a 11 jsou objekty, které umožnují komunikaci na specifické porty pro specifické IP adresy. Jedná se tedy o alias, který v pozadí obsahuje seznam adres.

Tabulka 4 - Firewall prostupy

ID	Zdroj VLAN	Cíl VLAN	Zdroj	Cíl	Port
1	100X	1001	192.168.1.0/24	192.168.1.0/24	9100-9102
2	100X	2002	192.168.1.0/24	192.168.2.0/24	445,139
3	1001	2002	192.168.1.0/24	192.168.2.0/24	445,139
4	2001	2002	192.168.2.0/24	192.168.2.0/24	22
5	Trust	3002	Any	192.168.3.0/24	1812,1813
6	100X	Untrust	192.168.1.0/24	Any	53,123,443,80
7	2001	3002,3001	192.168.2.0/24	192.168.3.0/24	22
8	3001	Untrust	192.168.3.0/24	Linux_Update_IP	80,443
9	3002	Untrust	192.168.3.0/24	Linux_Update_IP	80,443
10	2002	Untrust	192.168.2.0/24	Linux_Update_IP	80,443
11	2002	Untrust	192.168.2.0/24	Microsoft_Update_IP	80,443

Zdroj: Vlastní zpracování

IPTables jedná o program pro nastavení lokálních firewallových pravidel. Jednotlivá práva jsou filtrována pomocí IP paketů na úrovni jádra Linuxu. Tento nástroj bude nasazený na souborovém serveru, Radius serveru a IDS, který běží na operačním systému Linux distribuci Debian ve verzi 11. Pro ukázku je níže zobrazen výpis pravidel pro souborový server. Pravidla byla tvořena postupem rozděleným do 2 částí. V první části se zablokovala veškerá síťová komunikace. V druhé části se povolovali pouze nezbytně nutné a potřebné síťové komunikace pro provoz. Stejným principem zapínání nejnutnějších služeb se postupuje i u Firewallu.

```
1.  #Samba
2.  iptables -A INPUT -p tcp --dport 139 -s 192.168.2.0/24 -j ACCEPT
3.  iptables -A INPUT -p tcp --dport 445 -s 192.168.2.0/24 -j ACCEPT
4.  #SSH z PAW
5.  iptables -A INPUT -p tcp --sport 22 -s 192.168.3.17 -m state --state
    NEW,ESTABLISHED -j ACCEPT
6.  iptables -A OUTPUT -p tcp --dport 22 -s 192.168.3.17 -m state --state
    ESTABLISHED -j ACCEPT
7.  #internet
8.  iptables -A INPUT -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
9.  iptables -A INPUT -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT
10. iptables -A OUTPUT -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j
    ACCEPT
11. iptables -A OUTPUT -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j
    ACCEPT
12. #DNS , NTP
13. iptables -A OUTPUT -p udp --dport 53 -m state --state NEW,ESTABLISHED -j
    ACCEPT
14. iptables -A OUTPUT -p tcp --dport 53 -m state --state NEW,ESTABLISHED -j
    ACCEPT
15. iptables -A INPUT -p udp --sport 53 -m state --state ESTABLISHED -j ACCEPT
16. iptables -A INPUT -p tcp --sport 53 -m state --state ESTABLISHED -j ACCEPT
17. iptables -A OUTPUT -p udp --sport 123 -m state --state NEW,ESTABLISHED -j
    ACCEPT
18. iptables -A INPUT -p udp --dport 123 -m state --state ESTABLISHED -j ACCEPT
19. #ICMP
20. -A OUTPUT -p icmp -j ACCEPT
21. -A INPUT  -p icmp -j ACCEPT
22. #Blok vše ostatní
23. iptables -A INPUT -j DROP
24. iptables -A OUTPUT DROP
25. iptables -A FORWARD DROP
```

Pravidla povolují protokoly pro funkčnost samby z definovaného síťového rozsahu. Následuje sada pravidel pro SSH protokol, který definuje možnost přístupu z určité IP adresy. Za touto IP adresou je skrytá PAW stanice. Poté jsou obecná pravidla zahrnující protokoly NTP, DNS, HTTP a HTTPS a ICMP. Celý blok příkazů je zakončen blokací veškerého síťového provozu, který se neshoduje s žádným z pravidel ukázaných výše.

5.3.2 Ověření zařízení

Radius server, který bude především sloužit k omezení připojení všech necertifikovaných zařízení do sítě. Tímto krokem se zamezí potenciálním útočníkům připojení neautorizovaných zařízení. Tento bod se projevil v rámci první fáze 2 testu zajištění přístupu do lokální sítě. Po jehož provedení nebylo zařízení nijak ověřeno. V tento moment nemohlo dojít k zamezení komunikace se všemi místními zařízeními. S nasazením Radius serveru bude vyžádáno ověření přes certifikát. Pakliže zařízení nebude předkládat k ověření serveru platný certifikát, tak tomuto zařízení nebude umožněno komunikovat v lokální síti. Samotný server poběží na operačním systému Debian a bude využit Free Radius. Pro šetření nákladů byla opět zvolena vyřazená výpočetní technika, která nebyla již využívána provozem. Hlavními soubory pro úpravu

nastavení serveru se nachází v adresářové cestě */etc/freeradius/*. Jelikož je velké množství typů ověření viz kapitola 7.2. bude pro toto využití zvolena varianta PEAP s MSCHAPv2. V souboru *eap.conf* se právě tento parametr nastavuje v části „default_eap_type“. MSCHAPv2 se upravuje v části souboru mschap, kde se musí povolit a zároveň definovat, šifrování a také minimální velikost klíče na 128 bit. Pro správné a bezpečné fungování má server a prostředník mezi sebou tajemství (heslo), tito jednotliví klienti se definují v souboru *clients.conf*. V rámci tohoto souboru se specifikuje heslo, kterým se prostředník ověřuje vůči serveru, a to z důvodu, aby žádný prostředník nemohl serveru podvrhovat klienty. V případě napojení na AP, pro bezdrátové připojení, lze specifikovat, které účty se mohou připojovat v souboru *user*. V případě většího počtu uživatelů, by měl být Radius server napojený na databázi. Posledním krokem je definování SSL certifikátů, jenž se musí vygenerovat pomocí souboru CA.pl, který se specificky upraví pro server. Vygenerované certifikáty se musí definovat opět v souboru *eap.conf* a to v metodě TLS. V této části se specifikují privátní, veřejné klíče, dh a random soubor.

5.3.3 Hardening síťových prvků

Jedná se o nedílnou součást pro zvýšení bezpečnosti. V případě, že by se tato část vynechala, tak by mohla být náchylná k získání plné kontroly cizí entitou. Což by mělo za následek, že v případě získání plné kontroly nad jedním z páteřních prvků v síti by útočník mohl podvrhovat stránky, podvrhovat obsah, nahlížet kam jaká zařízení komunikují, nebo určitou blokaci komunikace. Zároveň jsou touto částí anulovány kritické zranitelnosti, jež byly zjištěni v rámci posledního testu v analýze rizik. Na níže uvedeném kódu je popsáno všeobecné zabezpečení pro Mikrotik routery, které doporučuje výrobce. (49) Tento princip je zaváděn na všech síťových prvcích. Hned v prvním kroku je odebírán výchozí uživatel admin, a to z důvodu, že by se jednalo o první účet, který by útočník zkoušel prolomit. Obecně se nejedná pouze o účet admin, ale o všechny výchozí přístupové údaje, které jsou veřejně dohledatelné. Následně se nastavuje, z jakého IP rozsahu se administrátor může přihlásit. Jako u koncových stanic je zapotřebí odebrat všechny nepotřebné služby a zakázat možnosti přihlášení, která se primárně nevyužívají, nebo se jedná o nezabezpečené protokoly. Dalším krokem je vynucení lokální DNS mezipaměti, kterou se útočník může pokoušet zachytit, nebo jí podvrhovat infikované překlady adres. Zároveň se zde vynucuje silnější kryptografie pro SSH protokol. Stejný proces u vypínání nevyužitých služeb se přenáší do vypínání nevyužitých fyzických rozhraní a IPv6. Některé Mikrotik routery obsahují

LCD displeje, které se doporučují vypnout, nebo jim nastavit PIN. Na závěr je aktualizovaný operační systém.

```
1.  #Odebrat výchozí účet nastavit od kud se lze přihlásti
2.    /user remove admin - odebrat admin účet
3.    /user set 0 allowed-address=192.168.2.17/32
4.  #Vypnutí služeb pro přihlášení
5.    /ip service disable telnet,ftp,www,api,api-ssl,winbox
6.  # povolené síťový rozsah ze kterého se lze přihlásit pro službu
7.    /ip service set adresa ssh=192.168.2.17/32
8.  #Zakázat služby pro jednoduchou správu zařízení.
9.    /tool mac-server set allowed-interface-list=none
10.   /tool mac-server mac-winbox set allowed-interface-list=none
11.   /tool mac-server ping set enabled=no
12.   /tool bandwidth-server set enabled=no
13. #Zakázat Neighbor Discovery Protokol - objevu další mikrotiky routery v síti
14.   /ip neighbor discovery-settings set discover-interface-list=none
15. #Další služby které jsou ve výchozím nastavení zapnuty
16.   /ip proxy set enabled=no
17.   /ip socks set enabled=no
18.   /ip upnp set enabled=no
19.   /ip cloud set ddns-enabled=no update-time=no
20. #Vypnutí lokální DNS chache
21.   /ip dns nastavit allow-remote-requests=no
22. #Vynucuje silnější krypto pro SSH
23.   /ip ssh set strong-crypto=yes
24. #Vypnutí fyzického rozhraní a IPv6
25.   /interface set x disabled=yes
26.   /ipv6 nd set [find] disabled=yes
27. #Vypnutí LCD
28.   /lcd set enabled=no -některé mikrotik routery mají LCD –zakázat
29. #Aktualizace systemu
30.   /systém package update
```

I přes vypnutí veškerých nevyužitých služeb na síťovém zařízení není zaručeno, že se jedná o plně zabezpečený prvek. Některé funkce pro zvýšení bezpečnosti se musí explicitně na jednotlivých L2 nebo L3 prvcích zapnout. Na ukázce nastavení níže je vyobrazeno nastavení pro Cisco směrovač, kterému jsou zapnuty jednotlivé zabezpečovací prvky. Jedná se o části, které jsou uvedeny v 7.1 Zabezpečení sítě. Nejprve se zapíná funkce Port security, která kontroluje, zdali pakety nepřicházejí z nepovolené MAC adresy. Na druhém řádku se zapíná funkce pro ochranu jednotlivých portů, jenž zamezí přeposílání provozu na L2 vrstvě mezi porty takto nastavenými. V následujícím řádku je zapnut STP pro zabránění vzniku smyček, například v případě chybného zapojení směrovače. Na řádcích 4 a 5 je globálně zapnuta ochrana proti podvržení DHCP Serveru na definované VLAN. Vlivem zapnutí této funkce lze využít kontrolu zdrojových IP adres, jenž automaticky aplikuje filtrování provozu na základě IP a MAC. Posledním bodem nastavení je dynamická kontrola protokolu ARP, který chrání před jeho zneužitím. Tato metoda využívá stejná data jako kontrola zdrojových IP adres.

Metoda kontroluje validitu zasílaného protokolu vůči svým záznamům. Tato funkce se zapíná globálně pro VLAN.

```
1.  SWITCH(config-if)#switchport port-security maximum 1
2.  SWITCH(config-if)#switchport protected
3.  SWITCH(config-if)#spanning-tree portfast
4.  SWITCH(config)#ip dhcp snooping
5.  SWITCH(config)#ip dhcp snooping vlan 1-4094
6.  SWITCH(config)#ip arp inspection vlan 1-4094
```

5.3.4 Detekční nástroj

IDS systém, který bude detekovat možná bezpečnostní rizika dle definovaných pravidel. Pro nasazení je využit open source systém Suricata na operačním systému Linux. Důvodem nasazení IDS je zajištění možné detekce při pokusu o možný bezpečnostní incident, čímž je získáno větší penzum času pro případnou nápravu. Suricate je v síti umístěna na span portu, který zrcadlí komunikaci z lokální sítě. Veškerá tato data jsou reálném čase porovnávaná s předdefinovanými pravidly, kdy při nalezení shody jsou zaznamenána. Jedná se tedy o pasivní bod, který pouze upozorňuje na možná bezpečnostní rizika. Pro snížení nákladů je celý systém naistalován na vyřazenou výpočetní techniku, kterou nebylo možno plnohodnotně využít pro provozní práci. Samotná konfigurace se upravuje v souboru v adresářové cestě: */etc/suricata/suricata.yaml*. V tomto souboru jsou upraveny body pro interní a externí rozsah viz výpis souboru níže. Jedná se pouze o část, která byla upravena, nebo je důležitou částí. V prvních řádcích je definovaný interní a externí rozsah sítě. Tento aspekt se definuje, aby pravidlům mohl být definován na směr útoku. Na řádku 5 jsou vypsány listy pravidel, které má pro svou detekci Suricata využívat. Předposlední část se zaměřuje na umístění, kde budou uloženy výstupy z této aplikace. Výpis kódu ze souboru je zakončen definováním fyzické rozhraní pro získávání dat ze sítě.

```
1.  vars:
2.    address-groups:
3.    HOME_NET: "[192.168.0.0/16]"
4.    EXTERNAL_NET: "!$HOME_NET"
5.  default-rule-path: /etc/suricata/rules
6.  rule-files:
7.    -rule_list.rules
8.  Default-log-dir: /var/log/suricata/
9.  af-packet:
10.   interface: eth0
11.
```

Krom těchto aspektů lze v rámci souboru *suricata.yaml* nastavovat, zdali je požadováno zachytávat pcap soubory, neboli záchyt síťové komunikace. Jsou zde popsány jednotlivé protokoly jako SSH, DHCP, které lze jednotlivě povolit, nebo zakázat. Lze také umožnit vytvářet statistiky, jako počítání paketů, využité paměti a další. Další možností, která může být využita je nastavení odesílání do Syslogu, kterým by jednotlivé události odesílal do technologií jako je SIEM nebo logmanagement.

Z nastavení Suricaty je patrné že listy pravidel jsou uloženy v adresáři */etc/suricata/rules/*. Zde mohou být uloženy jednotlivé listy pravidel, které slouží pro vyhodnocování dané komunikace. Na ukázce níže je zobrazeno 5 pravidel, které znázorňují jaké možnosti IDS/IPS systémy umožnují. Vzhledem k tomu, že se jedná o pasivní systém tak akce symbolizovaná prvním slovem může být pouze pasívní. IPS systému umožnují při vyhodnocování komunikaci blokovat. V těchto všech případech se jedná o alert. V případě vyhodnocení je uložena událost s tímto názvem. Pravidlo číslo jedna detekuje v rámci DNS komunikace TLD, které nejsou běžné. Tímto pravidlem se například může odhalovat phishing, kdy má útočník svou doménu na stránce s netypickou TLD. Druhé pravidlo sleduje TLS komunikaci, a to její JA3 hash. Tyto hash vznikají při počáteční výměně informací. Kdy pomocí tohoto otisku se odhalují podezřelé servery. Konkrétně v tomto případě se jedná o sledování otisku, který by mohl vést k možné podezřelé komunikaci se serverem, který byl v minulostí spojen s Emotet. Pravidlem na řádku 3, je zranitelnost Log4j z roku 2021, která byla označena jako zero-day s hodnocením CVSS 10 (Critická). Toto pravidlo sleduje možný datový řetězec, který obsahuje část útoku. První část v části „contenct“ je v čitelné podobě a její druhá část je zakódovaná v hexadecimálním tvaru. Čtvrté pravidlo se snaží pomocí TCP protokolu detekovat brute-force útok do interní sítě, a to za pomoci TCP SYN příznaků, kterých musí být 5 v rámci 30 vteřin. Posledním demonstračním pravidlem se hlídá, jestli nebylo využito TLS spojení verze 1.0 a 1.1. Tyto verze protokolů by se neměli využívat. IETF (Internet Engineering Task Force) výslovně uvádí, že se nesmí používat tyto verze. (50) Jedná se tedy o nepodporované verze protokolů.

```
1. alert dns any any -> any any (msg:"TGI HUNT Abused TLD .top in DNS";
   flow:established; dns_query; content:".top"; endswith; threshold:type limit,
   track by_src, seconds 60, count 1; classtype:bad-unknown; sid:2610020; rev:1;)
   address-groups:
2. alert tls any any -> any any (msg:"TGI HUNT JA3 SSL-Client Fingerprint
   Detected (Emotet/AutoIt/Ursnif)"; ja3_hash;
   content:"4d7a28d6f2263ed61de88ca66eb011e3";
   reference:url,engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-
   247362855967; sid:2610420; rev:1;)
3. alert tcp any any -> any any (msg:"TGI HUNT log4j with Base64";
   flow:established; content:"jndi|3a|"; fast_pattern; content:"Base64"; nocase;
   classtype:bad-unknown; sid:2610800; rev:1;)
4. alert tcp any any -> $HOME_NET 22 (msg:"Possible SSH brute forcing!"; flags:
   S+; threshold: type both, track by_src, count 5, seconds 30; sid:10000001;
   rev: 1;)
5. alert tls any any -> any any (msg:"match TLC version 1.0 and 1.1";
   ssl_version: tls1.0, tls1.1; sid:200031;)
```

V případě provozu na síti bude detekována určitá signatura, která se shoduje s pravidlem, tak výsledná událost je uložena v adresáři */var/log/suricata/fast.log*. Jednotlivé detekční události mají následující tvar, který je zobrazen níže. Z výpisu je jednoznačné z popisu pravidla, o jaký množný bezpečnostní incident se jedná.

O2/10/2022-05:01:22.510248 [**][1:3:2] Popis pravidla [**][Clasification: (null)] [Priority: 3]{typportu ICMP} 192.168.2.101 -> Cil

5.3.5 Hardening OS a aplikací třetích stran

Jedná se o téma, které lze řešit u téměř každé aplikace, jak po její aplikační, nebo síťově vrstvě dle ISO/OSI modelu. Touto částí jsou zajištěna nápravná opatření týkajících se hrozeb a dopadu, jenž byla zjištěna při provedených testech. Jedná se například o zamezení příchozí komunikace, nebo deaktivací loginů s velkým množstvím neúspěšných pokusů o přihlášení.

Téměř každý software má své specifické nastavení, nebo vydefinovanou komunikaci, které lze upravit. Tato komunikace se poté dá omezit nejen na koncovém zařízení. Vzhledem k tomu, že společnost využívá ke své práci většinu běžně dostupných aplikací od celosvětových společností, tak na většinu společností existují určité možnosti pro zvýšení jejich bezpečnosti. Nezisková organizace CIS (Centrum pro internetovou bezpečnost), která se snaží činit aktuální digitální svět bezpečnějším. Tuto snahu provádí skrze propagací ověřených postupů, které pomáhají správcům podniku chránit jejich infrastrukturu před kybernetickými hrozbami.

Aplikace a systémy, využité v rámci tohoto prostředí a lze na ně aplikovat určité rozšířené zabezpečení skrze CIS jsou:

- Adobe Acrobat Reader
- Google Chrome
- Windows OS
- Linux OS

Google Chrome je nejrozšířenější a nejvyužívanější aplikací napříč celým prostředím. Vzhledem k tomu, že se jedná o internetový prohlížeč, tak se jedná o jeden z možných vstupních bodů do interní sítě. Uživatele mohou skrze neopatrné procházení internetu přijít o interní data, jež mohou ohrozit chod společnosti. Proto se klade velký důraz na zvýšení bezpečnosti této aplikace.

V této části jsou popsány body, které se pomocí powershellového scriptu zapsaly do registrů operačního systému Windows. Vzhledem k tomu, že se jedná o cyklicky opakující se příkaz zápisu do registrů, je v níže uvedené ukázce vložena pouze část programu. Tento výňatek popisuje zápis do cesty v registrech, které se aplikují globálně na celé lokální zařízení, což znázorňuje část „HKEY_LOCAL_MACHINE“ a následuje cesta k dané politice. Jelikož se jedná o aplikace, tak veškeré jejich možnosti nastavení padají do části „SOFTWARE“ s podadresářem „Policies“, kde jsou jednotlivé aplikace. Tato specifikace cesty je vyobrazena na prvním řádku. V rámci 2 a 3 řádku je popsán možný zápis hodnot. Každý řádek se skládá z názvu politiky a typu zápisu její hodnoty a samotná hodnota.

```
1.  [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome]
2.  "ForceEphemeralProfiles"=dword:00000000
3.  "HideWebStoreIcon"=dword:00000001
```

Jednotlivé registry mohou povolovat, vynucovat, nebo zakazovat určité aspekty fungování prohlížeče. Výpis nejzajímavějších 20 bodů:

- **BrowserAddPersonEnabled** – Zakazuje nastavování nových profilů uživatele.
- **BrowserGuestModeEnabled** – Zakazuje spouštět profil hostům.
- **AutoplayAllowed** – Zakazuje automatické spouštění přehrávačů.
- **BrowserNetworkTimeQueriesEnabled** – Zakazuje dotazování prohlížeče na servery vlastníka z důvodu získání časového razítka.

- **DisableScreenshots** – Zakazuje získávání snímků obrazovky pomocí klávesových zkratek.
- **SSLVersionMin** – Vynucena minimální verze SSL/TLS.
- **VideoCaptureAllowed** – Zakazuje spuštění kamery všem stránkám.
- **AudioCaptureAllowed** – Zakazuje spuštění audia všem stránkám.
- **RemoteAccessHostAllowUiAccessForRemoteAssistance** – Zakazuje interakci vzdáleného uživatele v relacích vzdálené pomoci.
- **DefaultWebBluetoothGuardSetting** – Zakazuje všem stránkám využívat Bluetooth k přístupu k zařízení prostřednictvím Web Bluetooth API
- **SafeSitesFilterBehavior** – Zakazuje přistupovat na stránky s obsahem pouze pro dospělé.
- **RunAllFlashInAllowMode** – Zakazuje uživateli ukládat nová hesla do prohlížeče.
- **SafeBrowsingForTrustedSourcesEnabled** – Nastavuje provádění kontroly bezpečného prohlížení u všech stažených souborů
- **RemoteAccessHostFirewallTraversal** – Zakazuje procházení firewallem ze vzdáleného přístupu.
- **ForceGoogleSafeSearch** – Vynucuje bezpečné vyhledávání v prohlížeči

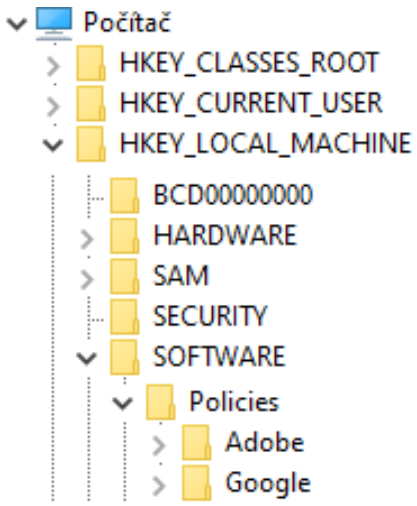
Adobe Acrobat Reader DC jedná se o aplikaci, která slouží především k prohlížení PDF souborů. Vzhledem k jejímu využití je stejně rozšířená jako internetový prohlížeč, tedy na každém koncovém uživatelském zařízení. Od jejího vzniku 1999 bylo vytvořeno přes 290 zranitelností, obecně na veškeré produkty od společnosti Adobe téměř 1400 zranitelností. (51) Z toho důvodu se zde klade stejný důraz na zvýšení bezpečnosti, jako u prohlížeče.

Zabezpečení aplikací Adobe lze vytvořit skrze uživatelské rozhraní, které si může nastavit každý uživatel, nebo skrze registry operačního systému. Zápis do registrů je typově stejný, jako u výše uvedeného prohlížeče. Data se aplikují na celý lokální počítač v části software v podadresáři politik, tedy na cestě *„\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe“*. Zde jsou zapisovány jednotlivé politiky podle dokumentace od výrobce. Níže je vypsáno Top 10 záznamů, které jsou nastaveny.

- **bEnableJS** – Globální zakázání spuštění Javascriptu v PDF.
- **bAskBeforeInstalling** – Bez dotazu nemůže být provedena žádná instalace.
- **bUpdater** – Povoluje nebo zakazuje automatické aktualizace.
- **bDisablePDFHandlerSwitching** – Zakazuje uživatelům v rámci aplikace měnit již nastavené nastavení, které by se propisovalo de registrů.
- **bProtectedMode** – Povoluje programu nastavení zvýšené ochrany systému a dat.
- **bEnhancedSecurityStandalone** – Kontroluje důvěryhodnost dokumentů, zakazuje vkládání skriptů prostřednictvím souborů FDF, XFDF a XDP u standalone aplikací.
- **bEnhancedSecurityInBrowser** – Kontroluje důvěryhodnost dokumentů, zakazuje vkládání skriptů prostřednictvím souborů FDF, XFDF a XDP při využití prohlížeče.
- **bEnableGlobalSecurity** – Zakazuje komunikaci napříč objekty.
- **bEnableFlash** – Umožnuje spustit Flash pouze důvěryhodných zdrojů.
- **bDisableTrustedFolders** – Definuje důvěryhodné lokální zdroj.
- **bDisableTrustedSites** – Definuje důvěryhodný síťový zdroj.

Na obrázku 28 níže je zobrazena část složek z kořenového adresáře v registrech. V části politik jsou umístěny složky pro Google a Adobe.

Obrázek 28 - Výpis registrů

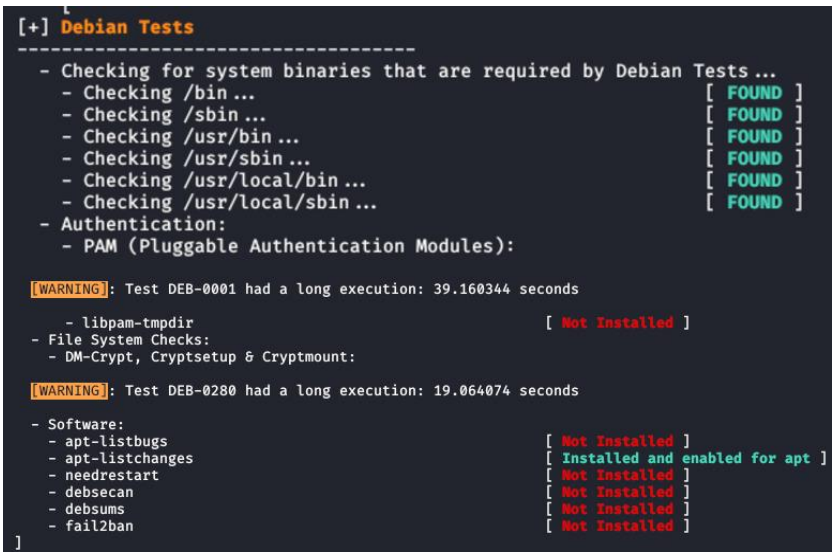


Zdroj: Vlastní zpracování

Windows hardening spočívá v omezení všech funkcí, které nejsou nutné k využití pro korektní běh operačního systému v jeho provozním režimu. Čím menší množství komponent tím se jeho údržba se stává jednoduší. Zvýšení bezpečnosti na této platformě může být skrze Powershell, který je natolik univerzální, že umožnuje veškeré potřebné kroky. Níže je popsána pouze část funkcí, které byli pomocí scriptu upraveny v systému. Pro zamezení možných komunikací mezi zařízeními bude upravený lokální firewall na stav blokování veškerého příchozího provozu. Pro svou obecnou činnost nepotřebuje žádný uživatel přijímat navázaná spojení. Kód se orientuje také na odebrání tzv. bloatware, neboli procesu, který může zpomalovat systém, využívat větší množství paměti, nebo výpočetní výkon. Jedná se o nežádoucí software. To samé platí i pro služby, jenž je ve výchozím nastavení v operačním systému Windows velké množství. Skrze registry se vypínají funkce jako Find My Device, Feedback, Telemetrie, povolení TLS verze 1.2, vypnutí IP verze 6 a další. Zároveň je nastavena politika hesel, kdy uživatel musí splnit minimální delku hesla a je zde nastaven také hranice neúspěšných pokusu o přihlášní pro zamknutí účtu.

Linux hardenig za pomocí programu Lynis, který kontroluje nastavení celého systému. Část jeho výpisu je zobrazena na obrázku 29. Jedná se o univerzální nástroj, který si podle typu operačního systému upravuje testovací postup. Kontroly nastavení se zaměřují na části jako Kernel, Boot a služby a systémové nástroje. Zároveň probíhá jednoduchý test operačního systému, kdy se kontroluje dostupnost základních složek. Náhled ověření zabezpečení systému je vidět na obrázku viz níže.

Obrázek 29 - Lynis



Zdroj: https://www.geeksforgeeks.org/lynis-security-tool-for-audit-and-hardening-linux-systems/

5.3.6 Aplikační architektura

Řízení přístupových účtů je hlavním pilířem bezpečnosti. Z bezpečnostní analýzy je patrné že se jedná o kritický bod. Touto částí je zamezeno zneužití jednoho přihlašovacího účtu na všech zařízeních a zároveň zamezení volnému přístupu na jednotlivé správy všech zařízení. Bez této části nelze považovat prostředí ze bezpečné. Vzhledem k tomu, že společnost využívá pouze jeden sdílený účet pro uživatele a jeden pro správu zařízení s neměnnými hesly, tak budou zavedeny úpravy v používání a politikách společnosti. Uživatelské účty přistupující na koncová zařízení nebudou vázáná jedním společným účtem na zařízení, ale budou zavedeny jmenné účty vázány k uživateli. Tyto přihlašovací údaje budou podléhat politice hesel, která bude vyžadovat komplexitu hesla ve smyslu velká, malá písmena, speciální symbol, číslo a minimální délka 12 znaků. Heslo s takovouto komplexitou je dle obrázku 16 dostatečně silné, aby nebylo prolomeno hrubou silou po dobu jednoho roku. Každý rok si uživatelé budou muset měnit vstupní hesla. Čímž bude zajištěno zajištění větší bezpečnosti oproti útokům hrubé síly a zároveň v případě nevědomého úniku bude zmenšeno časové okno pro jeho zneužití. U přihlašovacích údajích, které jsou mimo společnost, budou požadována stejná pravidla a zároveň k nim bude vynucováno dvoufázové ověření.

U administrativních účtů bude zavedena jmenná konvence, která bude podléhat definovanému tier modelu. Stanice a servery budou rozděleny podle kritičnosti do jednotlivých skupin. Popis složení těchto účtů je zobrazen v tabulce 5 níže.

Tabulka 5 - Pravidla názvů jmenných účtů

A	Administrativní účet
Číslo	Označení Tier 1 - Tier 1 2 - Tier 2 3 - Tier 3
.	Vizuální oddělení prefixu a části přihlašovacího účtu
Účet	Přihlašovací účet / hostname

Zdroj: Vlastní zpracování

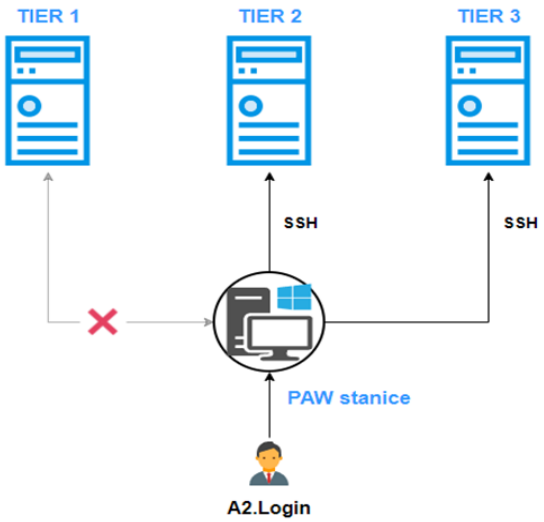
Přihlašovací údaje jsou rozděleny na 2 části. Prefixem je označení pomocí písmena „A“, že se jedná o účet administrativní. Za tímto písmenem je číslo, jenž vyznačuje Tier ukončené tečkou, která rozděluje prefix a jmenný přihlašovací název. Tento účet poté bude moc být využit pouze na přihlášení do zařízení, které spadá do daného Tier. U těchto účtů bude vyžadována rozdílná politika než u klasických jmenných. Hlavním rozdílem

je perioda změny hesel na půl rok, při změně v následujícím připojení a minimální délka nastavena na 16 znaků. V nejnižším Tieru 3 budou obsaženy koncové zařízení, ke kterým správce bude moc přistupovat pouze s přihlašovacími údaji „a3.login“. Jelikož se jedná o prostředí s malým počtem zařízení, jež nejsou v doméně, tak každé zařízení bude mít vlastní účet ve tvaru „a3.hostname“. Čímž se zabrání možnému zneužití jednoho účtu na všechna zařízení. Do vyššího Tier 2 je zahrnut souborový server, AP a tiskové řešení. V nejvyšším stupni označeným číslem jedna je zařazen nově využívaný rádius server a síťové prvky na páteřní lince do internetu. Všechny výše užité přihlašovací údaje mohou být využity pouze pro uživatelské přihlašování, v případě účtu využitého pro jiný účel jako je aplikace, tak je využit pouze prefix „app_“. Účty s tímto příznakem mohou vstupovat skrze Tier model, ale nesmějí se vyskytovat na zařízeních v Tier 3.

5.3.7 Vytvoření PAW

PAW (privileged access devices) stanice, jsou zařízení sloužící k přístupu pouze pro uživatele s vyšším oprávněním. Tento typ stanice je využit pro zvýšení bezpečnosti přístupu správy serverů. Jedná se o běžnou koncovou stanici, která nemá přístup do internetu a slouží pouze k přístupu zařízení ke spravovaným serverům. Tato stanice je síťově oddělena od ostatních, aby bylo zamezeno nechtěné komunikaci s ostatními koncovými zařízeními. Na tuto stanici se správce přihlašuje pomocí „a2.hostname“ a z tohoto zařízení se dále bude připojovat přes SSH protokol do dalších zařízení viz obrázek 30. Jedná se pouze o neúplné řešení pro co nejmenší množství nákladů. V případě, že by se nehledělo na množství využitých peněz, tak by se skrze PAW stanici přistupovalo na Jump Server pro daný Tier, z něhož by se poté mohlo přistupovat na jednotlivé prvky v dané části. V tomto případě se jedná o přímý přístup, kdy veškerá komunikace je omezena síťově přes firewall, kdy je zablokována veškerá příchozí komunikace a zároveň je umožněno pouze navazovat SSH spojení na jednotlivé zařízení.

Obrázek 30 - PAW v rámci Tier modelu



Zdroj: Vlastní zpracování

Zároveň by jednotlivé Tier neměli být rozděleny pouze logicky, ale také fyzicky na síťové vrstvě v rámci ISO/OSI modelu. Každý Tier by měl byt zařazen do vlastního síťového rozsahu, ve kterém by jednotlivé systémy byli rozděleny do svých specifických VLAN.

5.3.8 Auditování

Zaznamenávání událostí je základních aspektů, bez kterých nelze provádět plnohodnotnou forenzní analýzu. Každý operační systém umožnuje nadstavbu nad běžným záznamem informací. U zařízení s operačním systémem Windows byl využit program Sysmon a u zařízení s operačním systémem Linux je využito Auditd. Pomocí čehož se zvyšuje množství různorodých operací, které jsou zaznamenávány.

Sysmon je nástroj se nasazuje na všechny počítače ve společnosti z důvodu větší vizibility v prostředí, která umožní případnému forenznímu šetření útoku, nebo obecnému provoznímu nedostatku větší kontextové informace. Tyto informace mohou být jedním z více nepřímých ukazatelů na možné zneužití. Z důvodu, že Sysmon v základním nastavení generuje velké množství záznamů, které se poté stávají nepřehledné, je upraven konfigurační soubor tak, že omezuje množství sledovaných informací.

- Vytvoření procesu – Zaznamenává všechny procesy. Jsou zde také možnosti definování procesů, které jsou vyňaty ze sledování. Snahou je dosažení co největší přesnosti, aby se zabránilo spouštění cizích procesů, které se snaží pouze napodobit některý ze známých procesů. Dosažení větší přesnosti by nemělo být dosaženo pouze podle názvu souboru, ale například kombinací cesty a názvu.

Další úrovní by bylo zahrnout podepisování aplikací, ale tuto možnost Sysmon nepodporuje.

- Změny časových razítek na souborech pouze pro specifické soubory v adresářích uživatele, nebo všechny spustitelné soubory.
- Všechna navázaná spojení z definovaných programů jako je powershell, nmap. Také jsou vyspecifikované porty síťové komunikace, které jsou hojně využívány útočníky, jako RDP, Telnet, SSH.
- Sledování procesů, které vkládají kód do jiných procesů. Tímto krokem může Malware skrývat své akce.
- Vytvoření souboru na zařízení podle specifických přípon, kdy se sledují koncovky DLL, EXE, PS1 a další.
- Sledování zápisu dat do registrů, zde platí podobné podmínky jako u vytváření procesů. Operační systém Windows zavádí velké množství dat do registrů systému. Čímž se generuje velké množství událostí. Jelikož útočníci hojně využívají registry k zápisu dat, tak tato část musí být sledována. Z těchto důvodu se musí volit specifické části registrů které požaduje správce sledovat.
- Sledování vytvoření alternativních streamů v systému.

Upravený výňatek konfiguračního kódu XML pro Sysmon je zobrazený níže. Pro svou délku byl upraven pro názornost konfigurace. Kdy v první části jsou definovaný, jaké formáty otisků souborů budou ukládány. V řádku číslo 3 je uvedený parametr oznamující Sysmonu, vyžadující kontrolu certifikátů načtených ovladačů. V další fázi se již definují jednotlivé identifikátory s rozšířenými možnostmi flitrů, co je požadováno pro sledování a co není za pomocí příznaků *exclude/include*. Každý filtr začíná názvem daného souboru, jenž má sledovat. Na řádku 8 je údaj „ComandLine“, který sleduje, jestli proces svchost.exe nepoužil spuštění části s danými parametry. Tato část se při sepnutí nezaeviduje mezi události, jelikož je odebrána ze sledování viz řádek 7.

```
1.  <Sysmon schemaversion="1.10">
2.    <HashAlgorithms>md5,sha256,IMPHASH</HashAlgorithms>
3.    <CheckRevocation/>
4.    <EventFiltering>
5.      <!-- Event ID 1 == Process Creation -->
6.      <RuleGroup groupRelation="or">
7.        <ProcessCreate onmatch="exclude">
8.        <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
           dcomlaunch -s
           PlugPlay</CommandLine>
9.      </ProcessCreate>
10.     </RuleGroup>
```

```
    <!-- Event ID 2 == File Creation Time -->
    <RuleGroup groupRelation="or">
      <FileCreateTime onmatch="include">
        <Image name="technique_id=T1099,technique_name=Timestomp"
         condition="begin
         with">C:\Users</Image>
      </FileCreateTime>
    </RuleGroup>
    <RuleGroup groupRelation="or">
      <FileCreateTime onmatch="exclude">
        <Image condition="end
         with">AppData\Local\Google\Chrome\Application\chrome.exe</Image>
      </FileCreateTime>
    </RuleGroup>
  </EventFiltering>
</Sysmon>
```

Auditd je nastroj pro auditní záznamy pro operační systémy Linux. Pravidla lze dohledat v Linuxu na cestě „/etc/audit/audit.rules“ a konfiguraci auditního démona na cestě „/etc/audit/audit.conf“. Každé pravidlo, které se v tomto listu sepne, bude zauditováno. Níže je vyobrazena část pravidel ze souboru audit.rules. Pravidla hlídají například zápis do souboru *sudoers*, který definuje, jaké příkazy mohou, jací uživatelé spouštět. Také jsou v tomto výňatku hlídány zápisy do uživatelských skupin a souborů obsahující informace o heslech uživatelů. Poslední pravidlo sleduje zápis do souborů, které se starají o spouštění scriptů při startu, jenž využívají Systém V.

```
##Sudoers file changes
  -w /etc/sudoers -p wa -k actions
  -w /etc/sudoers.d/ -p wa -k actions

## User, group, password databases
  -w /etc/group -p wa -k etcgroup
  -w /etc/passwd -p wa -k etcpasswd
  -w /etc/gshadow -k etcgroup
  -w /etc/shadow -k etcpasswd
  -w /etc/security/opasswd -k opasswd

## System startup scripts
  -w /etc/inittab -p wa -k init
  -w /etc/init.d/ -p wa -k init
  -w /etc/init/ -p wa -k init
```

6. Závěr

Diplomová práce se zabývá Kybernetickou bezpečností malé podnikové IT infrastruktury. Hlavním cílem této práce bylo zabezpečit počítačovou síť z pohledu kybernetické bezpečnosti s co nejmenším finančním dopadem. Dílčím cílem práce bylo identifikovat a ohodnotit rizika spojená s možným dopadem kybernetických útoků na společnost.

Závěrečná práce byla rozdělena na dvě základní části, teoretickou a praktickou. Teoretická část práce byla věnována základním tématům, které se týkají kybernetické bezpečnosti. Tato témata byla popsána, jak z pohledu útoku, tak z pohledu zabezpečení.

Praktická část diplomové práce byla rozdělena do dvou základních fází. První byla Analýza bezpečnostních rizik a druhá Návrh zabezpečení a implementace.

V první fázi byl popsán postup pro zvýšení bezpečnosti v následujících bodech: popis společnosti, analýza bezpečnostních rizik, návrh zabezpečení a implementace. Jednotlivé části na sebe navazují a navzájem se doplňují.

Popis společnosti vychází ze stavu před touto diplomovou prací. Od začátku bylo patrné, že tato společnost neměla správně nastavenou síť. Hlavními příčinami tohoto stavu jsou nedostatečné množství finančních prostředků a zkrácený pracovní úvazek správce sítě pro práci na možném vylepšení stávajícího prostředí.

Samotná analýza rizik vychází ze sběru informací, testování a vyhodnocení. Části sběr informací a testování se prolínají. Navrženy byly tři testy pro získání podkladů. Jedná se o testy, které testují prostředí a uživatelé z vnějšího a vnitřního prostředí.

První test byl zvolen na základě nejčastěji se vyskytujícího útoku dle zprávy o stavu kybernetické bezpečnosti z roku 2020 od NÚKIB. Z této zprávy vyplývá, že nejčastějším útokem je zasílání podvodných e-mailů. První testem byl tedy phishing, který byl zasílán z venkovního prostředí na všechny uživatele společnosti. Tento test měl za cíl získat přihlašovací údaje uživatelů do e-mailových schránek a zároveň zjistit, jestli se tato hesla dají využít pro přihlášení do lokálních počítačů. Výsledky phishingu ukázaly, že 33 % uživatelů vstoupilo na podvrženou stránku a 15,5 % ze všech příjemců zadala své přihlašovací údaje.

Úkolem druhého testu bylo prokázat, jak náročné je získat přístup do interní sítě a následně zjistit přihlašovací údaje. Získání přístupu do interní sítě nebylo náročné, jelikož zde nebyla prováděná žádná kontrola na úrovní sítě. Každé zařízení, které se

připojilo do sítě se tedy stalo její součástí. Pro následné získání přihlašovacích údajů byl použit útok hrubou silou, jenž představuje testování všech možných kombinací hesel. Cílem tohoto testu nebylo pouze získat administrátorské heslo, ale také zjistit, jestli jsou v prostředí nastaveny politiky, které by tomuto typu útoků zabraňovaly. Jednalo se o kompletně úspěšný test, kdy se podařilo získat administrátorské heslo, které šlo aplikovat na všechna ostatní zařízení v síti.

Cílem třetího testu bylo získat informace o zranitelnostech v lokální síti. Poslední test byl závislý na úspěšnosti předchozího druhého testu. Bylo zapotřebí získat přístup do interní infrastruktury, aby následně mohlo dojít ke skenování zranitelností pomocí OpenVas. Bez získání přístupu by nemohlo dojít ke skenování. Software OpenVas slouží pro získání veřejně dostupných zranitelností k danému zařízení.

Výsledky těchto testů byly vyhodnoceny na základě tří parametrů: hrozba, zranitelnost a dopad. Výsledná hodnota těchto parametrů byla porovnávána vůči tabulce hodnocení rizik, která má předem definované rozsahy hodnot. Výsledkem byla kritická úroveň, která je definována jako neakceptovatelné riziko pro společnost a musí vést k okamžitému odstranění, nebo ukončení funkčnosti. Na základě informací získaných z provedených testů byla vyvozena nápravná opatření.

Druhá fáze byla zaměřena na aplikaci nápravných opatření pro snížení kritické hodnoty. Jednalo se o segmentaci z pohledu síťové i aplikační vrstvy, ověřování nových zařízení, zabezpečení síťových prvků a koncových stanic, vytvoření dedikované stanice pro správu a zvýšení auditování zařízení. Veškeré tyto body vycházejí z provedených testů a popisu společnosti. Po jejich implementaci došlo k úplnému nebo částečnému zamezení replikace prováděných útoků. Částečné odstranění se vztahuje pouze na první test – phishing, kde se musí pracovat s uživateli, a to především s jejich edukací v této problematice. V části zabezpečení byl kladen velký důraz na finanční náročnost. Pro aplikaci všech zmíněných bodů nebylo vynaloženo žádných finančních prostředků, jednalo se tedy čistě o práci s dostupnou výpočetní technikou.

Hlavní nedostatky zjištěné touto prací, jsou: plochá síť, přístup zařízení bez ověření, nezabezpečené síťové prvky, koncové stanice s jejich aplikacemi a nedostatečná aplikační architektura. Nejvýznamnější navržená doporučení k řešení zjištěných nedostatků ohledně kybernetické bezpečnosti jsou následující. Pomocí segmentace sítě byla rozdělena síť po logické a fyzické stránce, čímž byl vyřešen problém ploché sítě. Zařízení se rozdělila podle kritičnosti do jednotlivých skupin a zároveň každé této skupině byla

přidělena vlastní síť. Pro oddělení jednotlivých zařízení se využili VLAN. Pro vyřešení části přistupování nových zařízení do interní sítě byl zaveden Radius server, který ověřuje každé nové zařízení skrze certifikát. Bez správného certifikátu je zařízení odmítnuto. Ze zjištěných zranitelností při skenování pomocí softwaru OpenVas bylo zapotřebí zvýšit úroveň zabezpečení všech prvků v síti. Z dokumentací od výrobce vznikly zabezpečovací skripty, které se starají o zabezpečení sítových prvků a koncových stanic. Vlivem čehož došlo k odebrání zranitelností a zároveň nastavení bezpečnostních politik. V rámci aplikační architektury byl zaveden model dělení zařízení podle kritičnosti a zavedena stanice, která slouží pouze pro správu zařízení. Zároveň tato stanice nemá přístup do nejméně kritické skupiny.

V případě možnosti volného kapitálu na investici do inovací IT autor firmě doporučuje kroky, která by napomohla ke zvýšení kybernetické bezpečnosti. Při získání lepších zařízení by bylo možné využít například technologii SIEM, která by se starala o vyhodnocování základních bezpečnostních pravidel v reálném čase. Tato investice obsahuje pouze dostatečně výkonné zařízení. SIEM technologie například od společnosti IBM má verzi dostupnou zdarma, které má omezenou licenci. Další možnosti je vytvořit centrální Syslog server, kam se budou ukládat veškeré logy ze všech zařízení. Musí se jednat o vysoce zabezpečené zařízení, jelikož schraňuje zneužitelné informace ze všech zařízení a zároveň se musí zajišťovat duplicita dat pro případ poškození. Další úrovní zvýšení celé IT úrovně by bylo pořízení Windows server, který by umožnil vytvořit doménu, pro všechna koncová zařízení. Vlivem toho by byla ulehčena správa a publikace jednotlivých bezpečnostních politik. Závěrečným doporučením je zavedeni více faktorového ověření na zařízení, kdy tuto službu poskytuje například společnost ESET, od které je již využíváno antivirové řešení. Ve všech případech se jedná o body, které nelze využívat bez určité investice.

Stanovené cíle v úvodu práce se tak autorovi podařilo splnit. Byly zjištěny konkrétní nedostatky sítě. Navržená doporučení v závěru práce firmě mohou pomoci ke zlepšení jejich IT infrastruktury. Tato diplomová práce může svými poznatky posloužit libovolným společnostem ke zvýšení kybernetické bezpečnosti sítí, a to bez vynaložení finančních prostředků.

7. Citovaná literatura

1. consilium.europa.eu. *Kybernetická bezpečnost: jak EU řeší kybernetické hrozby.* [Online] 4. 1 2022. [Citace: 3. 2 2022.] https://www.consilium.europa.eu/cs/policies/cybersecurity/.

2. Sobers, Rob. Veronis.com. *134 Cybersecurity Statistics and Trends for 2021.* [Online] 16. 3 2021. [Citace: 2. 3 2022.] https://www.varonis.com/blog/cybersecurity-statistics.

3. NÚKIB. nukib.cz. *Národní úřad pro kybernetickou a informační bezpečnost.* [Online] 26. 07 2021. [Citace: 14. 02 2022.] https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf.

4. cisa.gov. *Stop RansomWare.* [Online] 2022. [Citace: 2. 3 2022.] https://www.cisa.gov/stopransomware#:~:text=Ransomware%20is%20a%20form%20of,ransom%20in%20exchange%20for%20decryption..

5. Cloudflare. cloudflare.com. *What is a DDoS attack?* [Online] 2022. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

6. ESET. eset.com. *Co je phishing?* [Online] 2022. https://www.eset.com/cz/phishing/.

7. Cynet. cynet.com. *Network Attacks.* [Online] 02 2022. [Citace: 02. 03 2022.] https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/.

8. Plummer, David C. datatracker.ietf.org. *rfc826.* [Online] [Citace: 14. 02 2022.] https://datatracker.ietf.org/doc/html/rfc826.

9. Behboodian, Navid. *ARP Poisoning Attack: An Introduction to Attack and Mitigations.* místo neznámé : CreateSpace, 2012. 1468068512.

10. Droms, R. datatracker.ietf.org/. *rfc2131.* [Online] 03 1997. [Citace: 16. 02 2022.] https://datatracker.ietf.org/doc/html/rfc2131.

11. Rey, Marina del. datatracker.ietf.org. *rfc793.* [Online] 08 1981. [Citace: 16. 02 2022.] https://datatracker.ietf.org/doc/html/rfc793.

12. Du, Wenliang. *Computer Security: A Hands-on Approach.* místo neznámé : CreateSpace Independent Publishing Platform. 1733003908.

13. amazon.com. *AWS Best Practices for DDoS Resiliency.* [Online] Amazon, 09 2021. [Citace: 11. 02 2022.] https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/aws-best-practices-ddos-resiliency.pdf#udp-reflection-attacks.

14. Santos, Omar. *CCNA Security 210-260 Official Cert Guide.* místo neznámé : Pearson Education (US), 2015. 1587205661.

15. Mockapetris, P. datatracker.ietf.org. *rfc1035.* [Online] 11 1987. [Citace: 11. 02 2022.] https://datatracker.ietf.org/doc/html/rfc1035.

16. Liska, Allan. *DNS Security.* místo neznámé : Syngress Media,U.S., 2016. 0128033061.

17. U. Blumenthal, B. Wijnen. datatracker.ietf.org/. *rfc3414.* [Online] 11 2002. [Citace: 18. 02 2022.] https://datatracker.ietf.org/doc/html/rfc3414.

18. S. HomChaudhuri, M. Foschiano. rfc-editor.org. *rfc5517.* [Online] 02 2010. [Citace: 10. 01 2022.] https://www.rfc-editor.org/rfc/rfc5517.txt.

19. Chebbi, Chiheb. *Advanced Infrastructure Penetration Testing: Defend your systems from methodized and proficient attackers.* místo neznámé : Packt Publishing, 2018. 9781788623414.

20. contrastsecurity.com. *Application Attacks.* [Online] 2022. [Citace: 02. 03 2022.] https://www.contrastsecurity.com/knowledge-hub/glossary/application-attacks#:~:text=What%20Is%20an%20Application%20Attack,application%20vulnerabilities%20written%20within%20code..

21. Willeke, Jim. ldapwiki.com. *LM Hash.* [Online] 07. 08 2018. [Citace: 19. 01 2022.] https://ldapwiki.com/wiki/LM%20hash.

22. Nuno-Tavares. microsoft.com. *NTLM vs KERBEROS.* [Online] 13. 04 2018. [Citace: 22. 1 2022.] https://answers.microsoft.com/en-us/msoffice/forum/all/ntlm-vs-kerberos/d8b139bf-6b5a-4a53-9a00-bb75d4e219eb.

23. Microsoft. microsoft.com. *Winlogon and GINA.* [Online] 01. 07 2021. [Citace: 22. 1 2022.] https://docs.microsoft.com/en-us/windows/win32/secauthn/winlogon-and-gina.

24. —. microsoft.com/. *Interactive Authentication.* [Online] 01. 07 2021. [Citace: 22. 01 2022.] https://docs.microsoft.com/en-us/windows/win32/secauthn/interactive-authentication.

25. JUNGLES, Patric, SIMONS, Mark a GRIMES, Roger. Mitigating Pass-the-Hash (PtH) Attacks. [Online] 2012. [Citace: 23. 01 2022.] http://goo.gl/datSeV.

26. Kaspersky. kaspersky.com. *Brute Force Attack: Definition and Examples.* [Online] [Citace: 25. 01 2022.] https://www.kaspersky.com/resource-center/definitions/brute-force-attack.

27. cloudnine.com. *How Long Will it Take to Crack Your Password?: Cybersecurity Trends.* [Online] 2019. [Citace: 11. 03 2022.] https://cloudnine.com/ediscoverydaily/electronic-discovery/how-long-will-it-take-to-crack-your-password-cybersecurity-trends/.

28. Hassan, Nihad A. *Ransomware Revealed: A Beginner's Guide to Protecting and Recovering from Ransomware Attacks.* místo neznámé : Apress, 2019. 1484242548.

29. Dossett, Julian. cnet.com. *A timeline of the biggest ransomware attacks.* [Online] 15. 11 2021. [Citace: 30. 1 2022.] https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/.

30. Cisco. cisco.com. *Základy síťové bezpečnosti pro malé podniky.* [Online] 2018. [Citace: 03. 03 2022.] https://www.cisco.com/c/dam/global/cs_cz/solutions/small-business/pdf/smb_networksecuritychecklist_cz.pdf.

31. Bouška, Petr. samuraj-cz.com. *Cisco IOS 24 - zabezpečení komunikace na portech.* [Online] 09. 11 2016. [Citace: 1. 12 2021.] https://www.samuraj-cz.com/clanek/cisco-ios-24-zabezpeceni-komunikace-na-portech/.

32. P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese. datatracker.ietf.org. *RFC3580.* [Online] 10 2003. [Citace: 2. 12 2021.] https://datatracker.ietf.org/doc/html/rfc3580.

33. Intel. intel.com. *802.1X Overview and EAP Types.* [Online] 10. 28 2021. [Citace: 19. 02 2022.] https://www.intel.com/content/www/us/en/support/articles/000006999/wireless/legacy-intel-wireless-products.html.

34. P. Eronen, H. Tschofenig, Y. Sheffer. tools.ietf.org. *An Extension for EAP-Only Authentication in IKEv2.* [Online] 2009. [Citace: 23. 02 2022.] https://tools.ietf.org/id/draft-eronen-ipsec-ikev2-eap-auth-07.html.

35. Stone, Mark. cybersecurity.att.com. *Firewalls explained: the different firewall types and technologies.* [Online] 10. 09 2020. [Citace: 26. 02 2020.] https://cybersecurity.att.com/blogs/security-essentials/what-is-a-firewall-types-technologies-explained.

36. MicroFocous. microfocus.com. *Application security.* [Online] 2022. [Citace: 04. 03 2022.] https://www.microfocus.com/en-us/what-is/application-security.

37. Microsoft. microsoft.com. *Privileged access model.* [Online] 07. 02 2022. [Citace: 23. 02 2022.] https://docs.microsoft.com/cs-cz/security/compass/privileged-access-access-model.

38. appsealing.com. *Application Hardening – An In-Depth Guide To Understand App Hardening.* [Online] 31. 8 2021. [Citace: 6. 2 2022.] https://www.appsealing.com/application-hardening/.

39. hysolate.com. *Windows Hardening: Detailed Checklist for Windows Server and Windows 10.* [Online] 2022. [Citace: 25. 02 2022.] https://www.hysolate.com/learn/os-isolation/windows-hardening-checklist-for-windows-server-windows-10/#:~:text=What%20is%20Windows%20Hardening%3F,that%20threat%20actors%20can%20exploit..

40. microsoft.com. *Sysmon.* [Online] 28. 01 2022. [Citace: 20. 02 2022.] https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon#:~:text=System%20Monitor%20(Sysmon)%20is%20a,changes%20to%20file%20creation%20time..

41. microsoft.com. *AppLocker.* [Online] 29. 10 2021. [Citace: 20. 02 2022.] https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview.

42. microsoft.com. *BitLocker.* [Online] 12. 03 2021. [Citace: 21. 02 2022.] https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview.

43. Grubb, Steve. linux.die.net. *auditd(8) - Linux man page.* [Online] [Citace: 21. 02 2022.] https://linux.die.net/man/8/auditd.

44. Tek-Tools. https://www.tek-tools.com/. *How to Secure Your Network Using IDS/IPS Tools.* [Online] 30. 05 2020. [Citace: 06. 03 2022.] https://www.tek-tools.com/security/best-ids-and-ips-tools#:~:text=Difference%20Between%20IDS%20and%20IPS&text=The%20significant%20difference%20between%20them,it%20based%20on%20a%20ruleset..

45. Karen Scarfone, Peter Mell. nist.gov. *Guide to Intrusion Detection and Prevention Systems (IDPS).* [Online] 02 2007. [Citace: 21. 02 2022.] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf.

46. suricata.readthedocs.io. *Suricata.* [Online] 2019. [Citace: 22. 02 2022.] https://suricata.readthedocs.io/en/suricata-6.0.0/configuration/.

47. IBM. ivm.com. *Why is SIEM important?* [Online] [Citace: 22. 02 2022.] https://www.ibm.com/topics/siem.

48. balbix.com. *What is the NIST Cybersecurity Framework?* [Online] 2021. [Citace: 13. 03 2022.] https://www.balbix.com/insights/nist-cybersecurity-framework/.

49. Mikrotik. wiki.mikrotik.com. *Manual:Securing Your Router.* [Online] MediaWiky, 31. 5 2019. [Citace: 3. 6 2022.] https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router.

50. K. Moriarty, S. Farrell. datatracker.ietf.org. *rfc8996.* [Online] 03 2021. [Citace: 16. 02 2022.] https://datatracker.ietf.org/doc/rfc8996/.

51. cvedetails.com. *The ultimate security vulnerability datasource.* [Online] 2022. [Citace: 17. 03 2022.] https://www.cvedetails.com/vendor/53/adobe.html.