Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Implementace opatření kybernetické bezpečnosti do firemní konvergované sítě

Diplomová práce

Autor: Bc. Stanislav Hladík

Studijní obor: IM2-K

Vedoucí práce: Ing. Pavel Blažek, Ph.D.

Hradec Králové Listopad 2021

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

…….

V Hradci Králové dne 15.11.2021 Bc. Stanislav Hladík

Poděkování:

Tímto bych rád poděkoval svému vedoucímu práce Ing. Pavlovi Blažkovi, Ph.D. za jeho odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování diplomové práce. Dále bych rád poděkoval svému firemnímu nadřízenému Ing. Tomášovi Pechancovi za umožnění využití firemních zdrojů a materiálů a za umožnění práce na firemní bezpečnostní problematice.

Anotace

Cílem diplomové práce je implementace opatření kybernetické bezpečnosti do konvergované síťové infrastruktury společnosti Saint-Gobain Adfors v reakci na vzestupnou tendenci kybernetických útoků po celém světě. Teoretická část práce popisuje infrastrukturní prvky, možnost jejich kompromitace a metody, jak na vzniklé hrozby reagovat. Praktická část práce se zabývá zavedením kybernetických opatření do prostředí firmy a je rozdělena do šesti dílčích implementačních kroků. V prvním kroku je zajištěno fyzické zabezpečení informačního serveru a síťového racku. Druhý krok řeší ochranu uživatelů a jejich zařízení formou „čistících stanic“ na USB disky. Třetí krok práce řeší ochranu síťových prvků infrastruktury, nastavením bezpečnostních metod u zařízení druhé síťové vrstvy. Ve čtvrtém kroku je implementován síťový firewall nové generace a popsány kroky, které vedly k jeho úspěšnému spuštění. V pátém kroku se práce zabývá bezpečností výrobních aplikací společnosti a šifrováním jejich konfiguračních souborů. V posledním kroku práce jsou nastíněny dva návrhy interních směrnic, které řeší vztah uživatele a správce s informačními systémy společnosti.

V závěru práce jsou zmíněny další možné kroky a návrhy, které by mohly v budoucnu dopomoci k dosažení adekvátní úrovně kybernetické bezpečnosti napříč sítí celé společnosti.

Klíčová slova

Bezpečnost, konvergovaná síť, firewall, switch, aplikace, infrastruktura, kybernetický útok

Annotation

Title: Implementing cybersecurity measures into a corporate converged network

The objective of the diploma thesis is the implementation of cybersecurity measures into a converged network infrastructure of Saint-Gobain Adfors in response to a worldwide upward trend of cyber-attacks. The theoretical part describes infrastructure elements, the way how to compromise, and methods how to respond to emerging threats. The practical part deals with the implementation of cyber measures into the corporate environment and is divided into six sib implementation steps. The first step leads to ensuring the physical security of the information server and network rack. The second step provides the protection of users and their equipment's in the form of control stations for USB disks. The third part of the thesis solves the protection of the network's infrastructure elements by settings security methods for the second network layer devices. The fourth step brings the implementation of the network new generation firewall and described the steps that led to its successful launch. The fifth step of the thesis deals with the security of the production applications of the company and with encrypting their configuration files. The last step of the work is outlined two proposals of internal directives that address the relationship between the user and the administrator with the company's information systems.

In the conclusion of the diploma thesis are mentioned other possible steps and suggestions, which could help in the future to modern and stable cyber security across the company.

Keywords

Security, converged network, firewall, switch, application, infrastructure, cyber attack

Obsah

Seznam tabulek

Seznam obrázků

Úvod

V dřívější době byly počítače osamocené pracovní jednotky vykonávající požadavky uživatelů nezávisle na okolním světě a pokud bylo potřeba sdílet pracovní soubor se spolupracovníkem, museli jste ho nahrát na přenosné úložiště a zdlouhavě přenášet.

Dnes jsou však počítače propojené pomocí síťových technologií, které se stávají nedílnou součástí našich životů. Síťové technologie otevírají obrovské možnosti komunikace mezi počítači, jež mohou být i stovky kilometrů vzdálené. Například je možné pracovat na úpravě dokumentu ve Wordu na jednom počítači a zároveň ho pročítat na jiném zařízení připojeném na stejné síti, nebo pomocí sítě sdílet tiskárny a jiná zařízení, což uživatele oprostí od náročného instalování ovladačů na každý počítač jednotlivě. Ve firemním prostředí už si asi nikdo z kancelářských pracovníků nedokáže představit život bez databázových systémů, kde jsou uložena všechna data, a které nahradily papírové kartotéky.

Sítě je však nutné kvalitně spravovat, protože opravdu rozsáhlé firemní sítě mohou obsahovat stovky, až tisíce koncových zařízení a infrastrukturních prvků, které běžný uživatel nevidí. Jedná se o infrastrukturní prvky, jako například router, switch, access point (AP), firewall a další zařízení nevyjímaje. Na každé takové zařízení je nutné brát ohled a věnovat mu servisní čas.

Pojem, na který se ve vztahu se sítěmi nesmí nikdy zapomínat, je zabezpečení počítačové sítě. Datové sítě jsou v dnešní době vystavovány mnohým kybernetickým útokům. Počet těchto útoků se může vyšplhat až k tisícům denně, což nás musí vést k myšlence, že je dobré se na zabezpečení počítačové sítě pořádně připravit. Mnoho z těchto kybernetických útoků jsou pouze lehké pokusy testující kvalitu našeho zabezpečení, například prohledávání a skenování sítě. Tyto typy útoků nejsou ve své podstatě ohrožující. Bývají ale předzvěstí větších útoků, které není dobré brát na lehkou váhu a je velmi vhodné proti nim použít sofistikovanější metody obrany.

Trendem rozšíření síťové infrastruktury jsou bezdrátové komunikační technologie. Bez těchto technologií si v moderním světě takřka žádná firma nedokáže představit plynulý běh svého pracovního procesu, ať už se jedná o firmu specializující se na počítačové technologie, účetnictví nebo na výrobní sféru. U bezdrátových technologií je ještě větší potřeba důrazu na kvalitní zabezpečení, jelikož u bezdrátové sítě mohou osoby, a tudíž i potenciální útočníci, kteří jsou vně fyzicky zabezpečeného místa, sledovat provoz bezdrátové sítě, analyzovat datové přenosy, případně přistupovat k aplikacím.

Bezdrátové technologie je tedy nutné budovat jak s ohledem k potřebám uživatele, tak s respektem k bezpečnostním požadavků. V rámci bezdrátových technologií existují různé bezpečnostní prvky, například protokoly WEP (Wired Equivalent Privacy), WPA, WPA2 (Wi-Fi Protected Access).

Každá firma by měla do své síťové infrastruktury zakomponovat více ochranných systémů a prvků, které do sebe svojí funkcionalitou zapadají jako dětská skládačka. Součásti síťového zabezpečení, jako například: Firewall, IDS (Intrusion Detection System), VPN (Virtual private Network) a antivirový software budou představeny na následujících stránkách, spolu s metodou, jak dané komponenty poskládat dohromady, aby tvořily efektivní ochranu firemní i domácí sítě.

Neméně důležitou součástí zabezpečení jak drátové, tak bezdrátové sítě je lidský faktor. Ten je obvykle nejslabším článkem kteréhokoliv zabezpečení informačního systému. A protože je každý systém právě tak silný (resp. slabý), jako jeho nejslabší článek, je nutno s tímto faktem pracovat v souladu s požadavky dnešní doby. Hrozby jsou v tomto směru opravdu rozmanité. Od nalezeného USB flash disku pohozeného na ulici, který zaměstnanec firmy vezme a vloží bez předchozí kontroly profesionálem do počítače, až po moderní trend přístupu k práci *BYOD* (Bring your own device), kde si zaměstnanci nosí svá vlastní chytrá zařízení (notebook, smartphone) do firemního prostředí. Tím jsou samozřejmě zvýšeny nároky na informační bezpečnost ve firmě.

Všechny tyto problémy je ale také nutné řešit s ohledem na finanční stránku věci a záleží na firmě jakou částku je ochotna vložit do svých bezpečnostních opatření. Je tak je výzvou pro každého IT pracovníka, aby se s tímto problémem zvládl vypořádat.

1 Historie sítí a datové komunikace

Již v začátcích budování komunikačních sítí se velmi přísně rozlišovalo mezi několika kategoriemi síťových přenosů a toto rozdělení přetrvává i dnes. Jednalo se o sítě pro hlasovou komunikaci, datovou komunikaci a pro zábavu. Pro hlasovou komunikaci se používaly pevné analogové sítě s komutací okruhů nebo rádiová síť. Zábavu obstarávaly výhradně sítě rozhlasového a televizního vysílání. Datová komunikace se začala vyvíjet jako poslední a ve svých začátcích byla velmi omezená, uměla buď přímé připojení mezi terminály a hlavním hostitelským počítačem po sériových linkách nebo vzdálené připojení přes modem. [1][17]

Ačkoli se měnily všechny tři zmíněné komunikační rámce, původní kategorizace však zůstala neměnná. Hlasová komunikace probíhala především pomocí analogového přenosu. Ústředny, které sloužily jako srdce analogového přenosu, se však z velké části zdigitalizovaly. Také vznikaly malé uživatelské pobočkové ústředny, které postupně obdržely stejné funkce jako velké servisní ústředny. V této době pomalu vstupovala na scénu také mobilní komunikace. V kategorii sítí týkající se zábavy se postupně rozšiřovaly kabelové sítě a systémy elektronických nástěnek. [1]

1.1 1961–1972 Vývoj a demonstrace prvních principů přepínání paketů

Změny, které se udály v datové komunikaci, byly nejvýraznější ze všech tří oblastí. Celé odvětví datových komunikací, počítačových sítí a internetu spadá do začátku 60. let 20. století, to byla doba, kdy byla dominantním prvkem komunikační technologie telefonní síť. Vzhledem k tomu, že v 60. letech velmi rostl výkon (a také cena) počítačů, bylo přirozené, že se začalo uvažovat o tom, jak tyto počítače propojit dohromady, aby mohly být sdíleny napříč uživateli stovky kilometrů vzdálenými. K účelu propojení počítačů byla nejprve využita již zmíněná telefonní síť. Zde se však brzy objevil problém s přepínaným připojením, protože telefonní síť pracuje na principu přepojování okruhů informací od odesílatele k příjemci, což je vhodná volba pro použití přenášení hlasu konstantní rychlostí mezi dvěma body. Pro komunikaci mezi počítači je však tento systém nepraktický, protože zde dochází k tzv. nárazovým intervalům činnosti, například odesílání příkazu na vzdálený počítač, následovaný určitým časem nečinnosti při čekání na odpověď z druhé strany. [5]

Dohromady tři skupiny badatelů, nezávisle na sobě, začaly zkoumat možnost přepínat pakety namísto přepínaní celých komunikačních obvodů. První publikovanou práci na téma technik přepínání paketů napsal Leonard Kleinrock v době, kdy ukončoval své studium na MIT (Massachusetts Institute of Technology). Leonard Kleinrock v této práci demonstroval efektivitu přepínání paketů pro plně vytížené datové spojení. V přibližně stejné době se Paul Baran a společníci z institutu Rand začali zabývat použitím přepínání paketů pro bezpečný přenos vojenskými sítěmi. Také vědci Donald Davies a Roger Scantlebury z Národního fyzikální institutu v Anglii rozvíjeli své poznatky o přepínání paketů. [5]

Vědecké práce z MIT, institutu Rand a NPL (National Physical Laboratory) položily základ podoby Internetu, tak jak ho známe dnes. Avšak historie Internetu je o mnoho delší a složitější. Kolegové z MIT Joseph Carl Robnett Licklider a Lawrence Roberts vedli v 60. letech 19. století počítačovo-vědecký program v ARPA (Advanced Research Projects Agency) ve Spojených státech amerických. Lawrence Roberts v té době představil komplexní plán projektu ARPAnet (první počítačovou síť na bázi přepínání paketů a prvního předchůdce Internetu). Jako vlastní síťový uzel byl použit univerzální počítač Honeywell DDP516, který byl naprogramován tak, aby fungoval jako tzv. IMP (Interface Message Processor). IMP fungoval jako uzel pro přepínání paketů v síti pro propojení účastníků sítě ARPAnet. Pro vzájemnou komunikaci mezi uzly byly použity pevné okruhy s přenosovou rychlostí 50 kbps a protokol NCP (Network Control Protocol). Do konce roku byla síť uvedena do provozu a její uživatelé mohli začít využívat výpočetní kapacitu superpočítačů, které byly touto sítí propojeny. Velikost Arpanetu však rostla raketovou rychlostí. V roce 1971 obsahoval celkem 15 uzlů a jejich počet neustále rostl. V roce 1972 měl Arpanet již 37 uzlů a o rok později se k němu připojily také první zahraniční uzly, konkrétně ve Velké Británii a v Norsku. [5][15]

Původní představa o funkcionalitě Arpanetu nebyla příliš správná. Prvotní funkce Arpanetu měla být možnost práce na vzdálených počítačích (prostřednictvím vzdáleného přihlašování). Praktické zkušenosti však ukázaly, že uživatelé využívají síť spíše pro odesílání a příjem elektronické pošty. Využívali totiž přenosové možnosti Arpanetu hlavně k přenosu osobních i neosobních vzkazů v rámci diskusí elektronických konferencí. Arpanet byl tedy především využíván k tomu, aby lidé na dálku spolupracovali na různých projektech, aby si předávali zkušenosti a poznatky, a aby se vzájemně informovali o aktuálním dění. Funkce to byly natolik lákavé, že o mnoho předčily prvotní možnost „počítání na dálku“. Tento trend také vydržel až do dnešních dní. [1][5][16]

1.2 1973–1983 Nástup TCP/IP, které nahradilo NCP

V roce 1973 spolupracovali Robert Kahn a Vinton Cerf na vývoji protokolu, který by spojoval rozličné sítě dohromady. Z tohoto pokusu se postupně stal TCP/IP (Transmission Control Protocol/Internet Protocol). Tento protokol měl plnit základní pravidla:

- Každá síť bude fungovat samostatně a nebude potřeba žádná vnitřní změna pro připojení k Internetu.
- Přenos dat bude fungovat na principu „nejlepší snahy“ tzn. pokud se paketu nepodaří dorazit do cíle, zdroj tento paket vyšle znovu.
- K propojování sítí mezi sebou se budou využívat tzv. černé skříňky (v prvotní fázi: brány (gateways), později: směrovače (routery)), které nebudou udržovat žádné informace o tocích procházejících paketů.
- Nebude existovat žádné globální řízení sítí na provozních úrovních. [1]

V prvotních fázích byl protokol **TCP** vyvinut jako obecný komunikační protokol předpokládající nespolehlivou síť. Zodpovědnost za spolehlivost komunikace v síti byla převedena na koncové uzly. Dále se TCP staral o směrování paketů v síti. V dnešním pohledu na síťové technologie a rozdělení vrstev plnil TCP protokol funkci transportní a síťové vrstvy (v roce 1978 se funkce směrování paketů od TCP oddělila, a protokol se měl nadále starat pouze o segmentování zpráv do paketů u zdroje a jejich opětovné sestavování u cíle, detekci chyb a opětovné vysílání ztracených signálů). [1]

Poté v roce 1976 vznikla první kniha o ARPNET (*Queuening Systems: Vol II, Computer Aplications, John Wiley and Sons*), kterou publikoval Leonard Kleinrock. Nedílnou součástí Internetu jako takového je bezesporu tzv. **IP** protokol (*Internet Protocol*), což je nejpoužívanější protokol pro komunikaci v počítačových sítích. Tento protokol má za úkol posílat pakety z jednoho zařízení do druhého. Specifikaci tohoto protokolu vytvořil Vint Cerf (*University of California, Los Angeles*) a Jon Postel (*Information Sciences Institue*). V tomto období dále probíhaly experimenty s TCP protokolem kvůli nalezení zjednodušené alternativy. Tento nový typ protokolu měl sloužit především službám, pro které nemusí být spolehlivé transportní služby výhodné. Kvůli těmto důvodům vznikl **UDP** protokol (User datagram protocol). V 70. letech tedy vznikly tři klíčové Internetové protokoly, které stále slouží, i po takřka 50. letech. V roce 1980 byl v sítích ARPANET,

BBN a UCB (University of California at Berkeley) zaveden experimentální provoz TCP/IP. Zde se využila adresace pomocí IPv4 a také systém **DNS** (Domain Name System). [1][5]

K obrovskému rozmachu Internetu, který se udál v 80. letech 20. století (na konci 70. let bylo k síti ARPANET připojeno cca 200 zařízení, zatímco na konci 80. let byl počet připojených zařízení k síti Internet okolo 100 000) přispělo mnoho pokusů vytvořit počítačovou sít propojující dohromady světové univerzity. Síť BITNET (Because It's Timet NETwork) poskytovala emailové a souborové přenosy mezi mnoha univerzitami na severovýchodě USA. CSNET (Computer Science Network) byl vytvořen k připojení k univerzitním výzkumům, aniž by bylo nutné připojit se k ARPANETU. [5][16]

V lednu roku 1983 bylo TCP/IP oficiálně zavedeno jako architektura ARPANETU, zde TCP/IP architektura vystřídala dosud sloužící protokol NPC. V tuto dobu byl také ARPANET rozdělen na dvě různé sítě (ARPANET pro výzkumné účely a MILNET (Military network) pro běžný provoz). [1]

1.3 1983–1990 Pokračování v šíření sítí

Paralelně s vývojem ARPANETU spustila Francie svůj vlastní projekt nazvaný **Minitel**. Tento ambiciózní plán měl „přivézt data" do každého domu ve Francii. Celý tento projekt byl plně sponzorován francouzskou vládou. Komunikační systém Minitel sestával ze sítě fungující na principu přepínání paketů (založeném na protokolu X.25), serverů Minitel a z levných terminálů s vestavěnými nízkorychlostními modemy. Minitel se však stal obrovským úspěchem až poté, co francouzská vláda darovala terminál do každé domácnosti, která o něho měla zájem. Minitel byl využíván až 20% francouzské populace a na jeho chodu se podílelo okolo 10 000 lidí. I přesto, že se tento projekt těšil obrovské oblibě, byl postupně nahrazen konkurencí v podobě Internetu. [5]

V letech 1985-86 byl zahájen program NSFNET (NSE National Science Foundation), který měl za úkol propojení 6 superpočítačových center. NSFNET se podílel na rozvoji Internetu sponzoringem v hodnotě 200 miliónů dolarů. [5]

1.4 1990 – současnost

Začátek 90. let byl poznamenán dvěma událostmi, které předpovídaly blížící se komercializaci Internetu. První událostí byl konec ARPANETU, projektu, který je právem nazýván jako předchůdce Internetu. Druhou událostí je bezpochyby vytvoření informačního systému **WWW** (World Wide Web**)** ve švýcarském vědeckém centru CERN, který přivedl

Internet do firem i domácností a tím ovlivnil miliony lidí. Web začal také velmi rychle sloužit jako platforma pro vývoj a vydávání tisíců nových aplikací. [5]

V návaznosti na vznik WWW vznikl roku 1992 první internetový prohlížeč **Mosaic**, který je předchůdcem všech dnešních moderních prohlížečů. Od roku 1994 se internet dále komercializuje a NSFNET se dále stává privátním projektem. Páteřní síť Internetu je komerčně provozována sítí vBNS (very high-performance Backbone Network Service), NFS (National Science Foundation) a MCI Telecommunications. Americký federální výbor FNC (Federal Networking Council) poté schválil definici Internetu jako globálního informačního systému, jenž:

- Je logicky propojený v globálně adresním prostoru založeném na protokolu IP nebo jeho rozšířeních.
- Podporuje komunikaci založenou na souboru protokolů TCP/IP nebo jeho rozšířeních.
- Poskytuje, používá a zpřístupňuje veřejně nebo soukromě služby vysoké úrovně založené na této komunikační infrastruktuře. [1][5]

V rozmezí let 1997–1999 byly zahájeny projekty nazvané Internet 2 a NGI (Next Generation Internet). Tyto projekty byly iniciovány americkou akademickou a výzkumnou obcí, podpořené sponzorskými aktivitami mnoha výrobců různých síťových zařízení UCAID (University Corporation for Advanced Internet Development). Toto uskupení mělo za cíl testovat rozšíření protokolu TCP/IP, s cílem zlepšení kvality služeb, garantování úrovní služeb pro kritické aplikace, skupinové vysílání a zavedení IPv6 pro pozdější využití v síti Internet. Oficiální spuštění proběhlo v únoru 1999. Sítí Internet 2 bylo propojeno 150 univerzit plně optickou páteřní sítí s cílovou propustností 9,6 Gbit/s. [1]

V roce 1998 vznikla společnost **ICANN** (Internet Corporation for Assigned Names and Numbers), která přebrala zodpovědnost za registraci doménových jmen od organizací IANA a NSI. [1]

Rok 2001 a BitTorrent, decentralizovaný komunikační protokol pro sdílení souborů peer to peer, spatřil světlo světa. Tato Open source technologie umožňuje uživatelům stahovat velké soubory z více hostitelů najednou, tím je odlišná od tradiční technologie stahování obsahu z jednoho dedikovaného serveru. BitTorrent je však velmi často zneužíván ke stahování nelegálního obsahu. V tomto roce také, po čtyřletém výzkumu na poli kryptografických protokolů, vydává NIST (National Institute of Standards and Technology) tzv. AES (Advanced Encryption Standard), což je standardizovaný algoritmus používaný k

šifrování dat v informatice. Klíč vytvořili belgičtí kryptografové Vincent Rijmen a Joan Daeman. AES nahradil již zastaralý šifrovací klíč DES (Data Encryption Standard), který byl přijat v roce 1977, ale byl již nedostačující proti kryptografickým útokům hrubou silou. [18]

Dalším velkým rokem Internetu a jeho historie se stal rok 2004. V tomto roce založil Mark Zuckerberg se svými kolegy z Harvardu světoznámou sociální síť Facebook. Společnost se poté velmi rychle stala globální a začala velmi rychle prosazovat politiku monetizace uživatelů. Tímto krokem se stala velkým rivalem společnosti Google. [18]

Na začátku roku 2006 začal Amazon Web Services pronajímat IT infrastrukturu. Tím byl stvořen pojem „Cloud computing“ což v sobě zahrnuje ukládání, zpracování dat a aplikací na vzdálených serverech. Cloud computing umožňuje jednoduché ukládání dat, stejně tak přístup k nim a práci s nimi. Díky Cloud computingu je také možné konečně využít potenciál mobilního přístupu k datům. Centralizace dat, kterou Cloud computing bezpochyby je, však také přináší výzvy v oblasti zabezpečení dat, se kterými se pracuje.

V roce 2009 spustil Satoshi Nakamoto síť kryptoměny Bitcoin. Jedná se o decentralizovaný, kryptograficky bezpečný peer to peer protokol tzv. Blockchain. Tato technologie umožňuje provádění ověřitelných transakcí bez potřeby centrálních entit. [18]

Dále se v roce 2010 podařilo Federální komunikační komisi prosadit zásady neutrální sítě a otevřeného internetu s tím, že ISP (Internet Services providers) musí nabízet stejný přístup k veškeré komunikaci na internetu, aniž by byly upřednostňovány konkrétní stránky nebo služby. [18]

Dalším zajímavým milníkem je rok 2013 a zjištění, které uskutečnil spolupracovník CIA Edward Snowden, jenž popisuje praktiky, jak Národní bezpečnostní agentura, pomocí telekomunikačních firem monitoruje chování občanů USA. V této kauze byly zainteresováni i velcí hráči na poli sociálních sítí (Google, Facebook, Microsoft a Yahoo).

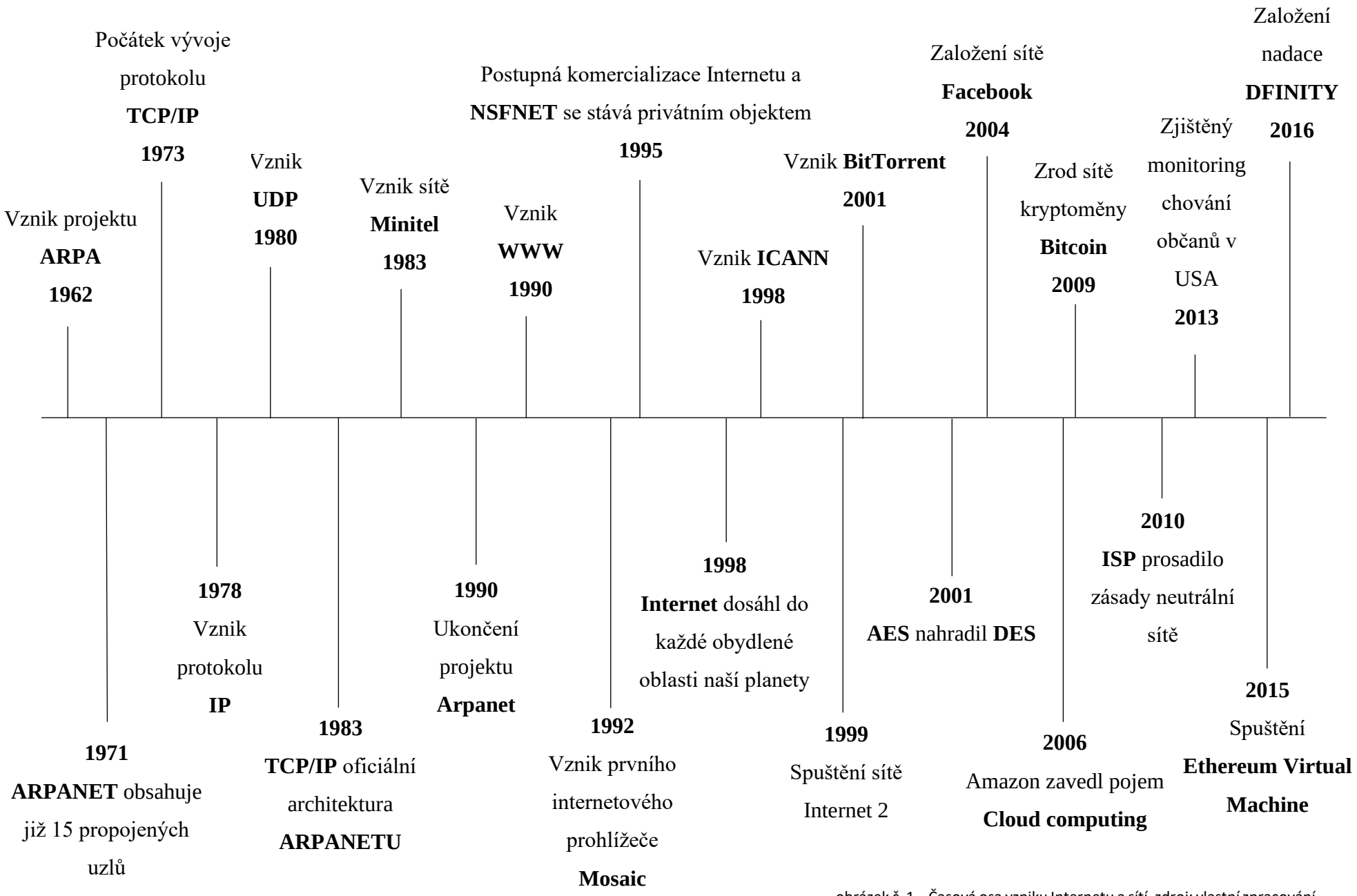
V roce 2015 bylo zaznamenáno spuštění Ethereum Virtual Machine, což je open-source blockchain výpočetní platforma, která se pro vývojáře stává oblíbenou kvůli způsobu nasazování decentralizovaných aplikací, jako jsou například hry, sociální média a platformy pro práci s decentralizovanými financemi. [18]

Následuje rok 2016 a založení nadace DFINITY ve švýcarském Curychu. DFINITY dále vlastní výzkumná centra v Palo Altu, San Franciscu, Tokiu a Curychu. Společnost se zaměřuje na vývoj „Internetového počítače“, jenž má změnit definici Internetu jako počítače, který hostí velké množství zabezpečeného softwaru. Projekt kombinuje technologii

blockchain a nové postupy kryptografie, tím vytváří decentralizované prostředí pro interoperabilní software, který běží přímo v otevřené síti. [19]

Směr vývoje Internetu, který probíhá v dnešních dnech je definován na základě růstu dalších blockchain protokolů pro pokročilé decentralizované sítě. Ty budou podporovat nové uživatelsky orientované modely služeb, které přesměrují dnešní hodnoty a kontroly Internetu na veřejnost. [18]

Na *obrázku č. 1* jsou pro představu zobrazeny nejvýznamnější události vzniku Internetu a propojených sítí na časové ose.



obrázek č. 1 – Časová osa vzniku Internetu a sítí, zdroj: vlastní zpracování

2 Síťové a komunikační prvky a s nimi spojená rizika kompromitace

Síť Internetu je kvůli stylu organizace, anonymitě, geografickému rozložení a politickému vlivu postižena kybernetickými útoky. Od prvního viru šířeného na disketách se útočníci stali profesionály, kteří mohou v prostředí celosvětové datové sítě, bez ohledu na geopolitické hranice, provádět akce, aniž by byli snadno identifikováni. Častým cílem útoků jsou infrastrukturní prvky, přes které se dostávají ke koncovým zařízením. Vzniká tak seznam typů kybernetických útoků, se kterými se může setkat takřka každý uživatel zařízení připojeného do internetové sítě a se kterými se musejí denně potýkat IT administrátoři napříč celým světem. [6]

Hrozby podle dopadu na uživatele a zařízení, lze rozdělit do čtyř kategorií:

- **Krádež informací** – Narušitel pronikne do počítače za účelem získání důvěrných informací, které má v zájmu prodat nebo použít k různým nelegálním účelům. Jedná se například o krádeže majetkových informací organizace (výzkum, vývoj, výroba).
- **Ztráta a manipulace dat –** Útočník vnikne do počítače, aby zničil nebo pozměnil datové záznamy. Příkladem ztráty dat mohou být případy, kdy útočník odešle virus do počítače s cílem přeformátovat nebo zašifrovat celý pevný disk počítače. Příklad manipulace dat může být proniknutí do databázových systémů firmy za účelem změny různých informací (např. obchodní položky).
- **Odcizení identity –** V tomto případě se útočník snaží odcizit osobní údaje nějaké cizí osoby za účelem převzetí její identity. Pomocí těchto informací může útočník získat právní dokumenty, požádat o úvěr nebo provádět neoprávněné online nákupy. Problémy s odcizením údajů jsou vyčísleny na miliardy dolarů ročně.
- **Narušení služeb (Disruption of service) –** V případě tohoto útoku je bráněno legitimním uživatelům v přístupu ke službám, na které mají nárok. Typicky se jedná o DoS útoky (Denial of service) na servery nebo síťová zařízení. [6]

2.1 Drátové přenosové cesty datové komunikace (pasivní síťové prvky)

Pojem **přenosová cesta** označuje formu přenosového média, které je použito pro přenos datových signálů. Ve světě datových komunikací se v zásadě jedná o dva typy přenosových cest. Prvním typem je komunikace **drátová** (měděné vodiče, koaxiální kabely, optická vlákna). Druhým typem přenosových cest je komunikace **bezdrátová** (typicky radiofrekvenční přenos). [17]

2.1.1 Koaxiální kabel

Technologie koaxiálního kabelu je již z pohledu počítačových sítí spíše historickou záležitostí. V dnešní době se tento typ asymetrického média používá spíše k přenosu signálu mezi anténou a přijímačem (televize, rádio). [17]

Koaxiální kabel se skládá ze dvou vodičů, kdy vnější vodič obaluje vnitřní (většinou měděný). Vnější vodič je často nazývaný jako stínění a vnitřní vodič jádro. Po vnitřním vodiči se přenášejí signály. Vnější vodič má za úkol odstiňovat vnitřní vodič od okolních vlivů (vnější elektromagnetické pole), stejně tak má bránit vyzařování signálu do vnějšího okolí. Samotný přenášený signál je tedy reprezentován napětím mezi oběma vodiči (vnitřním a vnějším), neboli také rozdílem elektrických potenciálů obou vodičů. [17][20]

Koaxiální kabel disponuje vyšší odolností proti elektromagnetickému rušení a proti vlivu indukovaných napětí nežli symetrický kabel, není ale dobře chráněn proti magnetickému rušení. Pro vysílání v základním pásmu se běžně používají kmitočty pod 50 MHz. Pro zvýšení rychlosti přenosu dat se používá modulace digitálního signálu na nosný vysokofrekvenční signál v LAN. [20]

V praxi existují dva typy koaxiálního kabelu:

- **Silný** (thick) – Je historicky starší a má několikanásobné vodivé opletení (až 4 vrstvy). Tento typ kabelu se používal výhradně v instalacích pro Ethernet (páteřní sítě), protože je sice kvalitnější oproti druhému typu, ale je náročnější na instalaci (ohyb, cena).
- **Tenký** (thin) – Má poloviční průměr oproti silnému koaxiálnímu kabelu a jednodušší provedení. Vodič v jádru je obklopen jedinou stínící vrstvou (obvykle měděná folie) oddělenou izolačním materiálem. Jediná stínící vrstva sice nechrání

tento koaxiální kabel před vnějšími vlivy jako vícevrstvé provedení, ale proti první variantě je o poznání levnější a ohebnější. [17][20]

Koaxiální kabely sehrály významnou roli v historii budování počítačových sítí, zejména lokálních. V dnešní době se ale koaxiální kabely nacházejí v sítích pouze výjimečně, protože byly nahrazeny kroucenou dvoulinkou, která přinesla do oboru počítačových sítí ucelenou metodiku výstavby moderních kabelových rozvodů.

2.1.2 Symetrický kabel (kroucená dvoulinka)

Symetrický kabel je složený z párů vzájemně zkroucených vodičů různých barev. Ze všech možných přenosových cest se jedná o tu nejméně nákladnou, avšak také nejméně výkonnou variantu. Signál, který je přenášen kroucenou dvoulinkou je vyjádřen rozdílem potenciálu obou vodičů v páru. Symetričnost obou zkroucených vodičů má vliv na zmenšení vnějších vlivů, které mohou na dvoulinku působit během datového přenosu. Pokud by nějaké vnější elektromagnetické pole indukovalo ve vodičích nějaké elektrické proudy, potom by byly v obou vodičích přibližně stejně velké a došlo by ke vzájemnému vyrušení. Toto vzájemné vyrušení vnějších vlivů však není dokonalé, proto se může vyrábět i dvoulinka v tzv. stíněném provedení STP (Shielded Twisted Pair), která má oproti své používanější nestíněné variantě UTP (Unshielded Twisted Pair) zvýšenou odolnost proti vnějším rušivým vlivům. [17][20]

Varianta symetrického kabelu, jako přenosové cesty je však omezena fyzikálními vlastnostmi mědi, ze které je vyrobena. Například přenos signálu o kmitočtu 15 MHz již vykazuje neúměrné ztráty na vedení. [17]

Symetrický kabel má dva druhy parametrů:

- Přenosové – útlum, impedance (kabel STP má impedanci 150 Ω, kabel UTP 100 Ω), latence signálu
- Vazební – ztráty přeslechem, ztráty rušením, šum [17]

Existují přesné specifikace Americké organizace EIA/TIA pro způsoby konstrukce, instalaci a zakončení kabeláže (např. minimální vzdálenosti kabelů od elektrických zdrojů šumu, možnosti umístění některých typů kabelů vedle sebe nebo způsoby instalace konektorů). [17]

Jak již bylo zmíněno, existují dvě varianty provedení symetrického kabelu:

- **Stíněný symetrický kabel** (STP) – Skládá se z měděných vodičů, které jsou obklopeny izolačním nevodivým materiálem (PVC). Dráty jsou vzájemně kolem sebe obtočeny, aby vytvořily dvojice. Důvodem je zlepšení elektrických vlastností kabelu. Minimalizují se tím přeslechy mezi páry a snižuje se interakce mezi dvojlinkou a jejím okolím. V párech jsou sdruženy vždy dva dráty pro vysílání, nebo pro příjem. Následně je každý pár chráněn ještě kovovou folií po celé délce kabelu a celý kabel je poté zabalen do izolačního pouzdra, které kromě izolace také drží dráty pohromadě. [17]
- **Nestíněný symetrický kabel** (UTP) – Je složen ze 4 kroucených drátů podle amerického standardizačního systému (AWG). Páry drátů jsou spolu vzájemně obtočeny, stejně jako je tomu u stíněného provedení. Nestíněná dvoulinka se podle EIA/TIA 568 dělí do 6 kategorií s následujícími charakteristikami: [17]
    - **Kategorie 1** – Žádná výkonnostní kritéria
    - **Kategorie 2 –** do 1 MHz (telefonní dráty)
    - **Kategorie 3** – do 16 MHz (Ethernet 10BASE-T, 100BASE-T4), úroveň pro přenos hlasových informací
    - **Kategorie 4** – do 20MHz (Token-Ring, 10BASE-T, 100BASE-T4), úroveň pro přenos dat
    - **Kategorie 5** – do 100 MHz (100BASE-TX, 10BASE-T, 1000BASE-T), úroveň pro přenos dat
    - **Kategorie 6** – do 250MHz (nová norma TIA/EIA-569-B.2-1) [17][20]

V dnešní době se používají již pouze kategorie 5 a 6. UTP cat. 5 se využívá především v domácích síťových rozvodech, zatímco UTP cat. 6 je využíván ve firemních infrastrukturách, kde jsou požadavky na rychlost přenosu o poznání vyšší. [20]

2.1.3 Optické kabely

Nejnovějším a do budoucna nejperspektivnějším přenosovým prostředkem používaným v rozlehlých i lokálních komunikačních sítích jsou optické kabely (světlovody). Důvodem je, že pro přenos dat co možná největší rychlostí potřebujeme volit takové způsoby přenosu, které mají šířku přenášeného pásma co možná největší. Světlo je z tohoto pohledu velmi dobrým médiem, jelikož má frekvenci přibližně 10^8 MHz. [1]

Optické kabely umožňují propustnost v řádu Tbit/s (10^{12} bit/s) a regenerace signálu je podle typu vysílače potřebná až po vzdálenosti několika desítek kilometrů, zatímco měděné kabely dosahují na vzdálenost jednoho km rychlosti maximálně 100 Mbit/s. Optická vlákna používající metodu vlnového multiplexu (přenos se multiplexuje více optickými signály v jednom optickém vlákně), ty mohou podporovat mnoho vlnových kanálů, z nichž každý může podporovat rychlost 2,5 až 10 Gbit/s, takže výsledná šířka pásma jediného vlákna může dosahovat až 1 Tbit/s. [1][21]

Celková podstata optického přenosu je přeměna informace z elektrického signálu na optický. Tato přeměna probíhá ve zdroji záření, kterým je svítící dioda (LED – Light emitting Diode), nebo laserová dioda. LED diody jsou mnohem levnější, jejich nevýhodou je však menší šířka pásma než u laserových diod. Infračervené vlny generované LED diodou tedy dosahují menších vzdáleností s přijatelnou chybovostí. Proto se používají v optických přenosových systémech, kterým stačí kratší dosah a menší šířka přenosového pásma. [1][21]

Na konci přenosu optickým vláknem dochází k detekci záření fotodiodou nebo fotorezistorem a k dalšímu zpracování. Nevýhodou optických vláken je však výrazná směrová orientace světelného signálu, proto nelze signál jednoduše přenášet jedním vláknem oběma směry současně. Množství přenesené informace optickým kabelem je při vhodné modulaci přímo úměrné výši kmitočtu, proto se stále přechází k vyšším kmitočtům. [1]

Optické kabely se dělí na dva druhy:

- **Jednovidové** (singlemode, monomode) – Velmi tenké optické vlákno s vysokou přenosovou kapacitou. Pro přenos světelného paprsku je využíván laser, který dosahuje velkých vzdáleností. Koherentní laserové světlo má konstantní vlnovou délku, a proto je zde dosaženo lepších výsledků nežli u mnohovidových vláken. [21]
- **Mnohovidové** (multimode) – Zde jsou místo laseru využity pro generování světla LED diody. Světlo zde sestává z několika světelných vlnových délek, protože dioda vysílá světlo všemi směry. Vygenerovaný paprsek vniká do jádra optického vlákna tak, že úhel dopadu paprsku s osou jádra je nenulový a jeho cestou optickým vláknem tak dochází k odrazům od okrajů optického vlákna. Kvůli tomu je celková vzdálenost dosahu světelného paprsku omezena. [21]

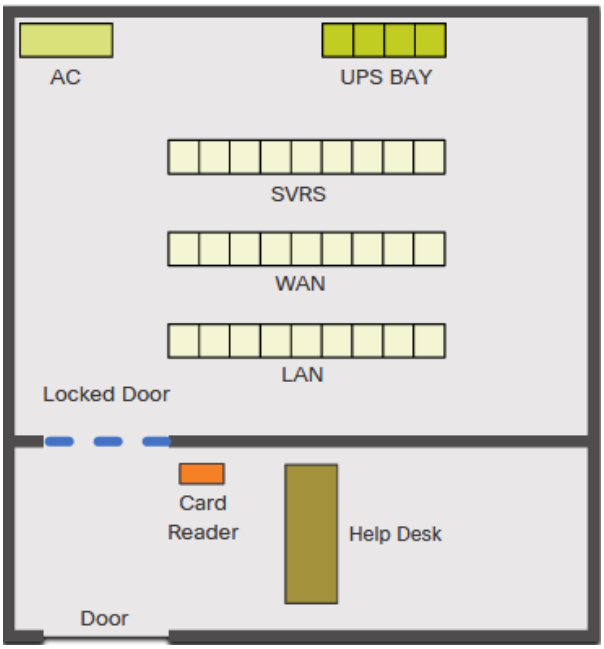
2.1.4 Možné ohrožení síťových prvků

Ohrožení síťových prvků lze rozdělit do následujících kategorií:

- **Hrozby napadení hardwaru –** Jakékoliv fyzické poškození serverů, routerů, switchů, kabeláže a také koncových stanic.
- **Nevyhovující prostředí –** Extrémní teploty a jejich výkyvy (např. nefunkční klimatizace v serverovně) nebo extrémní klima (přílišné vlhko nebo naopak sucho).
- **Hrozba nestálosti elektrického proudu –** Napěťové špičky, nedostatečné napájení a celková ztráta elektrické energie.
- **Hrozby při provádění údržbářských prací** – Špatné zacházení s klíčovými elektrickými součástmi (elektrostatický výboj), nedostatek důležitých náhradních dílů nebo špatné provádění kabeláže a jejího značení. [6]

2.1.5 Preventivní opatření

K odstranění těchto problémů musí být vytvořen a implementován kvalitní plán fyzického zabezpečení. Příkladem může být umístění všech kritických částí síťové infrastruktury do zabezpečené místnosti s omezenými přístupy a vlastní klimatizací (pokud je potřeba) a implementovat fyzické ochranu této místnosti (alarm, elektronicky ověřené přístupy, bezpečnostní kamery). *Viz obrázek č. 2*. [6]



obrázek č. 2 – Ukázka zabezpečené místnosti, zdroj: [6]

2.2 Bezdrátové sítě

Při současném vývoji síťových protokolů je využívání bezdrátových sítí ohromné. Existují tři hlavní pojmy ze světa bezdrátových sítí:

- **WLAN** (Wireless Local Area Network) – Jedná se obecně o jakoukoli bezdrátovou síť. Jde o bezdrátový ekvivalent LAN.
- **IEEE 802.11b –** Označení standardu standardizačního institutu IEEE (Institute of Electrical and Electronic Engineers). Jedná se o standard bezdrátové sítě v nelicencovaném pásmu 2,4 GHz. Na konci názvu tohoto standardu se mohou objevovat i jiná písmena nežli **b –** tím jsou zpravidla odlišeny jiné verze standardu a také skutečnost, že tato odnož pracuje s jinou frekvencí než její původce.
- **WIFI (Wireless Fidelity) –** Tato zkratka je často zaměňována s výrazem IEEE802.11b. Jedná se totiž o logo a označení udělované výrobkům pracujícím podle standardu 802.11b. [50]

Bezdrátové sítě typu IEEE 802.11b pracují ve frekvenčním pásmu 2,4 – 2,4835 GHz. Toto pásmo je také často označováno jako **ISM** (Industrial, Scientific, Medical). V tomto pásmu pracují zařízení od Bluetooth produktů až po mikrovlnné trouby a bezdrátové telefony. [3]

Ruku v ruce s boomem Wifi zařízení se na trh dostávají zařízení postavená na standardu IEEE 802.11a pracující v pásmu 5GHz. [3][50]

2.2.1 Možné ohrožení bezdrátových sítí

Bezdrátové sítě přinášejí mnoho výhod. Díky lepšímu přístupu k síti se zlepšuje produktivita. Konfigurace, rozšiřování a rekonfigurace sítě je rychlejší a levnější. Bezdrátové technologie však generují nové hrozby, na které je potřeba adekvátně reagovat. Například riziko zachycení komunikace je mnohem větší než u kabelových sítí, pokud není zpráva zašifrována nebo je zašifrována slabým bezpečnostním algoritmem, útočník ji může přečíst mnohem snadněji než v drátové komunikaci. Přestože jsou rizika u bezdrátových sítí jiná než u kabelových sítí, celkové cíle zabezpečení zůstávají stejné: Důvěrnost, zajištění integrity a zachování dostupnosti informací a informačních systémů. [3]

Bezdrátové sítě sestávají ze 4 základních komponent:

- Přenos dat pomocí rádiových frekvencí
- AP zajišťující propojení sítě

- Koncová zařízení a uživatelé

Každá z těchto komponent poskytuje útočníkovi cestu k útoku, která může mít za následek kompromitaci jednoho nebo více ze tří bezpečnostních cílů: Důvěrnosti, integrity a dostupnosti. [37]

Accidental association (Náhodná asociace)

Pokud se uživatel připojí k přístupovému bodu ze sousední společnosti, do které dosahuje bezdrátová síť. Daný uživatel ani nemusí vědět, že se taková událost naskytla. O narušení se však jedná z důvodu možného odhalení informací o společnosti, které by mohly být nějakým způsobem zneužity. [37]

Malicious association (Škodlivá asociace)

Případ, kdy útočník aktivně vytváří bezdrátová zařízení pro připojení k firemní síti, prostřednictvím jeho zařízení namísto APs společnosti. Tyto typy zařízení jsou známy jako „soft APs“, a jsou vytvořeny útočníkem pomocí softwaru, který maskuje síťovou kartu, aby vypadala jako legitimní AP. Jakmile se k těmto APs někdo pokusí připojit, útočník může získat přístupové údaje k legitimní firemní síti. Vzhledem k tomu, že bezdrátové sítě fungují na 2. vrstvě, ochrany 3. vrstvy, jako autentizace sítě nebo VPN, nepředstavují žádnou bariéru. [37]

Ad-hoc networks

Tento typ sítí může představovat bezpečnostní hrozbu. Ad-hoc jsou definovány jako peer to peer sítě mezi bezdrátovými počítači, které mezi sebou nemají AP. Tyto typy sítí mají obvykle malou ochranu, tu lze však značně zvýšit použitím šifrovacích metod. [37]

Další typy bezdrátových sítí

Bluetooth síť není brána jako bezpečná proti crackovacím metodám a měla by být považována za bezpečnostní riziko. Tuto technologii využívají čtečky čárových kódů, kapesní PDA, či bezdrátové sítě a kopírky. Z tohoto důvodu by se měli firemní IT pracovníci zaměřit na jejich bezpečnost. [37]

Identity theft (Krádež identity)

Situace, kdy je útočník schopen odposlouchávat síťový provoz a odhalit MAC adresy zařízení se síťovými oprávněními. Většina bezdrátových systémů dokáže filtrovat MAC adresy pro zajištění přístupu pouze autorizovaným zařízením se specifickou MAC adresou. V dnešní době však existuje velké množství programů, které mají možnost „sledovat“ provoz zabezpečené sítě. Pokud se tyto programy zkombinují s jiným softwarem, který umožní počítačům předstírat, že mají jakoukoli uživatelsky zadanou MAC adresu, je možné se přes toto zabezpečení snadno dostat. [37]

Wireless Man in the middle attack

Případ, kdy útočník nutí legitimní uživatele připojovat se přes tzv. soft AP. Jakmile je tento úkon proveden, útočník se připojí k opravdovému AP pomocí jiné bezdrátové karty, která nabízí ustálený datový provoz skrze hackerský počítač do skutečné sítě. Útočník poté může sledovat provoz proudící skrze jeho počítač. Nejčastější typ Man in the middle attack spoléhá na bezpečnostní chyby v protokolech challenge a handshake k provedení „de-authentification attack“. Tento útok přinutí počítače připojené k legitimnímu AP přerušit jejich spojení a znovu se připojit přes útočníkův soft AP. Man in the middle attack v dnešní době vylepšují různé softwary např. LANjack nebo AirJack, které automatizují mnoho kroků samotného procesu útoku. To, co dříve vyžadovalo určité schopnosti, dnes mohou zvládnout i tzv. script kiddies. Obzvláště citlivé na útoky jsou hotspoty, protože v těchto sítích je jenom malé, nebo dokonce žádné zabezpečení. [37]

Denial od service (DOS)

Denial of Service attack nastává, pokud se útočník snaží neustále zasypávat cílový AP nebo síť falešnými požadavky, chybovými zprávami nebo jinými příkazy. To způsobí značnou vytíženost samotného AP a nemožnost legitimních uživatelů připojit se do sítě nebo dokonce zhroucení celé sítě. Tyto útoky velmi často zneužívají protokoly Extensible Authentification Protocol (EAP). [37]

Network injection

V network injection využívá útočník APs, které čelí nefiltrovanému síťovému provozu, například: Spanning Tree Protocol (STP), Open Shortest Path First (OSPF), Routing Information Protocol (RIP) nebo Hot Standby router Protocol (HSRT). Útočník zde

injektuje síť falešnými re-konfiguračními příkazy, které ovlivní routery, switche a popřípadě inteligentní huby. Útok může ovlivnit celou síť a v nejhorším případě může být nutné přeprogramovat všechna inteligentní síťová zařízení do původního stavu před útokem. [37]

Caffe Latte attack

Další způsob, jak docílit prolomení zabezpečovacího algoritmu WEP. Podmínkou je, že útočník musí být v dosahu sítě, na kterou je mířen útok. K útoku je využíván proces, který zachytává ARP pakety vysílané klientským zařízením. S těmi dále manipuluje a odesílá je zpět klientovi. Klient poté opět generuje pakety, které se zachytávají specializovaným softwarem (např. airodump-ng). Následně lze dalším specializovaným softwarem (např. aircrack-ng) prolomit klíč WEP. [38]

2.2.2 Prevence útoků na bezdrátový přenos

Způsob, jakým fungují bezdrátové sítě generuje základní typy ohrožení:

- Interception (Zachycení)
- Alteration (Změna)
- Disruption (Narušení) [37]

Obrana bezdrátové sítě proti zachytávání

V zásadě existují dva typy opatření proti nechtěnému zachytávání a odposlechu bezdrátových sítí. První začleňuje metody, které ztěžují lokalizaci a zachytávání bezdrátových signálů. Druhá zahrnuje použití šifrovacích metod pro zachování důvěrnosti sítě, i když je bezdrátový signál zachycen. [3]

Techniky zakrytí signálu

Než může útočník začít zachytávat síťový přenos, musí nejprve identifikovat a lokalizovat bezdrátovou síť na kterou chce zaútočit. Nicméně existují kroky, které pomáhají organizacím ztížit lokalizaci jejich bezdrátových sítí. K nejjednodušším a nejlevnějším způsobům patří:

- Vypnutí Service Set Identifier (SSID) vysílaného bezdrátovým AP
- Přiřazení kryptovaných názvů SSID
- Redukce síly signálu na nejnižší úroveň, která stále poskytuje dostatečné krytí pro všechna potřebná zařízení [3]

Mezi efektivnější, ale také dražší varianty obrany patří:

- Použití směrových antén k omezení síly signálu v určitých sektorech
- Zavedení technik stínění signálu zvané TEMPEST pro blokování vyzařování bezdrátového signálu [3]

Šifrování

Nejlepší způsob ochrany informací přenášených přes bezdrátové sítě je šifrování veškerého bezdrátového provozu. Takřka všechny bezdrátové APs jsou schopny používat jeden ze čtyř standardů bezdrátového šifrování: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2 nebo WPA3. [39]

WEP

První šifrovací algoritmus pro standard 802.11, který vznikl za jediným účelem: Zabránit hackerům ve sledování bezdrátových dat, přenášených mezi klientskými zařízeními a APs. [3]

WEP používá pro autentizaci a šifrování proudovou šifru Rivest Cipher 4 (RC4). Ve standardu byl původně specifikován pouze 40bitový šifrovací klíč, který byl později nahrazen 104bitovým klíčem. [39]

Administrátor sítě zde musí ručně zadat a aktualizovat šifrovací klíč, který je kombinovaný s 24bitovým inicializačním vektorem (IV). Malá velikost IV zvyšuje pravděpodobnost, že uživatelé budou šifrovací klíče opakovat, což usnadňuje jejich prolomení. Tato vlastnost a několik dalších závažných chyb a zranitelností, např. problémový mechanismus autentizace, činí z WEP dnes již nepoužitelný šifrovací standard. [39]

WPA

Šifrovací standard, který byl od začátku svého uvedení brán jako prozatímní. WPA disponuje podnikovým režimem nebo režimem pro osobní použití. WPA-Extensible Authentification Protocol (WPA-EAP) používá přísnější ověřování 802.1x a vyžaduje použití ověřovacího serveru. Osobní režim, WPA-Pre-Shared Key (WPA-PSK), používá předem sdílené klíče pro jednodušší implementaci a management spotřebitelům a malým kancelářím. [3]

WPA je, stejně jako WEP, založen na šifrování RC4. Přesto, zde bylo zavedeno několik vylepšení, například použití Temporal Key Integrity Protocol (TKIP). Pro vylepšení tehdejší bezpečnosti obsahuje TKIP následující sadu funkcí:

- Používá 256bitový klíč
- Mixování klíčů na paket, což generuje jedinečný klíč pro každý paket
- Automatické vysílání aktualizovaných klíčů
- Zvětšen IV na 48 bitů
- Mechanismy ke snížení znovupoužití IV [39]

Technologie WPA, navržená Wi-Fi aliancí je zpětné kompatibilní s protokolem WEP. Na mnoha zařízeních podporujících WEP bylo možné zavést WPA pomocí aktualizace firmwaru. Toto rozhodnutí však znamenalo, že potenciál WPA nebyl plně využit a zabezpečení protokolu nebylo tak komplexní, jaké mohlo být. [39]

WPA2

Nástupce protokolu WPA byl ratifikován IEEE jako 802.11i v roce 2004. WPA2, stejně jako WPA podporuje osobní a podnikový mód. [3]

Ve WPA2 byly protokoly RC4 a TKIP nahrazeny dvěma silnějšími šifrovacími a autentizačními mechanismy. Jsou to:

- Advanced Encryption Standard (AES)
- Cipher Block Chaining Message Authentication Protocol (CCMP) [39]

WPA2 je však také zpětné kompatibilní, takže podporuje TKIP v případě, že zařízení nepodporuje CCMP. [39]

AES obsahuje tři symetrické blokové šifry. Každá šifruje a dešifruje data v blocích 128 bitů pomocí 128, 192 a 256bitových klíčů. Používání AES zvýšilo nároky na výpočetní výkon APs a klientských zařízení. Pokračující zlepšování počítačového a síťového hardwaru však problémy s výkonem velmi dobře mírnilo. [39]

CCMP chrání důvěrnost dat tím, že umožňuje přijímat data pouze oprávněným uživatelům sítě a používá autentifikaci pomocí šifrovacího blokového řetězce k zajištění integrity. [39]

Byl také zaveden plynulejší přechod z jednoho AP do druhého ve stejné síti Wi-Fi bez nutnosti opětovné autentizace pomocí předběžného ověřování nebo ukládání do mezipaměti Pairwise Master Key. [39]

WPA3

V roce 2018 začala Wi-Fi Aliance certifikovat WPA3, nejnovější protokol, který je považován za nejbezpečnější. Od června roku 2020 požaduje Wi-Fi Aliance od všech

zařízení, která mají mít její certifikaci, podporu protokolu WPA3. Také se zde stává standardem 128bitová kryptografická sada a jsou zakázány všechny zastaralé bezpečnostní protokoly. [3]

Ve WPA3-Enterprise je možné zvolit až 192 bitové bezpečnostní šifrování a 48 bitové IV pro zvýšenou ochranu citlivých dat. WPA3-Personal používá CCMP-128 a AES-128.

Původní PSK four-way handshake, který byl v předchozí verzi zdrojem zranitelností, je nahrazen Simultaneous Authentication of Equals (SAE), ve kterém může klient nebo AP iniciovat kontakt. Každé zařízení poté přenáší své autentizační údaje v diskrétní jednorázové zprávě, namísto vícedílné konverzace. SAE také eliminuje opětovné použití šifrovacích klíčů, protože při každé interakci vyžaduje nový kód. [39]

Prevence proti změnám zachycené komunikace

Zachytávání a změna bezdrátových přenosů představuje formu útoku Man in the middle attack. Výrazně snížit riziko tohoto útoku pomáhají dvě opatření:

- Silné šifrování
- Silná autentifikace uživatelů i zařízení [37]

Opatření ke snížení rizika DOS

Náchylnost na útok DOS je u bezdrátových sítí velmi vysoká. Organizace však mají možnost zavést mnoho opatření, jak útokům předcházet. Pečlivým průzkumem lokality lze identifikovat místa, kde se protínají signály z jiných zařízení. Výsledky těchto průzkumů je třeba brát v potaz při rozhodování o umístění APs. Pravidelnými kontrolami aktivity a výkonu bezdrátových sítí lze identifikovat problémové oblasti. Poté lze zvolit nápravná opatření zahrnující odstranění rušivých zařízení nebo vylepšující signál v problémových oblastech. [37]

2.2.3 Ochrana bezdrátových Access pointů

Nezabezpečené, špatně nakonfigurované APs mohou znatelně snížit kvalitu zabezpečení, tím že neodvrátí neoprávněný přístup do sítě. [3]

Kroky k zajištění bezpečnosti Access pointů

Organizace mohou zmírnit riziko neautorizovaného přístupu do sítě třemi základními kroky:

- Eliminace potenciálně nebezpečných APs – Nejlepší metoda, jak se vypořádat s potenciálně nebezpečnými nebo nechtěnými APs je použití 802.11x v síti, aby se musela všechna zařízení v síti autentizovat. Použití 802.11x předchází připojení neautorizovaných zařízení do sítě. [3]
- Správné nastavení všech autorizovaných APs – Organizace musí zajistit, aby byly všechny bezdrátové APs bezpečně nakonfigurovány. Velmi důležitá je změna všech výchozích, protože nastavení jsou jednoduše dohledatelná a mohou být snadno zneužitá útočníkem. [3]
- Použití autentifikace 802.1x na všech zařízeních – Silná autentizace všech zařízení, která se pokoušejí připojit k síti, slouží jako prevence, aby se nechtěné APs a neautorizovaná zařízení stala potenciálními zadními vrátky. Protokol 802.1x poskytuje silnou autentizaci před tím, než jsou zařízením přiřazeny IP adresy. [3]

2.2.4 Zabezpečení bezdrátové sítě

Z hlediska zabezpečení Access pointů vysílajících signál bezdrátové sítě je takřka samozřejmostí provést následující kroky, které velkou měrou pomáhají předejít případným bezdrátovým kybernetickým útokům.

Vypnutí Identifier Broadcasting

Většina bezdrátových routerů má funkci nazvanou Identifier Broadcasting (Vysílání identifikátorů). Funkce vysílá signál na jakékoli zařízení v okolí, a tím oznamuje přítomnost bezdrátové sítě. Pokud osoby, které se sítí pracují, již ví, že se zde tato síť nachází, už není nutné informace o ni dále vysílat. [3]

Změna výchozího identifikátoru bezdrátového routeru

Identifikátor routeru je standardně nastaven na výchozí hodnotu, kterou přiřazuje veškerému hardwaru daného modelu každý výrobce. I když je vypnutý Identifier Broadcasting, útočníci většinou znají výchozí ID většiny routerů a mohou se pomocí nich

pokusit proniknout do sítě. Identifikátor by měl mít podobu, kterou znají jenom administrátoři a která odpovídá účelu sítě. Stejné ID je poté potřeba nakonfigurovat i na bezdrátovém routeru a počítači, aby mohli komunikovat. Dále je důležité, aby heslo pro přístup mělo dostatečný počet znaků, protože čím je heslo kratší, tím je pro útočníka snazší ho prolomit. [3]

Změna výchozího hesla pro administraci routeru

Téměř každý výrobce síťového hardwaru pravděpodobně nastaví výchozí heslo a uživatelské jméno pro přístup do administrátorské části routeru. Také v tomto případě je nanejvýše vhodná změna tohoto hesla na nějaké, které znají jenom pověřené osoby. [37]

Povolení přístupu pouze konkrétním zařízením

Každý počítač, který může komunikovat se sítí má přiřazenou svou unikátní MAC adresu. Bezdrátové routery obvykle mají mechanismy, které povolují vstup do sítě pouze povoleným MAC adresám. [37]

Vypnutí bezdrátové sítě při nečinnosti

Útočníci se nemohou pokoušet proniknout do sítě, pokud je bezdrátový router vypnutý. Pokud je to v rámci firmy, nebo jejích úseků možné, vypínání bezdrátové sítě v době nečinnosti je mechanismus, který může pomoci s jejím zabezpečením. [37]

2.2.5 Školení a trénink uživatelů

Samotný uživatel je z pohledu bezdrátových sítí dalším pilířem bezpečnosti. Znalost bezpečnostních pravidel firmy je velmi důležitá. Proto by měli být uživatelé školeni bezpečnostními profesionály v pravidelných časových intervalech.

2.3 Router (směrovač)

Router je síťové zařízení, tzv. aktivní síťový prvek (prvek pracující se signály vysílanými skrze síť), který má za úkol přeposílání dat mezi počítačovými sítěmi. Data se přes internet odesílají ve formě tzv. datových paketů. Pakety se typicky předávají z jednoho routeru do druhého, dokud není dosaženo cílového uzlu.

Router má za úkol dva hlavní cíle:

- Rozhodování o cestě – Slouží k vytvoření spojení
- Přenos paketů po takto definované cestě [4]

Router je obvykle připojen ke dvěma datovým linkám z různých sítí. Jakmile datový paket dorazí z jedné připojené sítě, router přečte síťovou adresu z hlavičky paketu a rozhodne o místu určení. Poté pomocí informací z routovací tabulky nasměruje paket do další sítě na jeho cestě. Pro síťový provoz routery nabízejí funkci Access Control, kdy povolují přenos dat do lokální sítě jen určitým oprávněným počítačům. Tím je zajištěna bezpečnost privátních informací udržovaných uvnitř sítě. Mimo to provádějí routery také zpracování chyb, sledují statistické ukazatele o využití sítě a ošetřují záležitosti spojené s bezpečností v síti. [2]

Router je tedy základním stavebním kamenem internetových sítí. Bez routerů by Internet a sítě jako takové nemohly existovat. Důkazem důležitosti routerů jsou jejich jedinečné funkce:

- Dokážou podporovat současně několik různých protokolů (Ethernet, token ring, ISDN aj.). Dá se říct, že na úrovní internetové sítě jsou kompatibilní prakticky se všemi počítači.
- Propojují lokální sítě LAN s rozlehlými sítěmi WAN, takže umožňují výstavbu i velmi rozsáhlých internetových sítí s minimem centrálního plánování.
- Filtrují síťový provoz a izolují oblasti, které povolují nesměrové vysílání zpráv všem uživatelům v síti.
- Fungují jako bezpečnostní bariéry a kontrolují síťový provoz se seznamem přístupových oprávnění.
- Detekují případnou překážku v cestě a poté přesměrují pakety na záložní cestu. [4]

Routery se však nevyužívají pouze v lokálních sítích, jsou také nedílnou součástí páteřních spojů Internetu. [2]

Jakékoli informace posílané přes Internet (email, webová stránka) se standardně rozdělí do paketů o velikosti 1500 bajtů. Tyto pakety jsou poté přenášeny přes řadu routerů, z nichž každý posílá pakety dále po své cestě ke koncovému zařízení. Pakety jsou přenášeny vždy nejlepší možnou cestou. Tomuto stylu přenosu se říká síť s přepínáním paketů. Všechny pakety v odeslané zprávě mohou jít jednou cestou, anebo se každý paket může vydat úplně odlišnou cestou podle momentálního provozu a stavu sítě. Na cílovém počítači se z doručených paketů sestaví původní zpráva. [4]

Dá se říct, že veškeré směrovače jsou v Internetu propojeny do jedné velké pavučiny, ve které putují pakety vždy nejúspornější cestou, což zajišťuje jejich příchod do cíle v adekvátním čase. Lze namítnout, že by se pakety měly do cíle vydat takovou cestou, která vede přes co nejmenší počet směrovačů. Tato myšlenka ale nemusí být úplně uskutečnitelná, a to z toho důvodu, že tato cesta může být například zahlcena nadměrným internetovým provozem. Pokud směrovače tuto skutečnost zjistí, odesílají internetový provoz přes jiné směrovače tak, aby se odklonily od zahlcené části Internetu, čímž je docíleno efektivnějšího přenosu. [4]

Na první pohled se může toto vedení paketů zdát příliš komplikované, naopak je velmi efektivní, a to z následujících dvou důvodů:

- Síť dokáže lépe vyrovnat zatížení mezi různé komponenty (síťová zařízení)
- Pokud během přenosu zprávy vzniknou na určitém zařízení v síti nějaké problémy, mohou se pakety snadno odklonit mimo toto problematické místo a do cíle dorazí celá zpráva. [4]

Routery tvoří páteř Internetu. Díky průběžnému sledování informací k datovým paketům a vzájemnou výměnou stavu jednotlivých linek dokážou měnit konfiguraci cest pro zasílání těchto paketů, pokud v těchto cestách nastane nějaký nenadálý problém. [4]

2.3.1 Možná rizika napadení skrze Router

Síťový router je obzvláště citlivou součástí sítě na kybernetické útoky. Z tohoto důvodu je velmi vhodné se připravit na obrovské množství potenciálních útoků, kterými může být síťový router napaden.

Denial of Service (DOS)

Útok, jehož cílem je přetížit síťovou komponentu nebo celou síť, a tím ji znepřístupnit každému uživateli. Útočník dosáhne tohoto stavu zaplavením cíle obrovským množstvím požadavků nebo odesláním informací, které způsobí poruchu zařízení. [22]

Jsou známy dva typy DOS útoků:

- Flooding service – K tomuto typu útoku dochází, pokud systém přijímá příliš mnoho síťového provozu a přetíží se tím vyrovnávací paměť. To způsobuje zpomalení, a nakonec zastavení celého systému. Mezi populární Flooding attacks patří: [24]
    - Buffer overflow attacks – Nejčastější typ útoku, kterým se má poslat na síťovou adresu větší provoz, než jaký byl programátory navržený jako únosný. [24]
    - ICMP flood – Využívá špatně nakonfigurovaná zařízení pro odesílání falešných paketů, které provádí příkaz ping na každý počítač v síti, namísto jednoho konkrétního počítače. Síť je poté nucena reagovat stejným počtem paketů s odpovědí. To způsobí nepřístupnost sítě pro běžný provoz. [25]
    - Syn flood – Pošle žádost o připojení na server, ale nikdy nedokončí handshake. Útok pokračuje na každém volném portu. Ty jsou poté znehybněné čekáním na odpověď žadatele a nejsou dostupné pro běžné uživatele. [24]
- Crashing sevices – Využívají zranitelnosti způsobující zhroucení celého cílového systému nebo služby. Při útocích je odesílán vstup, který využívá chyb v cílovém zařízení a to následně havaruje nebo destabilizuje systém, takže k němu poté nelze získat přístup nebo jej použít. [24]

Packet Mistreating Attacks (PMA)

Napadení podobné útoku DOS. Při PMA se nasadí do paketů škodlivý kód určený k zmatení a narušení routeru a celé sítě. Škodlivé datové pakety mají za úkol tzv. „týrat“ router (český překlad PMA – Útok týrání pakety). Každý router má směrovací proces a zavedení těchto škodlivých paketů způsobí, že router již nezvládne zpracovávat pakety podle směrovací tabulky. [22]

Jelikož router nedokáže určit, kam příchozí pakety dále odesílat, v síti se začnou tvořit datové smyčky, což způsobuje velké přetížení sítě. [22]

Tento typ útoku je velmi těžké odhalit, proto je vhodné myslet na správné zabezpečení sítě a routerů již při instalaci síťové infrastruktury. [22]

Routing Table Poisoning (RTP)

Škodlivý uzel odesílá špatné aktualizace směrování, chybové zprávy nebo pozměněné legitimní informace do autorizovaných uzlů v síti. To může mít za následek přeposílání paketů routery po nesprávných trasách, přetížení v síti, vytváření smyček. Útočník může také úmyslně směrovat všechny příchozí pakety proti legitimním uzlům a tím je vystavit DOS útoku. [26]

Hit and Run (HAR)

Často také označované jako „testovací hacky“. Dochází k nim, když jsou do routeru zanesena škodlivá data prostřednictvím kódu. Útoky jsou nazvané testovací, protože pokud se útočníkovi nepodaří první útok, může dále zdokonalovat škodlivý kód a útočit pořád dokola. [22]

Útoky HAR jsou snadněji rozpoznatelné než předchozí útoky, protože router ovlivněný tímto útokem začne vykazovat netypické chování a zobrazovat neobvyklé aktivity. [22]

Persistent Attacks (PA)

Útoky velmi podobné HAR. Mají za cíl propašovat do routeru poškozený kód. Na rozdíl od HAR útoku jsou PA dlouhodobé, dokud útočník nedosáhne svého cíle. Útočníci pokračují s vkládáním škodlivého kódu do routovací tabulky, takže je velmi snadné zaměnit PA a RTP. Celkovým úkolem PA je napadat síťové zranitelnosti, a tím je odhalit. [22]

Brute Force

Útok hrubou silou lze aplikovat na mnoho zařízení a to, když se hacker snaží uhádnout heslo a získat přístup. K útoku se používají programy obsahující slovník s obrovským množstvím výrazů. Na základě síly hesla a kombinací, kterými se software snaží heslo uhádnout, může útok trvat krátkou dobu nebo také takřka nekonečně dlouho. [23]

Disgruntled Employee

Nespokojený nebo bývalý zaměstnanec se znalostí topologie sítě a přihlašovacích informací by mohl přistupovat k routerům a zařízením bez autorizace a ohrožovat tím firemní síť. [23]

2.3.2 Zmírnění rizik napadení routeru

Oblast obrany routeru proti útokům se dá rozdělit do 4 úrovní: Management, Kontrola, Data, anti-DDOS řešení. [29]

Ověřené postupy management úrovně

- Celoplošné zavedení a používání politiky, která vynucuje používání hesel na zařízeních.
- Implementace Role-Based Acces Control (RBAC – řízení přístupu na základě rolí). Je možné vytvořit skupiny uživatelů s určitými právy a k nim přiřadit dané uživatele nebo je také možné tvořit role a jednotlivé uživatele k nim přiřadit, tím se limitují činnosti, které mohou uživatelé provádět, pokud jsou připojeni k síti.
- Používání Authentication, Authorization a Accounting (AAA) – Řešení, jak kontrolovat, kdo je oprávněn přistupovat do sítě (authentication), co tam může dělat (authorization) a audit akcí, které během přístupu provedl (accounting).
- Používání Network Time Protocol (NTP) pro udržení aktuálního času v celé síti.
- Zajistit pevné IP adresy pro zařízení důležitá v síti.
- Zavedení System Logging Protocol (Syslog) a jeho zálohování do externích úložišť, aby ani administrátorské účty nemohly toto logování měnit nebo mazat.
- Deaktivace nepoužívaných služeb (UDP, SMBv1, Telnet). [29]

Ověřené postupy úrovně kontroly

Úroveň řízení se speciálně zaměřuje na obranu proti útokům, které mohou ohrozit CPU routeru.

- **Control Plane Policing (CoPP)** – Je možné definovat, jaký provoz může router jednoduše ignorovat např. HTTPS/SSH/SSL.
- **Control Plane Protection (CPPR)** – Detailnější než CoPP. Je rozdělen do tří podkategorií: zachytává síťový provoz mířící do specifické lokace, zachytává data, která požadují zásah CPU a Cisco Express Forwarding (CEF), který dokáže zachytávat specfické pakety. Existuje také funkce zvaná Selective Packet Discard (SPD), která umožnuje určovat paketům různé priority. [29]

Ověřené postupy datové úrovně

V datové úrovni se tradičně používá 6 metod, které dokážou ochránit router od většiny běžných hrozeb. [29]

Access Control List (ACL)

ACL filtruje směrované pakety na rozhraní přijímacího zařízení. Ty potom blokuje nebo dále přesměrovává. Zařízení zkoumá každý paket a určuje, co s ním provede na základě kritérií uvedených v ACL. [30]

Existují i další důvody, kromě bezpečnosti, proč nakonfigurovat ACL ve firemní síti. Může jít například o omezení aktualizací routování nebo zajištění řízení toku provozu. Pokud nejsou ACL v síti nakonfigurovány, mají všechny pakety procházející zařízením přístup ke všem částem sítě, ve které se nacházejí. [30]

ACL mohou hostiteli umožnit přístup k určité části sítě, zatímco jinému hostiteli mohou v tomto přístupu zabránit. Pomocí ACL je také možné definovat typ provozu, který je poté na rozhraní zařízení přesměrován nebo blokován. Může být například povolené pouze směrování elektronické pošty a zároveň blokován veškerý provoz přes Telnet. [30]

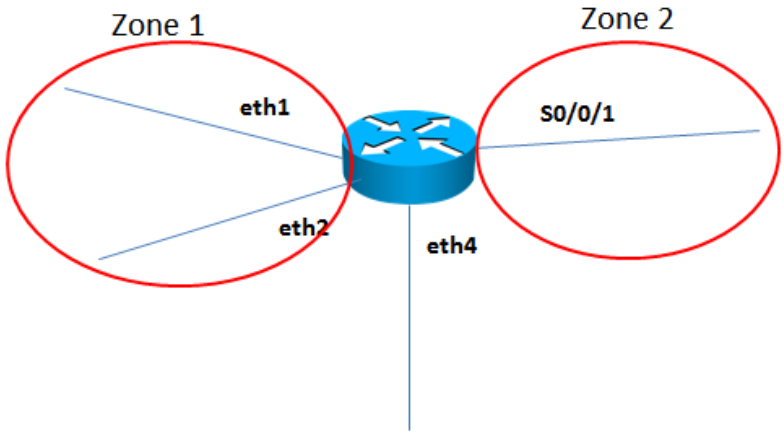
Context-Based Access Control (CBAC)

CBAC aktivně kontroluje aktivitu procházející zařízením. CBAC pracuje na principu ACL s tím rozdílem, že obsahuje příkaz ip inspect, kterým kontroluje protokol, jestli s ním nebylo manipulováno, než bude vpuštěn do sítě. V dnešní době jsou CBAC nahrazovány technologií Zone-Based Firewall. [31]

Zone-Based Policy Firewall (ZFW)

ZFW pracuje na podobném principu jako CBAC. Rozdíl je však v konceptu zón, kde různé zóny s různými rozhraními sdílejí stejné bezpečnostní atributy nebo stejné úrovně důvěry. Řešení oprávnění síťového provozu se řeší mezi zónami nebo v rámci zóny, ne mezi fyzickými rozhraními sítě. [32]

Na *obrázku č. 3* je znázorněn koncept síťových zón. Rozhraní eth1 a eth2 patří do zóny 1, rozhraní s0/0/0 patří do zóny 2 a rozhraní eth4 nepatří do žádné zóny. Výchozí nebo uživatelsky definovaná bezpečnostní politika bude použita v síťovém provozu mezi rozhraními zóny 1 a zóny 2. Žádná bezpečnostní politika nebude použita pro síťový provoz mezi rozhraními v zóně 1. Připojení a síťový provoz nebudou povoleny mezi rozhraními v zóně 1 nebo 2 a rozhraními, které nepatří do žádné zóny. [32]

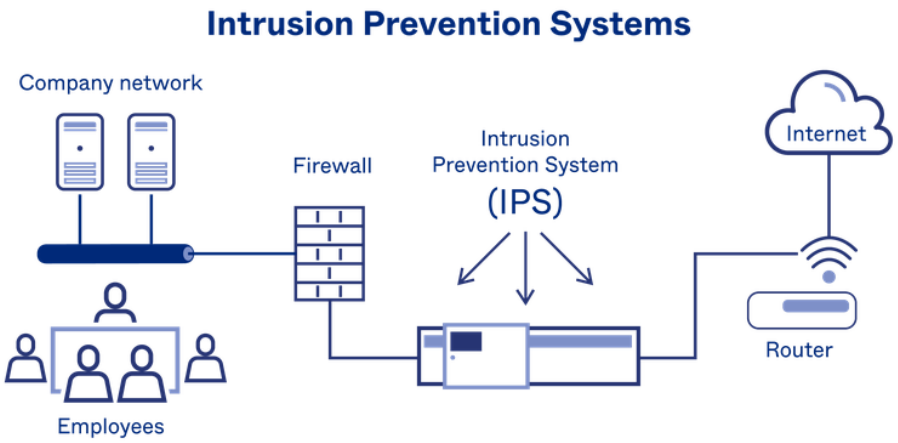


obrázek č. 3 – Koncept síťových zón, zdroj: [32]

Intrusion Prevention System (IPS)

Technologie zabezpečení sítě fungující jako prevence hrozeb. Zkoumá toky síťového provozu, aby detekovala případné ohrožení a tím zabránila případnému zneužití zranitelností. [33]

V síťové architektuře je IPS obvykle umístěn za Firewallem a poskytuje doplňující vrstvu analýzy, která detekuje nebezpečný obsah (*viz obrázek č. 4*). Narozdíl od svého předchůdce Intrusion Detection Systém (IDS) – jenž je pasivní systém, skenující síťový provoz a reportující v případě nálezu hrozby – je IPS umístěn přímo v komunikační cestě mezi zdrojem a cílem provozu, aktivně analyzující a v případě hrozby automaticky reagující. [34]



obrázek č. 4 – Zasazení IPS do síťové architektury, zdroj: [34]

Akce, kterými IPS reaguje na hrozby jsou následující:

- Odeslání upozornění administrátorovi
- Zahození škodlivého plaketu
- Blokování provozu ze síťové adresy
- Restart připojení [33]

Jelikož je IPS integrovaná komponenta zabezpečení, musí fungovat efektivně, aby nedocházelo ke snižování výkonu sítě a aby dokázala odhalit hrozby v reálném čase. [33]

IPS může obsahovat mnoho metod pro detekování síťových hrozeb, avšak dvě z těchto metod: Signature – Based Detection a Statistical Anomaly – Based Detection, jsou z pohledu využití dvěma hlavními metodami. [34]

Signature – Based Detection je metoda založená na slovníku jednoznačně identifikovaných vzorů nebo podpisů v kódu příchozích paketů. Pokud je odhalena hrozba, je podpis kódu uložen ve slovníků podpisů. [34]

Statistical Anomaly – Based Detection náhodně odebírá vzorky síťového provozu a porovnává je s předem vypočítanou základní úrovní výkonu sítě. Pokud je vzorek aktivity síťového provozu mimo parametry základního výkonu, provede IPS nutné akce, aby situaci dostal pod kontrolu. [34]

Původně byl IPS koncipován jako samostatné síťové zařízení. V dnešní době je však velmi často součástí bezpečnostních řešení routerů nebo hardwarových firewallů. [34]

TCP Intercept

Softwarová implementace v routeru pomáhající chránit TCP servery proti útoku SYN flooding. Ochrana probíhá tím způsobem, že TCP Intercept zachytává a ověřuje

požadavky na připojení TCP. V režimu zachytávání TCP Intercept zachytává pakety synchronizace TCP (SYN). TCP Intercept poté naváže spojení s klientem jménem cílového serveru. Pokud je úspěšný, naváže spojení s cílovým serverem jménem klienta a tím propojí obě strany. Pokusy o připojení z nedostupných hostitelů se nikdy nedostanou na server. [35]

Kvůli eliminaci nelegitimních požadavků se nastavují časové limity pro napůl otevřená připojení. [35]

Při vytváření zásad zabezpečení je možné definovat, jestli má TCP Intercept zachytávat všechny požadavky, či pouze ty, které pocházejí z konkrétních sítí, nebo ty, které jsou určeny pro konkrétní servery. Může být také nakonfigurována rychlost připojení a práh nevyřízených připojení. [35]

TCP Intercept může fungovat také pouze v režimu sledování. V tomto režimu pasivně sleduje požadavky na připojení procházející routerem. Pokud se připojení v nastaveném časovém intervalu nepodaří navázat, TCP Intercept zasáhne a pokus o připojení ukončí. [35]

Unicast Reverse Path Forwarding (URPF)

Technologický nástroj, který umožňuje routeru zkontrolovat dosažitelnost zdrojové adresy, ze které byly odeslány pakety. Tato schopnost umožňuje omezit výskyt falešných adres v síti. Pokud zdrojová IP adresa není platná, tak je paket zahozen. URPF může pracovat v jednom ze dvou režimů: striktní režim a volný režim. [36]

Ve striktním režimu URPF musí být pakety přijaty na rozhraní, které je poté použito i k odeslání zpětného paketu. Tím může být snížen i legitimní síťový provoz, který je přijímán na rozhraní, které nebylo určeno jako rozhraní pro odeslání zpětného paketu. K této situaci může dojít, pokud jsou v síti přítomny asynchroní routovací cesty. [36]

Ve volném režimu URPF musí být v routovací tabulce přítomna zdrojová adresa. Správci sítě mohou změnit toto chování a povolit výchozí routovací cestu při ověřování zdroje. Dále jsou zahozeny pakety, které obsahují zdrojovou adresu, pro kterou je návratová hodnota NULL. Je také možné definovat seznam, který povoluje či odepírá zdrojové adresy.

Ve firemních prostředích je velmi často potřeba použít kombinaci přísného a volného režimu. Volba jednotlivých režimů poté záleží na návrhu síťového segmentu, připojeného do rozhraní, kde je RPF nasazeno. [36]

V přísném režimu by mělo být URPF použito, pokud mohou správci zaručit, že všechny pakety přijaté na rozhraní pocházejí z podsítě přiřazené k rozhraní. Podsítě tvořené

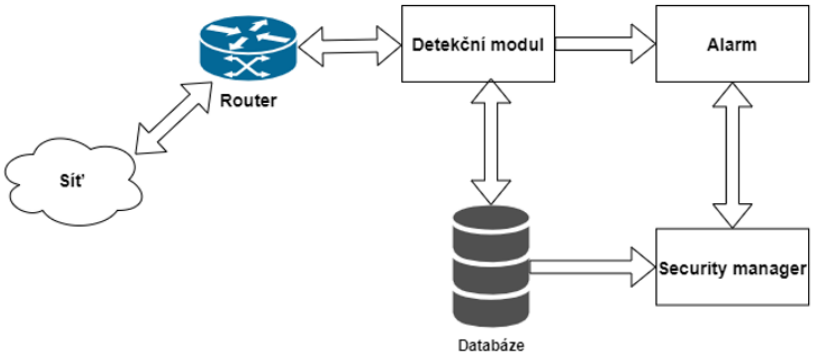
koncovými zařízeními nebo síťovými zdroji splňují tento požadavek. Tento návrh je vhodné použít v síti, kde je pouze jedna cesta dovnitř a jedna cesta ven. [36]

Volný režim se poté používá v nejvyšší vrstvě síťového rozhraní, ke kterému je přiřazena výchozí routovací trasa. [36]

Obrana proti DOS útokům

Existují tři architektury detekce a obrany se proti DOS útokům:

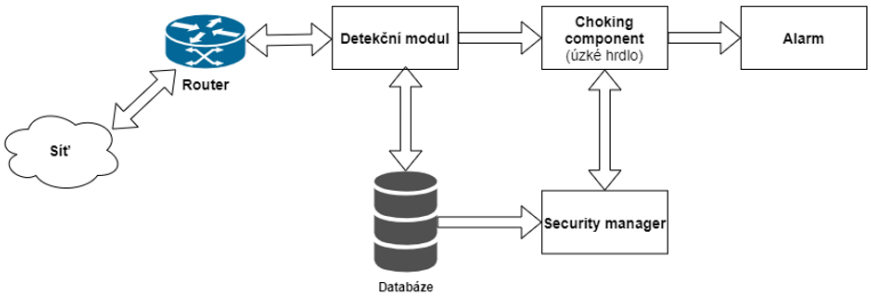
- **Victim-end defense mechanism** (Obranný mechanismus na straně oběti) (*viz obrázek č. 5*) – Toto řešení je implementováno právě na routeru cílové sítě. Detekční modul má za úkol objevit narušení na základě detekce podezřelého chování nebo detekce anomálie v komunikaci. Modul pravidelně ukládá výsledky komunikačních procesů. Detekce DOS útoku je zde relativně snadná, jelikož existuje mnoho dat pro porovnávání. Je to také nejčastější způsob obrany proti DOS útokům. Nevýhodou ale je, že během útoků se mohou zaplnit různé zdroje sítě oběti např. šířka pásma. Další nevýhodou je, že útoky jsou odhaleny až poté, co se dostanou k oběti. [27][28]



obrázek č. 5 – Architektura Victim-end defense mechanism, zdroj: [28]

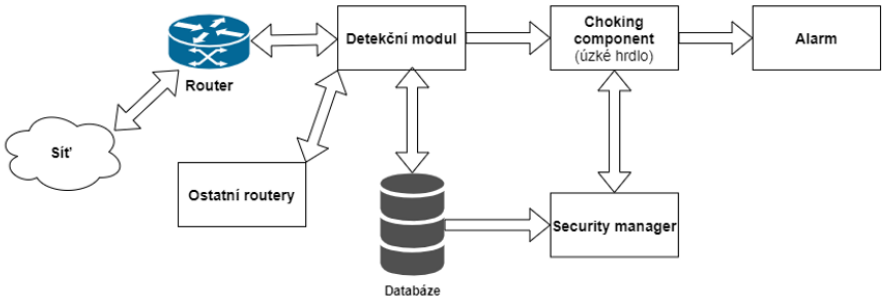
- **Source-end defense mechanism** (Obranný mechanismus na straně zdroje) (*viz obrázek č. 6*) – Architektura podobná obraně na straně oběti. Zde je přidaný modul, který porovnává statistiku odchozího a příchozího provozu se zahrnutými obvyklými profily komunikace. Tato metoda je nejlepší možnou obranou. Brání proti DOS útokům nejen na straně oběti, ale také na cestě. Problém je, že detekovat DOS útoky u zdroje není snadná záležitost. Důvodem je široká distribuce DOS útoků a jednotlivé zdroje se chovají podobně jako při běžném

provozu. Dalším problémem je obtížnost nasazení takového detekčního systému u zdroje komunikace. [27][28]



obrázek č. 6 – Architektura Source-end defense mechanism, zdroj: [28]

- **Intermediate network defense mechanism** (Obranný mechanismus uprostřed cesty) (*viz obrázek č. 7*) – Metoda, která je kompromisem mezi přesností detekce a spotřebovanou šířkou datového pásma, což je největší problém u Victim-end defense mechanism, respektive Source-end defense mechanism. Schéma umožnuje vzájemnou kooperaci, kde routery sdílejí informace s jinými routery. Tím je umožněna jednodušší detekce a tracebilita zdrojů útoků. Routery mohou také tvořit vzájemně překrývanou síť pro zjednodušené sdílení informací. Hlavní nevýhodou této architektury je její použitelnost, protože všechny routery v síti musí použít toto schéma, aby byla detekce co nejpřesnější. [27][28]



obrázek č. 7 – Architektura Intermediate defense mechanism, zdroj: [28]

2.4 Switch (přepínač)

V předchozí kapitole byla popsána činnost routeru, jehož pozice je mezi různými sítěmi. Internetová síť je totiž mnoho lokálních sítí propojených routery. Zpráva tak při své cestě prochází z jednoho routeru do druhého, až nakonec dorazí do cílové IP adresy.

Potom, jakmile se zpráva dostane přes poslední router, se musí dostat skrze síť ke správnému portu spojení, do kterého je zapojeno konkrétní zařízení, kterému je zpráva určena. Toto cílové zařízení, jako například osobní počítače nebo servery, jsou nějakým způsobem připojeny k této lokální síti. Router je určen k vzájemnému propojování různých sítí, takže k fyzickému propojení cílových zařízení je jeho využití nesmyslné. Objevují se tedy další zařízení, a to jsou switche, které umožňují cílovým zařízením připojení k lokální síti a jsou jejím základním kamenem. [4]

Switch je vysokorychlostní zařízení, které přijímá příchozí datové pakety a posílá je do jejich destinace v LAN síti a pracuje ve druhé (data link) nebo třetí (network) vrstvě OSI modelu. Switchi druhé síťové vrstvy se někdy také říká bridge (most), protože jeho funkce je přeposílání datových rámců mezi uzly nebo segmenty sítě. [2]

Switch třetí síťové vrstvy kombinuje funkcionality běžného switche a routeru. Funguje jako switch pro propojení zařízení, která jsou ve stejné podsítí, nebo virtuální LAN síti a má zabudovanou inteligenci pro směrování IP paketů. Dokáže podporovat routovací protokoly, kontrolovat příchozí pakety a dokáže rozhodovat o routování na základě zdrojové a cílové adresy. [4]

2.4.1 Možná rizika napadení

Všechna zařízení druhé vrstvy jsou považována na nejzranitelnější prvky v síťové infrastruktuře. Útoky prováděné na zařízení této vrstvy jsou z pohledu útočníka nejjednoduššími na nasazení v provozu cílové sítě. Tyto útoky lze, ale také eliminovat vcelku běžnými postupy, a to nastavením 2. síťové vrstvy v konfiguraci switche.

MAC address table overflow attack

MAC address table overflow attack je druh síťového útoku, kdy se útočník připojený do portu switche snaží „zaplavit“ MAC tabulku switche obrovským množstvím ethernetových rámců (Ethernet frames) s různou zdrojovou MAC adresou. Tabulka MAC adres switche disponuje pouze omezeným množstvím paměti, proto nedokáže switch dále ukládat MAC adresy, které přicházejí od zařízeních v síti. [7]

Poté co se zaplní tabulka MAC adres, switch přejde do Fail-open mode (režim otevření při poruše) a začne se chovat jako síťový hub (odesílání rámců do všech portů, podobně jako při broadcastové komunikaci). [7]

Jelikož odesílá switch všechny rámce na všechny porty v síti, tak také odesílá všechny rámce na útočníkův počítač (musí být fyzicky připojený k portu na switchi). Útočník tak získá data, která pro něho nejsou určená. [7]

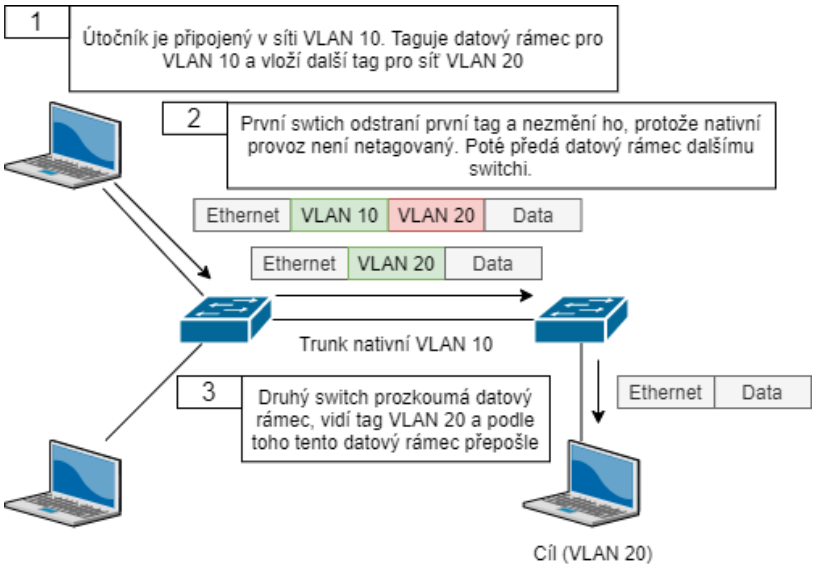
VLAN hopping attack

Tento typ hrozby umožňuje útočníkovi obejít omezení mezi různými VLAN sítěmi na 2. vrstvě síťové infrastruktury. Při správné konfiguraci portů na switchi by paket poslaný útočníkem musel projít routerem nebo jiným zařízením pracujícím na 3. síťové vrstvě k dosažení cíle v jiné VLAN síti. Nicméně, mnoho firemních sítí má slabou implementaci VLAN sítí nebo je mají špatně nakonfigurované, což umožňuje útočníkům provést právě již zmíněný druh útoku. Existují dvě hlavní metody kybernetického útoku VLAN Hopping:

Switch spoofing (Vydávání se za switch) – Těží ze špatně nastaveného trunk portu. Ve výchozím stavu má trunk port přístup do všech VLAN a posílá síťový provoz přes stejnou fyzickou linku mezi switchi. Útočník zde využívá faktu, že základní nastavení portu switche je *dynamic auto.* Útočník nakonfiguruje svůj počítač, aby se tvářil jako klasický síťový switch. *Spoofing* vyžaduje, aby byl síťový útočník schopen emulovat zprávy 802.1Q a DTP (Dynamic trunking protocol). Tím, že se útočník vydává za síťový switch a ostatní switche se s již zmíněným útočníkovým zařízením snaží navázat trunkové spojení, má útočník umožněn přístup do všech VLAN, které jsou povolené na daném portu. [8]

Double-Tagging attack (Útok dvojího tagování) (*viz obrázek č. 8*) **–** Využívá toho, jak pracuje hardwarové vybavení switche. Většina switchů vykonává pouze jednoúrovňové 802.1Q odpouzdření (de-encapsulation), což umožnuje útočníkovi přidat skrytý tag 802.1Q dovnitř síťového rámce. Zmíněný tag poté umožňuje, aby byl rámec přeposlán do VLAN sítě, kterou originální 802.1Q tag neobsahoval. Je důležité zmínit, že tento typ útoku funguje i v případě, že je trunk port zakázán, protože hostitel zpravidla posílá síťový rámec v segmentu, kde není trunkový port. [8]

Tento typ útoku je pouze jednosměrný a funkční pouze tehdy, pokud je útočník připojený do portu switche, který je ve stejné VLAN jako nativní VLAN síť trunkového portu. [9]



obrázek č. 8 – Dvojité zapouzdření, zdroj: [9]

Útok sestává celkem ze tří kroků.

- Útočník odešle dvakrát zapouzdřený síťový rámec do switche. Vnější hlavička má tag VLAN sítě, ze které útočník opravdu rámec odesílá, která je stejná jako nativní VLAN síť trunkového portu. Předpoklad je, že switch zpracovává rámec přijatý od útočníka z portu, který je trunkový nebo z portu s hlasovou VLAN sítí (Voice VLAN), protože switch by neměl přijímat takový síťový rámec na *access portu*. V ukázce na obr. 3 je nativní VLAN síť VLAN 10. Vnitřní tag obsahuje napadenou VLAN, tou je VLAN 20. [9]
- Síťový rámec dorazí na switch, ten po kontrole prvních 4 bajtů tagu 802.1Q zjistí destinaci VLAN 10, která je nativní VLAN sítí. Switch tedy odešle paket do všech portů v síti VLAN 10 po odebrání tagu s informací o síti VLAN 10. Na trunkovém portu switche je tag s VLAN 10 odstraněn a není přeznačen, protože je součástí nativní sítě. V tento moment je tag s informací o síti VLAN 20 stále nedotčený, protože nebyl zkontrolován prvním switchem. [9]
- Druhý switch v pořadí toku rámce si zkontroluje pouze vnitřní tag 802.1Q, vidí, že rámec je cílen do sítě VLAN 20. Druhý switch tedy odešle rámec do portu, na který je mířen útok, nebo jej zničí podle toho, jestli je na daném portu existující tabulka s MAC adresami, které mohou odesílat rámce do konkrétního portu switche. [9]

DHCP Attacks

Existují dva druhy útoků na DHCP a to: DHCP starvation a DHCP spoofing (DHCP server impersonation). Proti oběma typům útoků se brání pomocí implementace DHCP snooping. [6]

DHCP Starvation attack

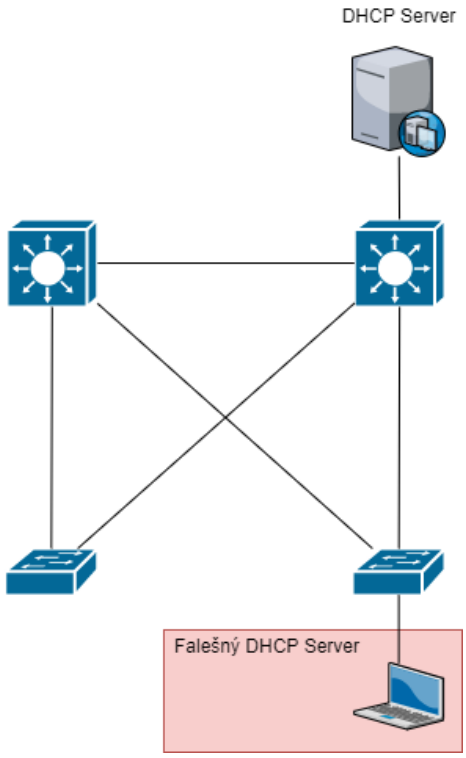
DHCP starvation je jednoduché implementovat, pokud nejsou zavedena žádná bezpečnostní opatření. Útočník požaduje všechny dostupné adresy z DHCP serveru zasláním velkého počtu požadavků na DHCP server s falešnými MAC adresami. I přesto, že je MAC adresa jednoznačný identifikátor rozhraní síťové karty (NIC) a je přidělena již výrobcem, je možné tuto adresu změnit softwarovou emulací. Každý požadavek s jinou MAC adresou považuje DHCP server za nový. Pokud útočník odešle velké množství takových požadavků, tak se fond adres DHCP vyčerpá. Tento stav vyčerpání způsobí, že noví síťoví klienti se nebudou moci připojit k síti. [10]

DHCP spoofing attack

Již zmíněný DHCP starvation může být útočníkův přípravný krok k zahájení sofistikovanější metody nazvané DHCP spoofing, kde útočník nejdříve vyřadí z provozu legitimní DHCP server, aby bylo jisté, že klienti nedostanou informace od něho, ale od falešného serveru. [10]

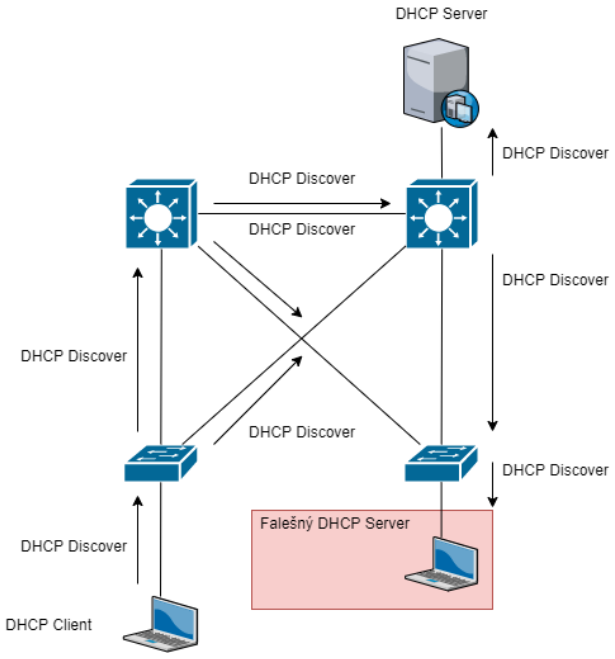
Detailní postup provedení DHCP spoofing je následující:

- Jak je znázorněné na *obrázku č. 9,* útočník připojí do sítě zařízení, které má za úkol tvářit se jako obyčejný DHCP server s tím rozdílem, že poskytuje klientům falešné konfigurační údaje IP. Je zapotřebí, aby byl falešný server připojený ve stejné podsíti a VLAN síti jako cílové počítače. [6]



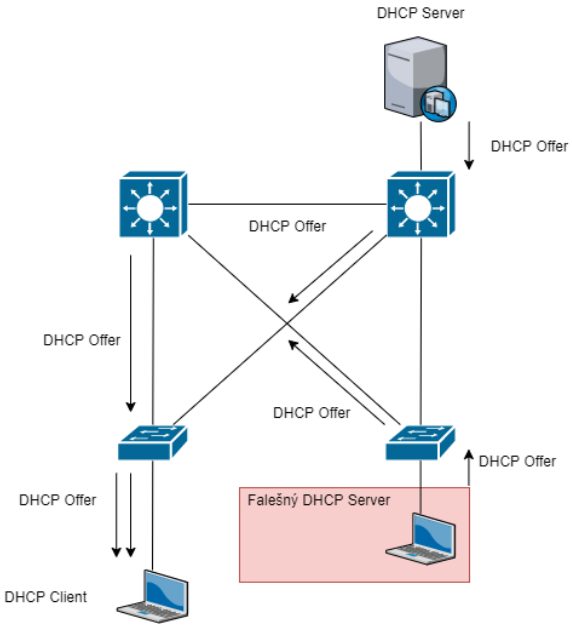
obrázek č. 9 – Připojení falešného serveru do sítě, zdroj: [6]

- Legitimní klienti se připojí do sítě a požadují konfigurační parametry IP od DHCP serveru. Nyní klient odešle broadcast zprávu DHCP Discover a čeká na odpověď od DHCP serveru. V tuto chvíli mu odpoví oba DHCP servery v síti. (*viz obrázek č. 10*) [6]



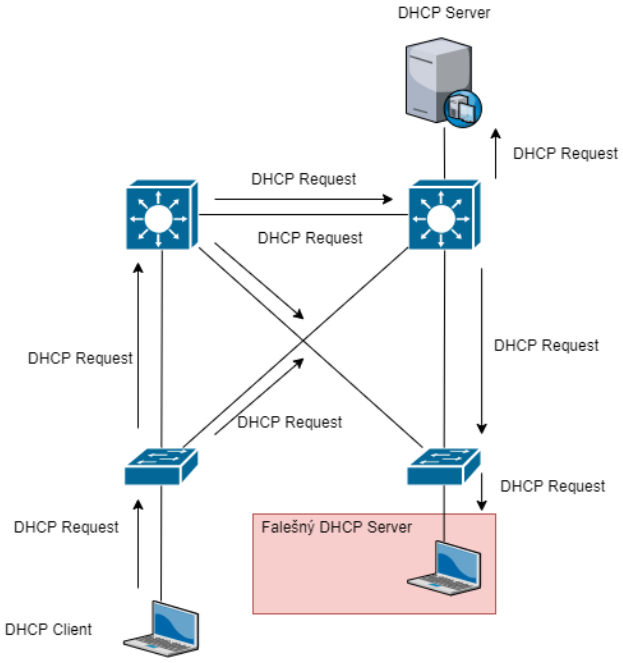
obrázek č. 10 – Klient odesílá broadcast požadavek DHCP Discover, zdroj: [6]

- Právoplatný DHCP odpoví chybnou konfigurací parametrů IP z důvodu vyčerpání zásoby platných IP konfigurací. Nicméně falešný DHCP server odešle klientovi DHCP offer obsahující konfigurační parametry IP definované útočníkem. Klient odpoví prvnímu offer paketu, který přijme. (*viz obrázek č. 11*) [6]



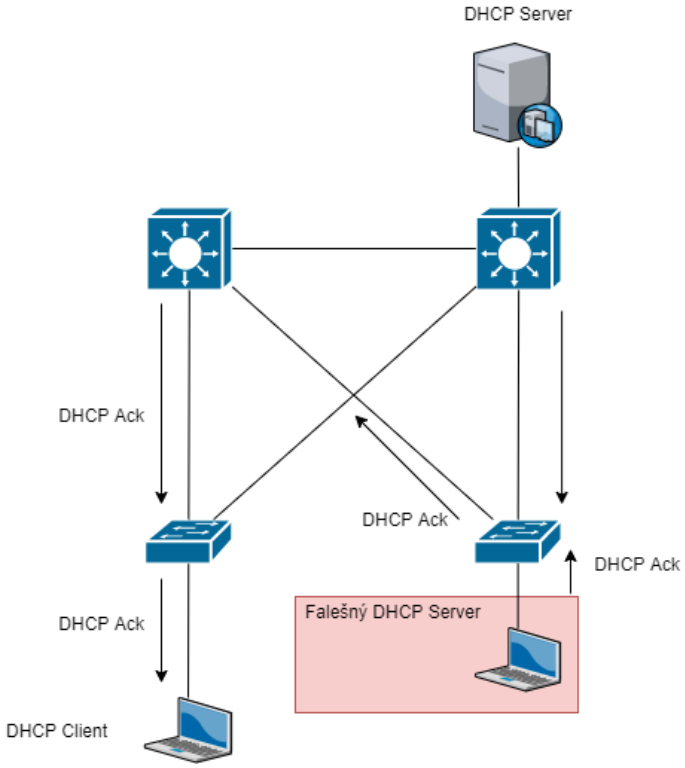
obrázek č. 11 – Odeslání DHCP Offer klientovi, zdroj: [6]

- Falešný offer paket je přijatý nejdříve, proto klient požaduje IP parametry definované útočníkem. (*viz obrázek č. 12*) [6]



obrázek č. 12 – Komunikace klienta a falešného DHCP serveru, zdroj: [6]

- Falešný server odpovídá klientovi a potvrzuje jeho požadavek. Legitimní server přestává komunikovat s klientem. (*viz obrázek č. 13*) [6]



obrázek č. 13 – Odpověď falešného serveru, zdroj: [6]

ARP attacks

Typ kybernetického útoku, který se provádí v LAN síti. Útok zahrnuje odesílání škodlivých ARP paketů na výchozí bránu za účelem změny párování IP adres vůči MAC adresám v její tabulce MAC adres. Jelikož je ARP protokol navržen pro výkon, ne pro zabezpečení, útok ARP Poisoning se provádí celkem snadno, pokud má útočník kontrolu nad počítačem v cílové síti LAN. [47]

Útok samotný probíhá tak, že útočník odesílá na výchozí síťovou bránu ARP reply message a informuje ji, že MAC adresa útočníkova zařízení by měla být propojena s IP adresou jeho cíle a obráceně, MAC adresa jeho cíle by měla být spojena s IP adresou útočníka. Výchozí brána přijme tuto zprávu a odešle změny na všechna ostatní zařízení v síti. Veškerý provoz cíle na jakékoli jiné zařízení v síti prochází počítačem útočníka, což útočníkovi umožňuje kontrolu, úpravu nebo přeposlání provozu na jeho skutečný cíl. Kvůli tomu, že útoky ARP Poisoning probíhají na nízké úrovni, tak uživatelé, kterých se tyto útoky týkají, si většinou neuvědomí, že je jejich síťový provoz kontrolován nebo upravován. [47]

STP attacks

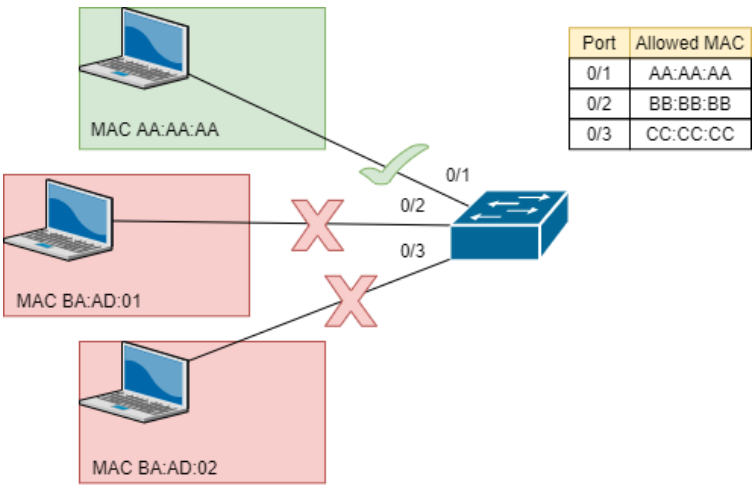
STP manipulation attack funguje na principu falšování root bridge v síťové topologii. Útočník vysílá změnu konfigurace STP BPDU, aby vynutil přepočet STP. Rozeslané BPDU oznamuje, že útočníkův systém má nižší prioritu bridge. Útočník poté dokáže na svém stroji sledovat různé datové rámce přeposílané z ostatních switchů. Přepočet STP může také způsobit DoS v síti tím, že každých 30 až 45 sekund způsobí přerušení při každé změně kořenového můstku. [48]

2.4.2 Jak zmírnit rizika napadení switche

Zmírnit riziko napadení switchů téměř na nulu musí být prioritou každé větší i menší společnosti. Níže jsou uvedeny techniky, díky kterým je možné takového zmírnění dosáhnout.

Jak předejít MAC address table overflow attack

Nejjednoduššíma a nejefektivnějším způsobem, jak předejít přetečení tabulky MAC adres je zavedení tzv. Port security na switchi. Port security omezuje počet platných MAC adres na jednom portu switche. Tento režim umožňuje správci sítě ručně nakonfigurovat MAC adresy povolené na jednotlivých portech nebo povoluje možnost switche dynamicky se naučit omezený počet MAC adres, které obslouží. Pokud je switch nakonfigurován v tomto režimu a obdrží datový rámec, je zdrojová adresa tohoto rámce porovnána s interním seznamem povolených MAC adres na switchi, které byly manuálně zadány, anebo dynamicky naučeny na portu. (*viz obrázek č. 14*) [6]



obrázek č. 14 – Znázornění funkce Port security, zdroj: [6]

Na *obrázku č. 14* je znázorněna funkce Port security, kde má switch povolené 3 MAC adresy funkcí Port security (AA:AA:AA, BB:BB:BB, CC:CC:CC). Ke switchi jsou připojené 3 počítače, ale pouze jeden počítač se switchem komunikuje, protože ostatní dva mají MAC adresy (BA:AD:01, BA:AD:02), jež se nenacházejí v uložených povolených MAC adresách na switchi. [6]

Obrana proti VLAN hopping attack

Nejlepší obrana proti těmto typům útoku je zajištění, aby byla nativní VLAN síť jiná než VLAN sítě, které jsou používané na portech switche. Další kroky k zamezení VLAN hopping attack jsou:

- Zakázat Dynamic trunking protocol (DTP) na portech switche, které nejsou trunkové (Cisco).
- Zakázat nepoužívané porty a přesunout je do nepoužívané VLAN sítě.
- Ručně povolovat linky na trunkových portech.
- Nastavit nativní VLAN síť, jinou než VLAN 1. [6]

Obrana proti DHCP útokům

Protiopatření a techniky boje proti DHCP útokům se odehrávají ve dvou vrstvách síťové architektury: fyzické a datové. [11]

Datová vrstva

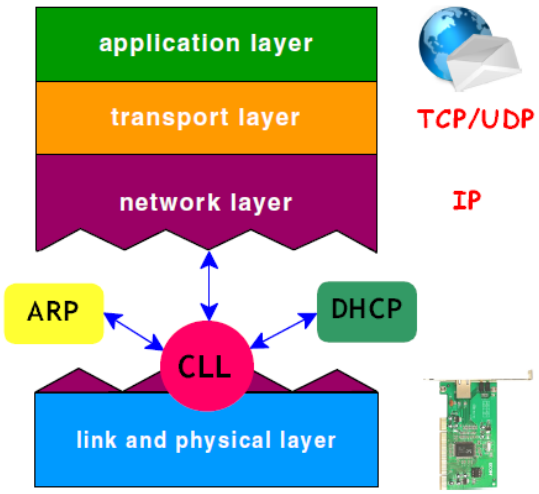
Většina DHCP serverů požaduje omezení výčtu klientů pomocí výčtu důvěryhodných MAC adres. Bohužel tyto MAC adresy mohou být zjištěny útočníkem a použity k získání IP adresy útočníkovým zařízením. [11]

Existuje metoda ověřování DHCP, založená na metodě předání přihlašovacího tokenu a zpožděného ověření pro zprávy DHCP. Metoda založená na tokenu požaduje, aby si server a klient vyměnili heslo nebo token skrze síť. Nevýhoda této metody je, že se informace posílají přes síť v podobě prostého textu, což znamená, že mohou být tyto tokeny snadno vypátratelné. V metodě zpožděného ověřování je použit sdílený symetrický klíč k autorizaci komunikace mezi serverem a klientem. Tato metoda má však nevýhody. Například je zde vyžadováno distribuování sdíleného klíče metodou *out of band*, což je typ komunikace, kde je vyžadováno sekundární ověření prostřednictvím samostatného komunikačního kanálu, spolu charakteristickým ID a heslem. [11] [12]

Další ověřovací metoda, použitelná ke zmírnění DHCP útoku, je metoda autentifikace skrze *Kerberos* server. Použití Kerberos serveru zvyšuje flexibilitu a poskytuje možnost meziregionální autentifikace. Nicméně tyto výhody jsou vyvažovány větší složitostí. Kryptografické klíče musejí být navíc sdíleny mezi Kerberos serverem a klienty.

Existuje také tzv. metoda ověření na základě certifikátu (CBDA). CBDA implementuje zpožďování základních komponent ověřování, tzn. že se spolu ověří DHCP server i DHCP klient sdíleným symetrickým klíčem, který znají obě strany ještě před tím, než započnou DHCP komunikaci, kromě toho se klient i server shodnou na společném identifikátoru, který může odkazovat na sdílený klíč, aniž by byl posílán přes fyzické medium. [13]

Metoda kryptografické linkové vrstvy v lokální síti je rozšíření zabezpečení 2. a 3. síťové vrstvy, které se nazývá vrstva kryptografických odkazů (CLL). (*viz obrázek č. 15*) [14]



obrázek č. 15 – Umístění CLL vrstvy, zdroj: [14]

Ve schématu této vrstvy by měla centrální autorita (CA), většinou se jedná o síťového administrátora, poskytovat základní certifikáty klientům po kontrole jejich MAC adresy. Klient poté může tento certifikát připojit ke zprávě DHCPREQUEST. DHCP server poté využije vrstvu CLL k ověření požadavku a následně vydá kompletní klientský certifikát odvozený od základního certifikátu. Kompletní certifikát obsahuje IP adresu, přidělenou k MAC adrese stroje. Tím je svázána identita uživatele na jeho MAC a IP adresu. Díky tomu, lze omezit počet DHCPREQUEST od uživatele v určitém časovém intervalu z důvodu ochrany proti DHCP starvation. Tato metoda ale bohužel trpí stejnými neduhy jako metody ověření na základě certifikátu, a to přidanou složitostí a sníženou flexibilitou. Metoda také

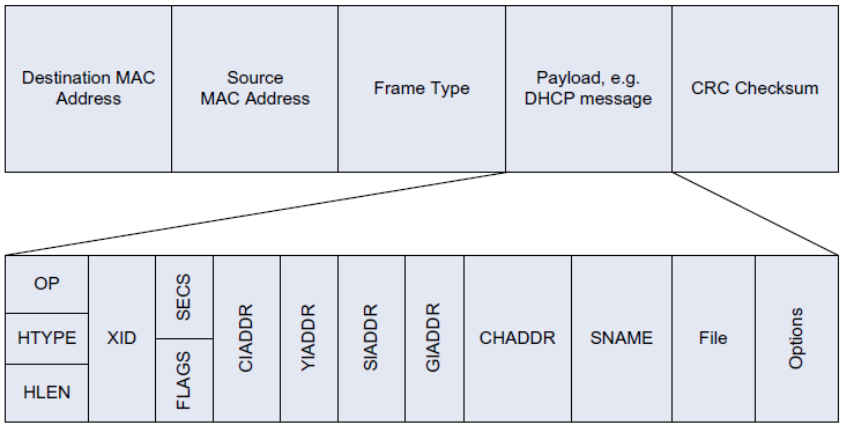
vyžaduje zásahy síťového administrátora kvůli přidělování základního certifikátu pro každého nového klienta připojeného do sítě. [14]

Jednou z jednodušších možností je počítání paketů DHCPREQUEST v určitém časovém intervalu. Jestliže číslo těchto paketů překročí určitý limit, systém vyhodnotí, že se jedná o DHCP starvation. Bohužel nevýhody této metody spočívají ve falešných oznámeních a poté taky v odmítnutí legitimních DHCPREQUEST zpráv na základě těchto falešných poplachů. Dále může také útočník obejít zabezpečení omezením počtu zpráv DHCPREQUEST. [14]

Rozhraní koncových prvků

Na rozhraní koncových prvků se lze útoku DHCP starvation účinně bránit omezením počtu povolených MAC adres na jednotlivých portech síťového switche. To lze nastavit u většiny běžně používaných switchů do firemních infrastruktur. Toto nastavení však může ochromit celkovou flexibilitu sítě, obzvláště pokud se jedná o velké komplexní firemní sítě. Tento problém lze však výrazně omezit dobrou organizací firemních sítí. Další nevýhodou takového řešení je, že je nepoužitelné ve sdílených bezdrátových sítích (WLAN), protože se tam připojuje mnoho zařízení k jednomu přístupovému bodu. [11]

Metoda *Port Security* může být útočníkem překonána tím, že schová svoji MAC adresu v hlavičce Ethernetového rámce a použije jinou padělanou MAC adresu. *Obrázek č. 16* popisuje Ethernetový rámec a v něm integrovaný paket DHCP. [11]

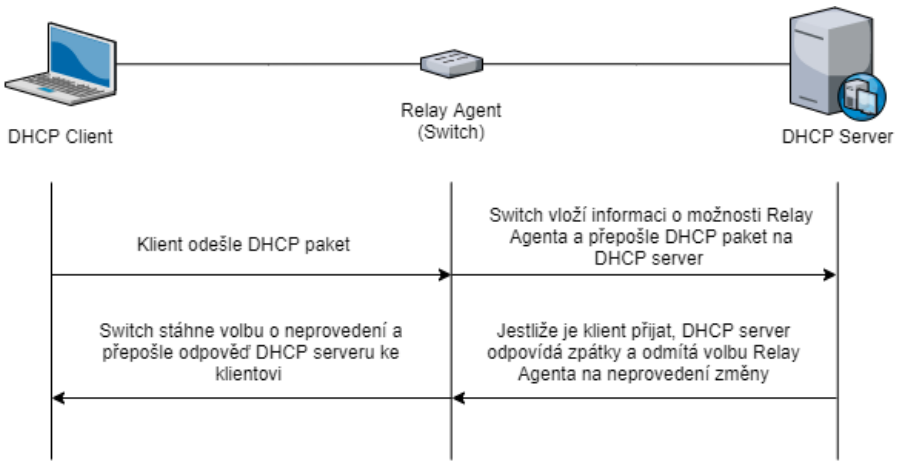


obrázek č. 16 – Ethernetový rámec s paketem DHCP, zdroj: [11]

K předejití útoku DHCP Starvation by měla být metoda Port Security kombinovaná s kontrolou MAC adresy v Ethernetovém rámci a MAC adresy v poli CHADDR v integrovaném DHCP paketu. [11]

Je také možné rozšířit možnosti ochrany DHCP použitím **Relay agenta (switch)**. *Obrázek č. 17* popisuje fungování Relay agenta, Ten má za úkol uchovávat číslo portu a ID

switche před posláním DHCP zprávy na DHCP serveru. Server tuto informaci použije ke kontrole rozdělení IP adres, a zhodnotí, jestli klient nepřesáhne počet povolených IP adres. Jestliže by klient tento počet přesáhl, bude požadavek ignorován. [11]



obrázek č. 17 – Základní výměna zpráv protokolu s použitím Relay agenta, zdroj: [11]

DHCP starvation attack může být také omezen limitováním počtu povolených MAC adres pocházejících od jednoho klienta ve sdílené síti. [11]

Nejméně složitým a zároveň nejúčinnějším opatřením ke zmírnění DHCP starvation attack je však implementace Port Security, nicméně je také velmi důležité plánování distribuce IP adres z DHCP poolu mezi různými porty. [11]

Obrana pro ARP útokům

K tomu, aby se zabránilo útokům ARP spoofing a ARP poisoning, musí být switch schopen zajistit, aby byly předávány pouze platné požadavky a odpovědi ARP. [6]

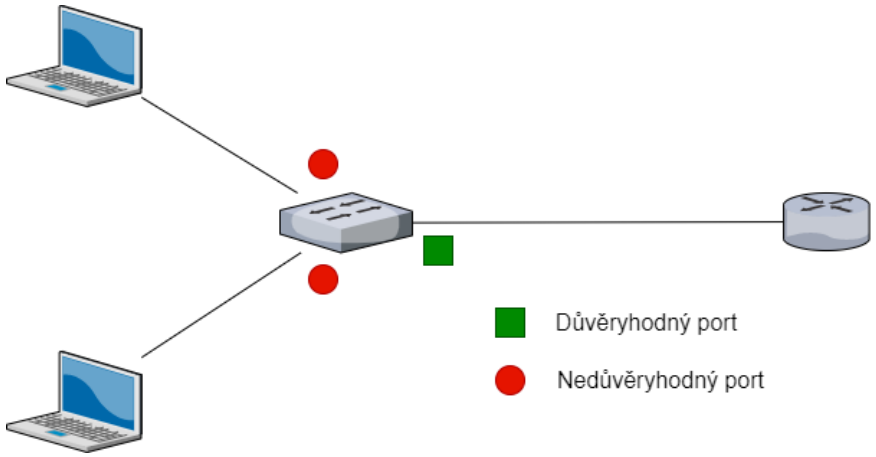
Funkce switchů Dynamic ARP inspection (DAI) vyžaduje DHCP snooping a pomáhá bránit ARP útokům tím, že:

- Nebude posílat neplatné nebo neopodstatněné ARP požadavky na jiné porty ve stejné VLAN.
- Přeruší všechny požadavky a odpovědi ARP na nedůvěryhodných portech.
- Ověří všechny přerušené pakety, jestli mají validní spojení IP-MAC.
- Zruší a loguje ARP požadavky, pocházející z neplatných zdrojů, aby se zabránilo ARP poisoning.
- Deaktivuje rozhraní, pokud dojde k překročení konfigurovaného počtu paketů ARP. [6]

Aby se zmenšila šance úspěšných útoků ARP spoofing a poisoning, je vhodné na switchích implementovat tato opatření:

- Povolit globálně DHCP snooping.
- Povolit DHCP snooping na vybraných VLAN sítích.
- Povolit Dynamic ARP Inspection na vybraných VLAN sítích.
- Nakonfigurovat důvěryhodného rozhraní pro DHCP snooping a ARP inspection. [6]

Doporučuje se také nakonfigurovat všechny přístupové porty switche jako nedůvěryhodné a všechny živé porty, připojené k ostatním switchům, jako důvěryhodné. (*viz obrázek č. 18*) [6]



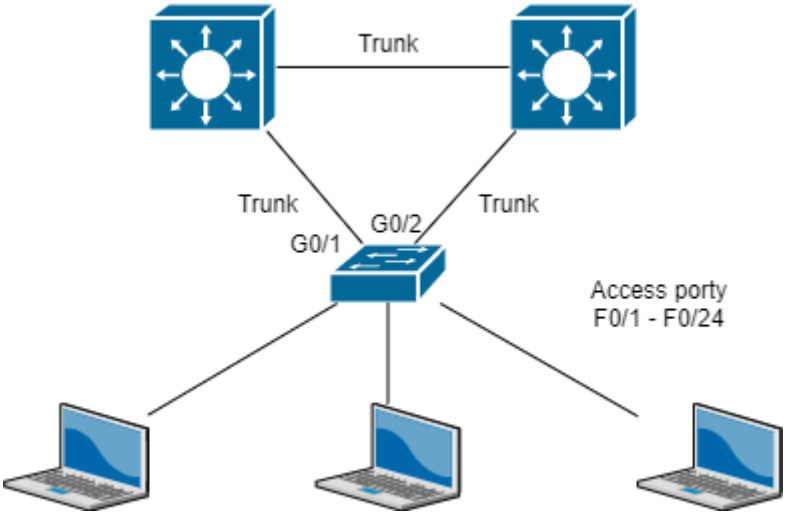
obrázek č. 18 – Důvěryhodné a nedůvěryhodné porty, zdroj: [6]

Obrana proti STP útokům

Pro předejití útokům proti STP je dobré použít PortFast a Bridge Protocol Data Unit (BPDU) Guard:

- PortFast – Způsobuje, že switch nebo trunkový port přejde do stavu předávání STP okamžitě nebo po události propojení, tím se obejdou stavy naslouchání a učení. Funkce PortFast se povoluje na úrovni portu, ten může být fyzický nebo logický. PortFast by měl být konfigurován pouze na portech připojených ke koncovým zařízením. [49]
- BPDU Guard – Chrání port před přijímáním BPDU STP, port však stále může STP BPDU přeposílat. Pokud je na portu, které má povolené BPDU Guard, přijat STP BPDU, port se vypne a stav portu se změní na Error-Disable. Podobně jako

PortFast, BPDU Guard by měl být nakonfigurován pouze na rozhraních připojených ke koncovým zařízením. Na *obrázku č. 19* je znázorněna konfigurace PortFast a BPDU Guard na Access portech. [49]



obrázek č. 19 – Konfigurace PortFast a BPDU Guard na Access portech, zdroj: [6]

2.5 Koncová zařízení

Zařízení, se kterými lidé pracují zdaleka nejvíce. Aby bylo možné jednotlivá zařízení od sebe odlišit, má každé koncové zařízení v síti adresu. Pokud chce jakékoli koncové zařízení iniciovat komunikaci, použije adresu kteréhokoli jiného koncového zařízení k určení místa, kam zprávu doručit.

Koncovými zařízeními obvykle jsou:

- Počítač (pracovní stanice, laptop, server)
- Síťová tiskárna
- Telefon VoIP
- Bezpečnostní zařízení
- Mobilní zařízení (mobilní telefony, tablety, čtečky karet, scannery čárových kódů) [41]

Zabezpečení koncových zařízení je stejně důležité jako zabezpečení ostatních prvků sítě. Existuje mnoho způsobů, jak může útočník ohrozit zabezpečení počítače, stejně jako způsobů, jak může hacker zkusit zcizit uživatelská data nebo infikovat počítač. Jakmile se jednou hrozba dostane bez povšimnutí do počítače, má tendenci vykazovat jenom málo příznaků o své přítomnosti, takže může v počítači přežít dlouho dobu, aniž by byla zpozorována. [41]

Online bezpečnost a prevence počítačové kriminality by měla být přímočará, protože online zločinci se obecně snaží dostat k cíli co nejrychleji a nejsnadněji. Čím je koncový systém zabezpečenější, tím je větší pravděpodobnost, že útočník obrátí svoji pozornost jinam. [41]

2.5.1 Možné ohrožení osobních počítačů, pracovních stanic a serverů

Osobní počítače, pracovní stanice a servery jsou, v případě bezpečnosti, nejvíce náchylné na uživatelské chyby. [40]

Chyby zabezpečení počítačů

Chyby zabezpečení jsou nedostatky v počítačovém softwaru, které vytvářejí slabiny v celkovém zabezpečení počítače. Tyto chyby lze také vytvořit nesprávnou konfigurací počítače. [40]

Malware

Jakýkoli rušivý software vyvíjený kyberzločinci za účelem poškození dat, poškození či zničení počítačů nebo celých počítačových systémů. Příklady typického malwaru jsou:

Viry, červy, trojské koně, spyware, adware a ransomware. [44]

Ransomware

Ransomware je malware, který využívá šifrování, aby znepřístupnil obětem jejich informace. Útočník poté obvykle požaduje výkupné za opětovné dešifrování informací. Ransomware je obvykle navržen tak, aby se šířil po síti a cílil na databázové a souborové servery. Jedná se o velmi rychle rostoucí hrozbu, která generuje miliardy dolarů na platby kyberzločincům a způsobuje značné škody a výdaje podnikům a vládním organizacím. [40]

K šifrování je využíváno asymetrické šifrování, to využívá pár klíčů k zašifrování a dešifrování dat. Veřejně-soukromý pár klíčů je generován útočníkem, přičemž soukromý klíč dešifruje soubory uložené na útočníkově serveru. Útočník zpřístupní oběti soukromý klíč až po zaplacení výkupného. Poslední ransomwarové útoky však ukázaly, že tomu tak nemusí být vždy a i po zaplacení výkupného se oběť nemusí dočkat odpovědi. Bez přístupu k soukromému klíči je skoro nemožné tyto soubory dešifrovat. [46]

Spyware

Spyware je druh malwaru, může být uživatelem stažen z pochybných webových stránek, emailových zpráv nebo souborových serverů. Kromě výčtu tradičních zdrojů tohoto nechtěného softwaru může uživatel stáhnout spyware také po licenčním souhlasu u jiného počítačového programu. [42]

Spyware je používán z mnoha důvodů. Obvykle se snaží sledovat a prodávat údaje o používání internetu nebo se snaží zachytávat informace o bankovních účtech nebo kreditních kartách uživatelů. Nějaké typy spywaru dokážou instalovat dodatečný software do počítače, který dokáže provádět změny v počítači. [42]

Spyware se dělí na 4 hlavní typy:

- Adware – Monitoruje historii prohlížeče a stažené soubory se záměrem předpovědět jaké služby a produkty daného uživatele zajímají. Adware se pokouší zobrazovat reklamy na produkty, aby uživatele nalákal na jejich nákup. Používá

se především k marketingovým účelům a jeho největším negativním dopadem je zpomalení počítače. [42]

- Trojský kůň – Maskuje se jako legitimní software. Může se např. tvářit jako aktualizace Javy nebo kteréhokoli softwaru. Trojský kůň je řízen třetí stranou a je používán k přístupu k osobním informacím. [42]
- Tracking cookies – Sledují uživatelské aktivity na webu, např. vyhledávání, historii a stahování. [42]
- System monitors – Zachytává téměř všechny činnosti, které uživatel na počítači provádí. Mohou být zaznamenány všechny stisky kláves, emaily, navštívené webové stránky, spuštěné programy. Často jsou tyto typy programů maskované jako freeware. [42]

Spam

Spam je digitální nevyžádaná pošta zasílaná hromadně přes internet nebo pomocí jakéhokoli systému elektronických zpráv. Zahrnuje nevyžádané zprávy, nechtěné reklamy, nabídky k prodeji atd. Je také vážným problémem zabezpečení, protože jej lze použít k doručování emailů, které mohou obsahovat trojské koně, viry a další typy škodlivého softwaru. [43]

Spam se děli na několik druhů:

- Emailový spam – Zanáší doručenou poštu a odvádí pozornost od důležitých emailů. [43]
- SEO spam – Známy také jako spamdexing. Jeho účelem je zneužívání metod optimalizace pro vyhledávače ke zlepšení hodnocení vyhledávání na webu spammera. SEO lze rozdělit do dvou podkategorií: [43]
    - Obsahový spam – Spammeři naplní své webové stránky oblíbenými klíčovými slovy, která obvykle nesouvisejí s jejich webem, aby se dostali v indexu vyhledávače co nejvýše. [43]
    - Odkazový spam – Jedná se o odkazy v diskusích na webových stránkách nebo příspěvky na fórech plné irelevantních odkazů. [43]
- Spam na sociálních sítích – Spammeři zde využívají výhod rychlé online socializace a pomocí falešných účtů šíří svůj vliv na sociálních platformách. [43]
- Mobilní spam – Spam ve formě SMS. Kromě nevyžádaných SMS zpráv jsou využívány také falešné mobilní notifikace. [43]

- Spam v online zprávách – Podobný emailovému spamu, ale rychlejší. K rozesílaní jsou využívány platformy jako např: WhatsApp, Skype, nebo Snapchat. [43]

Phishing

Typ útoku sociálního inženýrství určený k ukradení osobních dat včetně přihlašovacích údajů a čísel kreditních karet. K útoku dochází, když hacker vydávající se za důvěryhodnou entitu, podvede svoji oběť, aby otevřela email nebo zprávu. Příjemce je poté přesměrován na nepravý odkaz, což může vést ke spuštění instalace malwaru, odhalení citlivých informací nebo k jinému poškození. [45]

Útok může mít devastující následky. U fyzických osob to může zahrnovat neoprávněné nákupy, krádež finančních prostředků nebo krádež identity. [45]

V korporacích se phishing používá jako příprava pro větší útoky např. Advanced Persistent Threat (APT). V APT jsou zaměstnanci využiti, aby distribuovali malware v uzavřeném prostředí firmy nebo získali přístupy k zabezpečeným datům. [45]

2.5.2 Zabezpečení koncových zařízení

Existuje mnoho způsobů, jak zabezpečit koncová zařízení v domácím i firemním prostředí, jsou to např.:

- Ochrana heslem – jeden z nejdiskutovanějších problémů kolem kybernetické bezpečnosti. Najdou se však stále oblasti, které heslům nevěnují dostatečnou pozornost. Je nutné zajistit, aby byl na stolních počítačích, noteboocích a mobilních zařízeních nastaven silný přístupový kód. Pro zvýšenou obranu lze využít nástroj pro správu hesel a dvoufaktorové ověřování. [40]
- Aktuální software – Nejaktuálnější aktualizace softwaru by měli být instalovány, pokud mají být systémy bez bezpečnostních chyb. Se zařízeními, která nemohou přijímat nejnovější upgrady je potřeba zacházet podle speciálně definovaných pravidel. [40]
- Zamykání zařízení – Pokud pracovník opouští své pracovní místo, měl by si být vždy jistý, že má zamknutý počítač. [40]
- Zásady osobní online bezpečnosti – Společnosti by měli mít svůj kodex chování zaměstnanců v online prostředí. Pracovníci firmy by se měli poté těmito pravidly řídit. [40]

- Bezpečnostní software – Na každém zařízení by měl být nainstalovaný bezpečnostní software, který chrání počítač před hrozbami. [40]
- Obezřetnost – Uživatelé počítače by neměli otevírat potenciálně nebezpečné internetové stránky a emailové přílohy. Dále je nevhodné, aby měli uživatelé administrátorská práva ve svém pracovním počítači, mohlo by dojít k instalaci nebezpečných programů. [40]
- Zabezpečení firemních aplikací – Firemní aplikace by se měly řídit zásadami online bezpečnosti. Přihlašovací údaje aplikací by se neměly v žádném případě nacházet nikde v otevřené podobě. Komunikace mezi aplikacemi a servery by měla být šifrovaná, a měly by se využívat aktuální verze vývojových platforem. [40]

2.6 Konvergovaná síť

Síťová konvergence je koexistence telefonní, datové a video komunikace v rámci jedné sítě. Použití více komunikačních režimů v jedné síti by mělo zvýšit efektivitu a pohodlí, které infrastruktura se separátními sítěmi nemůže poskytnout. Konvergenci se také říká sjednocená komunikace. Součástí konvergentní sítě může být:

- Textová komunikace – Odesílání krátkých, alfanumerických zpráv mezi mobilními telefony, jak je implementováno mobilním operátorem.
- Prohlížení webových stránek.
- Voice over IP (VoIP) – Přenos hlasu a multimediálního obsahu pomocí síťového protokolu IP.
- Streamování médií – Odesílání video nebo audio obsahu v komprimované podobě přes síť. Video nebo audio je poté okamžitě přehráno, aniž by bylo uloženo na pevný disk nebo jiný úložný prostor.
- Videokonference – Živé, vizuální spojení mezi dvěma nebo více lidmi sídlícími na fyzicky oddělených místech za účelem komunikace.
- Hraní online her – Používání specializovaných aplikací (elektronických her nebo video her) na herních konzolích nebo na počítači.
- Elektronický obchod – Nákup a prodej zboží, služeb nebo finančních prostředků prostřednictvím elektronické sítě. [53]

Při návrhu konvergované sítě je důležité si hned na začátku uvědomit, jaký typ datového provozu bude sítí procházet. Pro návrh sítě jsou důležité čtyři atributy:

- Šířka pásma – Maximální kapacita průchodu datové sítě. Základní jednotka jsou bit/s (bity za sekundu). Běžně se však používají jednotky řádově vyšší (kbit/s, mbit/s, gbit/s).
- Propustnost – Aktuální rychlost síťového provozu procházejícího sítí. Měřeno v bit/s (kbit/s, mbit/s, gbit/s).
- Latence (Round Trip Time (RTT)) – Doba, kterou trvá přechod z jednoho bodu sítě do druhého. Měřeno v milisekundách (ms).
- Jitter – Odchylka latence v síti. [54]

Tyto čtyři parametry mohou být různě upřednostňovány podle toho, jak je potřeba optimalizovat síť a jaký datový provoz se má přenášet.

Pokud bude administrátor navrhovat síť, přes kterou bude procházet výhradně datový provoz, měl by se soustředit převážně na šířku pásma a pouze okrajově o latenci a jitter. Pokud by se přes tuto síť přenášel soubor o velikost např. 100 gbit rychlostí 10 mbit/s, trvalo by to přibližně 2 hodiny a 45 minut. Latence a jitter by tento čas navýšili pouze o 1–3 sekundy. [54]

Pokud by měl však administrátor za cíl navrhnout datovou síť přenášející VoIP provoz, měl by brát v potaz především latenci a jitter a částečně také šířku pásma. Pokud někdo s někým hovoří v reálném čase, velikost paketů není příliš velká. Je však velmi důležité, aby se každé slovo dostalo na druhý konec co nejrychleji. Telefonování přes síť by bylo takřka nepoužitelné, pokud by bylo každé slovo zpožděné o několik sekund. [54]

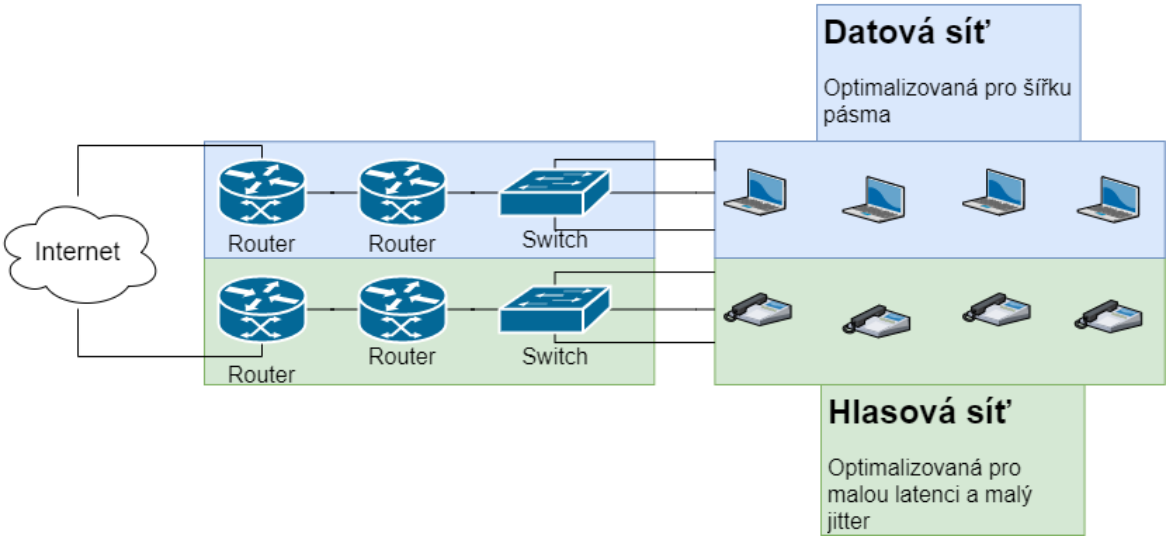
2.6.1 Porovnání konvergované a původní nekonvergované sítě

Celkově lze sítě rozdělit do tří typů:

- Původní nekonvergovaná síť
- Konvergovaná síť
- Konvergovaná síť využívající VLAN sítě [54]

Původní nekonvergovaná síť

Aby bylo dříve možné vyhovět různým prioritám, bylo nejjednodušším řešením vybudovat dvě na sobě nezávislé sítě. Jednu optimalizovanou na přenášení dat a druhou optimalizovanou pro přenos hlasového přenosu. *(viz obrázek č. 20) [54]*



obrázek č. 20 – Původní nekonvergované síť, zdroj: vlastní zpracování

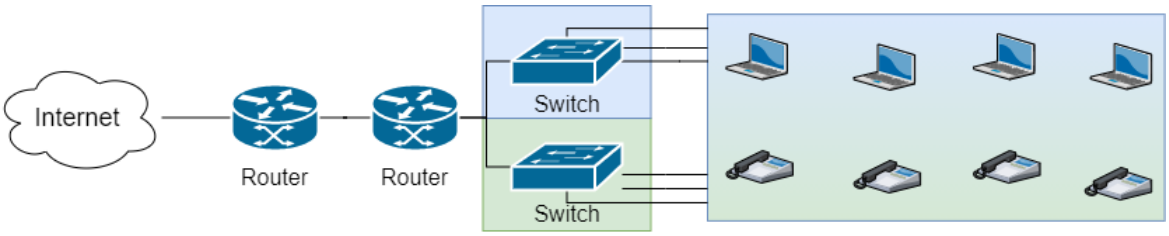
Konvergovaná síť

Jak pokročila síťová zařízení ve svém výkonu a funkčnosti, bylo možné provozovat datový i hlasový provoz na stejných síťových zařízeních (router, switch, aj.).

Síťová architektura však musí stále upřednostňovat různé charakteristiky pro hlasový nebo datový provoz. Musí být proto schopná jednotlivé síťové provozy od sebe odlišit.

Primární metoda, jak rozpoznat různá síťová zařízení a jejich nároky na síťový provoz je využití různých IP sítí. VoIP telefony mohou mít rozsah IP adres např. 172.16.2.0/24, a počítače jiný rozsah IP adres např. 172.16.7.0/24. V tomto případě se velmi často využívají fyzicky oddělené switche pro oddělení IP sítí. *(viz obrázek č. 21)*

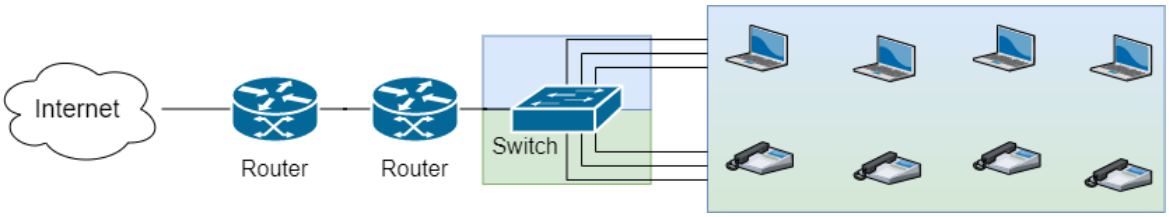
Síťová zařízení poté mohou aplikovat různé priority provozu sítě na základě IP adres cílových zařízení pomocí funkce Quality of Service (QoS). [54]



obrázek č. 21 – Konvergovaná síť, zdroj: vlastní zpracování

Konvergovaná síť využívající VLAN sítě

Stejného efektu, jako rozdělení sítí pomocí různých IP rozsahů, lze docílit použitím jednoho fyzického switche pro více sítí za použití VLAN. *(viz obrázek č. 22)* VoIP telefony i počítače jsou připojeny do stejného switche, ale jsou logicky oddělené do různých IP sítí pomocí VLAN, např.: VoIP VLAN a Datová VLAN. [54]



obrázek č. 22 – Konvergovaná síť využívající VLAN sítě, zdroj: vlastní zpracování

2.6.2 Bezpečnost konvergovaných sítí

Když docházelo k útokům na oddělené sítě, útočník měl přístup pouze k datům konkrétní sítě, do které se nu podařilo vniknout. Toto se změnilo, jakmile začaly všechny zdroje využívat stejnou infrastrukturu. Technologie konvergované sítě představuje pro síťové administrátory rozsáhlou bezpečnostní výzvu. Útočníkům umožňují konvergované sítě zakrýt jejich aktivity při procházení síťovými doménami, tomu se lze bránit pomocí tří základních bezpečnostních principů, jsou to:

- Řízení přístupu
- Ochrana zařízení a aplikací
- Síťová architektura dynamické odezvy [56]

Řízení přístupu

V mnoha sítích dnes nelze s jistotou říct, kdo nebo co se k nim připojuje a co tam mají za úkol. Je také důležité rozlišovat mezi špatným a dobrým využitím firemní síťové infrastruktury. Existují tři kritické funkce pro řízení přístupu do sítě: [55]

- Autentizace a detekce všech zařízení připojených do sítě – Protokoly jako 802.1x jsou vhodné pro řízení přístupu k síti počítačů s lidskými uživateli. Pro zařízení jako jsou IP telefony, kamery, multimediální zařízení aj. je však tradiční model autentizace, spočívající v předložení pověření a identity systému, neznámý. Přizpůsobení těmto technologiím vyžaduje tedy novou sadu autentizačních technik. [55]
- Autorizace všech připojených zařízení – Proces přidružení ověřeného zařízení k roli, která byla podnikem zadána. Mělo by být docíleno, aby síť věděla, že např. telefon smí tuto síť používat, ale navíc jaké oddělení nebo zaměstnanec má právo tento telefon používat. [55]
- Přidružení zásad, jakmile dojde k autentizaci a autorizaci – Dynamické mapování správných služeb, oprávnění a přístupu k připojeným zařízením. [55]

Ochrana zařízení a aplikací

Druhou funkcí bezpečné konvergované sítě je schopnost poskytnout aktivní ochranu používaným zařízením a aplikacím. Například VoIP je aplikace využívající jasně srozumitelné protokoly a úrovně provozu, proto by měl být komunikační systém schopný

definovat ochranné mechanismy, které zabrání zneužívání VoIP zařízení a aplikací tím, že neumožní využití protokolů, které nemají pro VoIP žádný význam. Je tedy potřeba, aby byl systém schopný: [55]

- Definovat zásady použití zařízení pro systém, kde je nechtěným aplikacím a protokolům globálně zakázán přístup k síti.
- Vytvořit a dynamicky aplikovat definici služeb, která urychlí a současně ochrání různé systémy od zneužití.
- Chránit systémy před jinými protokoly, než které používají, protože by mohly být použity k jejich kompromitaci a zneužití. [55]

Síťová architektura dynamické odezvy

Mechanismus, který zajišťuje, že když se v síti objeví něco nepředvídaného, co by mohlo ovlivnit spolehlivost nebo integritu konvergovaných systémů, může síť identifikovat hrozbu, lokalizovat její zdroj a dynamicky odstranit, izolovat nebo jinak kontrolovat tuto hrozbu v reálném čase. Je možné tak předejít rozsáhlému dopadu na systémy v infrastruktuře.

Dynamická odezva sestává z těchto elementů:

- Schopnost komplexně a detailně detekovat útok na síť nebo konvergovaný systém.
- Možnost oznámení a lokalizace bodu vniknutí hrozby do sítě.
- Schopnost změnit chování sítě v místě připojení, kde byla lokalizována hrozba. To by mělo být provedeno úpravou zásad, aby byla hrozba izolována a deaktivována. [55]

Budování sítě s ohledem na bezpečnost, zaměření řízení přístupu, proaktivní ochranu a dynamickou odezvu systému zajistí, že bude možné vybudovat základ pro síť, která bude použitelná pro téměř jakoukoli budoucí aplikaci nebo službu, bez ohledu na pochyby z případné bezpečnosti této sítě. [55]

2.7 Audit firemních sítí

Korporátní organizace jsou dnes velmi závislé na své síťové infrastruktuře, aby mohly bez problémů provádět své každodenní operace, což je dnes v prostředí vzdálených pracovišť stále důležitější. Povinností IT pracovníků je zajistit efektivní fungování s tím spojených síťových systémů. S dnešním exponenciálním rozšiřováním sítí se dramaticky zvyšuje i počet zranitelností a bezpečnostních mezer. Výpadek nebo závada sítě mohou mít za následek ztrátu příjmů společnosti i její dobrou pověst. [52]

Audit sítí je proces shromažďování, analýzy a studování dat sítě za účelem zhodnocení stavu sítě. Síťový audit poskytuje podnikům přehled o tom, jak úspěšné jsou v oblasti kontroly managementu sítě, obzvláště pokud jde o interní i externí směrnice o dodržování předpisů. Díky auditům dokážou IT pracovníci porozumět stavu svých sítí a přijímat potřebná opatření k nápravě případných nedostatků. Poznatky ze sběru dat lze použít k pochopení momentálního stavu sítě ve srovnání s průmyslovými standardy.

Síťový audit obvykle obsahuje analýzu těchto komponent:

- Implementace kontrol
- Dostupnost
- Bezpečnost
- Management
- Výkon [51]

Síťový audit pomáhá pracovníkům IT získat větší přehled o všech potenciálních problémech korporátní sítě a umožňuje je odstranit dříve, než způsobí prostoje, výpadek nebo jinak ovlivní výkonnost podniku. Díky síťovým auditům a hodnocením je také možné dosáhnout následujících dílčích cílů:

- Minimalizovat neznámé proměnné v korporátní síti.
- Odkrýt nové příležitosti zlepšování síťové infrastruktury.
- Splnit regulační požadavky a průmyslové standardy.
- Vytvořit budoucí plány správy síťové infrastruktury. [51]

Velmi důležité je také udržování záznamů o změně hardwaru, přidávání nových zařízení, změně konfigurací, instalaci nebo modifikaci firewallu, tedy operací, které jsou nezbytné pro optimalizaci výkonu a zabezpečení sítě. Kdykoli by došlo k poruše sítě, mohou IT pracovníci tyto záznamy použít k rychlé identifikaci a nápravě problému. [52]

V současné éře práce z domova organizace stále více adoptují způsob práce BYOD. S touto změnou pracovního stylu přichází také zvýšené nároky na robustnost datové sítě a větší bezpečnostní rizika. V organizacích, kde byl BYOD implementován, si musejí být IT pracovníci vědomi rizik a implementovat zásady pro management těchto zařízení, aby minimalizovali rizika. [52]

Ne ve všech firmách je však zaveden režim práce BYOD, i když se však zaměstnanci připojují ke korporátní síti pomocí podnikových zařízení, tak sítě procházejí neustálými změnami. Je tedy důležité, aby správci sítě tyto změny sledovali a pravidelně prováděli audity, aby zajistili, že zabezpečení a výkon sítě jsou na vysoké úrovni. [51]

Jak provést audit síťové infrastruktury

Přestože existují nástroje automatizující proces auditu, IT pracovníci mohou tyto akce provádět i manuálně. Audit sítě obvykle provádí síťový analytik, auditor informačních systémů nebo jiná osoba s odbornými znalostmi v oboru IT bezpečnosti a správy sítě. Automatické i manuální zpracování auditu má několik styčných bodů, jsou to: [52]

Inventura síťových zařízení

Je zásadní auditovat všechna zařízení připojená k síti v pravidelných časových intervalech. U všech zařízeních musí být zjišťováno, zda stále dostávají aktualizace firmwaru a zabezpečení od svých dodavatelů. Pokud zařízení tyto záplaty nedostávají, mělo by být organizací určeno, zda jsou již zastaralá a je nutné je vyměnit. [52]

Dostatečnost šířky pásma

Vyhnout se síťovým místům s nízkou průchodností je důležité pro zajištění komfortní práce koncového uživatele. Správci sítě by za tímto účelem měli pečlivě analyzovat firemní síť a porovnávat je s trendy ve využívání šířky datového pásma. Podrobná analýza může správcům pomoci vyhledat aplikace, které mají největší spotřebu a provést příslušné změny. [52]

Uživatelé a úrovně přístupu

Počet uživatelů se zvyšuje s rostoucí velikostí infrastruktury. Je tedy dobrým zvykem zaimplementovat politiku omezeného přístupu pro všechny uživatele. IT pracovníci poté mohou při auditu zjistit, jestli nebyly provedeny nějaké neoprávněné změny a pokud ano, tak na ně adekvátně zareagovat. [52]

Konfigurace sítě a pravidla firewallu

Změny v konfiguraci sítě se pravidelně dělají pro zlepšení výkonu sítě. Pravidla firewallu jsou také pravidelně aktualizována kvůli zajištění aktuální síťové bezpečnosti. Oba tyto druhy změn však musejí být kvalitně dokumentovány a auditovány, případné chyby mohou způsobit problémy v síti. [52]

Dostupnost a stav sítě

Důkladný audit dostupnosti a stavu sítě pomáhá IT administrátorům zjistit, která zařízení jsou náchylná k problémům a jaké změny v síti pravidelně způsobují výpadky. Tyto informace mohou být použity k tomu, aby se dalo těmto problémům vyhnout nebo aby je bylo možné okamžitě řešit. [52]

Pravidla provedení síťového auditu

Legitimně provedený audit by se měl bezvýhradně držet styčných bodů popsaných výše, k provedení kvalitního auditu však musí auditor také:

- Zaznamenat všechny podrobnosti auditu.
- Zdokumentovat všechny postupy a procesy týkající se auditu.
- Zkontrolovat systém řízení podnikových procedur.
- Vyhodnotit školící protokoly a operace.
- Zkontrolovat aktualitu bezpečnostních záplat pro síťový software.
- Potvrdit, zda jsou penetrační testy v souladu s pravidly a dostatečné.
- Testovat součásti softwaru co nejkomplexněji.
- Identifikovat bezpečnostní díry ve firewallu.
- Zajistit, aby všechna citlivá nebo důvěrná data byla uložena odděleně a bezpečně.
- Zajistit šifrování úložného média na jakémkoliv firemním zařízení.
- Zkontrolovat zabezpečení bezdrátových sítí.
- Vyhledat a identifikovat všechny neautorizované access pointy.
- Zkontrolovat proces monitorování protokolu událostí.
- Sestavit obsahově komplexní zprávu o auditu.
- Poslat závěrečnou zprávu příslušným zainteresovaným stranám. [51]

Automatizace auditu síťové infrastruktury

Existuje několik možností nástrojů automatizujících proces auditu. Při výběru nástroje je však nutné, aby IT administrátoři potvrdili, že nástroj má potřebnou funkcionalitu, identifikuje problém, měří jeho dopad a pomáhá poskytovat pomoc při řešení problému.

Pro skenování sítě mohou být použity běžné nástroje např. NetStumbler (na starších počítačích) nebo jeho nástupce inSSIDer. Další typy nástrojů např. ManageEngine Network Configuration Manager nebo N-able® RMM jsou řešení typu vše v jenom a nabízí software pro monitoring sítě, vytváření sestav zachycování dat, správu oprav, informace o narušení dat, možnosti zálohování a obnovy, aj. [51][52]

Další specializované crackovací nástroje, např. Aircrack-ng, mohou být použité pro testování šifrování bezdrátové sítě.

3 Zavedení bezpečnostních metod ve firmě Saint-Gobain ADFORS

Je zcela zřejmé, že aplikace zásad kybernetické bezpečnosti je dlouhotrvající a velmi náročný proces. V dalších kapitolách následuje výčet činností, kterých se podařilo dosáhnout před a během psaní diplomové práce. Do budoucna se však počítá s rozšířením kybernetických opatření a bezpečnostních pravidel, které pomohou firmě v boji s kybernetickými riziky.

Bezpečnostní nastavení provedená v rámci informačního systému však bohužel nejsou všemohoucí. Všechny dosavadní aktivity podniknuté v boji proti kybernetickým hrozbám je potřeba podpořit pravidelným školením všech zaměstnanců, kteří využívají k práci ve firmě informační technologie. Školení by se mělo zaměřit na bezpečnost používání informačních technologií a také na novinky, které informační svět přináší velmi často. Školení by však zaměstnance nemělo zbytečně zdržovat od jejich primární pracovní činnosti. Z tohoto pohledu se jako vhodná kombinace variant školení jeví:

- Interaktivní online školení se závěrečným testem nabytých znalostí v případě pravidelného bezpečnostního školení.
- Školení za fyzické přítomnosti firemního nebo externího IT pracovníka v případě školení nového softwaru.

Školení by ideálně mělo obsáhnout všechny okruhy činností, na které se vztahuje činnost běžného zaměstnance např.:

- Emailová komunikace
- Pravidla internetových přístupů
- Pravidla při používání informačních zdrojů
- Podporované programové vybavení
- Evidence hardwaru a softwaru
- Pravidla při využívání vlastních zařízení
- Ochrana citlivých údajů (personální data, know-how)
- Pravidla určená pro používání certifikátů a elektronických podpisů zaměstnanců

Školení by měla být i pro běžné uživatele co nejvíce srozumitelná a ideálně by měla obsahovat i praktický trénink, kde by byli účastníci školení vystaveni reálným situacím z kybernetického světa.

3.1 Zabezpečení kritických zařízení proti fyzickému ohrožení

Jak již bylo zmíněno, velkou hrozbou bezpečnosti zařízení ve firmě jsou přírodní nebo okolní vlivy, které mohou působit negativně na počítačové prvky. Původní stav fyzického zabezpečení ve firmě nebyl uspokojivý. Původně byl určený jeden server pro kancelářské i výrobní procesy. Tento server byl společně se síťovými zařízeními umístěn v jedné vybrané místnosti v kancelářské budově. Z hlediska budoucí udržitelnosti bylo však nutné provést změny, které odpovídají dnešním moderním standardům.

Počátkem změny bylo nakoupení nových serverů značky Dell a jejich rozdělení do různých místností podle typu určení. Server pro činnosti ředitelství (Kofax, K2 agendy, apod…) byl umístěn v původní místnosti starého serveru. Druhý server, určený pro potřeby výrobní části firmy (skladové aplikace, výrobní file server, apod…) byl umístěn do nově vybrané místnosti v závodní administrativní budově. *(viz obrázek č. 23)*

obrázek č. 23 – Instalace DELL racku do serverovny, zdroj: vlastní zpracování

V každé serverové místnosti jsou nainstalovány 2 UPS baterie, které dokážou udržet server v provozu až 18 minut při výpadku elektrického proudu.

Dále byla v obou serverovnách naistalována speciální vyvýšená podlaha, která slouží jako ochrana proti případným záplavám. *(viz obrázek č. 24)*

obrázek č. 24 – Ukázka speciální vyvýšené podlahy, zdroj: vlastní zpracování

Dále jsou v serverovnách nainstalovány klimatizační jednotky, aby se předešlo případnému přehřívání všech informačních komponent. *(viz obrázek č. 25)*

obrázek č. 25 – Klimatizační jednotky v serverovně, zdroj: vlastní zpracování

Jistící skříň ke klimatizačním jednotkám je z důvodu bezpečnosti umístěna ve fyzicky oddělené místnosti s vlastním zamykacím systémem, aby se předešlo neodbornému manipulování s jističi určenými ke klimatizačním jednotkám a jejich následnému vypnutí.

Pokud by však došlo k náhlému vypnutí okruhu elektrické energie, který napájí klimatizace, mají jednotky zabudovanou funkcionalitu odeslání upozorňující SMS zprávy pověřené osobě, aby byl dotyčný pracovník informovaný a mohl neprodleně zasáhnout.

Serverovna je také zabezpečena elektronickým zámkem a alarmem pro zajištění vstupu pouze oprávněným a poučeným osobám. Pokud by se do serverovny dostala nepovolaná osoba, alarm se spustí a SMS zprávou upozorní odpovědné osoby. *(viz obrázek č. 26)*

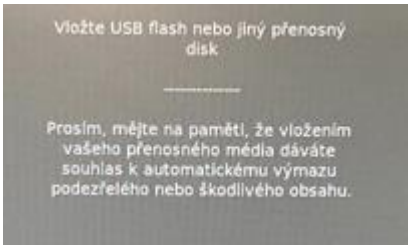
obrázek č. 26 – Elektronický zámek, zdroj: vlastní zpracování

Možným zlepšením do budoucna by mohla být implementace teplotního čidla, které by měřilo celkovou teplotu v místnosti nezávisle na klimatizačních jednotkách a v případě neopodstatněného zvýšení teploty by aktivovalo PLC jednotku (nebo jiné IoT zařízení), která by měla za úkol vyhodnotit situaci a popřípadě upozornit odpovědného pracovníka.

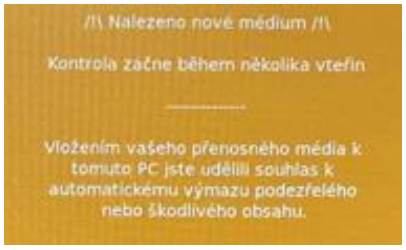
3.2 Projekt čistících stanic

Projekt čistících stanic řeší problematiku zavlečení škodlivého kódu do infrastruktury firmy vlastními zaměstnanci. Může nastat situace, že zaměstnanec firmy najde před firmou pohozený USB disk a chce si ho ponechat. V nějakých případech však může být USB disk infikován škodlivým kódem. Pro tyto případy se nyní nachází v areálu firmy 20 stanic (budoucí plán počítá s navyšováním počtu dekontaminačních stanic). Jako hardware stanic byl použit počítač Lenovo Thinkcentre s nainstalovaným operačním systémem Linux Mint, program dekontaminačních stanice je napsán v jazyce Python.

Po vložení neověřeného disku do dekontaminační stanice program automaticky načte médium a spustí jeho kontrolu. Na *obrázku č. 27* je zobrazena úvodní obrazovka čistící stanice, po vložení podezřelého disku se automaticky spustí program, který začne prohledávat vložené médium. *(viz obrázek č. 28)*

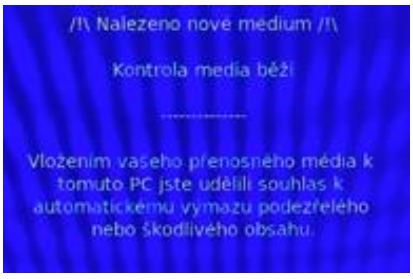


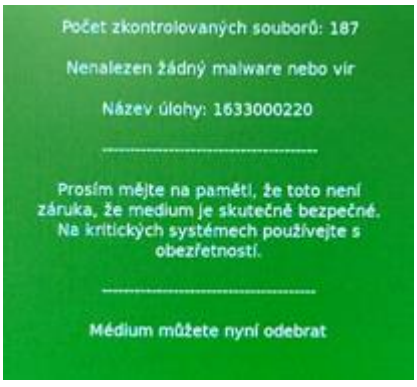
obrázek č. 27 – Úvodní obrazovka čistící stanice, zdroj: vlastní zpracování



obrázek č. 28 – Zahájení kontroly vloženého média, zdroj: vlastní zpracování

Dále je uživatel informován o probíhající kontrole média (*viz. obrázek č. 29*), tato kontrola trvá cca 1 minutu a pokud program nenajde žádný škodlivý kód, ponechá data na USB disku beze změny a vypíše závěrečné informace. (*viz. obrázek č. 30*)





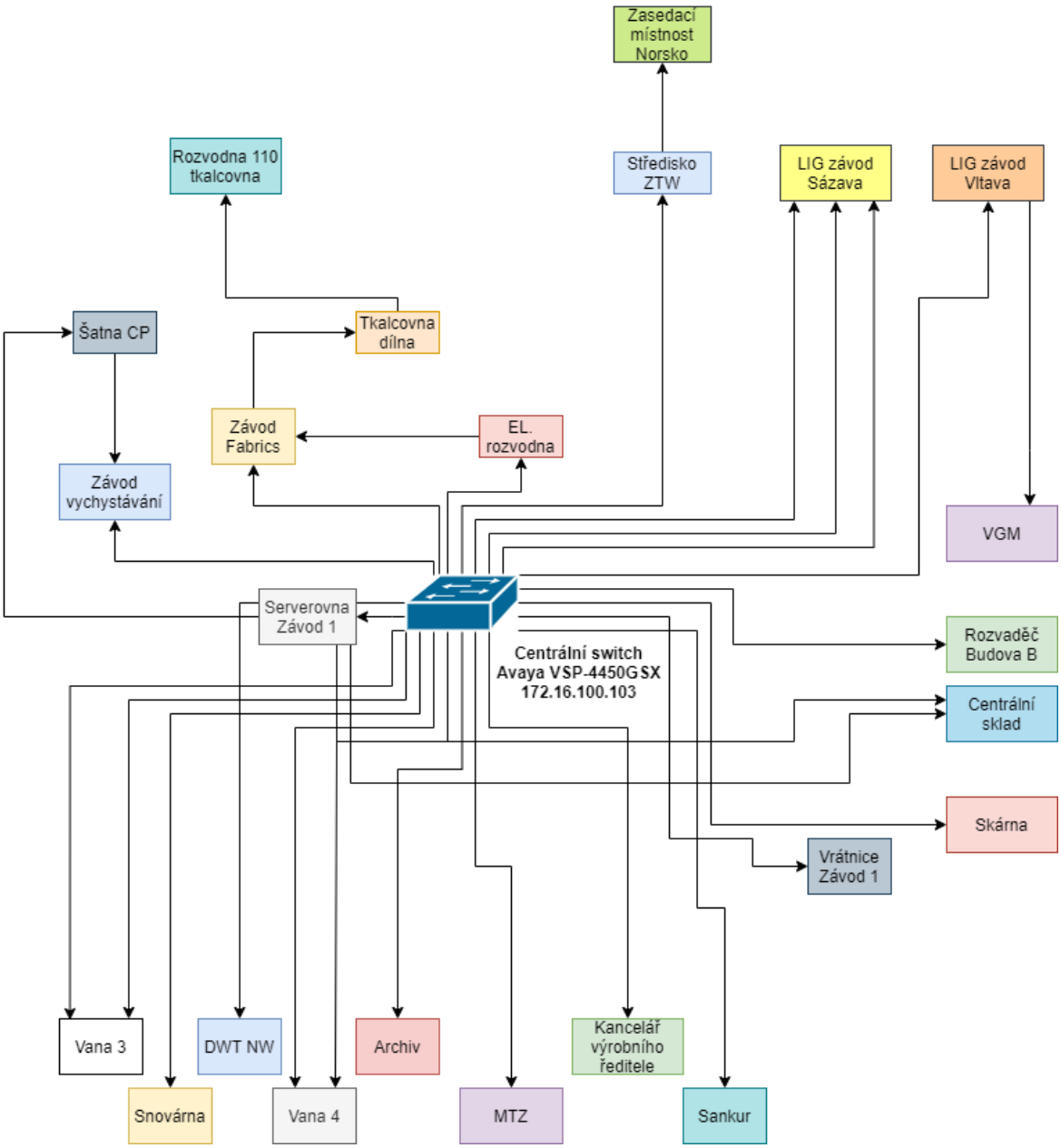
obrázek č. 29 – Kontrola vloženého média, zdroj: vlastní zpracování

obrázek č. 30 – Výsledek kontroly, zdroj: vlastní zpracování

V opačném případě se celý disk zformátuje, a veškerá data na disku jsou nenávratně smazána.

3.3 Analýza a konfigurace aktivních síťových prvků

V síťové infrastruktuře firmy Adfors se nachází cca 2500 zařízení, z toho 90 switchů a jeden Layer 3 switch, který přesměrovává komunikace mezi jednotlivými VLAN sítěmi. Na *obrázku č. 31* je znázorněno zjednodušené schéma síťové architektury ve firmě Adfors. Podrobnější analýza rozvržení switchů se nachází v příloze „Síťová architektura Adfors.png“.



obrázek č. 31 – Zjednodušené schéma síť. architektury, zdroj: vlastní zpracování

Distribution Level síťové infrastruktury je nezbytné zabezpečit tak, aby činnost infrastruktury s pomocí standardních protokolů nebyla ohrožena špatnou konfigurací na této a Access Level úrovni. Switche, které se nachází ve výrobní části, jsou z historického

hlediska složeny z několika druhů od různých výrobců (Aruba Cisco, Nortel). Cílem, na kterém se již pracuje, je sjednocení platformy switchů po celé firmě. Pro tento účel byl vybrán výrobce Aruba.

V kapitolách níže je znázorněna konfigurace dvou vybraných switchů z firemního prostředí. Ostatní výrobní switche byly nakonfigurovány podle potřeb konkrétních provozů, kde jsou umístěny.

Zařízení jsou zároveň rozdělena do VLAN sítí (*viz tabulka č. 1*), kterých je ve firmě celkem 74. Úplný seznam VLAN sítí ve firmě Adfors lze nalézt v příloze „Seznam virtuálních sítí firmy Saint-Gobain Adfors“.

VLAN	Název	Popis	Počet zařízení
2	admGR	Generální ředitelství administrace	x
3	admZ1	Závod 1 administrace	x
4	admGR_2	Generální ředitelství administrace 2	x
5	admZ1_2	Závod 1 administrace 2	x
6	Doch_AP	Zařízení docházkového systému	34
7	ArubaLIT	Zařízení Aruba	x
8	Sit158	Síť 158	x
10	Interco_MPLS	Síť Multiprotocol Label Switching (MPLS)	x
11	Interco_L3_PA	Síť Layer 3 Palo Alto	x
12	Interco_L3_GRE	Síť Layer 3 GRE	x

tabulka č. 1 – Ukázka VLAN sítí, zdroj: vlastní zpracování

3.3.1 Segmentace do VLAN sítí

Hlavní cíl segmentace do různých VLAN sítí je rozdělení administrativní sítě generálního ředitelství a výrobní sítě, do které jsou zahrnuty zařízení související s výrobou a jejími technologiemi.

Síť generálního ředitelství

Pro síť generálního ředitelství je vyčleněna VLAN 105 a VLAN 297.

VLAN 105 – SG net

Na tuto síť dopadají nejtvrdší definovaná pravidla a regulace co se týče bezpečnosti. Výčet pravidel je následující:

Počítače připojené do sítě musejí mít vždy nainstalovanou nejaktuálnější verzi operačního systému a všechny bezpečnostní aktualizace. Pokud tak není z nějakého důvodu

učiněno, počítač je v Active Directory (AD) označen jako zastaralý a není možné ho připojit k počítačové síti.

Dále jsou definována pravidla:

- Není dovoleno připojovat do sítě zařízení jiná než firemní (notebooky, počítače).
- Uživatel nesmí procházet nepovolené webové stránky.
- Uživatel není oprávněn instalovat aplikace do svého firemního zařízení.

VLAN 297 – WIFI SG net

Další virtuální síť VLAN 297 je stejně jako VLAN 105 vyčleněna pro zařízení administrativní části generálního ředitelství, tato síť je však určena pro bezdrátová připojení. K VLAN 297 se z velké části připojují pracovníci pomocí mobilních telefonů. K síti je možné se připojit pouze pomocí mobilního telefonu, který je definován ve firemním katalogu povolených zařízení (Apple IPhone SE, Samsung Galaxy A32) a má nainstalovaný software předepsaný společností.

Výrobní síť

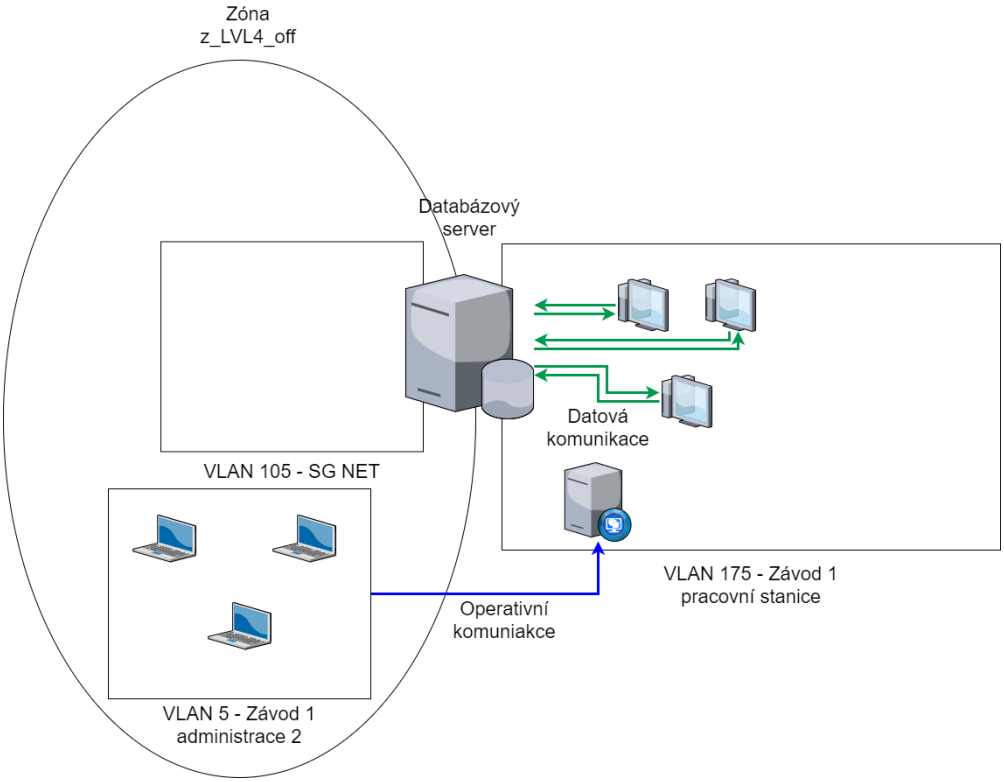
Výrobní síť je pomocí virtuálních sítí rozdělena do různých segmentů podle svého primárního určení. Výpis těch nejdůležitějších segmentů je následující:

VLAN 175 – Původní pracovní stanice

Do této sítě patří počítače umístěné po celé výrobní části závodu, které už svojí bezpečností neodpovídají dnešním standardům. Počítače disponují operačním systémem Windows XP Professional Embedded. Rychlá výměna za zařízení podporující dnešní standardy není možná, protože na počítačích běží mnohdy kritické programy pro výrobní procesy naprogramované v programovacím jazyce Delphi. Proto je nutné nejdříve všechny aplikace přeprogramovat pomocí modernějších jazyků, bohužel tato migrace ještě nějaký čas potrvá. Z důvodu zajištění bezpečnostních principů není z celé této sítě přístup do internetu.

Komunikace počítačů uvnitř této sítě s ostatními systémy probíhá skrze databázový server sloužící jako mezivrstva, ze které jsou data dále distribuována do systému SAP, kde jsou dále zpracovávána. Databázový server má v tuto chvíli dvě síťové karty, jednu pro komunikaci s počítači ve VLAN 175 a druhou, která se nachází v doménové VLAN 105 pro standardní operace procházející skrze firewall Palo Alto PA 3220.

Pro vzdálené servisní připojení do počítačů je vyhrazený jump server, do kterého se pracovník IT odpovědný za výrobní sektor připojí pomocí Remote Desktop Services (RDP), odtud se se již pomocí specializovaného softwaru na vzdálené připojení UVNC připojuje do jednotlivých výrobních počítačů. *(viz obrázek č.32)*

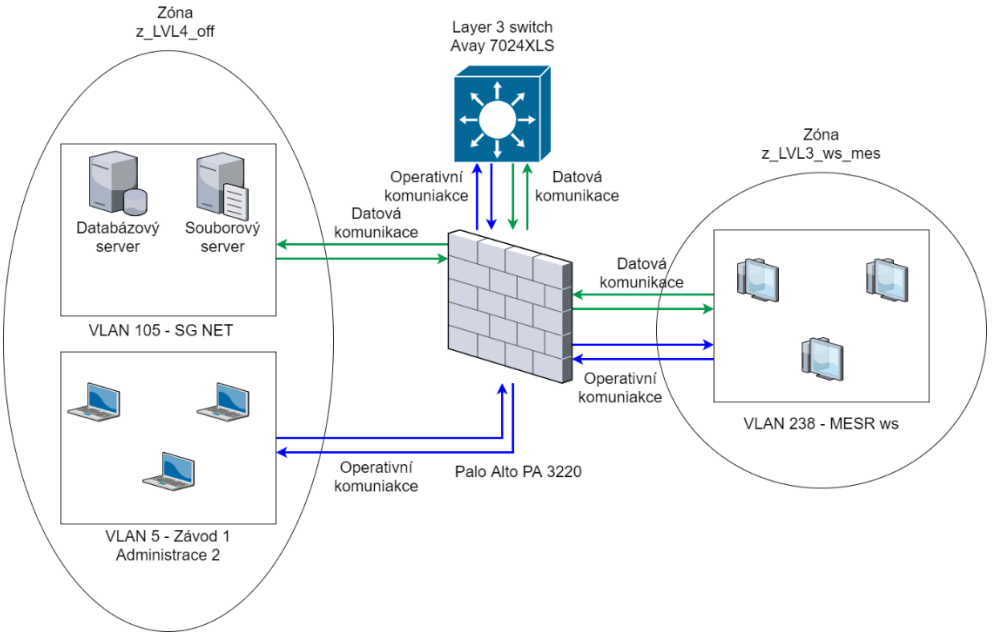


obrázek č. 32 – komunikace původních prac. stanic s okolím, zdroj: vlastní zpracování

VLAN 238 – Nastupující pracovní stanice

Do virtuální sítě VLAN 238 spadají zařízení postupně nahrazující původní počítače z VLAN 5. Tyto počítače již disponují operačním systémem Windows 10 IoT Enterprise. Komunikace počítačů s vnějšími ERP systémy probíhá stejně jako u předchozí virtuální sítě skrze databázový server, ze kterého jsou data dále interpretována. Pracovní stanice ve VLAN 238 komunikují také se souborovým serverem, kvůli případným aktualizacím výrobních programů a jiného softwaru.

Vzdálené servisní připojení k těmto počítačům probíhá přes speciálně vyhrazené pracovní počítače IT administrátorů (3 zařízení), která musejí být připojená ve VLAN 105. *(viz obrázek č. 33)*



obrázek č. 33 – Komunikace nových prac. Zařízení s okolím, zdroj: vlastní zpracování

VLAN 180 – Kamery

Virtuální síť spadající pod výrobní část podniku. V této síti jsou umístěny všechny kamery. Záznamy z kamer jsou ukládány a dále zpracovávány na specializovaném serveru pomocí softwaru Milestone XProtect. Pokud má mít uživatel přístup ke kamerovým záznamům, musí být splněny tyto podmínky:

- Uživatel musí mít na počítači naistalovaný specializovaný software XProtect Smart client.
- Počítač musí být připojený ve VLAN 105 (běžní uživatelé) nebo VLAN 5 (IT administrátoři)
- Uživatel musí mít na serverové části programu vydefinované uživatelské jméno a heslo.

Záznamy z kamerových systémů jsou využívány i specializovanými programy pro vykazování zabalených výrobků. Tyto programy přistupují ke kamerovým záznamům přímo přes webové rozhraní jednotlivých kamer. Podmínkou však je, aby se počítač využívající záznam z kamery nacházel v zóně definované jako z_LVL3_ws_MESR (VLAN 238), potom je požadavek na komunikaci, procházející přes firewall Palo Alto PA 3220 povolen, protože odpovídá pravidlu definovanému jako MESR_kamery. *(viz obrázek č. 34)*

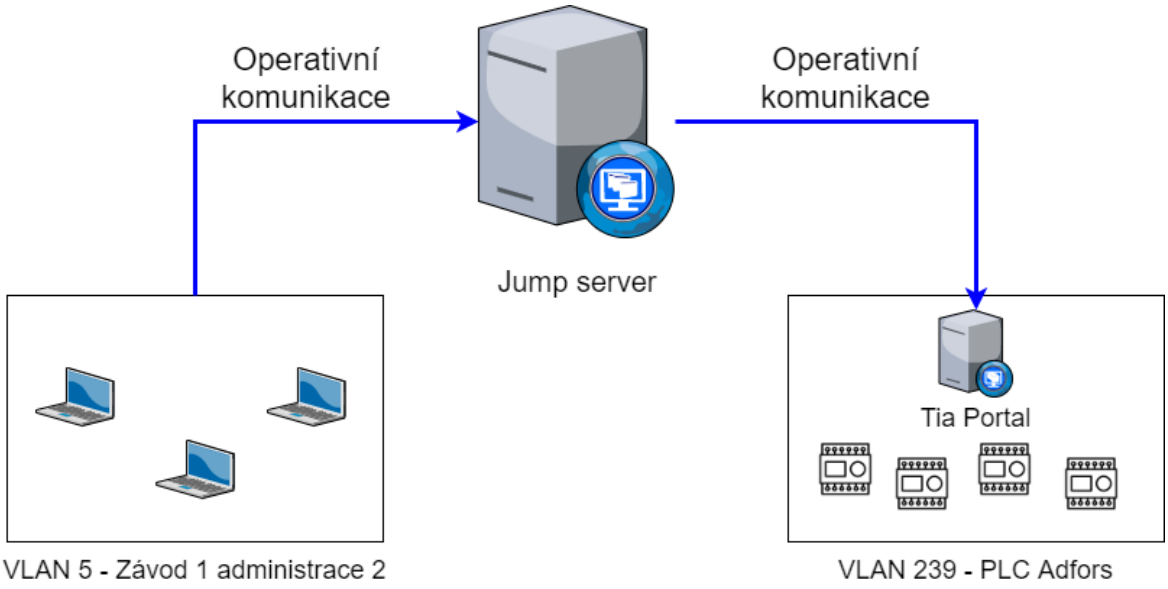
From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
z_LVL3_ws_MESR	z_LVL4_bms	10.220.238.148	172.16.105.147	80	web-browsing	allow	MESR_kamery

obrázek č. 34 – Povolení požadavku komunikace firewallem, zdroj: vlastní zpracování

VLAN 239 – PLC Adfors

Síť obsahující všechna PLC zařízení firem dodávajících do Saint-Gobain Adfors výrobní technologie. PLC jednotky se mohou lišit podle dodavatelské firmy, v největším zastoupení ve firmě je ovšem PLC SIMATIC S7-300 od firmy Siemens. Komunikace mezi PLC prvky a zbytkem výrobní sítě (především aplikace obsluhující tisky etiket a zobrazovací aplikace) probíhá cestou, že PLC zařízení ukládá své údaje do textových souborů na souborovém serveru a odtud jsou službami, naprogramovanými lokálním programovacím týmem, kontrolovány a odesílány do výrobního databázového serveru, kde jsou dále zpracovávány.

Práce a připojení k PLC zařízením, z důvodu programování logických operací, probíhá skrze jump server. Odpovědní a zaškolení pracovníci se mohou připojit k jump serveru pouze, pokud jsou připojeni do závodní administrátorské VLAN sítě (VLAN 5) z jiných virtuálních sítí se není možné připojit z důvodu bezpečnosti zařízení. Přístup k VLAN 5 má pouze úzce definovaný okruh pracovníků. Po připojení do jump serveru se může pracovník pomocí RDP připojit na server obsluhující PLC zařízení. *(viz obrázek č. 35)*



obrázek č. 35 – Komunikace s PLC přes jump server, zdroj: vlastní zpracování

Někdy je nutné, aby se k OT zařízením připojovali i externí pracovníci (vývoj nových výrobních linek, externí technologie), proto byla pro práci a připojení na PLC zařízení definována tato pravidla:

- Je zakázáno připojovat OT zařízení (zařízení, které monitoruje nebo řídí stroje) na lokální internet nebo 4G modem.

- Vzdálené připojení je možné pouze přes skupinovou VPN (MobilePASS token + Cisco AnyConnect client).
- Připojování k OT technologii je možné pouze z tzv. jump serveru.
- Pokud je třeba se připojovat k PLC musí být součástí dodávky i tzv. inženýrská stanice instalovaná s technologií, na kterou se dodavatel připojí z jump serveru.
- Pracovní stanice nesmí běžet pod administrátorským účtem.
- Na pracovních stanicích musí být zakázané nepoužívané USB porty v BIOSu.
- Na pracovních stanicích musí být zaslepené nepoužívané USB porty (Lindy Lock USB Port Blocker).
- Na pracovních stanicích musí být zakázané USB disky.
- Všechna výchozí hesla musí být změněna na vlastní.
- Nepoužívané aplikace jako jsou hry apod., musí být odinstalované.
- Nepoužívané služby musí být zakázané.

VLAN 204 – Síť zařízení PBX (IP telefony)

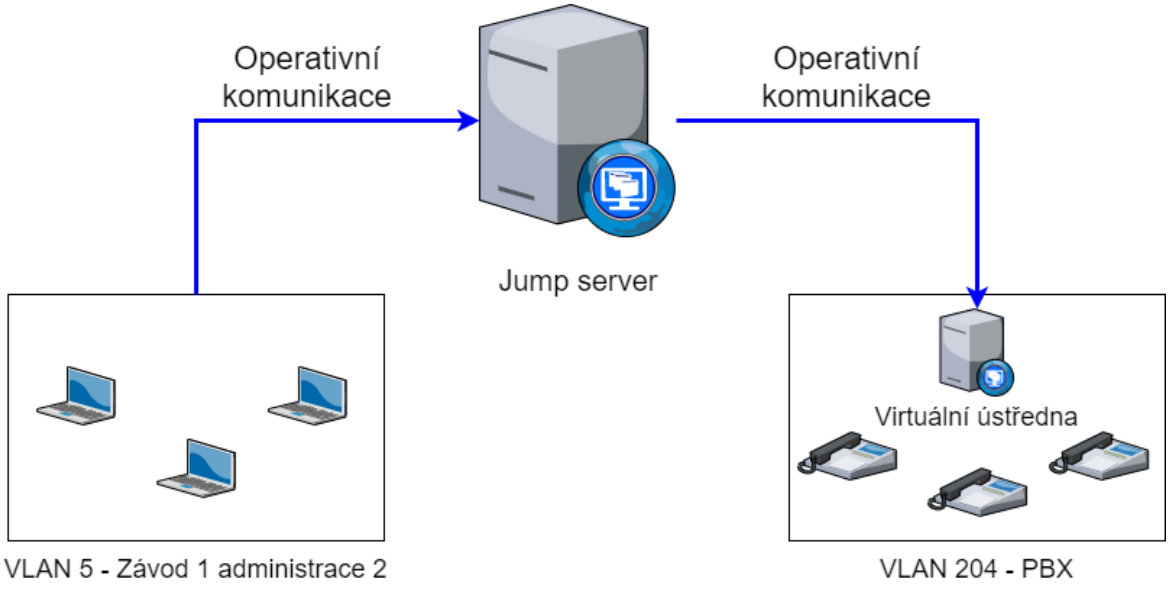
Úplně nejdříve měly telefony ve firmě Saint-Gobain Adfors vlastní síť a fyzickou telefonní ústřednu. Již před zavedením firewallu Palo Alto PA 3220 byly telefony převedeny do konvergované sítě, byly však virtuálně umístěny do sítě VLAN 105 – SG Net s rozsahy IP adres znázorněnými v *tabulce č. 2*.

10.220.131.0/24
10.220.132.0/22
10.220.137.0/24
10.220.139.0/24
10.220.158.0/24
10.220.166.0/24
10.220.234.0/24

tabulka č. 2 – Rozsahy IP adres IP telefonů, zdroj: vlastní zpracování

Umístění do sítě VLAN 105 však není vhodné, jak z pohledu výkonu sítě, tak ani z pohledu bezpečnosti, protože virtuální ústředna, pomocí které se telefonům přiřazují klapky, byla také umístěna v síti VLAN 105 a přistupovat k ní mohl kdokoli, kdo se v síti VLAN 105 nacházel (celé administrativní oddělení).

Nyní byly IP telefony a virtuální ústředna přesunuty do sítě VLAN 204 a zóny firewallu z_LVL4_pbx. K ústředně se nyní připojuje přes jump server obdobným způsobem, jakým se připojují IT pracovníci k PLC zařízením. *(viz obrázek č. 36)*



obrázek č. 36 – Komunikace s vir. ústřednou přes jump server, zdroj: vlastní zpracování

Komunikace mezi telefony a virtuální ústřednou probíhá pomocí protokolů Real-time Transfer Protocol (RTP) a Real-time Transfer Control Protocol (RTCP). RTP slouží pro přenos hlasu a RTCP slouží pro monitoring statistiky přenosu a QoS. Přenos probíhá přes nepřiřazené porty přidělené podle IP adresy zařízení (např. 16463, 16465, 49200, 49385). *(viz obrázek č. 37)*

Source	Destination	To Port	Application
10.220.204.9	10.220.234.104	49200	rtp-base
10.220.234.104	10.220.204.9	16465	rtcp

obrázek č. 37 – Porty a protokoly používající zařízení PBX, zdroj: vlastní zpracování

VLAN 100 - Management switchů

V prostředí, jako je výrobní část firmy Saint-Gobain Adfors, je nutností mít všechny switche plně pod správou. Z lokálního IT byli vydefinováni 3 pracovníci pro management switchů. Pro samotnou správu je nutné mít zařízení připojené do sítě VLAN 100 a mít definovaný účet na RADIUS server, který provádí autentifikaci, autorizaci a logování činností při připojení na firemní switche.

3.3.2 Nastavení Port Security (Cisco, Aruba)

Na úrovni Access Level síťové hierarchie je potřeba provést nastavení, v nichž bude zabezpečen přístup do sítě, pokud možno jen oprávněným zařízením a uživatelům. Jedna z velmi jednoduchých metod používaná síťovými administrátory, jak zabezpečit síť proti neoprávněnému přístupu, je zakázání všech nepoužívaných portů na switchi. Pokud má například switch 24 Fast Ethernet portů a z toho 2 porty jsou používané, je velmi vhodné zbylých 22 portů nezapojovat a pokud to není možné, pak je aspoň softwarově deaktivovat.

Konfigurace Cisco switch

Pro přehled všech dostupných portů switche se použije příkaz „show interface status“. Z celkových 10 zapojených portů je 8 fast ethernet portů zapojeno do koncových zařízení a 2 gigabit ethernet porty jsou připojené k dalším switchům. (*viz obrázek č. 38*)

```
Cisco2960_ROZ_BUD_B#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    105        auto    auto  10/100BaseTX
Fa0/2                        connected    105        auto    auto  10/100BaseTX
Fa0/3                        notconnect   1          auto    auto  10/100BaseTX
Fa0/4                        notconnect   1          auto    auto  10/100BaseTX
Fa0/5                        notconnect   1          auto    auto  10/100BaseTX
Fa0/6                        connected    105        auto    auto  10/100BaseTX
Fa0/7                        connected    105        auto    auto  10/100BaseTX
Fa0/8                        notconnect   1          auto    auto  10/100BaseTX
Fa0/9                        connected    105        auto    auto  10/100BaseTX
Fa0/10                       connected    105        auto    auto  10/100BaseTX
Fa0/11                       connected    105        auto    auto  10/100BaseTX
Fa0/12                       connected    105        auto    auto  10/100BaseTX
Fa0/13                       notconnect   1          auto    auto  10/100BaseTX
Fa0/14                       notconnect   1          auto    auto  10/100BaseTX
Fa0/15                       notconnect   1          auto    auto  10/100BaseTX
Fa0/16                       notconnect   1          auto    auto  10/100BaseTX
Fa0/17                       notconnect   1          auto    auto  10/100BaseTX
Fa0/18                       notconnect   1          auto    auto  10/100BaseTX
Fa0/19                       notconnect   1          auto    auto  10/100BaseTX
Fa0/20                       notconnect   1          auto    auto  10/100BaseTX
Fa0/21                       notconnect   1          auto    auto  10/100BaseTX
Fa0/22                       notconnect   1          auto    auto  10/100BaseTX
Fa0/23                       notconnect   1          auto    auto  10/100BaseTX
Fa0/24                       notconnect   1          auto    auto  10/100BaseTX
Gig0/1                       connected    1          auto    auto  10/100BaseTX
Gig0/2                       connected    1          auto    auto  10/100BaseTX
```

obrázek č. 38 – Aktivní a neaktivní porty (Cisco), zdroj: vlastní zpracování

Po kontrole, které porty jsou aktivní a které neaktivní, se příkazem „interface range fa0/3-5, fa0/8, fa0/13-24“ vybere daný rozsah fast ethernet portů a ty se poté příkazem „shutdown“ administrativně vypnou. (*viz obrázek č. 39*)

```
Cisco2960_ROZ_BUD_B(config)#interface range fa0/3-5, fa0/8, fa0/13-24
Cisco2960_ROZ_BUD_B(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
```

obrázek č. 39 – Vypnutí neaktivních portů (Cisco), zdroj: vlastní zpracování

Konfigurace Aruba switch

Jelikož jsou switche od firmy Aruba odlišné od switchů Cisco. Pro přehled dostupných portů a jejich aktivity se používá příkaz „show interface brief“. (*viz obrázek č. 40*)

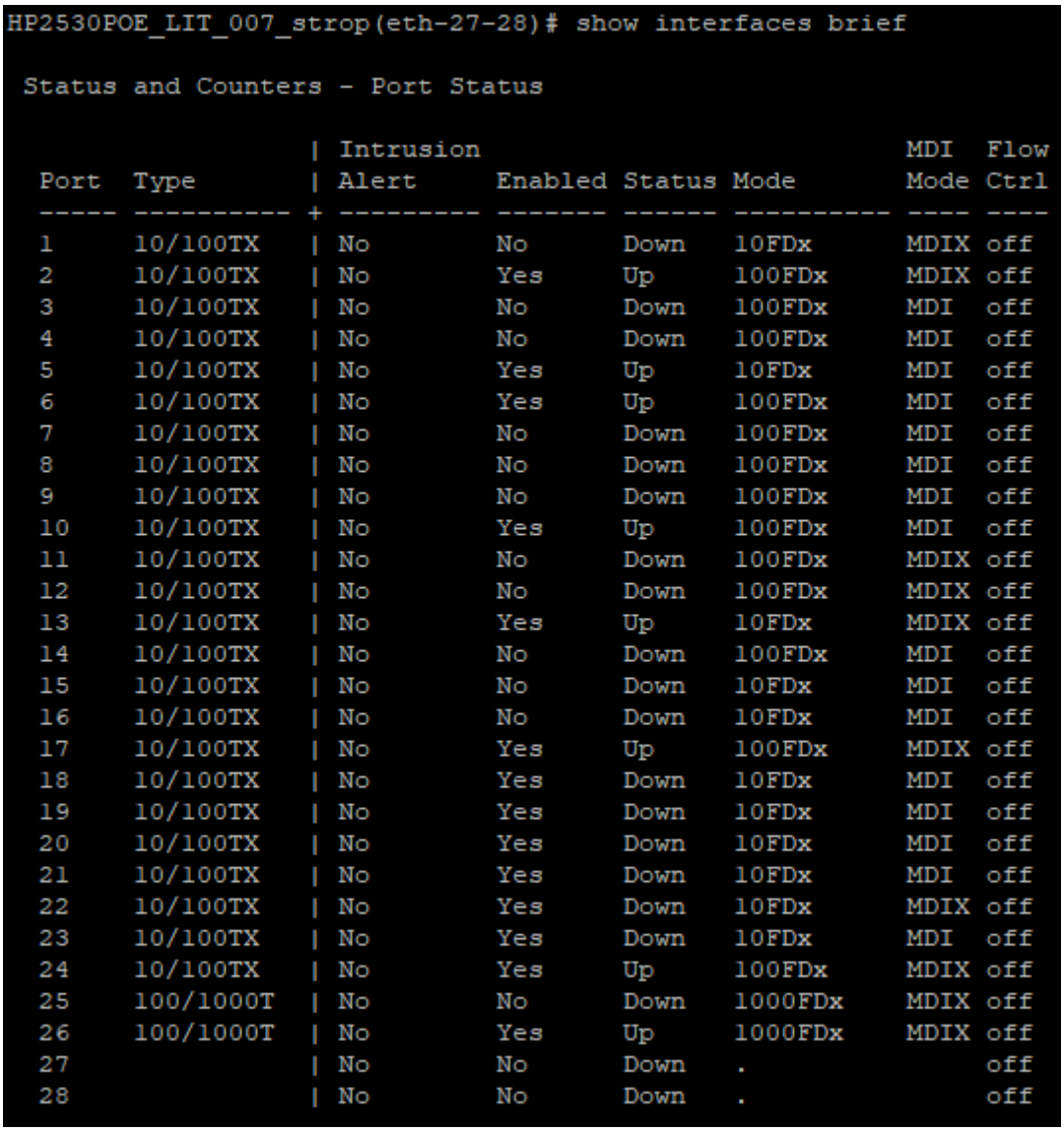
```
HP2530POE_LIT_007_strop# show interfaces brief

 Status and Counters - Port Status

                  | Intrusion                              MDI  Flow
 Port  Type       | Alert     Enabled Status Mode          Mode Ctrl
 ----- ---------- + --------- ------- ------ ---------- ---- ----
 1     10/100TX   | No        Yes     Down   10FDx       MDIX off
 2     10/100TX   | No        Yes     Up     100FDx      MDIX off
 3     10/100TX   | No        Yes     Down   100FDx      MDI  off
 4     10/100TX   | No        Yes     Down   100FDx      MDIX off
 5     10/100TX   | No        Yes     Up     10FDx       MDI  off
 6     10/100TX   | No        Yes     Up     100FDx      MDI  off
 7     10/100TX   | No        Yes     Down   100FDx      MDIX off
 8     10/100TX   | No        Yes     Down   100FDx      MDI  off
 9     10/100TX   | No        Yes     Down   100FDx      MDIX off
 10    10/100TX   | No        Yes     Up     100FDx      MDI  off
 11    10/100TX   | No        Yes     Down   100FDx      MDI  off
 12    10/100TX   | No        Yes     Down   100FDx      MDIX off
 13    10/100TX   | No        Yes     Up     10FDx       MDIX off
 14    10/100TX   | No        Yes     Down   100FDx      MDIX off
 15    10/100TX   | No        Yes     Down   10FDx       MDIX off
 16    10/100TX   | No        Yes     Down   10FDx       MDI  off
 17    10/100TX   | No        Yes     Up     100FDx      MDIX off
 18    10/100TX   | No        Yes     Down   10FDx       MDI  off
 19    10/100TX   | No        Yes     Down   10FDx       MDI  off
 20    10/100TX   | No        Yes     Down   10FDx       MDI  off
 21    10/100TX   | No        Yes     Down   10FDx       MDI  off
 22    10/100TX   | No        Yes     Down   10FDx       MDIX off
 23    10/100TX   | No        Yes     Down   10FDx       MDI  off
 24    10/100TX   | No        Yes     Up     100FDx      MDIX off
 25    100/1000T  | No        Yes     Down   1000FDx     MDIX off
 26    100/1000T  | No        Yes     Up     1000FDx     MDIX off
 27               | No        Yes     Down   .                off
 28               | No        Yes     Down   .                off
```

obrázek č. 40 – Aktivní a neaktivní porty (Aruba), zdroj: vlastní zpracování

Pro názornou ukázku, zde bude zakázán pouze první port switche (Port1). Port se vybírá příkazem *interface[ethernet]* a poté se příkazem *disable* učiní neaktivním (*viz obrázek č. 41*). Tento postup se zopakuje pro všechny porty, kde se status nachází ve stavu down. Zda jsou zmíněné porty neaktivní se opět zkontroluje příkazem „show interface brief“. (*viz obrázek č. 42*)

```
HP2530POE_LIT_007_strop(config)# interface 1
HP2530POE_LIT_007_strop(eth-1)# disable
```

obrázek č. 41 – Vypnutí neaktivních portů (Aruba), zdroj: vlastní zpracování



```
HP2530POE_LIT_007_strop(eth-27-28)# show interfaces brief

 Status and Counters - Port Status

                   | Intrusion                                  MDI   Flow
 Port  Type        | Alert     Enabled Status Mode       Mode  Ctrl
 ----- ----------- + --------- ------- ------ ---------- ----- ----
 1     10/100TX    | No        No      Down   10FDx      MDIX  off
 2     10/100TX    | No        Yes     Up     100FDx     MDIX  off
 3     10/100TX    | No        No      Down   100FDx     MDI   off
 4     10/100TX    | No        No      Down   100FDx     MDI   off
 5     10/100TX    | No        Yes     Up     10FDx      MDI   off
 6     10/100TX    | No        Yes     Up     100FDx     MDI   off
 7     10/100TX    | No        No      Down   100FDx     MDI   off
 8     10/100TX    | No        No      Down   100FDx     MDI   off
 9     10/100TX    | No        No      Down   100FDx     MDI   off
 10    10/100TX    | No        Yes     Up     100FDx     MDI   off
 11    10/100TX    | No        No      Down   100FDx     MDIX  off
 12    10/100TX    | No        No      Down   100FDx     MDIX  off
 13    10/100TX    | No        Yes     Up     10FDx      MDIX  off
 14    10/100TX    | No        No      Down   100FDx     MDI   off
 15    10/100TX    | No        No      Down   10FDx      MDI   off
 16    10/100TX    | No        No      Down   10FDx      MDI   off
 17    10/100TX    | No        Yes     Up     100FDx     MDIX  off
 18    10/100TX    | No        Yes     Down   10FDx      MDI   off
 19    10/100TX    | No        Yes     Down   10FDx      MDI   off
 20    10/100TX    | No        Yes     Down   10FDx      MDI   off
 21    10/100TX    | No        Yes     Down   10FDx      MDI   off
 22    10/100TX    | No        Yes     Down   10FDx      MDIX  off
 23    10/100TX    | No        Yes     Down   10FDx      MDI   off
 24    10/100TX    | No        Yes     Up     100FDx     MDIX  off
 25    100/1000T   | No        No      Down   1000FDx    MDIX  off
 26    100/1000T   | No        Yes     Up     1000FDx    MDIX  off
 27                | No        No      Down   .                off
 28                | No        No      Down   .                off
```

obrázek č. 42 – Aktivní a neaktivní porty (Aruba), zdroj: vlastní zpracování

3.3.3 Switch: Nastavení obrany proti VLAN hopping

Pro obranu proti VLAN hopping se používají tyto metody zabezpečení switche:

- Zakázání DTP (auto trunking) na ne-trunkových portech.
- Zakázání nepoužívaných portů a jejich přiřazení do nepoužívané VLAN sítě.
- Manuální spuštění trunkové linky na trunkovém portu.
- Zakázání DTP na trunkových portech.
- Nastavení jiné VLAN sítě nežli VLAN 1, jako nativní síť.

Konfigurace Cisco switch

Switch je propojen s dvěma dalšími switchi porty Gig0/1 a Gig0/2, poté jsou k němu připojeny koncová zařízení na portech Fa0/3-5, Fa0/8, Fa0/13-24. Zbylé porty jsou nepoužívané (*viz obrázek č. 43*).

```
Cisco2960_ROZ_BUD_B#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    105        auto    auto  10/100BaseTX
Fa0/2                        connected    105        auto    auto  10/100BaseTX
Fa0/3                        notconnect   1          auto    auto  10/100BaseTX
Fa0/4                        notconnect   1          auto    auto  10/100BaseTX
Fa0/5                        notconnect   1          auto    auto  10/100BaseTX
Fa0/6                        connected    105        auto    auto  10/100BaseTX
Fa0/7                        connected    105        auto    auto  10/100BaseTX
Fa0/8                        notconnect   1          auto    auto  10/100BaseTX
Fa0/9                        connected    105        auto    auto  10/100BaseTX
Fa0/10                       connected    105        auto    auto  10/100BaseTX
Fa0/11                       connected    105        auto    auto  10/100BaseTX
Fa0/12                       connected    105        auto    auto  10/100BaseTX
Fa0/13                       notconnect   1          auto    auto  10/100BaseTX
Fa0/14                       notconnect   1          auto    auto  10/100BaseTX
Fa0/15                       notconnect   1          auto    auto  10/100BaseTX
Fa0/16                       notconnect   1          auto    auto  10/100BaseTX
Fa0/17                       notconnect   1          auto    auto  10/100BaseTX
Fa0/18                       notconnect   1          auto    auto  10/100BaseTX
Fa0/19                       notconnect   1          auto    auto  10/100BaseTX
Fa0/20                       notconnect   1          auto    auto  10/100BaseTX
Fa0/21                       notconnect   1          auto    auto  10/100BaseTX
Fa0/22                       notconnect   1          auto    auto  10/100BaseTX
Fa0/23                       notconnect   1          auto    auto  10/100BaseTX
Fa0/24                       notconnect   1          auto    auto  10/100BaseTX
Gig0/1                       connected    1          auto    auto  10/100BaseTX
Gig0/2                       connected    1          auto    auto  10/100BaseTX
```

obrázek č. 43 – Aktivní a neaktivní porty (Cisco), zdroj: vlastní zpracování

Na portech, které jsou připojeny ke koncovým zařízením, se deaktivuje trunking přímým nastavením access modu (*viz obrázek č. 44*).

```
Cisco2960_ROZ_BUD_B(config)#interface range fa0/1-2, fa0/6-7, fa0/9-12
Cisco2960_ROZ_BUD_B(config-if-range)#switchport mode access
```

obrázek č. 44 – Nastavení access portů (Cisco), zdroj: vlastní zpracování

Porty, které se momentálně nepoužívají, se z důvodu bezpečnosti deaktivují přiřazením do nepoužívané VLAN sítě (*viz obrázek č. 45*).

```
Cisco2960_ROZ_BUD_B(config)#interface range f0/3-5, f0/8, f0/13-24
Cisco2960_ROZ_BUD_B(config-if-range)#switchport mode access
Cisco2960_ROZ_BUD_B(config-if-range)#switchport access vlan 999
Cisco2960_ROZ_BUD_B(config-if-range)#shutdown
```

obrázek č. 45 – Nastavení neaktivních portů (Cisco), zdroj: vlastní zpracování

Porty gig0/1 až gig0/2 propojují konfigurovaný switch s dalšími switchi ve výrobě, proto je na nich manuálně povolený trunking. Je také důležité změnit výchozí VLAN síť z VLAN (která bývá nastavena od výrobce) na VLAN 999. Na rozhraních jsou také povoleny VLAN sítě 100 a 105, které jsou potřebné i pro připojené switche. (*viz obrázek č. 46*).

```
Cisco2960_ROZ_BUD_B(config)#interface range gig0/1-2
Cisco2960_ROZ_BUD_B(config-if-range)#switchport mode trunk
Cisco2960_ROZ_BUD_B(config-if-range)#switchport nonegotiate
Cisco2960_ROZ_BUD_B(config-if-range)#switchport trunk native vlan 999
Cisco2960_ROZ_BUD_B(config-if-range)#switchport trunk allowed vlan 100,105
```

obrázek č. 46 – Nastavení trunkových portů (Cisco), zdroj: vlastní zpracování

Konfigurace Aruba switch

Switche značky Aruba, které se postupně ve firmě stávají standardem, mají narozdíl od Cisco switchů zvolen jiný přístup k nastavování přenosu VLAN sítí na různé porty. V Aruba switchích se porty nastavují k VLAN sítím, a pomocí klíčových slov tagged a untagged se určuje druh síťového provozu.

U vybraného Aruba switche je situace složitější, protože se zde nachází větší síťový provoz. První budou přiřazeny porty k VLAN sítím, které nemusí dále přenášet síťový provoz (*viz tabulka č. 3*).

Virtuální síť	Untagged port
Vlan 5	2, 3, 5, 6, 15–23
Vlan 7	24
Vlan 105	9
Vlan 132	23
Vlan 200	11, 14
Vlan 207	8
Vlan 238	4, 7
Vlan 239	10, 13

tabulka č. 3 – Přiřazení untagged portů k VLAN sítím, zdroj: vlastní zpracování

Přiřazení se provádí příkazem *vlan<1-4094> untagged [Port-Number] (viz obrázek č. 47).* Toto nastavení se provedlo pro všechny vypsané porty *v tabulce č. 3*.

```
HP2530POE_LIT_007_strop(config)# vlan 5 untagged 3
```

obrázek č. 47 – Nastavení untagged portů (Aruba), zdroj: vlastní zpracování

Nepoužívané porty je vhodné dát do nepoužívané VLAN sítě *(viz obrázek č. 48)*, jedná se o porty 1, 3, 4, 7-9, 11, 12, 14–16, 18–23, 25, 27, 28.

```
HP2530POE_LIT_007_strop(config)# vlan 999 untagged 1
```

obrázek č. 48 – Nastavení neaktivních portů (Aruba), zdroj: vlastní zpracování

Port 24 propojuje switch s wifi AP, proto je nutné ho nastavit jako tagged port do VLAN 297, což je virtuální síť WIFI SG net. *(viz obrázek č. 49)*

```
HP2530POE_LIT_007_strop(config)# vlan 297 tagged 24
```

obrázek č. 49 – Nastavení tagged portu (Aruba), zdroj: vlastní zpracování

3.3.4 Switch: Nastavení obrany DHCP

Účinným nástrojem, jak zabránit DHCP spoofing je nastavení funkce port Security. Nicméně útočné nástroje jako Gobbler mohou být nakonfigurovány, aby využívaly MAC adresu aktuálně využívaného rozhraní jako zdrojovou ethernetovou adresu, ale v datové části DHCP zadají jinou ethernetovou adresu. Je tedy potřeba implementovat i další řešení, aby se případným útokům předcházelo co nejefektivněji.

K zefektivnění obrany switche budou použity tyto kroky:

- Povolení DHCP snooping.
- Na důvěryhodných portech použití příkazu ip dhcp snooping trust.
- Omezení počtu zpráv DHCP discovery, které mohou být přijímány na nedůvěryhodných portech.
- Povolení DHCP snooping podle VLAN sítí nebo rozsahu VLAN sítí použitím příkazu ip dhcp snooping vlan.

Konfigurace Cisco switch

Na firemním Cisco switchi se nejprve nastaví DHCP snooping v global configuration módu. Rozhraní vedoucí k dalším switchům (gig0/1, gig0/2) jsou nastaveny jako důvěryhodné. Rozhraní vedoucí ke koncovým zařízením (fa0/1 – fa0/24) jsou ve výchozím stavu nastaveny jako nedůvěryhodné a limit rychlosti je u nich nastavený na 6 paketů za sekundu. DHCP snooping je poté povolen na VLAN sítích 105 a 297. *(viz obrázek č. 50)*

```
Cisco2960_ROZ_BUD_B(config)#interface range gig0/1-2
Cisco2960_ROZ_BUD_B(config-if-range)#ip dhcp snooping
Cisco2960_ROZ_BUD_B(config)#interface range gig0/1-2
Cisco2960_ROZ_BUD_B(config-if-range)#ip dhcp snooping trust
Cisco2960_ROZ_BUD_B(config-if-range)#exit
Cisco2960_ROZ_BUD_B(config)#interface range fa0/1-24
Cisco2960_ROZ_BUD_B(config-if-range)#ip dhcp snooping limit rate 6
Cisco2960_ROZ_BUD_B(config-if-range)#exit
Cisco2960_ROZ_BUD_B(config)#ip dhcp snooping vlan 105,297
Cisco2960_ROZ_BUD_B(config)#end
```

obrázek č. 50 – DHCP snooping (Cisco), zdroj: vlastní zpracování

Konfigurace Aruba switch

U Aruba switche se také nejprve nastaví dhcp-snooping v global configuration módu. Poté se na portu 23 (port vedoucí k dalšímu switchi) nastaví důvěryhodný přístup. U dalších portů, počínaje portem 1, se nastaví limit 6 paketů za sekundu. Nakonec se povolí dhcp-snooping na VLAN síti 105. *(viz obrázek č. 51)*

```
HP2530POE_LIT_007_strop(config)# dhcp-snooping
HP2530POE_LIT_007_strop(config)# dhcp-snooping trust 24
HP2530POE_LIT_007_strop(config)# interface 1
HP2530POE_LIT_007_strop(eth-1)# dhcp-snooping max-bindings 6
HP2530POE_LIT_007_strop(eth-1)# exit
HP2530POE_LIT_007_strop(config)# dhcp-snooping vlan 105
```

obrázek č. 51 – DHCP snooping (Aruba), zdroj: vlastní zpracování

3.3.5 Nastavení obrany proti ARP útokům

Pro prevenci ARP spoofing a z toho vyplývajícího ARP poisoning, musí být na switchi pravidla kontroly předávání pouze validních ARP dotazů a odpovědí.

K tomu pomáhá funkce ARP inspection (DAI), která vyžaduje předchozí nastavení DHCP snooping a pomáhá předcházet ARP útokům tím, že:

- Nepředává poškozené nebo neplatné požadavky ARP jiným portům ve stejné VLAN síti.
- Zachytává všechny ARP požadavky a odpovědi na nedůvěryhodných portech.
- Ověřuje všechny zachycené pakety, jestli mají platné IP-to-MAC spojení.
- Maže a loguje požadavky ARP pocházející z neplatných zdrojů.
- Deaktivuje rozhraní, jestliže je překročen počet DAI paketů ARP.

Pro zavedení DAI je tedy nutné na switchi provést tyto kroky:

- Globálně povolit DHCP snooping.
- Povolit DHCP snooping na vybraných VLAN sítích.

- Povolit DAI na vybraných VLAN sítích.
- Nakonfigurovat důvěryhodné rozhraní pro DHCP snooping a ARP inspection.

Konfigurace Cisco switch

Je opět velmi doporučeno nakonfigurovat, všechny přístupové porty switche jako nedůvěryhodné a všechny porty propojené s jinými switchi jako důvěryhodné.

Z předchozí kapitoly je již DHCP snooping povolený, pokud by nebyl, musel by se povolit, jelikož DAI vyžaduje tabulku vazeb DHCP snooping. Dále se povolí ARP inspection na VLAN síti 105. Porty gig0/1, gig0/2 jsou propojeny s dalšími síťovými zařízeními, a proto se nastaví jako důvěryhodné pro ARP inspection. *(viz obrázek č. 52)*

```
Cisco2960_ROZ_BUD_B(config)#ip arp inspection vlan 105
Cisco2960_ROZ_BUD_B(config)#interface range gig0/1-2
Cisco2960_ROZ_BUD_B(config-if-range)#ip arp inspection trust
```

obrázek č. 52 – ARP inspection (Cisco), zdroj: vlastní zpracování

Konfigurace Aruba switch

Na Aruba switchi se příkazem *arp-protect* aktivuje funkce arp protect na VLAN síti 132. Port 24, který je propojený s AP se nastaví jako důvěryhodný. *(viz obrázek č. 53)*

```
HP2530POE_LIT_007_strop(config)# arp-protect vlan 105
HP2530POE_LIT_007_strop(config)# interface 24
HP2530POE_LIT_007_strop(eth-24)# arp trust
```

obrázek č. 53 – ARP protect (Aruba), zdroj: vlastní zpracování

3.3.6 Nastavení obrany proti STP útokům

PortFast obchází odposlouchávání STP a stavy učení pro minimalizaci potřebného času, po který musí přístupový port čekat na STP. Avšak jestliže je PortFast nastaven na portu propojující další switch, je zde velké riziko zacyklení STP.

PortFast může být povolen na jednotlivých rozhraních použitím příkazu spanning-tree portfast v konfiguraci rozhraní. Alternativně může být PortFast nakonfigurován globálně příkazem spanning-tree portfast default v globálním módu switche.

I přesto, že je PortFast nastavený, rozhraní bude stále odposlouchávat BPDU. Pokud jsou BPDU neočekávané, mohou být náhodné nebo také součástí neoprávněných pokusů o přidání cizího switche do sítě.

Jestliže jsou na portech, kde je povolen BPDU Guard, přijaty nějaké BPDU rámce, port spadne do stavu chybového deaktivování. To znamená, že pro další provoz musí být

manuálně opětovně povolen nebo automaticky oživen příkazem **errdisable recovery cause bpduguard** v globálním konfiguračním módu.

BPDU Guard může být povolen na portu použitím příkazu **spanning-tree bpduguard enable** v konfiguračním módu rozhraní nebo může být povolen na všech portech, kde je povolený PortFast, příkazem **spanning-tree portfast bpduguard default** v globálním konfiguračním módu.

Konfigurace Cisco switch

U firemního Cisco switche jsou připojená koncová zařízení na porty Fa0/1-2, Fa0/6-7, Fa0/9-12 spanning-tree portfast se tedy nastaví speciálně pro ně. *(viz obrázek č. 54)*

```
Cisco2960_ROZ_BUD_B(config)#interface range fa0/1-2, fa0/6-7, fa0/9-12
Cisco2960_ROZ_BUD_B(config-if-range)#spanning-tree portfast
```

obrázek č. 54 – Spanning tree PortFast (Cisco), zdroj: vlastní zpracování

Pokud by se PortFast nastavil globálně, je z důvodu možného zacyklení lepší toto nastavení odebrat u portů směřujících k dalším switchům (gig0/1, gig0/2). *(viz obrázek č. 55)*

```
Cisco2960_ROZ_BUD_B(config)#spanning-tree portfast default
Cisco2960_ROZ_BUD_B(config)#interface range gig0/1-2
Cisco2960_ROZ_BUD_B(config-if-range)#no spanning-tree portfast
```

obrázek č. 55 – Spanning tree PortFast global (Cisco), zdroj: vlastní zpracování

U portů, které mají již povolený PortFast (Fa0/1-2, Fa0/6-7, Fa0/9-12), se nastaví BPDU Guard. *(viz obrázek č. 56)*

```
Cisco2960_ROZ_BUD_B(config)#interface range fa0/1-2, fa0/6-7, fa0/9-12
Cisco2960_ROZ_BUD_B(config-if-range)#spanning-tree bpduguard enable
Cisco2960_ROZ_BUD_B(config-if-range)#exit
```

obrázek č. 56 – Spanning tree BPDU Guard (Cisco), zdroj: vlastní zpracování

Je možné BPDU Guard nastavit globálně pro všechny porty, které mají již povolenou funkci PortFast. *(viz obrázek č. 57)*

```
Cisco2960_ROZ_BUD_B(config)#spanning-tree portfast bpduguard default
```

obrázek č. 57 – Spann. tree BPDU Guard glob. (Cisco), zdroj: vlastní zpracování

Konfigurace Aruba switch

U zařízení značky Aruba se STP PortFast nastavuje příkazem *spanning-tree[Port-Number] admin-edge-port. (viz obrázek č. 58)*

```
HP2530POE_LIT_007_strop(config)# spanning-tree 1 admin-edge-port
```

obrázek č. 58 – Spanning tree PortFast (Cisco), zdroj: vlastní zpracování

BPDU Guard se nastaví pomocí příkazu *spanning-tree[Port-Number] bpdu-protection. (viz obrázek č. 59)*

```
HP2530POE_LIT_007_strop(config)# spanning-tree 1 bpdu-protection
```

obrázek č. 59 – Spanning tree PortFast (Cisco), zdroj: vlastní zpracování

3.3.7 Nastavení SSH a RADIUS serveru

Na každém switchi se z důvodu bezpečnosti odebral přístup pomocí protokolu Telnet, který byl nahrazen přístupem přes SSH protokol. *(viz obrázek č. 60)*

```
aaa authentication ssh login radius local
```

obrázek č. 60 – Povolený SSH protokol, zdroj: vlastní zpracování

Pro vzdálený přístup ke switchům bylo na všech switchích odebráno lokální ověřování a nahradilo se autentifikaci pomocí RADIUS serveru. *(viz obrázek č. 61)*

```
radius-server host 10.220.135.226
```

obrázek č. 61 – Povolený RADIUS server (Cisco), zdroj: vlastní zpracování

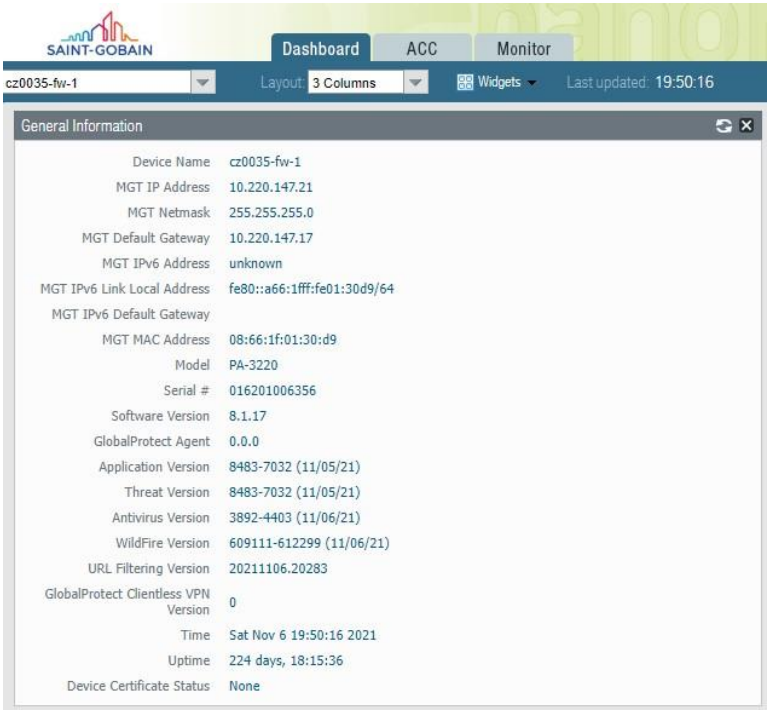
3.4 Zavedení Palo Alto PA 3220 – Next Generation firewall

Původně byl ve firemní síti nasazen firewall IPFire nainstalovaný na Linuxovém serveru, který chránil počítače a zařízení umístěna ve výrobní části firemní sítě. Tento Open Source Firewall je určen spíše pro malé podniky nebo kanceláře. Z tohoto důvodu byl nahrazený zařízením Palo Alto PA 3220 – Next Generation firewall.

Next Generation firewall slouží pro hloubkové inspekce paketů, tato inspekce přesahuje kontrolu a blokování portů nebo protokolů, kterou poskytují běžné firewally. Dále přidává inspekci na úrovni aplikací, kde kontroluje části kódu. Pro rozlišení bezpečných aplikací se dají používat whitelisty nebo ověřené podpisy k rozlišení bezpečných aplikací od těch potenciálně nebezpečných.

V síťovém prostředí je Firewall Palo Alto PA 3220 umístěn mezi všemi VLAN sítěmi (VLAN 105 – SG net, výrobní VLAN 238 atd.) a kontroluje všechen síťový provoz, který je veden mezi těmito sítěmi i provoz, který míří ven ze sítě.

Na úvodní stránce firewallu (*viz obrázek č. 62*) jsou informace jako například název zařízení, IP adresa, maska podsítě, výchozí brána, dále například číslo modelu nebo verze aplikace, antiviru a analytického prostředí WildFire. Dále jsou zde cesty, které vedou do umístění různých logovacích souborů, kde je možné si prohlédnout různé bezpečnostní události.



obrázek č. 62 – Palo Alto úvodní Dashboard, zdroj: vlastní zpracování

Palo Alto PA 3220 má mnoho monitorovacích funkcí a dokáže sledovat tok dat aplikací a také kolik síťových prostředků potřebují ke svému provozu. Aplikace zde mají různé kategorie (bussiness systems, general-internet, networking, media, apod…), které jsou zobrazeny podle množství zkontrolovaných bytů nebo jiných měřítek (sessions, threats, content, URLs, users). (*viz obrázek č. 63*)

Application	Risk	Bytes	Sessions	Threats	Content	URLs	Users
vmware	2	23.3G	15.6k	0	0	0	36
zscaler-private-access	1	6.4G	37.3k	427	0	0	379
web-browsing	4	5.6G	574.6k	2.1k	1.7k	0	510
ssl	4	5.3G	117.5k	730	0	0	798
youtube-base	4	3.2G	1.2k	0	0	0	28
mssql-db-unencrypted	2	2.8G	24.0k	0	0	0	94
ms-ds-smbv3	3	2.3G	6.4k	1.4k	3.4k	0	629
active-directory-base	2	1.5G	2.4k	0	0	0	511
ldap	2	658.2M	26.5k	156	0	0	589
oracle	2	338.5M	15	0	0	0	2
others	others	2.8G	566.5k	3.7k	1.0k	0	0

obrázek č. 63 – Palo Alto Application Usage, zdroj: vlastní zpracování

Dále PA zaznamenává aktivitu aplikací na portech, které nejsou standardně určené pro dané použití, například port SSL používá ve většině případů port 443, zatímco v konkrétním případě (naprogramované aplikace externích společností pro výrobní stroje) používá port 80, což signalizuje jako potencionální riziko zabezpečení firemní sítě. (*viz obrázek č. 64*)

Port	Application	Risk	Bytes	Sessions	Threats	Content	URLs	Users
80	ssl	4	598.7M	5.1k	0	0	0	359
80	facebook-video	4	181.1M	87	0	0	0	5
9080	ssl	4	148.4M	18.3k	0	0	0	2
2082	web-browsing	4	129.7M	913	0	0	0	58
2089	ms-sms	3	27.6M	1.8k	558	0	0	401
5061	ssl	4	19.5M	13	0	0	0	6
38383	web-browsing	4	18.7M	54	0	0	0	1
8084	vmware-carbon-black	1	13.9M	751	0	0	0	33
8080	ssl	4	10.2M	86	0	0	0	21
9524	ssl	4	7.3M	494	0	0	0	259
others	others	others	25.0M	2.4k	296	104	0	0

obrázek č. 64 – Palo Alto App. Non Standard Port, zdroj: vlastní zpracování

Palo Alto PA 3220 má možnost blokovat aktivitu aplikací nebo podezřelých uživatelských akcí. Toho docílí vnitřní kontrolou kódu aplikací. Pokud odhalí v aplikaci například část kódu, která má za úkol odesílat emaily, komunikaci v rámci této aplikace zablokuje. *(viz obrázek č. 65)* Aplikace musí být poté manuálně povolena proškoleným pracovníkem.

Name	From Zone	To Zone	Source address	Destination address	Application	Action	Severity
NON SYN TCP	z_LVL4_off	z_LVL4_off	10.220.135.225	10.220.238.142	not-applicable	drop	informational

obrázek č. 65 – Zablokování komunikace na firewallu, zdroj: vlastní zpracování

Identifikované hrozby se řadí podle vážnosti situace do čtyř kategorií:

- Informační
- Nízká
- Střední
- Vysoká
- Kritická

Na dané hrozby má firewall PA definované reakční aktivity, které použije v závislosti na provedené definici pravidel. PA může reagovat těmito způsoby:

- Upozornit členy bezpečnostního týmu
- Povolit akci
- Zablokovat IP adresu zdrojového zařízení
- Odmítnout komunikaci
- Zahodit komunikaci
- Restart klienta
- Restart zdroje i klienta
- DNS Sinkhole

Globálním bezpečnostním týmem Saint-Gobain Adfors byla vydefinována pravidla, kdy při dvou nejnižších úrovních vážnosti situace je komunikace zahozena a informovaný přidělený člen bezpečnostního týmu. Při stupních vážnosti od střední po kritickou jsou již server i client resetovány. *(viz obrázek č. 66)*

Name	Location	Count	Rule Name	Threat Name	Severity	Action	Packet Capture
as_sgt	Shared	Rules: 5	critical	any	critical	reset-both	disable
		Exceptions: 1	high	any	high	reset-both	disable
			medium	any	medium	reset-both	disable
			low	any	low	alert	disable
			informational	any	informational	alert	disable

obrázek č. 66 – Pravidla Závažnosti hrozby, zdroj: vlastní zpracování

Firewall také jednotlivé zachycené hrozby loguje, a informace zobrazuje v přehledné formě, kde lze najít typ, jméno, zóny (odchozí a příchozí) a další informace.

Kromě mnoha dalších přehledů a funkcí, je ve firewallu Palo Alto zobrazen přehled aktivních a neaktivních rozhraní. K aktivním rozhraním byly lokálním IT týmem přiděleny předem vydefinované síťové zóny: *(viz tabulka č. 4)*

- z_LVL2_Phatec – Zóna zařízení Phatec
- z_LVL3_kardex – Zóna zařízení Kardex
- z_LVL3_mgt – Zóna managementu zařízení
- z_LVL3_osi_esonic – Zóna zařízení Esonic
- z_LVL3_ws_Eurest – Zóna pracovních stanic Eurest
- z_LVL3_ws_mes – Zóna industriálních zařízení MES
- z_LVL4_bms – Zóna systému správy budov
- z_LVL4_mgt – Zóna managementu zařízení
- z_LVL4_off – Zóna ředitelství
- z_LVL4_pbx – Zóna zařízení PBX
- z_LVL5_WAN – Zóna WAN připojení

Interface	Security Zone
ethernet1/1	z_LVL5_wan
ethernet1/2	none
ethernet1/2.6	z_LVL4_bms
ethernet1/2.30	z_LVL3_osi_esonic
ethernet1/2.33	z_LVL4_bms
ethernet1/2.82	z_LVL3_ws_EUREST
ethernet1/2.102	z_LVL4_mgt
ethernet1/2.136	z_LVL4_off
ethernet1/2.156	z_LVL4_off
ethernet1/2.170	z_LVL4_mgt
ethernet1/2.186	z_LVL4_off
ethernet1/2.201	z_LVL3_ws_mes
ethernet1/2.202	z_LVL2-0_phatec
Ethernet1/2.203	Z_LVL4_pbx
ethernet1/2.241	z_LVL4_off
ethernet1/2.300	z_LVL3_kardex
ethernet1/2.1030	z_LVL3_mgt

tabulka č. 4 – Definované zóny síťového provozu, zdroj: vlastní zpracování

Dalším úkolem lokálního týmu IT bylo nadefinování pravidel síťového provozu tak, aby co nejvíce odpovídala realitě před zavedením PA 3220, díky těmto pravidlům se dá předejít nechtěným zásahům do provozu, kde jsou výpadky kritické např. zaznamenávání informací z tavných van do databázového systému Velínu. Výčet vydefinovaných, nejdůležitějších pravidel pro výrobní část firmy je znázorněn v *tabulce* č. 5.

Name	Location	Type	Src. Zone	Dst. Zone	Application	Service
Ind_vs to wan	cz0015	interzone	z_LVL3_ws_mes	z_LVL5_wan	any	tcp-1433 tcp-12200 tcp-12201
Ind_vs to wan-1	cz0015	interzone	z_LVL3_ws_mes	z_LVL5_wan	any	tcp-139 tcp-445
z_LVL5_wan_do_LVL3_ws_mes_1	cz0015	interzone	z_LVL5_wan	z_LVL3_ws_mes	any	tcp-102 tcp-9100 tcp-3000
office to ind-vs-2	cz0015	interzone	z_LVL4_off	z_LVL3_WS_mes	any	tcp-9100
wan to ind-vs-1	cz0015	interzone	z_LVL5_wan	z_LVL3_ws_mes	any	tcp-5405
Phatec_PLC	cz0015	interzone	z_LVL5_wan	z_LVL2-0_phatec	any	tcp-102
Flows fo IP cameras	cz0015	interzone	z_LVL4_mgt z_LVL4_off	z_LVL4_bms	any	tcp-80 tcp-554 tcp-37777
z_LVL4_off_z_LVL5_wan	cz0015	interzone	z_LVL4_off	z_LVL5_wan	any	any
z_LVL5_wan_do_LVL4_off	cz0015	interzone	z_LVL5_wan	z_LVL4_off	any	any
VNC_indu_wan	cz0015	interzone	z_LVL5_wan	z_LVL3ws_mes	any	tcp-5900
Kardex_control	cz0015	interzone	z_LVL5_wan	z_LVL3_kardex	any	tcp-81
switch radius	cz0015	interzone	z_LVL4_mgt	z_LVL5_wan	any	udp-69 udp-1645
DHCP_MES_WS	cz0015	interzone	z_LVL3_ws_mes	z_LVL5_wan	any	udp-67
Kardex_srv_tp_MES	cz0015	interzone	z_LVL5_wan	z_LVL3ws_mes	any	tco-9090

tabulka č. 5 – Definovaná pravidla síťového provozu, zdroj: vlastní zpracování

Celkem bylo definováno 76 pravidel síťového provozu mezi zónami síťové infrastruktury, aby bylo docíleno plynulého síťového provozu ve všech oblastech firmy.

Výstupy firewallu Palo Alto PA 3220 spravuje outsourcovaný bezpečnostní tým, který má za úkol reagovat na požadavky od lokálních bezpečnostních, síťových a programových týmů. Původ outsourcovaného týmu (Indie) umožňuje zajistit odbornou práci a neutralitu zaměstnanců při vyřizování požadavků. Požadavky, které zadávají lokální týmy, jsou dvojího druhu:

- Nové požadavky
- Incidenty

Nové požadavky

V tomto případě mají specialisté externího týmu standardní pracovní režim s reakční dobou podle priority požadavku.

- Nízká priorita – Vyřízení do tří dnů
- Střední priorita – Vyřízení do jednoho dne
- Vysoká priorita – Vyřízení v rámci hodin

Do nových požadavků spadá například vytváření nových pravidel síťového provozu. Při zavádění firewallu Palo Alto PA 3220 se pravidla síťového provozu teprve definovala, takže první dva měsíce provozu fungoval v režimu any-to-any, kdy je síťový provoz povolen mezi všemi zónami kromě explicitních výjimek. V průběhu těchto dvou měsíců se vytvářeli pravidla odpovídající síťovému provozu ve firmě Saint-Gobain Adfors. Například pro lokálně naprogramovanou aplikaci přehledu kamer bylo nutné založit pravidlo pro povolení komunikace na TCP portu 1433 z důvodu přístupu aplikace na lokálně nainstalovanou SQL databázi na kamerovém serveru.

Incidenty

Incidenty mohou být buď vyvolané informováním bezpečnostního pracovníka samotným firewallem nebo mohou být iniciovány pracovníky lokálních informačních týmů. Při řešení manuálně jsou definovány tři stupně naléhavosti incidentu (3 – nízká, 2 – střední, 1 - vysoká) a pracovník má jednu hodinu na poskytnutí odpovědi na zadaný incident.

Zadávání požadavků i manuálních incidentů probíhá skrze webový tiketovací portál Service Now, kam má přístup pouze omezený okruh uživatelů (lokální administrátoři IT).

3.5 Zabezpečení firemních aplikací

Ve firmě Saint-Gobain Adfors se ve velké míře využívají aplikace naprogramované speciálně pro jednotlivé situace ve výrobní části firmy. K programování se využívá .NET framework a programovací jazyk C#. Původní stav aplikací nebyl z bezpečnostního hlediska dostatečný. Přihlašovací údaje se nacházely v podobě nezašifrovaného textu v konfiguračním souboru aplikace. *(viz obrázek č. 67)*

```
<connectionStrings>
  <!--Přihlášení do DB_Prihlaseni-->
  <add
    name="Prihlaseni"
    connectionString="
                      Server = 192.168.0.1;
                      Initial Catalog = DB_Prihlaseni;
                      User ID = dbPrihlaseni;
                      Password = ukazka
                      "
    />
  <!--Přihlášení do DB_Aplikace-->
  <add
    name="Aplikace"
    connectionString="
                      Server = 192.168.0.1;
                      Initial Catalog = DB:Aplikace;
                      User ID = dbAplikace;
                      Password = ukazka
                      "
    />
  <!--Přihlášení do DB_Prihlaseni s Intergrated security-->
  <add
    name="Prihlaseni_Admin"
    connectionString="
                      Server = 192.168.0.1;
                      Initial Catalog = DB_Prihlaseni;
                      Integrated Security=SSPI
                      "
    />
  <!--Přihlášení do DB_Aplikace s Integrated security-->
  <add
    name="Aplikace_Admin"
    connectionString="
                      Server = 192.168.0.1;
                      Initial Catalog = DB_Aplikace;
                      Integrated Security=SSPI
                      "
    />
  <!--Přihlášení pro přehled uživatelů-->
  <add
    name="LCP_Roboti.Properties.Settings.DB_Prihlaseni_DataSet"
    connectionString="
                      Data Source=192.168.0.1;
                      Initial Catalog=DB_Prihlaseni;
                      Integrated Security=True"
    providerName="System.Data.SqlClient"
    />
</connectionStrings>
```

obrázek č. 67 – Původní stav přihl. údajů, zdroj: vlastní zpracování

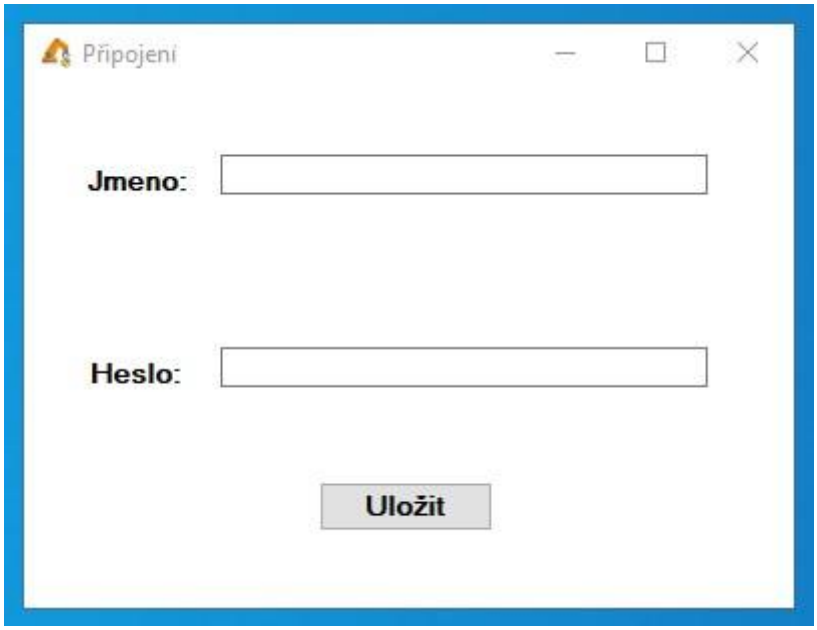
Pokud by se v tomto případě dostal útočník fyzicky k počítači a měl znalosti o konfiguračních souborech .NET aplikací mohl by se bez problému dostat k nezašifrovaným datům a přihlašovat se k serverům, kde se často nachází citlivé výrobní informace.

Před prvním spuštěním na počítači se v konfiguračních souborech již upravených programů nenachází citlivé informace sloužící pro připojení k firemním informačním systémům. *(viz obrázek č. 68)*

```
<connectionStrings>
  <!--Přihlášení do DB_Prihlaseni s Intergrated security-->
  <add
    name="Prihlaseni_Admin"
    connectionString="
                      Server = 192.168.0.1;
                      Initial Catalog = DB_Prihlaseni;
                      Integrated Security=SSPI
                      "
    />
  <!--Přihlášení do DB_Aplikace s Integrated security-->
  <add
    name="Aplikace_Admin"
    connectionString="
                      Server = 192.168.0.1;
                      Initial Catalog = DB_Aplikace;
                      Integrated Security=SSPI
                      "
    />
  <!--Přihlášení pro přehled uživatelů-->
  <add
    name="LCP_Roboti.Properties.Settings.DB_Prihlaseni_DataSet"
    connectionString="
                      Data Source=192.168.0.1;
                      Initial Catalog=DB_Prihlaseni;
                      Integrated Security=True"
    providerName="System.Data.SqlClient"
    />
</connectionStrings>
```

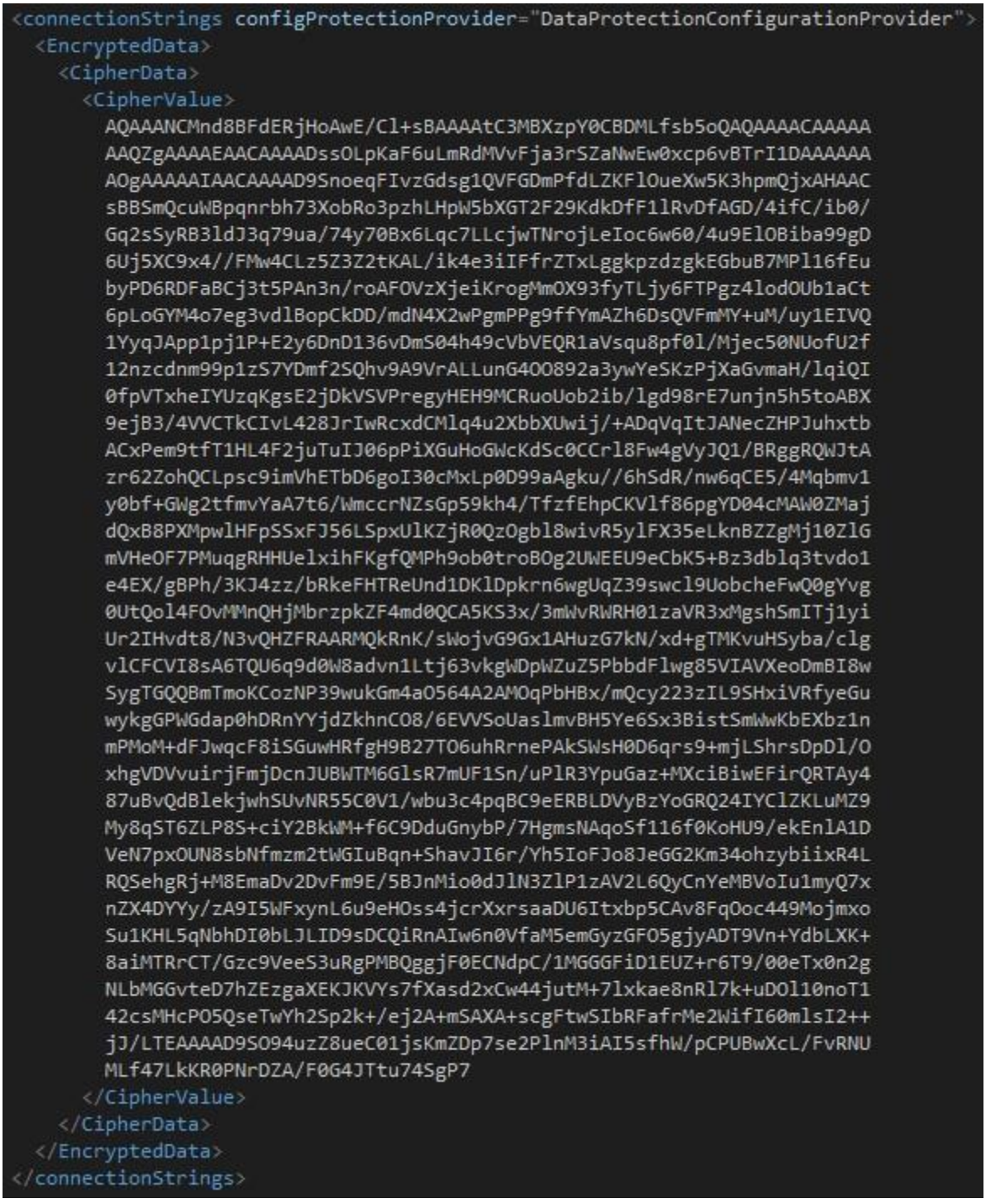
obrázek č. 68 – Stav přihl. údajů před prvním spuštěním, zdroj: vlastní zpracování

Po prvním spuštění, které vždy vykonává programátor dané aplikace nebo správce znalý problematiky, se zobrazí výzva se zadáním uživatelského jména a hesla potřebného pro přístup k IS určeným pro výrobní potřeby. *(viz obrázek č. 69)*



obrázek č. 69 – Okno vyzývající k přihlášení uživatele, zdroj: vlastní zpracování

Zadané údaje se poté automaticky uloží do konfiguračního souboru, ale již v nečitelné podobě pro běžného uživatele, který by si chtěl dané přihlašovací údaje prohlédnout z pracovní stanice. *(viz obrázek č. 70)*



obrázek č. 70 – Nový stav přihl. údajů v config souboru, zdroj: vlastní zpracování

3.6 Interní směrnice společnosti

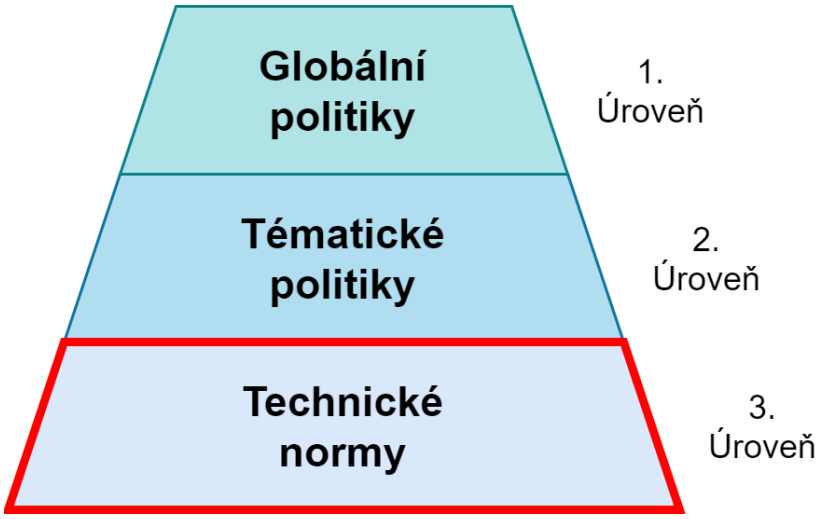
Praktickým výstupem práce jsou také dva návrhy interní směrnice, které neobsahují odkazy na kritické firemní informace. Směrnice jsou vytvořeny, aby doplnily případná školení uživatelů. Při tvorbě návrhů směrnic byl zohledněn předmět podnikatelské činnosti a velikost společnosti Saint-Gobain Adfors. Při aplikaci těchto interních směrnic je možné zaměstnance odkázat na obecná ustanovení zákoníku práce *(§38 odst. 1 písm. b) – povinnosti zaměstnance vyplývající z pracovního poměru, §301 a – jiné povinnosti zaměstnance*). Disciplinární tresty a odpovědnosti zaměstnance při porušení povinností ve zmíněných interních směrnicích by poté měly být v souladu s (*§52 písm. g) – Zaměstnavatel může dát zaměstnanci výpověď jen z těchto důvodů, §55 b) – Zaměstnavatel může výjimečně pracovní poměr okamžitě zrušit jen tehdy, nebo §250 – Odpovědnosti zaměstnance za náhradu škody zaměstnavateli*). Vnitřní směrnice byly sepsány s ohledem na normu ČSN EN ISO/IEC 27001.

Evidenci a zpracování osobních údajů v souvislosti se zaměstnaneckými podpisy směrnic je také třeba sladit s Obecným nařízením na ochranu osobních údajů neboli GDPR (Nařízení EU 2016/679).

Ve společnosti Saint-Gobain Adfors se dokumentace dělí do tří úrovní:

- Globální politiky
- Tematické politiky
- Technické normy

Oba návrhy interních směrnic se svým zařazením řadí do třetí úrovně firemní dokumentace, a to do technických norem. *(viz obrázek č. 71)*



obrázek č. 71 – Korpus dokumentace Saint-Gobain Adfors, zdroj: vlastní zpracování

První směrnice, „Bezpečnostní pravidla pro uživatele společnosti Saint-Gobain Adfors“, má za cíl upozornit běžné uživatele na nebezpečí a prohřešky, kterým by se měli vyhnout a také pravidla, která by měli dodržovat. Na akceptování a dodržování těchto pravidel dohlíží vedoucí pracovník.

Druhý dokument, „Práva a povinnosti správce systému ve společnosti Saint-Gobain Adfors“, představuje soubor práv a povinností pro administrátory různých firemních, informačních systémů. Dokument musí být podepsán každým správcem systému, jinak mu musí být odebrána všechna privilegia, dokud není zjednána náprava.

Shrnutí

Implementaci bezpečnostních opatření popsaných v praktické části diplomové práce se věnoval tříčlenný tým výrobních IT specialistů firmy Saint-Gobain Adfors, jehož jsem členem.

Před zavedením sofistikovanějších opatření jsme do nově zbudované serverovny výrobní části podniku nainstalovali nový server, který je určený výhradně pro informační potřeby závodů napříč celou fabrikou. Po nainstalování racku a serveru byla v serverovně zavedena opatření, která předchází možným poškození serveru. První opatřením bylo nainstalování dvou UPS zdrojů, které jej udrží zapnutý až 18 minut po výpadku elektrického proudu. Druhým opatřením je vyvýšená podlaha chránící server před případnými povodněmi nebo únikem vody. Toto opatření bylo nutné zavést, protože se serverová místnost nachází v přízemní části administrativní budovy závodní části firmy. Třetím jsou pak dvě klimatizační jednotky, které mají za úkol udržovat v serverové místnosti stálou teplotu.

Druhým projektem, jehož implementaci jsem měl plně na starost, bylo zavedení „čistících stanic“ na vybraná firemní pracoviště. Do dnešního dne bylo v areálu firmy rozmístěno 20 stanic. Zaměstnancům firmy, kteří mají podezření na potenciální nebezpečnost jejich USB flash disku, je tak k dispozici zařízení pro provedení okamžité kontroly.

Třetím dílčím cílem, byla konfigurace na druhé síťové vrstvě přístupových prvků proti případným kybernetickým útokům. Mým úkolem bylo zakreslit topologii a zanalyzovat aktuální situaci síťových zařízení ve firmě a navrhnout opatření. Následnou implementaci konfiguračních zabezpečení (Port Security, obranu proti VLAN hopping, obranu DHCP, obranu proti ARP útokům, obranu proti STP útokům) jsme si s kolegy z výrobního IT týmu rovnoměrně rozdělili.

Dále bylo rozhodnuto, z bezpečnostních důvodů rozdělit síť do více virtuálních sítí, než byl počáteční stav. Z původní výrobní virtuální sítě, kde se nacházely počítače společně s tiskárnami a jinými zařízeními byly postupně vydefinovány a nastaveny sítě pro Původní pracovní stanice, nastupující pracovní stanice, kamery, PLC zařízení, telefony, management switchů a další.

Rozdělení do více virtuálních sítí proběhlo v návaznosti na zavedení Next Generation firewallu Palo Alto PA 3220. Rozhodnutí o nasazení tohoto firewallu bylo dáno našemu lokálnímu IT týmu od globálního IT bezpečnostního týmu Saint-Gobain. Na zapojení,

konfiguraci a tvorbě definic vlastních pravidel síťového provozu se podílel celý tříčlenný tým lokálního IT týmu.

Mým dalším úkolem bylo nalezení řešení pro zabezpečení konfiguračního souboru obsahujícího připojovací řetězce do databází, kde jsou uložena výrobní data. V práci znázorněný postup šifrování přihlašovacích údajů je již z velké části implementován do všech výrobních programů napsaných v jazyce C#, které přistupují do výrobních databází.

Na základě znalosti administrace výrobních počítačů a z pozice programátora aplikací výrobní části firmy, jsem sepsal dva návrhy interních směrnic, které řeší vztah uživatele a správce vůči systémům patřící firmě Saint-Gobain Adfors. Tím je naplněno zabezpečení datového provozu na všech úrovních.

Závěr

Cílem diplomové práce „Implementace opatření kybernetické bezpečnosti do firemní konvergované sítě“ byla aplikace bezpečnostních (projekt čistících stanic, konfigurace síťových prvků, zavedení Palo Alto, zabezpečení firemních aplikací) a manažerských (interní bezpečnostní směrnice – „Bezpečnostní pravidla pro uživatele společnosti Saint-Gobain Adfors“, „Práva a povinnosti správce systému ve společnosti Saint-Gobain Adfors“) metod ke zvládnutí bezpečnostních výzev, kterým firma Adfors čelí a bude čelit po celou dobu své existence.

Prvotním impulzem zamyšlení se nad dosavadní kybernetickou bezpečností byl bezpečnostní incident, který se stal v červnu roku 2017. Tento incident měl za následek dvoudenní výpadek administrativy nejenom centrály Saint-Gobain Adfors, ale i všech sesterských firem po celém světě. Práce na zabezpečení ITC infrastruktury firmy tedy započaly již před tvorbou této diplomové práce a popsanou realizací nekončí. V rámci životního cyklu implementace budou provedeny další testy a následná nastavení.

Boj proti kybernetickým hrozbám nelze vyřešit jednou implementací s trvalou platností. Je naprosto jasné, že jde o kontinuální boj, ve kterém se nesmí ani na chvíli polevit. Důvodem je jednak vývoj kybernetických hrozeb, ale také rozvoj a změny spravovaného prostředí datové sítě. Příkladem může být nedávno způsobený posun ke vzdálené práci z domova z důvodu epidemiologické situace, kdy vzešly požadavky na mnohem větší míry zajištění kybernetické bezpečnosti zaměstnanců při připojení takřka odkudkoli. Zde bylo čerpáno ze zkušeností zabezpečení provozních technologií, kde existují osvědčené postupy fyzického oddělení kritických úkonů. Například pracovník, pracující vzdáleně s kritickým programem, by mohl mít jednoúčelový notebook, který bude vykonávat pouze jediný úkol a nebude mít přístup k emailu, sociálním sítím a dalším běžným uživatelským aplikacím.

Do budoucna bude také nutné zamyslet se nad pojmem Industry 4.0, který rezonuje většinou velkých korporací. Kybernetickou bezpečnost v Industry 4.0 nelze řešit stejným způsobem jako v nynějším výpočetním prostředí, protože nárůst počtu zařízení a s nimi spojených problémů bude markantní. V těchto a podobných případech může do hry vstoupit umělá inteligence a strojové učení. Strojové učení by mohlo nahradit nedostatek bezpečnostních specialistů a monitorovat síťový provoz z hlediska jakýchkoliv odchylek v chování informačního systému. Umělá inteligence by se věnovala objevování skrytých vzorů při zpracovávání velkého množství dat.

Zajímavým vylepšením bezpečnosti sítě firmy Saint-Gobain Adfors by také mohlo být řešení zabezpečení a monitoringu sítě zvané Flowmon. Nástroj dokáže z velké části automatizovat proces monitoringu síťového provozu a detekci potenciálních hrozeb, což by mohlo být pro naše lokální IT oddělení velkou pomocí při zdokonalování firemních bezpečnostních prvků.

Jak je patrné, implementace navržených řešení je pouze začátkem tohoto boje. Bude nutné se neustále zamýšlet nad novými výzvami v oboru kybernetické bezpečnosti a přicházet s novými řešeními, která nám umožní, stále modernější informační technologie.

Použité zdroje:

[1] PUŽMANOVÁ, Rita. TCP/IP v kostce. České Budějovice: Kopp, 2004. ISBN 80-723-2236-2.

[2] NORTHCUTT, Stephen. Bezpečnost sítí: velká kniha. Brno: CP Books, 2005. Security (CP Books). ISBN 80-251-0697-7.

[3] BARKEN, Lee. Wi-Fi: jak zabezpečit bezdrátovou síť. Brno: Computer Press, 2004. ISBN 80-251-0346-3.

[4] VELTE, Toby J. a Anthony T. VELTE. *Síťové technologie Cisco: velký průvodce*. Brno: Computer Press, 2003. Administrace (Computer Press). ISBN 80-722-6857-0.

[5] A brief history of computer networking and the Internet. Apache HTTP Server Test Page powered by CentOS [online]. Copyright © 2004 [cit. 08.02.2021]. Dostupné z: http://www2.ic.uff.br/~michael/kr1999/1-introduction/1_09-history.htm

[6] NetAcad Course UI. NetAcad Course UI [online]. Copyright © 2021 [cit. 09.06.2021]. Dostupné z: https://lms.netacad.com/course/view.php?id=247872

[7] What is MAC flooding attack and How to prevent MAC flooding attack. 301 Moved Permanently [online]. Copyright © 2008 [cit. 14.06.2021]. Dostupné z: https://www.omnisecu.com/ccna-security/what-is-mac-flooding-attack-how-to-prevent-mac-flooding-attack.php

[8] 2021 VLAN Hopping Attacks & Mitigation Best Practices | AT&T Cybersecurity. AlienVault is now AT&T Cybersecurity [online]. Copyright © 2021 [cit. 23.06.2021]. Dostupné z: https://cybersecurity.att.com/blogs/security-essentials/vlan-hopping-and-mitigation

[9] VLAN Security and Design (3.3) > Cisco Networking Academy's Introduction to VLANs | Cisco Press . *Cisco Press: Source for Cisco Technology, CCNA, CCNP, CCIE Self-Study | Cisco Press* [online]. Copyright © 2021 Pearson Education, [cit. 01.07.2021]. Dostupné z: https://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=10

[10] ScienceDirect. ScienceDirect [online]. Copyright © [cit. 04.07.2021]. Dostupné z: https://www.sciencedirect.com/science/article/abs/pii/S0045790612001140

[11] MUKHTAR, Husameldin, Khaled SALAH a Youssef IRAQI. Mitigation of DHCP starvation attack [online]. 2012, 38(5), 1115-1128 [cit. 05.07.2021]. ISSN 00457906. DOI: 10.1016/j.compeleceng.2012.06.005

[12] What is out-of-band authentication? - Definition from WhatIs.com. Information Security information, news and tips – SearchSecurity [online]. Copyright © 2018 [cit. 18.07.2021]. Dostupné z: https://searchsecurity.techtarget.com/definition/out-of-band-authentication

[13] GLAZER, Glenn, Cora HUSSEY a Roy SHEA. Certificate-Based Authentication for DHCP. Thesnowpit [online]. 2003, 2003(1), 1-14 [cit. 22.07.2021]. Dostupné z: http://www.thesnowpit.ca/research/other/cbda.pdf

[14] OSTROVSKY, Rafael a Roberto DE PRISCO, VISCONTI, Ivan, ed. CLL: A Cryptographic Link Layer for Local Area Networks. Security and Cryptography for Networks [online]. Amalfi, 2008, s. 30-48 [cit. 28.07.2021]. ISBN 978-3-540-85855-3. Dostupné z: https://link.springer.com/content/pdf/10.1007%2F978-3-540-85855-3.pdf

[15] What does INTERFACE MESSAGE PROCESSOR mean? Definitions.net [online]. Copyright © 2001 [cit. 15.08.2021]. Dostupné z: https://www.definitions.net/definition/INTERFACE+MESSAGE+PROCESSOR

[16] PETERKA, Jiří. Internet: Na počátku byl ARPANET .... *EArchiv.cz: Archiv článků a přednášek Jiřího Peterky* [online]. Praha: COMPUTERWORLD.CZ, 1996, 12.9.1996 [cit. 26.08.2021]. Dostupné z: https://www.earchiv.cz/a95/a504c502.php3

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

[18] Internet Evolution: A Timeline History of the Network – The Reboot. *The Reboot – Let's build a better internet.* [online]. Copyright © 2016 [cit. 16.08.2021]. Dostupné z: https://thereboot.com/internet-evolution-a-timeline-history-of-the-network/

[19] DFINITY Foundation | Internet Computer. DFINITY Foundation | Internet Computer [online]. Copyright © 2021 [cit. 18.08.2021]. Dostupné z: https://dfinity.org/

[20] PETERKA, Jiří. Internet: Koaxiální kabel a kroucená dvoulinka. EArchiv.cz: Archiv článků a přednášek Jiřího Peterky [online]. Praha: COMPUTERWORLD.CZ, 1996, 12.9.1996 [cit. 26.08.2021]. Dostupné z: https://www.earchiv.cz/a92/a207c110.php3

[21] PETERKA, Jiří. Internet: Optické kabely. EArchiv.cz: Archiv článků a přednášek Jiřího Peterky [online]. Praha: COMPUTERWORLD.CZ, 1996, 12.9.1996 [cit. 26.08.2021]. Dostupné z: https://www.earchiv.cz/a92/a208c110.php3

[22] The 5 most common router attacks on a network – Intelligent CIO Europe. *Home – Intelligent CIO* [online]. Copyright © 2021 Intelligent CIO [cit. 24.08.2021]. Dostupné z: https://www.intelligentcio.com/eu/2017/10/16/the-5-most-common-router-attacks-on-a-network/

[23] The Disadvantages of Unpatched Computers on a LAN | Small Business - Chron.com. *Small Business - Chron.com* [online]. Copyright © 2021 Hearst [cit. 24.08.2021]. Dostupné z: https://smallbusiness.chron.com/disadvantages-unpatched-computers-lan-67316.html

[24] What is a denial of service attack (DoS)? - Palo Alto Networks. *Global Cybersecurity Leader – Palo Alto Networks* [online]. Copyright © 2021 Palo Alto Networks. All rights reserved [cit. 26.08.2021]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

[25] What is an ICMP Flood DDoS Attack? | NETSCOUT. *Security, Application & Network Performance | NETSCOUT* [online]. Copyright © 2021 [cit. 26.08.2021]. Dostupné z: https://www.netscout.com/what-is-ddos/icmp-flood

[26] International Journal of Advanced Research in Computer Science and Software Engineering: Security Issues in Manet: A Survey on Attacks and Defense Mechanisms [online]. 2013. 2013 [cit. 26.08.2021]. ISSN 2277 128X.

[27] Merouane, M. An approach for detecting and preventing DDoS attacks in campus. Aut. Control Comp. Sci. 51, 13–23 (2017). [cit. 26.08.2021] DOI:10.3103/S0146411616060043

[28] A Survey on Defense Mechanisms countering DDoS Attacks in the Network – Scientific Figure on ResearchGate. Copyright © 2015 [cit. 06.08.2021] Dostupné z: https://www.researchgate.net/figure/Architecture-for-intermediate-network-based-DDoS-mechanism_fig3_276282054

[29] Common Attacks On Routing Protocols And How To Mitigate Them | by M'hirsi Hamza | Medium. *M'hirsi Hamza – Medium* [online]. Copyright © 2019 [cit. 07.08.2021] Dostupné z: https://hamzamhirsi.medium.com/common-attacks-on-routing-protocols-and-how-to-mitigate-them-11ec0cad08d7

[30] Security Configuration Guide: Access Control Lists, Cisco IOS Release 15M&T – Access Control List Overview and Guidelines [Support] - Cisco. *Cisco – Networking, Cloud, and Cybersecurity Solutions* [online]. Copyright © 2021 [cit. 08.08.2021] Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/15-mt/sec-data-acl-15-mt-book/sec-acl-ov-gdl.html

[31] Configure Context-Based Access Control (CBAC) - Cisco. *Cisco – Networking, Cloud, and Cybersecurity Solutions* [online]. Copyright © 2021 [cit. 12.08.2021] Dostupné z: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/13814-32.html

[32] Cisco Learning Network. [online]. Copyright © 2021 [cit. 12.08.2021] Dostupné z: https://learningnetwork.cisco.com/s/article/zone-based-firewall-part-1

[33] What is an Intrusion Prevention System? - Palo Alto Networks. *Global Cybersecurity Leader – Palo Alto Networks* [online]. Copyright © 2021 Palo Alto Networks. All rights reserved [cit. 12.09.2021]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

[34] Intrusion Prevention System: What Is An IPS? How Do They Work? | Okta Singapore. *Okta | Identity for the internet* [online]. Copyright © 2021 Okta. All rights reserved. [cit. 12.09.2021]. Dostupné z: https://www.okta.com/sg/identity-101/intrusion-prevention-system/

[35] Security Configuration Guide: Denial of Service Attack Prevention, Cisco IOS Release 15M&T – Configuring TCP Intercept (Preventing Denial-of-Service Attacks) [Support] - Cisco. *Cisco – Networking, Cloud, and Cybersecurity Solutions* [online]. Copyright © 2021 [cit. 21.08.2021] Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_dos_atprvn/configuration/15-mt/sec-data-dos-atprvn-15-mt-book/sec-cfg-tcp-intercpt.html

[36] Understanding Unicast Reverse Path Forwarding. [online]. Copyright © 2021 [cit. 21.08.2021] Dostupné z: https://tools.cisco.com/security/center/resources/unicast_reverse_path_forwarding

[37] Choi, Min-Kyu & Rosslin, John & Robles, Rosslin & Hong, Chang-Hwa & Kim, Tai-Hoon. (2008). Wireless Network Security: Vulnerabilities, Threats and Countermeasures. International Journal of Multimedia and Ubiquitous Engineering. 3.

[38] cafe-latte [Aircrack-ng]. *Aircrack-ng* [online]. Copyright © 2021 [cit. 23.08.2021] Dostupné z: https://www.aircrack-ng.org/doku.php?id=cafe-latte

[39] Differences Among WEP, WPA, WPA2 and WPA3 Wireless Security Protocols. *Purchase Intent Data for Enterprise Tech Sales and Marketing – TechTarget* [online]. Copyright © 2021 [cit. 02.09.2021] Dostupné z: https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2

[40] Computer Threats | Monster.com. *Monster Jobs – Job Search, Career Advice & Hiring Resources | Monster.com* [online]. Copyright © 2021 Monster Worldwide [cit. 20.09.2021]. Dostupné z: https://www.monster.com/career-advice/article/computer-threats-protect

[41] 1.2.1.2 End Devices. *Cisco Networking Academy — National University of Mongolia, МУИС-ХШУИС-Сиско академи* [online]. Copyright © 2021 [cit. 21.09.2021] Dostupné z: http://cisco.num.edu.mn/CCNA_R&S1/course/module1/1.2.1.2/1.2.1.2.html

[42] What is spyware? And how to remove it. *Norton™ Official Site | Antivirus, VPN & Security Software* [online]. Copyright © 2021 NortonLifeLock Inc. [cit. 21.09.2021]. Dostupné z: https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html

[43] What is Spam? | How to Detect and Prevent Spamming | Avast. [online]. Copyright © 2021 [cit. 24.09.2021] Dostupné z: https://www.avast.com/c-spam

[44] What is Malware? - Definition and Examples – Cisco. *Cisco – Networking, Cloud, and Cybersecurity Solutions* [online]. Copyright © 2021 [cit. 25.09.2021] Dostupné z: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html#~what-is-malware

[45] What is phishing | Attack techniques & scam examples | Imperva. *Cyber Security Leader | Imperva, Inc.* [online]. Copyright © 2021 Imperva. All rights reserved [cit. 23.09.2021]. Dostupné z: https://www.imperva.com/learn/application-security/phishing-attack-scam/

[46] What Is Ransomware? | McAfee. [online]. Copyright © [cit. 23.09.2021]. Dostupné z: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware.html

[47] 302 Found. *DDoS Services: Cloud Security Products and Solutions | Radware* [online]. Copyright © 2021 [cit. 02.10.2021]. Dostupné z: https://www.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning/

[48] STP Manipulation Attacks – Authentication Proxy. *Cisco Certified Expert* [online]. Copyright © 2021 [cit. 03.10.2021]. Dostupné z: https://www.ccexpert.us/authentication-proxy/stp-manipulation-attacks.html

[49] PortFast and BPDU Guard. *Aruba | Enterprise Networking and Security Solutions* [online]. Copyright © 2021 [cit. 08.10.2021]. Dostupné z: https://www.arubanetworks.com/techdocs/ArubaOS_64x_WebHelp/Content/ArubaFrameStyles/Branch%20Office/PortFast%20and%20BPDU%20Guard.htm

[50] Klement, Milan. (2017). Technologie bezdrátových sítí – základní principy a standardy. DOI:10.5507/pdf.17.24451565.

[51] How to Perform a Network Audit: A Step-By-Step Guide – N-able. *MSP Tools and Resources – N-able* [online]. Copyright © 2021 [cit. 01.11.2021]. Dostupné z: https://www.n-able.com/blog/how-to-perform-network-audit

[52] How do you do a network audit? - Network Configuration Manager. *ManageEngine – IT Operations and Service Management Software* [online]. Copyright © 2021 [cit. 01.11.2021]. Dostupné z: https://www.manageengine.com/network-configuration-manager/network-audit.html

[53] *Practical Networking .net – Networking presented simply, practically, and applicably* [online]. Copyright © 2021 [cit. 04.11.2021]. Dostupné z: https://www.practicalnetworking.net/stand-alone/converged-network/

[54] What is Network Convergence? - Definition from WhatIs.com. *Converged and hyper-converged infrastructure systems news and information – SearchConvergedInfrastructure.com* [online]. Copyright © 2021 [cit. 04.11.2021] Dostupné z: https://searchconvergedinfrastructure.techtarget.com/definition/network-convergence

[55] Three keys to a secure converged network | Computerworld. *IT news, careers, business technology, reviews | Computerworld* [online]. Copyright © 2004 IDG Communications, Inc. [cit. 05.11.2021]. Dostupné z: https://www.computerworld.com/article/2565924/three-keys-to-a-secure-converged-network.html

[56] DAWKINS, J., K. CLARK, G. MANES a M. PAPA. A Framework for Unified Network Security Management: Identifying and Tracking Security Threats on Converged Networks. *Journal of Network and Systems Management* [online]. 2005, **13**(3), 253-267 [cit. 05.11.2021]. ISSN 1064-7570. doi:10.1007/s10922-005-6292-x

Seznam příloh

Seznam virtuálních sítí firmy Saint-Gobain Adfors

VLAN	Název	Popis	Počet zařízení
2	admGR	Generální ředitelství administrace	12
3	admZ1	Závod 1 administrace	15
4	admGR_2	Generální ředitelství administrace 2	X
5	admZ1_2	Závod 1 administrace 2	X
6	Doch_AP	Zařízení docházkového systému	34
7	ArubaLIT	Zařízení Aruba	x
8	Sit158	Síť 158	x
10	Interco_MPLS	Síť Multiprotocol Label Switching (MPLS)	x
11	Interco_L3_PA	Síť Layer 3 Palo Alto	x
12	Interco_L3_GRE	Síť Layer 3 GRE	x
13	PA_HA_control	Palo Alto High Availability (HA) control	x
14	PA_HA_datapl	Palo Alto High Availability (HA) data, aplikace	x
21	IntercoLX6S4	Interconnection LX6 a S4	x
22	IntercoLX3	Interconnection LX3	x
34	Switch_MGM_SGTS	Management switchů v SG net	x
51	Int_DMZ_Cont	Interconnection Demilitarized Zone	x
80	Int_T-Mobile	Interconnection T-Mobile	x
81	Data_HOD_T-mob	Data Hodonice T mobile	x
82	Compas_4G	Compas 4G	x
90	Int_Fortech	Interconnection T-Mobile	x
91	SpojKornice	Spoj s externím skladem Kornice	x
99	Spoj_HOD	Spoj s externím závodem Hodonice	x
100	Swich_MGM	Switch management	109
101	ESX_MGM	Wmware ESXI management	x
102	wifi_techno_mgm	Technologická wifi management	x
105	SG	SG net	229
106	PC_mimo_SG	Počítače mimo SG net	39

107	wifi_techno_data	technologická wifi data	x
108	Wifi_ssid_open	Wifi síť pro hosty	x
109	Kardex	Zařízení Kardex	18
110	Wifi_mob_udrzba	Wifi síť pro mobilní údržbu	49
111	Guzzetti_DWT	Zařízení Guzzetti na provoze DWT	17
132	puvodniVLAN1	Původní VLAN1	x
156	Hod_156	Hodonice síť 156	41
175	Z1_ws	Závod 1 pracovní stanice	67
180	Kamery	Síť kamery	98
185	Tiskarny	Síť pro tiskárny v SG net	102
199	Techn_porbox	Technologické portboxy	18
200	Techno	Technologická síť	155
201	Circ	Síť zařízení Circutor	82
202	VPN_Bruckner	Síť pro zařízení pro linky Brückner	10
203	BCI	Síť pro zařízení BCI	36
204	PBX	Síť pro zařízení PBX	108
207	VS_LIT	Síť Velín Sázava Litomyšl	96
209	OEP_AMETEK_LIG	Síť zařízení Ametek závod LIG	5
210	COV	Síť zařízení na čističce odpadních vod	8
211	Chlazeni_V3_IP_r	Síť zařízení chlazení Vana3	8
212	Phatec	Zařízení Phatec	115
213	Aura_robot	Síť pro zařízení Aury robot	75
214	Siemens_Sazava	Zařízení Siemens linka Sázava	25
215	Siemens_Vltava	Zařízení Siemens linka Vltava	28
216	NavijeckyV4	Navíječky vana 4	63
217	ProjektSoft	Zařízení ProjektSoft	26
218	VPNPristupyTech	VPN přístupy k technologiím	x
219	Cygnet	Zařízení Cygnet	21
220	Fapros_VPN	VPN Fapros	x
221	Chemtec_VPN	VPN Chemtec	x
222	Rozvodna_ABB	Síť zařízení rozvodny ABB	243
223	Mereni_TEX_Hor	Síť měření	242
224	MGM_server_stor	Server management	x

225	Esonic_campen	Síť Esonic Campen	234
226	TrimaPLC	Síť PLC Trima	4
227	Chemtec_vany	Síť Chemtec Vany	8
228	Recyklace_PC	Síť PC na recyklaci	6
229	EthermVany	Síť Vany Ethermvany	11
230	HoneywellLCP	Síť LCP Honeywell	9
231	Eurest_sql_data	Síť Eurest Data	x
238	MESR_ws	Síť work station MESR	48
239	PLC_adfors	Síť Adfors PLC	7
241	Hod_241	Síť 241 Hodonice	x
242	SKF_vibration	Síť vibration SKF	2
297	SGwifi	WIFI v SG net	x
850	O2_MPLS	Síť O2 Multiprotocol Label Switching (MPLS)	x
1110	IDMZ	Síť IDMZ	x

Bezpečnostní pravidla pro uživatele společnosti Saint-Gobain Adfors

Autor: Stanislav Hladík

Obsah

1 Úvod

Uživatelé jsou nejkritičtějším článkem počítačové bezpečnosti. Proto by měli být průběžně vzděláváni a je nutné všem uživatelům neustále připomínat základní pravidla pro bezpečné používání počítačů a služeb.

Každý uživatel by si měl být vědom faktu, že je nedílnou součástí širší počítačové bezpečnosti. Že bezpečnost jeho pracovní stanice není záležitostí pouze správce informačního systému, ale že samotný uživatel se na bezpečnosti své pracovní stanice i celé komunikační sítě aktivně podílí. Každé koncové zařízení s narušenou bezpečností se může stát přestupním prvkem pro útok na ostatní zdroje v síti. Z tohoto důvodu se počítačová bezpečnost týká všech prvků i té nejobyčejnější pracovní stanice, protože **každý systém je nejsnáze napadnutelný zevnitř**.

1.1 Základní zásady

- Přístupy k používání firemních informačních systémů (IS) jsou omezeny používáním jednotlivých uživatelských účtů. Účty jsou vždy zřizovány určenými IT pracovníky. Přístup k IS a jeho používání je možné pouze na základě autentizace zaměstnance ke svému vlastnímu účtu.
- Uživatelské účty se zřizují zásadně pro konkrétního zaměstnance tak, aby vždy pracoval v IS ve svém účtu a byl jasně identifikovatelný. Proto jsou ve všech IS zakázány skupinové a lokální účty.
- Přístup k IS provádí zaměstnanec přihlášením ke konkrétnímu IS, a to jeho vlastním uživatelským jménem a heslem pro přístup k danému IS.

2 Pravidla používání hesel

Automatické nástroje nemají problém vyzkoušet stovky tisíc hesel během několika minut. Z tohoto důvodu je použití běžných slov (vyskytujících se ve slovníku) jako hesel nevhodná. Nedoporučují se ani jména oblíbených knižních, či filmových hrdinů, záměna znaků ležící na stejné klávese nebo použití identifikačních dat uživatele (adresa bydliště, datum narození, čísla dokladů). Hesla by měla obsahovat i jiné než alfanumerické znaky. Měla by být také dostatečně dlouhá – min. 12 znaků – a musí se měnit 1x za 3 měsíce.

Dále je nutné dodržet následující pravidla:

- Hesla se nesmí ukládat v počítači v nezašifrované podobě obyčejného textu a nesmějí být na pracovišti snadno dostupná (na nástěnce, v šuplíku, na monitoru atd.)
- Hesla se nesmějí prozrazovat žádným dalším osobám (ani správce nesmí znát heslo bez dohledatelného písemného souhlasu uživatele). Přihlašovací údaje by neměly být zadávány v situacích, kdy by mohlo dojít k jejich odpozorování.
- Při opuštění pracovní stanice musí každý zaměstnanec provést potřebné úkony, aby nedošlo k zneužití jeho účtu (uzamknout počítač, odhlásit se apod.).
- V případě přístupu k více systémům, službám, nebo strojům, které nejsou spravovány centrálně, není vhodné používat všude stejné heslo.
- Nepoužívat funkci zapamatovat heslo pro příští použití, která je nabízena internetovými prohlížeči nebo poštovními klienty.

2.1 Ochrana obsahu zpráv a osobní identity

Nejtypičtějším příkladem, kdy může dojít k odposlechu obsahu zprávy nebo zcizení elektronické osobní identity, je elektronická pošta. Útočník, který má potřebné znalosti a možnosti (odposlech síťové komunikace nebo přímý přístup k souborům na poštovním serveru) se může dostat k uživatelovým poštovním souborům vcelku snadno. Dále kdokoli na světě může odeslat email, který bude mít jako adresu odesílatele uvedenou adresu samotného uživatele.

Proti těmto hrozbám se lze nejsnadněji bránit těmito kroky:

- Šifrování elektronické pošty založené na asymetrické kryptografii (PGP klíče, X.509 certifikáty).

- Zavedení elektronického podpisu. Elektronický podpis je také řešením i při ochraně integrity zprávy. Umožňuje totiž zjištění, jestli nebyla zpráva cestou změněna.

3 Povinnosti zaměstnanců

- Za uplatňování bezpečnostních pravidel a provoz IS zodpovídají především bezpečnostní IT pracovníci. IT pracovníci při nastavování a správě IS postupují v souladu s obecnými pravidly bezpečnosti, směrnicí „Práva a povinnosti správce systému“ a správného a efektivního využívání IS.
- Veškeré práce prováděné na technickém zařízení, které zajišťuje provoz IS, smí provádět pouze odpovědný zaměstnanec IT. Ostatním zaměstnancům je přísně zakázáno provádět jakékoli úpravy či zásahy do IS.
- Zaměstnanci mají zakázáno modifikovat systémová nastavení, připojovat nebo odpojovat síťové kabely a konektory ve stávajících zařízeních. Zaměstnanci také nesmí do zařízení zaměstnavatele (PC, notebook, laptop) kopírovat neautorizovaný software nebo takový software stahovat prostřednictvím internetu.
- Zaměstnanec je povinen používat IS výhradně k plnění svých pracovních povinností. Veškeré informace zpracovávané jednotlivými IS jsou považovány za majetek zaměstnavatele.
- Zaměstnanec je odpovědný za patřičné zabezpečení a uzavření svého pracovního místa v době své nepřítomnosti. Při odchodu ze svého pracoviště musí ověřit řádné vypnutí všech elektrických zařízení, uzavření oken a zajistit vstup na pracoviště uzamčením. Tato pravidla platí i pro krátkodobé opuštění pracoviště.
- Vedoucí zaměstnanci nesou odpovědnost za implementaci a patřičné dodržování uvedených pravidel a nesou plnou odpovědnost za seznámení svých podřízených pracovníků se všemi povinnostmi, které vyplývají z tohoto vnitřního předpisu.
- Každý zaměstnanec je povinen neprodleně nahlásit odpovědnému pracovníkovi IT každé jednání nebo podezření na toto jednání, které je v rozporu s uvedenými pravidly.

4 Doporučení pro zaměstnance

Následující pravidla se týkají všeobecné bezpečnosti, a proto by je měli uživatelé bedlivě dodržovat a řídit se jimi při pohybu v internetovém prostředí ze svého firemního počítače.

- **Neotevírat** podezřelé emaily a obzvláště ne jejich přílohy.
- Na emailovou poštu, která se zdá jako spam, **neodpovídat**. V případě, že uživatel odpoví, jenom potvrdí funkčnost své adresy.
- Do počítače připojovat pouze ověřená USB zařízení (je vhodné využít kontrolní stanice umístěné v areálu společnosti)
- Citlivá data, která nejsou určená pro každého, je vhodné zašifrovat a mít je archivované pouze v šifrované podobě.
- Instalaci programů a aplikací přenechat na odborných IT pracovnících.

5 Účinnost

Tento vnitřní předpis nabývá účinnosti dnem ……

V (místo)…… (dne) ……

Podpis a razítko zaměstnavatele: ……

Práva a povinnosti správce systému ve společnosti Saint-Gobain Adfors

Autor: Stanislav Hladík

Obsah

1 Úvod

Informace, know-how a související systémy jsou zásadní prvky pro realizaci činností a úkolů v Saint-Gobain.

V této souvislosti tedy náležitá správa dat a zdrojů, které je podporují, přenášejí a zpracovávají, přispívá přímo k plnění a úspěšnému dokončení těchto úkolů a činností. Pracovníci, kteří mají tuto správu na starosti, obecně označovaní jako „správci IT“, mají rozsáhlá přístupová práva. V textu níže bude termín **správce** označovat jakoukoliv osobu ve smluvním vztahu se společností, které byl svěřen úkol vyžadující práva správce v informačním systému Saint-Gobain Adfors.

V některých případech je nutné, aby správci měli při plnění svých povinností přístup k informacím nebo údajům jiných uživatelů, které jsou jinak považovány za důvěrné. Pravidelně také provádějí úkony, které mohou mít značný dopad: změny mechanismů ochrany, vytváření nebo modifikace uživatelských účtů a souvisejících práv, mazání souborů, přenos dat apod. Jakýkoliv takový úkon může při nesprávném provedení vést k závažným důsledkům, jako je nedostupnost určitých aplikací nebo zrušení, pozměnění či vyzrazení zásadních informací.

Tito pracovníci hrají kvůli svým výsadám a zvláštním pravomocem zásadní roli, vyžadující diskrétnost a diplomacii. Jejich přístup musím být nestranný. Zásahy, které provádějí, nesmí přesáhnout jejich pravomoci, ani být prováděny v jejich vlastní prospěch. Je proto nezbytné stanovit pravidla, která je nutné dodržovat.

Vedoucí IT pracovník musí být na svoji žádost informován o identitě správců IT; může požadovat konzultace k jejich pracovní náplni, oprávněnosti být správcem nebo významným prvkům smlouvy, aby ověřil relevantnost a řádné využití udělených přístupů.

Účelem této listiny je připomenout práva a povinnosti správce v souvislostech jeho odborných činností. Tato listina nemění závazky a úkoly neoddělitelně spojené s prováděním činností správce.

S tímto dokumentem se proto musí seznámit, přijmout jej a podepsat všichni správci.

2 Role správce

Správci mají za úkol zajistit provoz a zabezpečení IT zdrojů společnosti, za které nesou odpovědnost a také úkonů, které se na nich mají provádět.

Mezi tyto zdroje patří:

- Servery
- Zařízení síťové infrastruktury
- Webové služby
- Aplikace, Software
- Databáze
- Uživatelské počítače, pracovní stanice
- Tiskárny
- Kopírky
- Tablety
- Telefonní zařízení

Stejně tak musí být zajištěny i každodenní činnosti správy související s jejich úkoly (konfigurace, kontrola, údržba, aktualizace, podpora apod.). Správci mají ve vztahu ke zdrojům, za které nesou odpovědnost, významná práva.

Disponování těmito právy s sebou nese velkou odpovědnost za jejich uplatňování. Jakékoli nenáležité, nesprávné zneužití pravidel stanovených v této listině, může mít závažný dopad na informační systémy. Správce se proto zavazuje tato svoje práva neporušit a uplatňovat je náležitým způsobem.

Zejména zakázány jsou činnosti:

- **Nahlížet do dat obsažených ve zdrojích, za které nesou odpovědnost** (důvěrné, soukromé, odborné, nebo osobní údaje).
- **Provádět úkony, které mohou být potenciálně nebezpečné** pro zabezpečení informačního systému

Správci mají klíčovou roli, která je založená na důvěře. Proto je nutné zavést do praxe předpisy, které se zavazují respektovat.

3 Práva správce

Správci mají právo přijmout jakákoliv nezbytná opatření v rozsahu své působnosti, která povedou k řádnému plnění jejich úkolů, za předpokladu, že budou dodržovat platné zákony, zásady a bezpečnostní pravidla společnosti Saint-Gobain Adfors a zajistí řádný chod, údržbu zdrojů a zabezpečení informačních systémů.

Zejména jejich práva jsou:

- Nakládat s uživatelskými účty, vybavením, síťovými službami, skupinami a souhlasy (vytváření, deaktivace, členství v AD skupinách, obnovení hesla, zásady skupiny, DS spojení atd.).
- Provádět technické kontroly souborů nebo databází, systémových emailů, připojení k internetu, aby zajistili jakýkoliv bezpečnostní incident, který by mohl ohrozit řádné fungování a bezpečnost informačních systémů, přičemž musí dodržovat podmínky „Práv a povinností správce“ při využívání počítačových zdrojů a komunikačních sítí.
- Zpracovat (zjistit, analyzovat, zakázat …) jakoukoli operaci nebo přístup do počítače, který by mohl způsobit bezpečnostní riziko (např. použití zakázaného softwaru, prohlížení potenciálně škodlivých webových stránek atd.) .
- Kontrolovat správné využití licence k používanému softwaru a IT nástrojům.

4 Povinnosti správce

Správci jsou povinni zachovávat mlčenlivost v souvislosti se svými činnostmi, a proto:

- By měli číst data v informačních systémech nebo k nim udělovat přístup, pouze pokud jsou předmětem výslovné žádosti jejich vlastníka a v rámci zavedeného postupu nebo ve specifických případech stanovených zákonem.
- Nesmí si prohlížet údaje, ke kterým mají přístup z titulu jejich pracovních výsad (identifikátory, citlivé informace o uživateli atd.), a přístup k nim neumožní druhým osobám, kromě výjimečných případů (oficiální souhlas uživatele nebo zvláštní případy zohledněné zákonem) nebo s oficiálním povolením vydaných od subjektů těchto informací.
- Musí dodržovat svoji povinnost zachovat mlčenlivost. Nesdělí ani nepoužijí žádné informace, o kterých se mohli dozvědět v průběhu plnění svého úkolu. Použití dat z informačních systémů je možné pouze s výslovným souhlasem vlastníka dané informace a potvrzením managementu správce.
- Bez výslovného souhlasu osoby, které byl určitý zdroj přidělen, nesmí k takovému zdroji přistupovat, a to ani do pracovních stanic daného uživatele s využitím softwaru pro vzdálený přístup.

Jakýkoliv přístup do zdrojů informačních systémů musí být **časově omezen na nezbytnou dobu pro požadovaný úkol.** Správci jsou navíc striktně podřízeni bezpečnostním pravidlům a omezením stanoveným v rámci jejich úkolu.

- Proto tedy nesmí zneužívat výsadní práva, jež jim byla svěřena, musí respektovat práva třetích stran (soukromí, duševní vlastnictví třetích stran atd.) a své činnosti omezí na zdroje IT, které spadají do jejich působnosti, a to tak, že se budou držet cílů, ke kterým směřují jejich úkoly. Zejména konfigurace a přístupová práva lze měnit pouze v souladu s administrativním protokolem nebo postupem.
- Nebudou se řídit žádnými pokyny vydanými neznámou osobou, budou muset informovat svého nadřízeného a bezpečnostní tým o jakémkoliv požadavku, který se zdá nepatřičný.
- Jakýkoliv požadavek zahrnující přístup k osobním údajům nebo jejich sdělení musí být správci předložen písemnou formou z důvodu zpětné dohledatelnosti.
- Správci nesmějí obcházet žádné bezpečnostní postupy, nesmějí deaktivovat mechanismy zpětné dohledatelnosti. Správci jsou odpovědní za sledování a

zajištění aplikace pravidel kybernetické bezpečnosti. Například přístup na internet ze serveru je zakázán.

- Správce musí kontrolovat a zajišťovat uplatňování standardů firmy Saint-Gobain Adfors.

V případě bezpečnostního incidentu:

- Musí informovat svého přímého nadřízeného a bezpečnostní tým, který je odpovědný za řízení bezpečnostních incidentů, o jakémkoli narušení bezpečnosti, který zjistí nebo o kterém se dozví, a to hned poté, co se o nich dozvěděli.
- Musí uchovávat protokoly z auditu nezbytné ke zvládnutí incidentu a k jakémukoli budoucímu šetření v návaznosti na postup, který zajistí, aby si tyto prvky zachovaly svoji průkazní povahu.

Správci **zajistí ochranu výsadních práv** spojených se svojí pozicí:

- Budou dodržovat postupy nastavené pro správu relací a zvláštní pozornost budou věnovat ochraně pracovní stanice používané ke správě.
- Budou dodržovat platné bezpečnostní předpisy vytvořené za účelem ochrany používání výsadních práv, které jim byly uděleny, včetně následujících pravidel:
    - Automaticky změní výchozí účet a hesla použitá při konfigurování sytému.
    - Dodrží pravidla výběru hesel (délka, kombinace písmen a číslic, složitost) a pravidelně hesla mění.
    - Hesla nikdy nesdílí.
    - Používá účty s výsadním přístupem ke svým činnostem a potřebám přímo souvisejícím s úkoly správy nebo provozu, za kterou nese odpovědnost.
    - Seznam správců musí být omezen na minimální počet osob a musí procházet pravidelnou revizí.

5 Kontroly a sankce

Správci se zavazují, že budou dodržovat zákony a pravidla stanovená a platná v rámci společnosti Saint-Gobain Adfors při využívání počítačových zdrojů a komunikačních sítí.

Jakýkoliv úkon provedený v rámci informačních systémů se musí zaznamenat do protokolu takovým způsobem, aby bylo možné identifikovat uživatele, který danou operaci provádí. Kromě toho se také mohou provádět příležitostné kontroly za účelem revize úkonů provedených správci.

Pokud se zjistí, že správce tuto politiku nedodržel, společnost může použít disciplinární sankce odpovídající závažnosti daného úkonu nebo jakékoli jiné sankce definované v jeho smlouvě.

Pokud se prokáže, že správce porušil příslušné zákony, bude daná osoba za své konání odpovědná, bude podléhat občanskoprávnímu nebo trestněprávnímu postihu stanovenému zákonem.

6 Prodloužená povinnost

Povinnosti správce postupovat obezřetně a zachovávat mlčenlivost zůstávají v platnosti i po odebrání administrativních práv, ať už k takovému odebrání došlo z důvodu změny úkolu nebo na základě ukončení či vypršení smlouvy mezi společností a správcem.

Od této povinnosti může být upuštěno, pokud se daná data stala veřejně známými nebo pokud byla předem zavřena písemná dohoda se společností.

7 Závazek správce

Níže podepsaný, ……, tímto jako správce informačních systémů prohlašuji, že jsem si „Práva a povinnosti správce systému Saint-Gobain Adfors“ přečetl a zavazuji se je dodržovat. Zavazuji se postupovat s naprostou obezřetností a zcela zachovávat profesní tajemství, zejména pokud jde o veškeré údaje, dokumenty a soubory, o kterých se dozvím při výkonu svých povinností s ohledem na jakýkoli externí, nebo interní subjekt.

V (místo)…… (dne) ……

Podpis: ……

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání diplomové práce

Autor: **Bc. Stanislav Hladík**

Studium: I1900347

Studijní program: N0688A140001 Informační management

Studijní obor: Informační management

Název diplomové práce: **Implementace opatření kybernetické bezpečnosti do firemní konvergované sítě**

Název diplomové práce AJ: Implementing cybersecurity measures into a corporate converged network

Cíl, metody, literatura, předpoklady:

Obsahem práce je zhodnotit možná rizika kompromitace firemních sítí, nalézt vhodná řešení a navrhnout postup implementace do infrastruktury konvergované firemní sítě.

Osnova diplomové práce:

1) Úvod

2) Princip fungování sítí

3) Rešerše a hdonocení rizik kompromitace sítí

4) Vhodná řešení bezpečnostních problémů

5) Návrh implementací

6) Řešení vhodné pro firemní síť Adfors a K2 Mechatronics

7) Implementace řešení

8) Shrnutí

9) Závěr

1) Stephen John Bigelow, Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. Brno: Computer Press, 2004. ISBN 80-251-0178-9.

2) Milan Berka, Bezpečná počítačová síť: správa, konfigurace, diagnostika a řešení problémů. Praha: Dashöfer, 2009. ISBN 80-862-2979-3.

3) Todd Lamle, CCNA: výukový průvodce přípravou na zkoušku 640-802. Brno: Computer Press, 2010. ISBN 978-80-251-2359-1.

4) Rita Pužmanová, Bezpečnost bezdrátové komunikace. Brno: Computer Press, 2005. EAN: 9788025107911

5) Lee Barken, Jak zabezpečit bezdrátovou síť Wi-Fi. Brno: Computer Press, 2005. EAN: 9788025103463

6) Brandon James Carroll, Bezdrátové sítě Cisco. Brno: Computer Press, 2005. EAN: 9788025128848

Garantující pracoviště: Katedra informačních technologií, Fakulta informatiky a managementu

Vedoucí práce: Ing. Pavel Blažek, Ph.D.

Datum zadání závěrečné práce: 15.9.2020