Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Bezpečnost počítačových sítí

Bc. Maximilian Chilcenco

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Maximilian Chilcenco

Informatika

Název práce

Bezpečnost počítačových sítí

Název anglicky

Computer network security

Cíle práce

Diplomová práce je tematicky zaměřena na užití bezpečnostních technologií v počítačových sítích ve vnitropodnikové infrastruktuře. Hlavním cílem je uvést a zhodnotit tyto technologie, definovat a představit budoucí trendy a následně demonstrovat samotné nasazení technologie do vybraného podniku.

Dílčí cíle:
- Definice pojmu počítačová síť
- Klasifikace zabezpečovacích technik a metod
- Aktivní síťové prvky – přehled a parametry
- Kybernetické útoky – klasifikace a charakteristika
- Implementace a konfigurace vybrané technologie
- Závěry a doporučení

Metodika

Při zpracování teoretické části bude vycházeno z odborné literatury, internetových zdrojů a vlastních zkušeností autora. Užitá metodika při zpracování bude především analýza, syntéza a studium dané problematiky.

V praktické časti bude realizován vlastní návrh řešení, který bude danou problematiku demonstrovat. Bude se jednat o implementaci, konfiguraci a následnou správu vybrané bezpečnostní technologii sítě, která bude působit ve vnitropodnikovém prostředí. Samotné vyhodnocení teoretické a praktické části řešení problematiky diplomové práce je shrnuto v závěru a doporučení.

Doporučený rozsah práce

50-60 stran

Klíčová slova

síť, router, switch, firewall, protokol, malware, SSH, bezpečnostní technologie

---

Doporučené zdroje informací

BEJTLICH, Richard. The practice of network security monitoring: understanding incident detection and response. San Francisco: No Starch Press, 2013. ISBN 978-159-3275-099.

CARTHERN, Chris, William WILSON, Richard BEDWELL a Noel RIVERA. Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA, 2015. ISBN 0306465604.

DARAS, Nicholas J. Computation, Cryptography, and Network security. New York, NY: Springer Science Business Media, 2015. ISBN 978-331-9182-742.

MCMILLAN, T. – EBRARY, INC. *Cisco networking essentials : e-book*. Indianapolis, Ind.: John Wiley & Sons, Inc., 2012. ISBN 978-1-118-09759-5.

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

doc. Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 31. 5. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 28. 11. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 28. 03. 2023

Čestné prohlášení

Prohlašuji, že svou diplomovou práci Bezpečnost počítačových sítí jsem vypracoval(a) samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor(ka) uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31.03.2023 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Jiřímu Vaňkovi, Ph.D., za odborné připomínky a rady při vedení diplomové práce. Zároveň bych rád poděkoval Ministerstvu spravedlnosti České republiky, které mi poskytlo materiály a potřebné zdroje k vypracování této práce.

Bezpečnost počítačových sítí

Abstrakt

Hlavním úkolem diplomové práce je pojednat o bezpečnosti počítačových sítí, představit klady a zápory této technologie, následně demonstrovat vlastní návrh řešení pomocí virtualizačního nástroje VMware. Diplomová práce pojednává o hlavním principu fungování technologie, zmiňuje možné druhy kybernetických útoků, demonstruje práci s reálnými produkty z praxe a odborné konfigurační postupy. Na základě cenové kalkulace lze vyhodnotit počáteční náklady na zavedení bezpečnostních síťových technologií do podniku.

Klíčová slova: síť, router, switch, firewall, protokol, malware, SSH, bezpečnostní technologie

Computer network security

Abstract

The main goal of the master thesis is to discuss the security of computer networks, presents pros and cons of this technology and demonstrates the own solution using virtualization tool called VMware. The master thesis discusses the main principle of the technology, mentions possible types of cyber attacks, demonstrates work with real products from the practise and professional configuration procedures. Based on the price calculation, it is possible to evaluate the initial costs of network security technologies into the company.

Keywords: network, router, switch, firewall, protocol, malware, SSH, security technology

Obsah

1. Úvod

Pomalu ale jistě se lidstvo přesouvá do digitálního prostředí. Veškeré naše aktivity, data, osobní informace, podnikové informace a další cenná aktiva jsou ukládaná alespoň z části na internetu. Každý den můžeme spatřit nová zařízení, která jsou postupně připojována do světové globální sítě. S tímto faktem je i úzce spjatý termín zabezpečení sítě a kybernetická bezpečnost.

S rozvojem sítových technologií přichází i rozvoj digitální kriminality. Útočníci často míří po velkých organizacích, kdy je láka vidina zisk ve formě výkupného či prodeje ukradených citlivých informací. Neodmítnou ale ani data běžného uživatele. I když je tato tématika velmi populární, stále existují podniky a organizace, kteří nedbají na bezpečnostní protokoly a postupy. Organizace neinvestují dostatečné finanční prostředky do kybernetického odvětví. O to větším rizikům organizace čelí, pokud se s podobnou situací setká a je nucena zaplatit výkupné útočníkovi. V praxi také nazývané jako ransom.

Nemusí dojít ani k odcizení dat, aby taková událost měla pro firmu fatální následky. Často stačí jen dočasné vyřazení služby, třeba ve formě útoku DoS či DDoS. Nefunkční služba je pro podnik finančním nákladem, ušlým ziskem a také vizitka pro konkurenci a stále klienty.

Diplomová práce má za úkol pojednat o sítové technologii jako takové, definovat síťové modely, topologie sítí a představit druhy zabezpečení v sítích. V další částech diplomové práce budou představeny nejčastější typy sítových útoků, typy útočníků a jak se proti takovým útokům bránit. Nesmíme zapomínat, že útočníci se nenacházejí jen z vnější strany podniku, ale i v samotné organizaci. Například ve formě naštvaných zaměstnanců, kteří by rádi dané organizaci uškodili před odchodem ze zaměstnání.

V praktické části bude demonstrován vlastní návrh řešení. K demonstraci bude použit testovací model, který bude vytvořen, nakonfigurován a zabezpečen pomocí speciálních bezpečnostních postupů. Výsledná konfigurace a bezpečnost modelu bude otestována pomocí speciálního nástroje pro skenování zranitelností. Veškeré konfigurace a metodologické postupy použité v praktické části jsou převzaté z takzvaných best practise využívané v praxi.

2. Cíl práce a metodika

2.1. Cíl práce

Diplomová práce je tematicky zaměřena na užití bezpečnostních technologií v počítačových sítích ve vnitropodnikové infrastruktuře. Hlavním cílem je uvést a zhodnotit tyto technologie, definovat a představit trendy a následně demonstrovat samotné nasazení technologie do vybraného podniku.

Dílčí cíle:

- Definice pojmu počítačová síť
- Klasifikace zabezpečovacích technik a metod
- Aktivní síťové prvky – přehled a parametry
- Kybernetické útoky – klasifikace a charakteristika
- Implementace a konfigurace vybrané technologie
- Závěry a doporučení

2.2. Metodika

Při zpracování teoretické části bude vycházeno z odborné literatury, internetových zdrojů a vlastních zkušeností autora. Za pomocí analýzy, syntézy a studiu dané problematiky.

V praktické časti bude realizován vlastní návrh řešení, který bude danou problematiku demonstrovat. Následuje vytvoření virtuálního stroje a jeho konfigurace při použití softwaru VMware. Samotné vyhodnocení teoretické a praktické části řešení problematiky diplomové práce je shrnuto v závěru a doporučení.

3. Teoretická východiska

3.1. Počítačová síť

Jedná se o technologii propojující aktivní a pasivní prvky, kterým umožnuje mezi sebou komunikovat nebo sdílet data. Prvek v počítačové sítí nemusí být jen osobní počítač či notebook. Může se jednat o jakékoliv zařízení, které bude v sítí figurovat. Tuto technologii nazýváme Ethernet. K zajištění správného fungování této technologie se v praxi využívat protokol pod jménem TCP / IP. (5)

V síti rozdělujeme prvky na aktivní a pasivní, dle jejich vlastností.

Aktivní prvky v síti aktivně pracují s datovým signálem. To znamená, že ho například přijímají, zpracovávají, opravují a posílají dál. Typickým příkladem aktivního prvku v sítí může být router, switch, fyzický firewall.

Pasivní prvky signál jen přenášejí, nedochází zde k žádným úpravám či modifikacím. Příkladem pasivního síťového prvku jsou metalické či optické kabely nebo konektory. (5)(6)

3.2. Počátky počítačové sítě

Počátky počítačové sítě sahají do 60 let 19. století. Přesněji se jedná o rok 1964, kdy americká společnost RAND Corporation dostává od vlády USA za úkol vytvořit síť, která by byla odolná proti výpadkům některých síťovích uzlů.

Organizace RAND přichází s vlastním řešením. Navrhla tyto body:

- Síť bude decentralizovaná. Nebude žádný centrální bod, který by komunikaci řídil
- Síť bude i nadále fungovat po výpadku jednoho z uzlů

Dostáváme se k otázce, jak budou data pomocí této sítě přenášena. Přichází nový způsob přenášení dat, označován jako přepojovaní paketů. Tento nový přenos dělí přenášená data na malé celky označovány jako pakety. Paket disponuje příslušnou hlavičkou s informacemi. Například adresou odesílatele nebo příjemce.

Roku 1969 vzniká americká společnost ARPA, která je pod částečným vedením ministerstva obrany USA. Tato společnost přichází se svým řešením. Vzniká první síť pojmenovaná jako ARPANET. Síť měla prozatím 4 uzly, které spojovaly americké univerzity. Hlavním úkolem vytvořené sítě bylo ověřit funkčnost přepojování paketů. To se jí daří a postupem času se začínají připojovat nové uzly do ARPANET sítě.

Roku 1972 síť ARPANET disponuje 37 uzly. O rok později se připojují i zahraniční velmoci jako Norsko a Velká Británie. [5][6]

V roce 1886 dochází k zavedení a plné podpoře protokolu TCP/IP.

Vznikají nové druhy obchodních příležitostí. Rozrůstá se i komerční trh v tomto odvětví. Každým rokem přibývaly nové sítě, které byly následně zapojovány do sebe, aby tvořily jeden celek. V roce 2004 sít nazývaná jako internet disponuje přes 10 000 000 milionu uživatel.

V roce 2005 firmy přicházejí s cloudovým řešením. Sdílení a uchování dat nabírá zcela jiný směr.

Dnes je internet již nepostradatelnou součástí lidského života. Díky internetu máme přístup k informacím potřebné pro běžný život. Navzdory všech přínosu tato technologie přinesla i zápory ve formě zdravotních či dušeních poruch a nárust stresu v běžném životě člověka. [5][6]

3.3. Referenční model ISO/OSI

Model představuje počítačovou síť z teoretického hlediska. Komunikační princip v síti rozděluje na 7 vrstev. Následně tyto vrstvy popisuje a vysvětluje spolupráci mezi nimi. Hlavním úkolem modelu je standardizování počítačových sítí. V roce 1984 byl model přijat jako mezinárodní normu společností ISO, pod označením ISO 7498. [8][9]

Jak již bylo zmíněno, tento model obsahuje 7 vrstev. Jedná se o vrstvy: fyzickou, linkovou, síťovou, transportní, relační, prezentační a aplikační. Každá z vrstev má svoji úlohu. Počátek přenosu začíná v aplikační vrstvě a končí ve fyzické. První tři vrstvy ISO modelů obstarávají přenos dat. Řeší problém, jakým způsobem budou data přeneseny

příjemci. Poslední tři vrstvy mají za úkol obstarávat komunikaci mezi aplikacemi a definovat, jaká data budou přenášena. Transportní vrstva funguje jako spojovací prvek mezi těmito vrstvami. (8)(9)

Fyzická vrstva – Zajišťuje přenos dat ve formě bitů mezi příjemcem a odesílatelem. Tuto vrstvu můžeme přiřadit spíše k elektrotechnické části, tak jak obstarává především přenášení dat po fyzikální stránce. To znamená, pod jakým napětím budou přenášena data ve formě nul a jedniček za pomocí elektrických signálů. Fyzická vrstva definuje, jak dlouho bude vysílán jeden signál, jaký kabel nebo typ konektoru je zapotřebí použít. (8)(9)

Linková vrstva – Zatím co fyzická vrstva definuje jen přenosovou cestu. Linková vrstva zajišťuje, aby data byla seskupena do jednotlivých datových bloků, nazývané jako rámce. Tyto rámce jsou definovány právě linkovou vrstvou. Dochází zde k definování počátku a konce datového bloku. Linková vrstva řídí samotné zahájení komunikace, průběh i ukončení.

Právě na linkové vrstvě lze spatřit MAC adresaci. Jedná se o adresování zařízení pomocí speciálních adres. Při komunikaci na přenosové cestě může docházet k různým poruchám či rušením. Tento fakt může být důsledkem ztráty přenášených bitů. Linková vrstva má za úkol narušené bity detekovat, opravit a následně znovu odeslat příjemci již v opravené formě a s původním obsahem. (8)(9)

Síťová vrstva – Jak bylo uvedeno u předešlé vrstvy, linková vrstva dokáže přenášet data jenom mezi odesílatelem a příjemce, kteří se nachází na stejném datové lince. Pokud by se příjemce nacházel v jiném uzlu, linková vrstva by tuto komunikaci již obstarat nedokázala. Přichází proto síťová vrstva s IP adresací. Jedná se o identifikaci síťového rozhraní uvnitř sítě. Přenášené rámce se mění v této vrstvě na pakety. Nejkratší přenosovou cestu obstarává router s takzvaným routingem neboli směrováním. (8)(9)

Transportní vrstva – V této vrstvě se již nebude pracovat s pakety, ale segmenty. Hlavním úkolem transportní vrstvy je přenášené pakety zapouzdřit do segmentů, které jsou následně odesílány. Po úspěšném přenosu jsou data ze segmentů rozbalena. Velkou novinkou na této vrstvě je užití portů. Porty se v síťových technologiích užívají k rozlišení aktivních služeb

fungujících v jednom datovém uzlu. Hlavní protokoly, které najdeme na transportní vrstvě jsou TCP a UDP.

TCP – Spojovaný, spolehlivý. Čeká vždy na potvrzení při zahájení vysílání a při doručení. Tento protokol je velmi spolehlivý, avšak díky neustálému čekání na potvrzení je poměrně pomalý. (10)(11)

UDP – Nespojovaný, nespolehlivý. Na žádné potvrzení nečeká a rovnou vysílá. UDP nedisponuje garancí úspěšného přenosu dat. Protokol je nespolehlivý, avšak o dost rychlejší než TCP. Aplikace si sama vybírá, jaký z těchto dvou protokolů použije. (10)(11)

Relační vrstva – Jak již název napovídá, tato vrstva má na starosti vytváření, udržování, řízení a ukončování relací mezi účastníky přenosu. Veškerá komunikace mezi těmito uzly probíhá skrz relace. (8)(9)

Prezentační vrstva – Data, která jsou přenášená v sítí mohou mít mnoho podob. Aby byla nastavená norma pro universální komunikaci, byla vytvořená prezentační vrstva. Vrstva má za úkol převádět, formátovat, šifrovat či dešifrovat přenášená data na společnou abecedu nebo znakovou sadu. Hlavním cílem je, aby se oba finální uzly dorozuměly. (8)(9)

Aplikační vrstva – Aplikační vrstva vytváří prostředí pro aplikace. Celá aplikace se však v této vrstvě nenachází ale jen její část, které má na starosti komunikaci. Každá aplikace je různorodá, používá jiné mechanismy, využívá jiný programovací jazyk. Část, která má na starosti komunikaci v sítí je sjednocená, právě díky této vrstvě. Jako hlavním příkladem užití aplikační vrstvy lze uvést odesílání elektronické pošty, síťové tiskárny nebo vzdálený přístup. (8)(9)

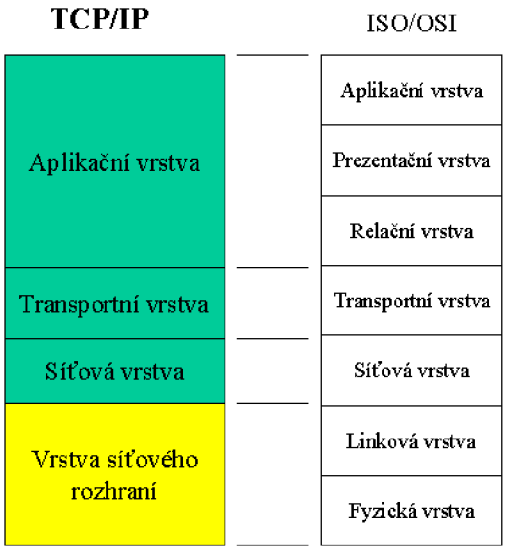
3.4. Model TCP/IP

Předešlý referenční model ISO/OSI se považuje za teoretický model. Společným zájmem bylo o standardizaci síťových technologií při stanovení jednoho obecného modelu. Model TCP/IP vyplývá z praxe a užití v reálném životě. Dnešní síťové technologie jsou postavené na tomto modelu. Typickým příkladem je komunikace počítačů v internetu.

Model TCP/IP na rozdíl od ISO/OSI má jen 4 vrstvy. Jsou to vrstvy: síťového rozhraní, síťová vrstva, transportní a aplikační. Některé vrstvy byly redukovány z důvodu jejich nadbytečného výskytu. Díky tomu mohly být sloučené do jedné vrstvy a tím zjednodušit celkový model. Jedná se o vrstvu fyzickou a linkovou. Tyto vrstvy byly spojeny do vrstvy síťového rozhraní. Vrstva relační, prezentační a aplikační se spojily do jednotné aplikační vrstvy.

TCP/IP pracuje s mnoha protokoly. Proto se jí taky přezdívá rodina protokolů. Mezi tyto protokoly zařazujeme například: IP protokol, IPv4, TCP, UDP, ARP a mnoho dalších.

Celý model je postavený na jednoduchém principu. Ve zkratce protokol TCP má na starosti zapouzdření dat do jednotlivých paketů, obstarává přenos pomocí fyzické vrstvy a následný přenos. IP protokol obstarává adresaci odesílatele a příjemce, vymezení nejlepší cesty pro přenos neboli routing a uskutečnění přenosu dat. Od toho vzniká spojení TCP a IP. (10)(11)



Obrázek 1 – Porovnání TCP/IP a ISO/OSI modelu

Zdroj: https://www.muzeuminternetu.cz/offwebs/archiv/a708s600/a708s684.htm

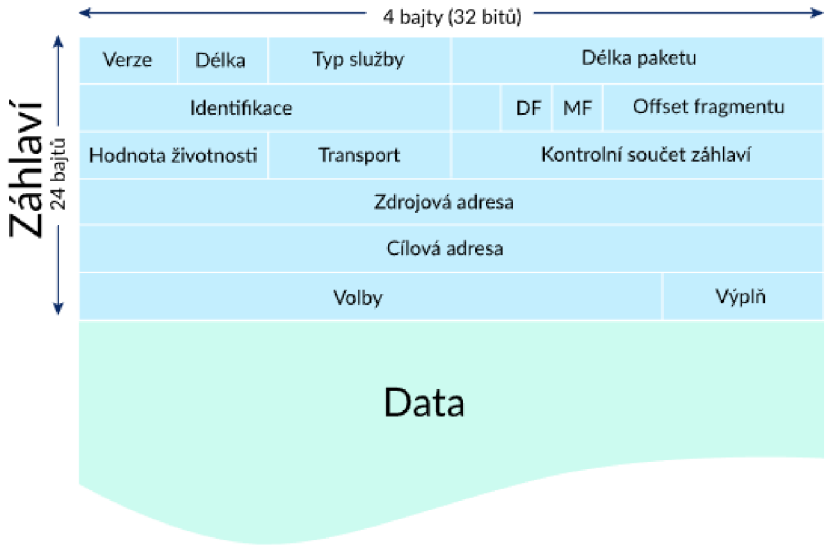
3.4.1. Paket

Paket v počítačových síti reprezentuje blok dat, který je pomocí sítí přenášen. Základní způsob přenášení paketů v sítích stojí na principu přepojování paketů. Tento princip můžeme najít jak u modelu TCP/IP tak i ISO/OSI. (12)

Kdyby data putovala samovolně v sítích, byl by v tom jasný nepořádek. Aplikace by nedokázaly rozeznat jaká data jsou pro nich, která má zahodit a které zase přeposlat dál. Struktura paketů je jasně daná. Obsahuje základní atributy v hlavičce jako například adresa odesílatele či adresáta, o jakou službu se jedná, a nakonec i samotná data. Podrobné schéma struktury paketu lze vidět na obrázku č. Obrázek 2 – Složení síťového paketu. O doručení paketu se stará router. Pomocí IP adresy uvedené v hlavičce paketu hledá optimální cestu pro doručení. (12)

Aby nedošlo k nekonečné smyčce odesílání paketů v sítí, například kvůli zadání špatné adresy příjemce, byl vyvinut atribut TTL – Time to live. Tato hodnota se vždy snižuje o jednotku, pokud paket projde routerem. Pokud TTL vyprší, aniž by byl paket doručen majiteli, paket se jednoduše zahodí, aby nedocházelo k zahlcovaní sítě.

Hlavička paketu obsahuje paritní bit sloužící pro výpočet nebo detekci narušených dat v průběhu přenosu. (13)(14)



Obrázek 2 – Složení síťového paketu

Zdroj: https://cs.khanacademy.org/computing/informatika-pocitace-a-internet/x8887af37e7f1189a:internet/x8887af37e7f1189a:ip-adresy/a/ip-packets

3.4.2. IP Adresa

Jedná se o logické adresování síťových zařízeních v sítích, pomocí protokolu IP. Typická IP adresa v protokolu IPv4 dosahuje maximální velikosti 32 bitů. IP adresa obsahuje 4 oktety, které jsou od sebe oddělené tečkou. Tyto oktety mohou nabývat hodnot 0 až po 255. Adresy jsou vyjádřeny pomocí desítkové a šestnáctkového soustavy, avšak některé složitější technické výpočty používají dvojkovou soustavu. Dochází tedy k převádění adres mezi soustavami. (12)

Adresy dělíme na veřejné a privátní. Zpočátku celý princip byl založený jen na veřejných adresách. Protokol IPv4 disponuje maximálně 2^{32} počtem adres, tedy 4 294 967 296. Postupem času a vývojem síťových technologií razantně přibývali uživatelé a síťová zařízení. Nastala situace, kdy si lidé začali uvědomovat nedostatek veřejných IPv4 adres.

Přichází rozdělení na veřejné a privátní sítě. Kupříkladu celá organizace komunikuje mezi sebou v LAN síti pomocí vnitřních IP adres. Pokud komunikace bude směřována ven do internetu, všechny tyto požadavky budou registrovány pod jednou IP adresou. (14)(15)

IP adresa disponuje dvěma částmi. Adresa zařízení nebo uzlu v síti a takzvaný prefix, který identifikuje, o jakou síť se jedná. Samotný prefix lze vyjádřit pomocí síťové masky. Maska sítě slouží k rozeznání, jaká část adresy slouží pro podsíť a která naopak vyjadřuje samotný uzel. Maska sítě udává velikost sítě.

Názorným příkladem IP adresy s maskou je 192.168.10.1/24, kdy se jedná o adresu 192.168.10.1 s maskou 24 neboli 255.255.255.0. (14)(15)

3.5. Síťové prvky

Již bylo pojednáno o sítích jako takových, je na čase zmínit jejich prvky. V počítačových sítích mezi sebou komunikují různí účastnici. Komunikace probíhá přes přenosová média při dodržování určitých pravidel pro přenos a protokolů. Lze definovat dvě skupiny prvků v sítích. Jedná se o aktivní a pasivní prvky. Jejich dělení a vysvětlení následuje níže. (16)

3.5.1. Aktivní síťové prvky

Jak již samotný název napovídá, jedná se o prvky, které jsou svojí povahou nebo vlastnostmi aktivní. Prvky se aktivně podílí na komunikaci v sítích. Tyto činnosti mohou být například odesílání či přijímaní signálu, jeho oprava či modifikace. Mezi aktivní síťové prvky lze zařadit router, repeater, hub, switch nebo síťovou kartu.

3.5.2. Pasivní síťové prvky

Pasivní síťové prvky se signálem nijak nepracují. Jednoduše ho přenáší. Nedochází k žádnému generování či modifikaci signálu. Jedná se o prostředníky, kteří tvoří přenosovou cestu. Patří sem přenosová media nebo konektory.

Všechna přenosová media nejsou stejná. Liší se například svojí přenosovou rychlosti, typem kabelu či technologií. Nejběžnější přenosová média v sítích jsou kabely typu kroucené dvojlinky, koaxiální kabely, optická vlákna či konektory. Nejpoužívanější typ konektoru je RJ-45. [16]

Obrázek 3 – Pasivní prvky, druhy konektorů

Zdroj: http://ijs2.8u.cz/index.php?option=com_content&view=article&id=19&Itemid=124

3.6. Topologie sítí

Efektivita využití počítačových sítí spočívá především na jakém typu neboli topologii bude síť provozována. Pod pojmem topologie počítačových sítí rozumíme uspořádání síťových prvků v síti a druh zapojení. Komunikaci v topologii zajišťuje fyzická vrstva. [17][18]

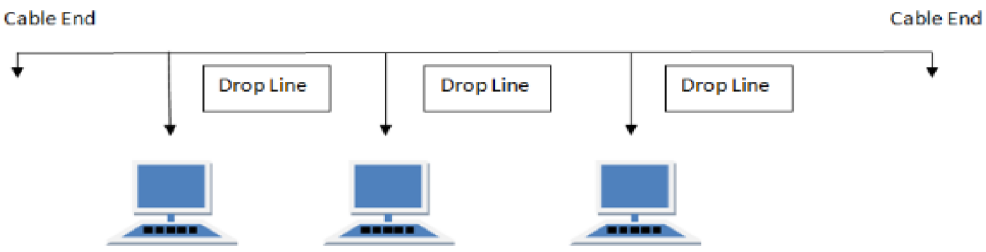
Mezi základní topologie sítí patří:

- Sběrnicová topologie
- Kruhová topologie
- Hvězdicová topologie
- Stromová topologie
- Mesh topologie
- Point to point

Sběrnicová topologie neboli také nazývaná jako BUS**,** je tvořena jednou páteřní linkou. Pomocí odbočovačů se připojují ostatní síťové prvky. Aby nedošlo ke zpětnému odesílání signálu na koncích odboček jsou zabudovány takzvané terminátory. Počáteční signál je odesílán na začátku páteřní linky. Signál přijímají všichni účastníci komunikace. Jen adresovaný příjemce tento signál zpracovává.

Výhody sběrnicové topologie jsou nízké náklady na zřízení a provoz. Využívá se zde koaxiální kabel. Ideální řešení pro malé a dočasné sítě.

Nevýhodou je naopak počet stanic, které mohou být do sítě připojeny. Malá přenosová rychlost a závislost připojení na páteřní síti. [17][18]



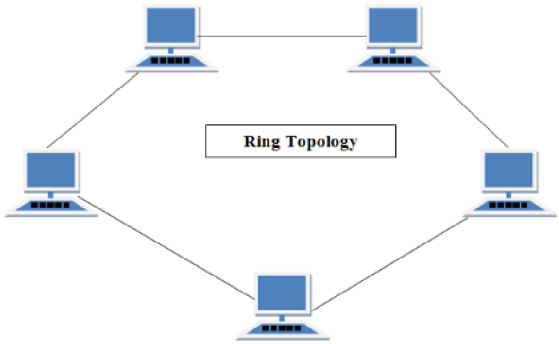
Obrázek 4 – Sběrnicová topologie sítě

Zdroj: https://www.educba.com/types-of-network-topology/

Kruhová topologie, jak již název napovídá, má tvar kruhové zapojení. Prvky v sítí jsou mezi sebou propojeny do tvaru uzavřeného kruhu. Signál i v této topologii projde všemi účastníky stojící po cestě, ale jen adresát signál přijímá. Všechny prvky figurujících v síti zaujímají funkci repeaturu, také nazývaný jako opakovač. Účastnící komunikace signál přijmou, opraví a odešlou již opravený cílové stanici. Tato topologie může nabývat větších rozměrů než sběrnicová topologie.

Hlavním výhodou kruhové topologie je oprava a zesílení odesílaného signálu. Není zapotřebí užití terminátorů a data vždy putují jen jedním směrem, tudíž i menší šance na kolize.

Nesmí se opomenout tvar zapojení. Pokud vypadne alespoň jeden prvek v topologii, vypadne celá síť. Dojde k narušení celé komunikace. Opět se potýkáme se zbytečným zahlcením sítě, kdy signál prochází přes všechny účastníky. [17][18]



Obrázek 5 – Kruhová topologie sítě

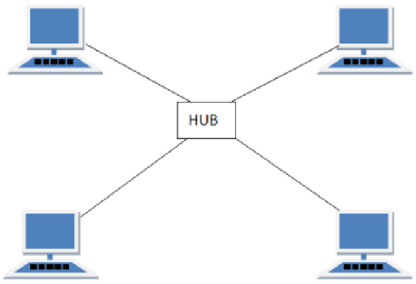
Zdroj: https://www.educba.com/types-of-network-topology/

Hvězdicová topologie po úplném zapojení připomíná tvar hvězdy, od toho je odvozen i její název. Jedná se o topologii s centrální prvkem uprostřed topologie. Ve většině případech se jedná o hub, nebo u novějších sítí switch. Hlavním rozdílem mezi hubem a switchem je tabulka IP adres, kterou switch disponuje. Na základě této tabulky switch dokáže identifikovat v jakém uzlu se nachází odesílatel a příjemce. Odeslanou zprávu odesílá napřímo bez žádných odboček a jen příslušným adresátům. Hub takovou tabulkou nedisponuje. Odeslaný signál putuje na všechny stanice a jen adresát danou zprávu přijímá.

Hlavní vymožeností této topologie je možnost výpadku jednoho z uzlů sítě. Pokud dojde k takovému výpadku, odstaví se jen samotný uzel. Výpadek jednoho uzlu nemá vliv na fungování celkové sítě. To u předešlých topologií neexistovalo. Připojení nových prvků do sítě je zcela jednoduší. Stačí zapojit nový uzel do hubu či switche a je ihned připojen do komunikace.

Výhody této technologie je centrální prvek, který řídí odesílání dat v topologii. Pokud nastane výpadek jednoho z uzlu, celá síť bude fungovat i nadále. Topologie přináší snadnější a dostupnější rozšiřování sítě bez nutnosti odstávky. Zmenšení kolizí, jednoduší identifikaci a opravu chybných uzlů.

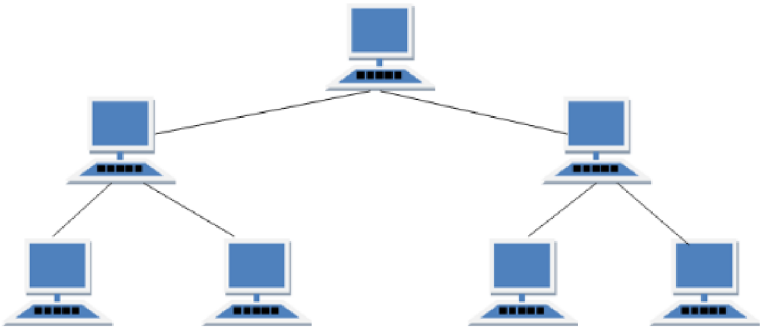
Hlavní nevýhodou je centrální prvek, tak jak je na něm celá topologie postavená. Pokud dojde k výpadku tohoto prvku síť bude nepoužitelná. [17][18]



Obrázek 6 – Hvězdicová topologie sítě

Zdroj: https://www.educba.com/types-of-network-topology/

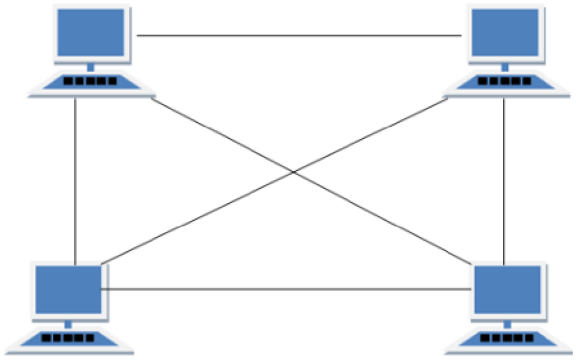
Stromová topologie zaujímá tvar stromu. Jedná se o stejný princip zapojení jako u hvězdicové topologie. Je tvořená více centrálními prvky, tedy huby nebo switchy, kdy jsou vzájemně mezi sebou propojeny. [17][18]



Obrázek 7 – Stromová topologie sítě

Zdroj: https://www.educba.com/types-of-network-topology/

Mesh topologie neboli peer to peer propojení. Každý komunikuje s každým. Užití této technologie je především v menší sítích, pokud není zapotřebí centrálního prvku, který by tok dat řídil. Hlavní výhodou je imunita vůči výpadku. Pokud jeden z uzlů vypadne, data si najdou adresáta pomocí jiné cesty. Velkou nevýhodou zde může být spotřeba kabelů. Může docházet k situaci zbytečného plýtvání kabely a zapojování samého uzlu vícero komunikačními cestami. [17][18]



Obrázek 8 – Mesh topologie sítě

Zdroj: https://www.educba.com/types-of-network-topology/

3.7. Zabezpečení počítačových sítí

Díky rozšiřujícím se sítovým technologiím a sítím docházelo k rozšiřování skupiny uživatelů, kteří tuto technologii užívali na denní bázi. Podniky začaly vnímat sítové prostředí jako příležitost pro svoje produkty. Spolu s nárůstem běžných uživatelů se začali objevovat

i uživatelé s nekalými úmysly, kteří objevili v těchto technologiích slabiny. Tyto slabiny mohly být použity k jejich obohacení. Donedávna tématika sítové bezpečnosti nebyla do takové míry veřejně probíraná. Podniky a uživatelé si mysleli, že jejich data putující skrz internet jsou v bezpečí.

Začaly vznikat různé organizace a sdružení s návrhem pro sjednocení bezpečnostních pravidel a metod, které by zefektivnily obranu vůči kybernetickým útokům. Docházelo k sjednocování standard, protokolů a globálních bezpečnostních pravidel. Vzniká i další odvětví v IT zaměřující se především na IT securitu nazývané cyber security. V dnešní době lze pozorovat velký nárůst právě v tomto odvětví. Především nárust poptávky po odborných specialistech a konzultacích.

Hlavní zabezpečovací zásady a pravidla stanovují vláda daného státu ve spolupráci s příslušnými úřady a specialisty. Tyto zásady a pravidla mohou být v podnicích doplněná o interní dodatky, které by měly být na pracovišti dodržovány. Pro Českou republiku existuje hlavní kontrolní úřad NUKIB – Národní úřad pro kybernetickou a informační bezpečnost, o tomto subjektu bude pojednáno později.

Hlavním důvodem, proč by každý uživatel či podnik měl zabezpečovat své sítě, je unik nebo poškození dat. Může se jednat například o narušení integrity vnitropodnikových dat čili narušení jejich pravosti, ztrátu dat, unik informací a další věci spojené s bezpečnostním rizikem. I když většina útočníků cílí za vidinou zisku, může se v tom skrývat mnohem více. Únik osobních informací může být na pokraji veřejné bezpečnosti. Reagovat na již proběhlé útoky není efektivní. Úkolem kybernetické bezpečnosti, nebo preventivní zabezpečení sítě jako takové, je být vždy o krok před útočníkem. To znamená eliminovat hrozbu ještě před tím, než vůbec vznikla. Proto by podniky a běžní uživatelé neměli ignorovat tento fakt a investovat dostačující prostředky do správných technologií, které zabrání budoucím škodám. [19][20]

3.7.1. Typy útoků

3.7.1.1. Malware

Také nazývaný jako malicious software, v překladu škodlivý virus, je ve většině případech balíček virů, které spolupracují a utočí jednotně. Malware je dnes nejvíce používaným typem útoků, jelikož se může tvářit na první pohled jako úplně jiný typ souboru. Celý princip malwaru spočívá v tom, že si uživatel stáhne, otevře infikovaný soubor nebo klikne na škodlivý odkaz, který ho následně přesměruje na infikovanou stránku. Malware může způsobit ztrátu a krádež dat, udělení přístupu nad napadeným počítačem nebo dokonce se může dál samovolně šířit v síti. Existují různé druhy malwaru, mezi základní typy patří: [21][22]

Ransomware – proniknutí do uživatelského počítače, odepření přístupu k datům, následné zašifrování dat a vydírání výkupného, takzvaného ransomu, ve formě kryptoměn. Útočník slibuje zaslání dešifrovacího klíče po zaplacení. Stává se, že žádný dešifrovací klíč neexistuje. Proto se obecně nedoporučuje platit výkupné útočníkovi. [21][22][23]

Phishing – druhý nejznámější typ malwaru, v překladu rybaření. Jedná se o metodu, kdy útočník nastraží odkaz či celou webovou stránku. Ta se tváří na první pohled jako legitimní. Útočník vytvoří přesnou kopii podvržené stránky. Například se může jednat o světové organizace nebo banky. Následně útočník zašle odkaz na tuto podvrženou webovou stránku, většinou ve formě emailové zprávy. Nic netušící uživatel v domněnce, že se jedná o originální a legitimní stránku se pokusí o přihlášení. Zadá svoje přihlašovací údaje, které se zobrazí útočníkovi. Tento typ malwaru je v poslední době velmi efektivní, jelikož hackerské útoky se neustále vyvíjí a zdokonalují. Útočníci se již nemusí pokoušet o užití hrubé síly při prolomování hesel. Stačí jen chytře vytvořený odkaz či webová stránka. V důsledku nedostačujícího zaškolení uživatele, nebo pracovníka organizace celý úkon provede sám uživatel. Tak jak poskytne útočníkovi všechny potřebné údaje. Více k tomuto tématu se lze dočíst u Sociální inženýrství. [21][22][23]

Trojský kůň – dnes již moc nepoužívaný, ale v blízké minulosti hodně populární. Jednalo se o druh softwaru, který po otevření souboru vytvořil zadní vrátka, takzvaný backdoor, pro útočníka. Ten se mohl pomocí přístupu připojovat na infikovanou stanici bez jediné

zmínky o přítomnosti. Útočníci pomocí tohoto viru zapínali potají webkamery na stanicích, pořizovali fotografie a videa obětí. Následně docházelo k vydírání. (21)

Červ – škodlivý software, který se dokáže sám množit a šířit pomocí počítačových síti. Infikovaní počítače pak dělali vše, co jim útočník nařídil. Dříve se jednalo o zasílání škodlivých emailů všem příjemců v privátních adresářích. Nyní tato metoda již není tak účinná. Proto se tento malware přetvořil v nový účel. Dnes nazývaný jako botnet. (21)

Botnet – stejný princip jako u červů. Samovolné šíření přes počítačové sítě. S velkým rozdílem, že infikovaná stanice neprojevuje žádné znaky ani zmínky hacknutí. Infikovaná stanice vyčkává na správnou chvíli nebo potají těží kryptoměny, kdy vlastník stanice nemusí nic poznat, jelikož zatížení a chování viru je opravdu minimální. Velkým nebezpečím nastává, pokud botnet síť infikovaných počítačů obsahuje přes stovky nebo tisíce stanic. Ty vyčkávají na povel útočníka. Botnet je často spojovaný s DoS a DDoS útoky. Tisíce počítačů z různých IP adres posílají dotaz na jeden určitý cíl. (23)

Adware – jak již z názvu vyplývá jedná se o malware, který způsobuje zobrazování nevyžádané reklamy na hostitelském zařízení. Většinou ve formě neustále vyskakujících reklamních oznámení. (22)

Rootkit – velmi složitě detekovatelný malware. Malware se instaluje přímo do ovladačů zařízení či do samotného Biosu[1]. Tím pádem pokročilé viry dokážou obejít celý operační systém, jelikož se škodlivý kód zavádí pokaždé při startu počítače. Nejednoduší řešení je reinstalace celého počítače. Dnešní Biosy dokážou tyto externí programy detekovat a odstranit. (22)

Spyware – škodlivý malware, který má za úkol sledovat činnosti uživatele. Většinou spojené s následným vydíráním, kdy útočník může sledovat uživatele přes jeho vypnout webkameru, pořizovat fotografie a pak následně oběť vydírat či prodávat tento materiál na Dark Webu[2]. (22)

---

[1] Bios – základní softwarové vybavení počítače.

[2] Skrytá část WWW služby. Běžní prohlížeče nemohou přistupovat k těmto webovým adresám. Je zapotřebí speciální webový prohlížeč pod jménem Tor.

3.7.1.2. SQL Injection

Typ útoku pomocí SQL dotazu. Útočník převážně cílí na server, avšak může útok směřovat i na uživatele. Škodlivý kód je zadán do vyhledávacího pole v prohlížeči. Celý princip spočívá v dotazování serveru pomocí SQL syntaxe. Pokud databázový server nemá ošetřené vstupy právě proti tomuto typu útoku, útočník může pomocí obyčejných příkazů měnit, mazat či číst data z databáze serveru. (21)(22)

3.7.1.3. Sociální inženýrství

Na rozdíl od ostatních typů útoku, kdy útočník vytvoří škodlivý kód nebo jinou přístupovou metodu, aby mohl pokrýt co nejvíce obětí, je sociální inženýrství velmi subjektivním typem útoku. Celý proces začíná vytipováním oběti, následně přichází sbíraní informací o dané osobě z veřejně dostupných informací na internetu či sociálních sítích. Dalším krokem je příprava speciálního scénáře, dle kterého bude v případě útoku postupováno. Jak se říká, představivosti se meze nekladou. Což právě platí u vynalézavosti útočníků v tomto typu útoku. Útočnici neustále přichází s novými metodami a triky, které jsou použity na uživatele.

Pokud má útočník dostatek informací o oběti, stačí na základě spoofingového útoku[3] změnit svoji lokaci či telefonní číslo a postupovat dle daného plánu. Názorným příkladem může být matka tří dětí, která volá bankéři. Bankéř pod tlakem brečících děti a zmatku vyzradí nepatrnou, ale citlivou informaci útočníkovi, který se skrývá v roli beznadějné matky. Díky této informaci útočník je o krok blíže ke svému cíli a může svůj útok opakovat na další oběť, například na další osobu v daném podniku. Tento proces bude opakován tak dlouho, až se útočníkovi podaří získat cenné informace, po kterých touží. (23)

3.7.1.4. Cros-Site Scripting

Cross-Site scripting funguje na podobném principu jako SQL injection. Útočník se v tomto typu útoku zaměřuje především na uživatele. Infikovaný script vloží na svůj web či veřejné fórum. Script zaujímá ve většině případech podobu pop up okna. Uživatel na

[3] Spoofing – zfalšování lokace, telefonního čísla či webové adresy.

na infikovaný objekt interakcí zareaguje a tím se spustí samotný script. Útočník využívá chyb ve webových aplikacích či samotných webech. Tímto útokem lze získat citlivé informace o oběti jako například verze prohlížeče, cookies či jiná nastavení na osobním počítači uživatele. Zjištěné údaje, jako zmíněná verze prohlížeče, lze využít ve spolupráci s malwarem k dalším útokům. [21][22]

3.7.1.5. DoS a DDoS útok

DoS, v celém znění Denial-of-Service neboli odepření služby je jedním z typu hackerských útoků. Cílem útočníka je vyřazení z funkčnosti službu či celou organizaci. Odepření služby může být jako primárním cílem, nebo jako jeden z cílů celkového útoku, kdy po shození přichází další etapy útoku. Celý princip útoku spočívá v zahlcování a přetěžování cíleného subjektu. Subjekt nedokáže ustát nápor příchozích požadavků a jednoduše se zhroutí. Obecně systémy mohou být uvedeny do provozu zpět během několika minut, většinou se jedná o jednotky hodin. Cílená služba bývá po útoku kompletně odstavená.

Útok lze kategorizovat na dvě skupiny. DoS útok většinou pochází z jednoho zdroje. DDoS útok využívá celou síť počítačů zahlcujících jeden cíl. Je zde i úzce spjat malware pod názvem Botnet. Jak již bylo zmíněno, úkolem Botnetu není odstavit jednoho malého uživatele, ale infikovat jeho stroj a vyčkat na lepší příležitost. Tyto infikované stanice se nazývají zombies. Když je vybrán cíl a připraven útok, stovky až tisíce těchto zombies počítačů začnou zahlcovat a odesílat požadavky na jeden cíl. Takový útok zapříčení selhání systému a jeho vyřazení. [21][22][23]

3.7.1.6. Hrubý útok na hesla

Hrubý útok na hesla jako jeden z mála využívá hrubou sílu k dosažení cíle. Útočník za pomocí výkonného stroje s vysokým výpočetním mechanismem zkouší náhodné varianty hesel, až dokud ho takzvaně neprolomí. Opět se může jednat o spolupráci mezi jednotlivými typy útoků, nejčastěji v doprovodu se sociálním inženýrstvím. Útočník nejdříve provede průzkum oběti, zjistí potřebné informace. Kupříkladu jméno domácího mazlíčka, datum narození sourozence atd. Druhou variantou útoku může být čistě namátková. Na internetu lze najít seznamy hesel jak napadených uživatelů či jen prolomených hesel. Tyto seznamy

hesel jsou veřejně dostupné od různých institucí právě k tomu, aby si uživateli ověřili, zdali bylo jejich heslo prolomeno. Další místem, kde se lze s takovým seznamem hesel lze setkat je Dark Web.

Technika a výpočetní výkon, který je použit k útoku jsou velmi výkonné. Kombinace takových strojů dokáže zpracovat několik milionů operací za sekundu. Útočník zkouší všechna možná slovní spojení, kombinace čísel a znaků. Pokud heslo oběti nemá dostatečnou délku a obsahuje jen základní znaky, může se jednat o jednotky sekund, než útočník heslo prolomí. [23]

3.7.2. Typy útočníků

Když byly síťové technologie vytvořeny a celý svět se propojil skrz kabely, nikdo nepomyslel, že takový vynález století bude použit ke kriminálním účelům či k jakémukoliv nezákonnému typu obohacení. Jak se celý internet vyvíjel, vyvíjeli se s ním i uživatelé, kteří byli technicky zdatnější než běžní uživatelé. Slovo hacker neznamenalo vždy jen zápornou osobu, která má za úkol napadnou počítač a uškodit, ba naopak.

3.7.2.1. Hacker

V minulosti se jednalo o technika či programátora, který měl za úkol spravovat sítě a systémy. Hlavní podstata byla nacházení chyb a bezpečnostních rizik v těchto systémech. Následovala jejich oprava. Jak ovšem čas plynul a lidská chamtivost rostla, tyto odbornicí si uvědomili, že díky svým schopnostem mohou získat o mnoho více než ve svém zaměstnání. V ten okamžik se rozdělili technici na dvě skupiny. Na White hat hackera a Black hat hackera. Dnes již evidujeme i Grey hat hackera. [24][25]

White hat hacker – neboli také dnes nazývaný jako etický hacker je osoba, která vykonává svoji činnost zcela korektním způsobem z pohledu zákona. To znamená, že testuje odolnost bezpečnostních zabezpečení jen od systémů, od kterých má povolení. Etičtí hackeři dnes zastupují globálních organizace a nabízejí své služby celosvětově. Může se jednat i o menší podnikatele obsluhující vlastní klientelu. Jak bylo uvedeno, vždy pracují se systémy, ke kterým mají povolení, nebo majitelé o těchto testovacích úkonech vědí. V dnešní době je velmi populární penetrační testování. Společnost najme etického

hackera, který se snaží dostat do vnitropodnikové sítě nebo testuje externí či interní perimetr. Dokonce existují bount programy[4] od velkých společnosti, jako například firma Apple. Za nalezení chyb či bezpečnostních rizik v jejich systému vyplácí až miliony amerických dolarů. (25)

Black hat hacker – jsou osoby, které se snaží napadnou a prolomit systémy organizací nebo uživatelů v důsledku dosažení cenných informací a dat. Velkým rozdílem oproti White hat hackerovi je, že Black hat hackeři se pokouší dostat do systému nezákonně, na základě hrubé síly či jiných nelegálních praktik. Tím pádem k tomu nemají svolení a jejich jednání není v souladu se zákonem. Zde už slovo hacker nabírá klasickou podobu záporné postavy, která se snaží ukrást či zašifrovat data. Následně ve formě kryptoměny vydírat výkupné. (25)

Grey hat hacker – je osoba stojící mezi White hat a Black hat hackerem. To znamená, že svoji činnost nedělá za účelem zisku, ale neprovozuje ani nic legálního. Grey hat hacker zkouší neboli penetruje systémy a aplikace bez svolení majitelů služeb. Na rozdíl od Black hat hackera nemá v úmyslu nikomu uškodit. Tyto osoby berou hackování jako zálibu a výzvu, kdy se rádi zdokonalují ve svém koníčků. Jednoduše po proniknutí do systému zase odcházejí, bez napáchání jakýchkoliv škod. V ojedinělých případech podají anonymní typ na úpravu těchto bezpečnostních rizik na komunitních fórech. (25)

3.7.2.2. Hactivisté

Je skupina hackerů, většinou se jedná o black hat v tom lepším případu i grey hat, kdy primárním cílem těchto útočníků nejsou zisky, ale pozornost a světová známost. Jedná se o organizované skupiny. Tyto skupiny nesdíly myšlenky s aktuálním systémem světových politik. Svým jednáním poukazují na lidské faktory jako lži v politice, korupce a další kriminální jednání, které se dějí běžně ve vysoce postavené společnosti.

Nejznámější skupinou hactivistů jsou Anonymous. Tato skupina grey hat hackerů poukazuje na lidské nedostatky skrz své kybernetické útoky a následném veřejném kárání

[4] Bug bounty program je soutěž pořádaná organizací, která umožní etickým hackerům otestovat zabezpečení jejich systému. Pokud etický hacker nalezne novou potenciální hrozbu v jejich systému či infrastruktuře, měl by dostat peněžní odměnu právě ve formě bounty.

na sociálních sítích. Názorným příkladem je nynější invaze ruského státu na Ukrajinu. Skupina Anonymous pomocí kybernetických útoků na ruské vládní systémy získala citlivá data, která pak publikovala veřejně.

Hactivisté chtějí být viděni a usilují o slávu. Existují tajné společnosti, dokonce skryté skupiny hackerů, které jsou dotované státem. Tyto programy jsou ovšem tajné a veřejnosti nepřístupné. Žádný stát se nepřizná k takovému jednáni, ale existují volně dostupné důkazy či materiály o existenci takovýchto skupin. Stát nasazuje tyto skupiny v případě politických konfliktů. Pokud je zapotřebí přijmout opatření, ale chce prozatím svůj cíl jen varovat a poukázat na svojí moc. (26)

3.7.3. NÚKIB

V plném znění Národní úřad pro kybernetickou a informační bezpečnost je hlavním a kontrolním orgánem pro kybernetickou bezpečnost v České republice. Tento úřad sídlí v Brně. Jeho hlavní činností je dohlížení a zajišťování bezpečnostních opatření v oblasti kybernetické bezpečnosti. Taktéž uděluje tresty za nedodržování těchto postupů, zajištuje vzdělávání v dané oblasti a celkově koordinuje státní orgány v kybernetickém odvětví.

Národní úřad pro kybernetickou a informační bezpečnost monitoruje aktuální hrozby, zavádí včasné opatření a poskytuje konzultace pro napadnuté subjekty. (27)

Obrázek 9 – NÚKIB

Zdroj: https://www.nukib.cz/

3.7.4. Kryptografie a bezpečnostní certifikáty

Kryptografie spadá to vědeckého oboru kryptologie, která spočívá v utajování informací. Kryptologie používá matematické algoritmy k zašifrování a dešifrování utajovaného obsahu. Kryptologii můžeme dále rozdělit na:

Kryptografie – věda zabývající se vytvářením šifrovacích algoritmů a šifrovacích klíčů
Kryptoanalýza – věda zabývající se dešifrováním, odhalení původního zašifrovaného obsahu
Steganografie – věda zabývající se utajováním informací. Nejedná se přímo o šifrovaní, ale o zahalení původní zprávy do náhodného obsahu. Například obrazu, videa či zvukové stopy.

Šifrovat lze dvěma způsoby. Bud se jedná o jednosměrné symetrické šifrování, kdy zašifrovaná zpráva již nejde dešifrovat zpět. Obousměrné šifrování neboli asymetrické šifrování umožnuje utajovanou zprávu, jak zašifrovat, tak i pomocí dešifrovacího klíče zpět rozšifrovat. (45)

3.7.4.1. Symetrické šifrování

Symetrické šifrování se využívá u utajovaných informací. Původní hodnota není podstatná. Zašifrovaná zpráva se nazývá HASH[5]. Tento hash slouží pro porovnání, zdali se jedná o totožnou zprávu. Hashovací funkce je unikátní tím, že sebemenší změna v původní originální zprávě vyvolá velkou změnu ve finálním hashi. Hashovací funkce je odolná vůči kolizím a nelze použit kryptoanalýzu, tedy rozšifrování původního obsahu.

Hlavním užitím symetrického šifrování je ukládání hesel ve formě hashu, kdy není podstatné samotné původní heslo v textové podobě, ale výsledný hash. Tento hash je následně někde uchováván. Pokud uživatel zadá heslo, například pro přihlášení do systému, tento vstup se přes stejnou hashovací funkci zašifruje a ověří, zdali finální hash odpovídá tomu původnímu. Databáze všech hashu bývá uložena na serveru. Tím pádem provozovatel

[5] Hash – matematická funkce, která převádí vstupní data do hashovacího tvaru. Závisí na délce vstupu a hashovací funkci. Ukázkovým hashem je například: FCD3 D682 D544 F211 321D

databáze nezná hesla uživatelů, ale i tak je schopen autentizovat uživatele na základě daného hashe. (45)

Na stejném principu fungují i antiviry. Ukládají si vytvořené hashe v sytému. Od každého souboru vytvoří otisk hashe. Pokud dojde k napadení systému či podezřelé úpravě hodnot souborů, antivir porovná aktuální hash a původní hash. Pokud jsou oba hashe shodné, daný soubor je nepozměněn. Pokud je hash odlišný, antivir detekuje případnou změnu v souboru a přijme opatření. (45)

Hashovací funkce:

- ***MD5*** – Stará a v dnešní době již nepoužívaná hashovací funkce. Jedná se o 128bit hashování, nevhodný pro ověřování integrity dokumentů z důvodu častých kolizí.
- ***SHA-1*** – 160bitový hash, již nedostačující.
- ***SHA-2*** – Dnes nepoužívanější typ hashovací funkce. Existují 224, 256 a 512bitové verze. Uživateli nebo systém si zvolí hashovací funkci. Aktuální využití pro generování elektronických podpisů a certifikátů.
- ***Rainbow tables*** – Světová tabulka se základními slovy a jejich vygenerovanými hashi. (45)

3.7.4.2. Asymetrické šifrování

Asymetrické šifrování lze dešifrovat a na rozdíl od symetrického šifrování lze zjistit původní obsah. Celý princip je založen na privátním a veřejném klíči. K vytvoření privátního klíče je nezbytné použít matematické funkce a algoritmy. Nejznámější funkcí pro generování klíčů je RSA. Z privátního klíče se vytváří veřejný klíč. Tento proces nelze obrátit, to znamená z veřejného klíče nelze vytvořit privátní klíč.

Ve zkratce, pokud je použit tento typ šifrování, odesílatel zašifruje data veřejným klíčem příjemce. Příjemce po obdržení zašifrované zprávy jí může dešifrovat pomocí svého privátního klíče. Privátní klíč by neměl být nikdy, nikde zveřejněn z důvodu kompromitace klíče a následného zneužití. Tyto klíče jsou ukládaný lokálně na stanicích. Privátní klíče nelze vyexportovat. (45)

3.7.4.3. Elektronický podpis

Elektronický podpis se stal důležitým aspektem k zajištění integrity osob a dokumentů, z důvodu zamezení podvrhovaní zpráv či vydávání se za někoho jiného.

Jedná se o podpis, který je odesílán formou elektronické pošty. Odesílatel se takzvaně podepíše. Příjemce u tohoto emailu vidí, že zpráva byla podepsána odesílatelem. Podepsaný email má speciální signaturu s majitelem podpisu. Pomocí tohoto atributu lze ověřit, zdali má odesílatel platný certifikát a další podrobnosti o odesílateli.

Elektronický podpis by měl zaručit: [45]

Autenticitu – jedná se o člověka, kterému patří daný podpis
Časová stopu – na základě podpisu lze určit čas, kdy zpráva byla podepsána a odeslána
Integritu – v podepsané zprávě nedošlo po přenášené cestě ke změnám. Jedná se o původní a nepozměněný dokument
Legitimnost – dodává dokumentu legitimní status. Pokud osoba podepíše zprávu svým elektronickým podpisem, nemůže tento fakt odepřít. [45]

Celý princip elektronického podepisování bude následně vysvětlen:

- K původní zprávě se vytvoří hash, tento hash je zatím nezašifrovaný a volně čitelný
- Odesílatel zašifruje svůj elektronický podpis pomocí svého privátního klíče
- Zároveň k tomu zašifruje hash zprávy veřejným klíčem adresáta. Je použit veřejný klíč adresáta, aby ho mohl příjemce rozšifrovat svým privátním klíčem
- Probíhá přenesení zprávy a digitálního podpisu
- Příjemce obdrží zašifrovanou zprávu a digitální podpis
- Pomocí veřejného klíče rozšifruje digitální podpis a ověří autenticitu a integritu dokumentu
- Následně pomocí svého privátní klíče rozšifruje hash k přenášené zprávě
- Následuje porovnání hashe zprávy s původním rozšifrovaným hashem z digitálního podpisu

- Pokud se oba hashe shodují, jak ten z digitálního podpisu, tak i z přenášené zprávy, bylo docíleno ověření integrity a autenticity přenášené zprávy
- Aby nedocházelo k zatěžování přenosové cesty, nešifruje se celá přenášená zpráva, ale jen hash.[45]

3.7.4.4. Certifikát

Elektronický certifikát slouží k prokázaní identity v digitálním prostředí. Certifikát je vydán na základě otisku veřejného klíče. Vystavení certifikátu probíhá u příslušné certifikační autority. Na základě ověření identity a podání žádanky o vydání certifikátu je certifikát danou certifikační autoritou vygenerován.

Privátní klíč se vytváří sám, při vytváření žádosti o vydání certifikátu. Sám se automaticky ukládá do uložiště lokálního počítače nebo na příslušné přenosové médium. Po odeslání žádosti o vydání certifikátu se osoba dostaví na lokaci certifikační autority.

Rozdělujeme dva typy certifikátu. Certifikát kvalifikovaný a komerční. Kvalifikovaný certifikáty jsou vydávány jen ověřenými certifikačními autoritami. Celý proces podléhá dle zákonného postupu. Komerční certifikáty nemusí být vydávaný certifikačními autoritami. Každý soukromý podnik si může generovat svoje certifikáty pro interní účely.

Certifikační autority vystavují certifikáty výhradně na základně bezpečnostních a certifikačních politik. Celý princip těchto certifikátu spočívá na důvěryhodnosti a statusu certifikační autority. Pokud je certifikační autorita napadena a zkompromitována, všechny vydané certifikáty jsou nedůvěryhodné a neměly by se nadále používat, tak jak ztratily svůj účel. [45]

V České republice nalezneme certifikační autority jako Česká pošta, eIdentita a První certifikační autorita. Světové certifikační autority jsou GeoTrust, Comode a další. [45]

Obrázek 10 - Čipová karta pro uchování a přenášení certifikátů

Zdroj: https://www.smartcardsreaders.shop/acos5-evo-192kb-pki-cipova-karta-sim.html

3.7.5. Zabezpečovací technologie

K docílení zabezpečení domácí či vnitropodnikové sítě se užívají speciální zařízení, která poskytují alespoň základní formu síťové ochrany. Tyto zařízení mohou mít formu softwarového nebo fyzického typu. Taktéž se mohou vyskytovat samostatně nebo součástí all in one řešení.

Základní balíček bezpečnostních technologií se nazývá UTM řešení. Jedná se o variantu pro domácnosti nebo malé podniky. Tento balíček technologií obsahuje základní firewall, proxy server, antivirus, IPS atd. Obsah tohoto balíčku záleží na produktu či poskytovali služby. Na první pohled se řešení může zdát jako dostačující, pokud jste běžný uživatel či malý podnik s pár zaměstnanci, ale určitě tato volba nebude tou správnou pro světovou organizaci. Opět nutno podotknout, že investování do zabezpečení je stejně důležité, jako investování do všech ostatních odvětví podnikání. Prevence je jediný způsob obrany vůči útokům. Reagovat již na způsobilé škody není moudré a už vůbec ne efektivní.

Bezpečnostní technologie mohou mít podobu softwaru, který fungují na stanicích. Taktéž se mohou vyskytovat ve fyzické podobě většinou ve formě zařízení, které je následně zapojeno a provozováno v serverovně. Fyzické zařízení budou vždy výkonnější a spolehlivější než ty softwarové. Tak jak jsou dedikovány čistě pro svůj účel. Následuje pojednání o těchto technologiích. (45)

3.7.5.1. Firewall

Firewall přestavuje prvním, základním a hlavním prvkem v oblasti zabezpečení počítačových sítí. Ve zkratce firewall zabraňuje neoprávněnému přístupu z veřejného internetu do interní sítě.

Toto zařízení se může vyskytovat jak ve fyzické formě, působící v serverovém datacentru, nebo software. Většinou provozováno na hostitelském zařízení. Firewall obsahuje tabulku IP adres, kde je uvedeno, jaké IP adresy a porty jsou důvěryhodné a jaké naopak je potřeba blokovat. Povolené IP adresy se nazývají ve slangovém jazyce prostupy. Na trhu lze najít mnoho druhů firewallu jako například stavové, filtrovací, nex-gen atd. Všechny ale mají společný úkol. Blokovat neautorizovanou či podezřelou komunikaci. (45)

Jelikož firewall kontroluje a řídí veškerou komunikaci, je velmi důležité nepodceňovat konfiguraci a správu tohoto bezpečnostního prvku. Nekorektní konfigurace firewallu může způsobit nedostupnost celé vnitropodnikové sítě či jiné závažné poruchy a výpadky. Taktéž pokud budou ve firewallu nastavené chybné signatury pro detekci podezřelé komunikace, může být tato chyba využita ve prospěch útočníka. Špatně nakonfigurovaný firewall může být takzvaně děravý. To je hlavní důvod, proč by firewall v podniku měla spravovat kompetentní a zkušená osoba. (45)

Stavový firewall – Jedná se o nejběžnější a o nejpoužívanější typ firewallu. Pojmenování stavový odvozeno na základě vlastnosti kontroly stavů filtrování paketů, který firewall kontroluje ve stavové tabulce.

Hlavní výhodou je kontrola přístupu a filtrování paketů, čímž je docíleno základním typem ochrany vůči vnějším nežádoucím dotazům. Zároveň je docíleno nižšího zatížení vnitropodnikové sítě. Komunikace probíhá jen od povolených zdrojů či aplikací. Stavový firewall je efektivní vůči typům útoku jako je DoS a spoofing.

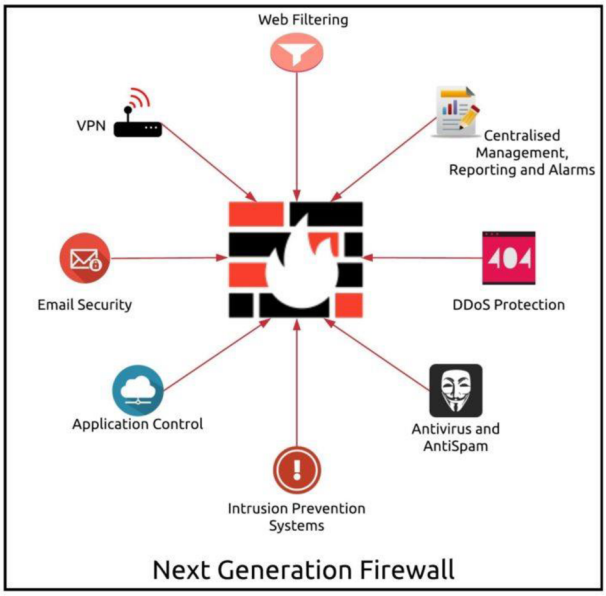
Velkou nevýhodou těchto firewallu je neschopnost kontroly uživatelů a aplikací. Kontrola probíhá na síťové vrstvě, to je ovšem nedostačující. Vnější hrozby mohou přicházet i z aplikačních vrstev. (30)(45)

Paketový filtr – Nejstarší typ firewallu. Celý princip spočívá na kontrole komunikace z určitých adres a portů. Technologie je poněkud dnes již zastaralá, tak jak nepřináší dostatečnou schopnost ochrany. Nicméně celý princip je velmi jednoduchý. Na rozdíl od dnešních stavových či nex-gen firewallů i rychlejší. Proto se i dnes najdou místa, kdy tyto firewally jsou používané. Příkladem je nutnost přenesení velkého objemu dat při menším důkladu na jejich ochranu. (30)(45)

Aplikační brána – Také dnes nazývaná jako proxy firewall. Komunikace probíhá za pomocí klienta, který se dotazuje konečného serveru. Avšak mezi nimi na komunikační cestě stojí proxy firewall. Celou komunikaci zprostředkovává a zabezpečuje. Vypadá to, že se klient doptává finálního serveru. Ve skutečnosti to dělá za klienta aplikační brána, která požadavek zpracuje, přepošle, a to samé udělá i s odpovědí od serveru. Název aplikační brána pojímá z fungování na aplikační vrstvě. Velkou výhodou toho řešení je přidání další vrstvy ochrany. Serveru se nedotazuje napřímo klient, ale aplikační brána. (30)(45)

Next-Generation firewall (NGFW) – Firewall nové generace, který by měl přinést nové vymoženosti v IT odvětví. Next-Generation firewall disponuje novými technologiemi, které by měly celoplošně pokrýt bezpečnost interních sítí. Next-Gen firewall funguje jak na sítové, tak i aplikační vrstvě. Novou vymožeností je i kontrola aplikací, prevencí vůči unikům informací, nazývané jako IPS, a eliminace hrozby ve formě sandboxu. (28)

Firewall nové generace obsahuje technologie všech předešlých typů firewallu a samozřejmě i něco navíc. Toto technologické řešení může být ideální pro menší nebo začínající podniky, které hledají základní formu zabezpečení sítě. NGFW (Next-Generation Firewall) do jisté míry nahrazuje antivirus, proxy server či již zmíněný systém prevence průniku IPS. (28)(29)



Obrázek 11 – Next-Generation firewall, popis fungování

Zdroj: https://firewall.firm.in/tag/next-generation-firewalls/

3.7.5.2. Proxy

Proxy server zprostředkovává komunikaci mezi klientem a serverem, na které se klient pomocí svých požadavků dotazuje. Historicky proxy server byl vynalezen k ukládání neboli cachování často používaných webových stránek za účelem rychlejšího načtení právě z cache paměti. Postupem času se však tato technologie mírně přizpůsobila technologickému posunu v IT. Nyní funguje primárně jako bezpečnostní prvek. (31)(32)

Pokud by se každý klient napřímo dotazoval serveru mohlo by to znamenat potenciální bezpečnostní riziko. Ne každý dotaz by mohl být legitimní. Jak bylo pojednáno v předešlých kapitolách, běžným útokem by mohl být SQL Injection či podobné hrozby. Uživatel odešle svůj požadavek přes webový prohlížeč, tento požadavek je převzat proxy serverem, který se následně doptává na odpověď serveru. K samotnému serveru přistupuje napřímo proxy server, ne uživatel. Zpětnou odpověď opět proxy server zpracuje a odešle uživateli. (31)(32)

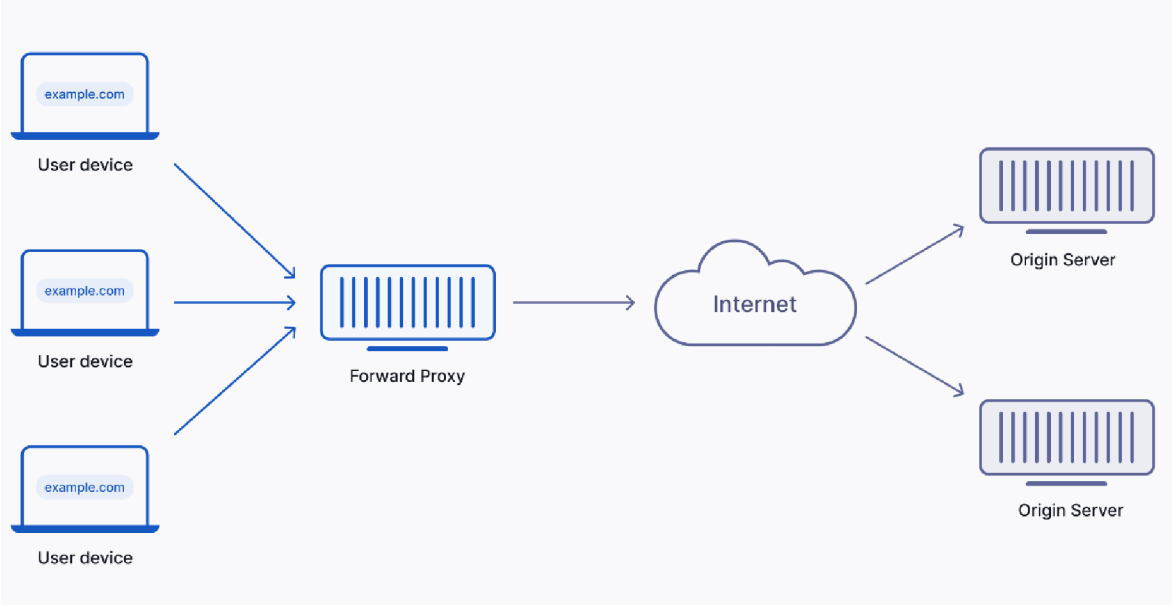
Proxy server se v dnešní době může vyskytovat jak ve fyzické podobě, tak i softwarové. Na trhu lze narazit na desítky různých proxy serverů. Každý z nich má svůj účel a využití. (32)

Hlavními důvody, proč využívat proxy servery ve vnitropodnikové sféře jsou:

- Možnost blokace URL odkazů a příchozích IP adres
- Cachování webových stránek a jejich rychlejší načtení
- Klienti přistupují na internet pod jistou anonymitou
- Možnost kontroly příchozích a odchozích webových stránek do podniku
- Antivirová kontrola
- Balancing[6] a rozvržení zátěže (31)

Na první pohled se může proxy server zdát jako ideální řešení, které nemá chyby. Ale jak jistě víme, každá technologie má své nedostatky. Celá myšlenka centralizování přístupu přes jeden přístupový bod do internetu sebou nese i jistá rizika. Jelikož proxy server přistupuje do internetu, může být jeho IP adresa detekována. Tím pádem v případě kybernetického útoku bude proxy server napaden jako jeden z prvních. Pokud se odstaví proxy server, nebude mít celá organizace přístup na internet a tím jsou spjata i další rizika. Řešením tohoto nedostatku může být instalováním více proxy serverů a nastavení balacingu mezi nimi. Při výpadku jednoho proxy serveru by druhý server včas přebral zátěž a dokázal zajistit plynule fungování podniku. (31)

[6] Balancing – za pomocí balanceru, což je aktivní sítový prvek, lze nastavit jistá pravidla pro předávání zátěže, tedy balancování mezi zařízeními.



Obrázek 12 – Princip fungování proxy serveru

Zdroj: https://www.upguard.com/blog/proxy-server

3.7.5.3. DLP

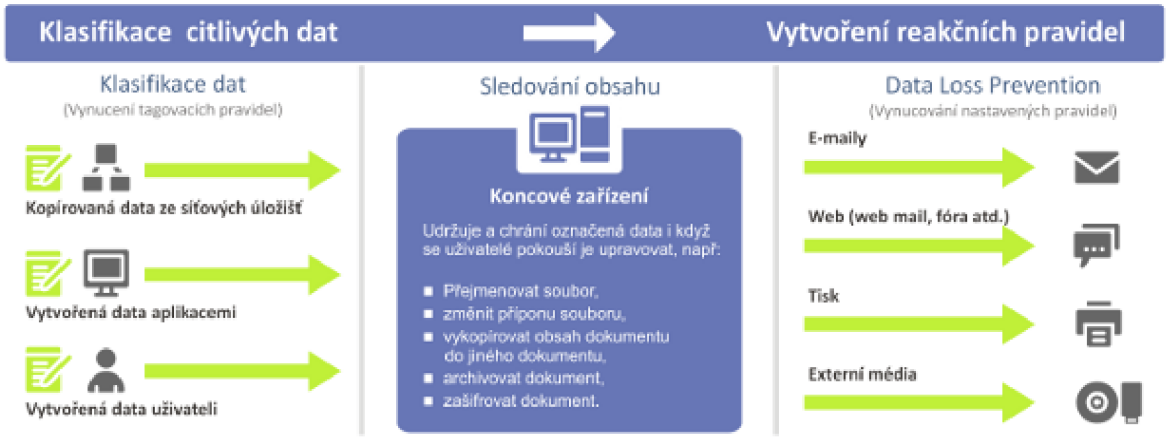
V celém názvu data lose protection neboli ochrana před ztrátou dat, je technologie, která brání uniku dat z vnitropodnikového prostředí. Útočnicí, kteří mají zájem o podnikové data se nemusí nacházet jen na internetu. Podniková data a citlivé údaje jsou mnohdy velmi cenné a tvoří takzvaný know-how celé firmy, za které konkurence ráda zaplatí nemalé peníze.

Z výzkumu vyplývá, že více jak polovina zaměstnanců mají oprávnění k tomu, aby si podniková data samovolně stahovala na přenositelné media. Následně mohou samovolně používat a připojovat do počítačů osobní flash disky a jiná zařízení tohoto typu. Po práci tyto média odnáší domů. Organizace se dostává k velkému riziku ztráty dat či následného odcizení ze soukromých počítačů zaměstnanců.

DLP technologie slouží k zabránění a omezení těchto činností. Při instalaci DLP systému si podnik musí sám nadefinovat, které údaje jsou pro něho citlivé. Na základě tohoto rozhodnutí je bude DLP technologie skenovat a kontrolovat. Tento krok je ze všech nejtěžší, jelikož definovat a neustále aktualizovat citlivá data je velmi náročné.

DLP technologii lze najít na třech místech výskytu. Nejčastěji ve formě agenta na uživatelských počítačích, agent na centrálních databázích či serverech, nebo jako síťový prvek kontrolující provoz na síti.

Po definici, jaký typ dat bude DLP kontrolovat, přichází nastavení bezpečnostních politik. Například jaké úkony může zaměstnanec s daty provádět, kdo může data v dané databázi mazat a editovat, jak vysoké oprávnění musí mít uživatel, aby mohl připojit flash disk a další omezení na základě vnitropodnikových bezpečnostních politik a směrnic. (33)(34)



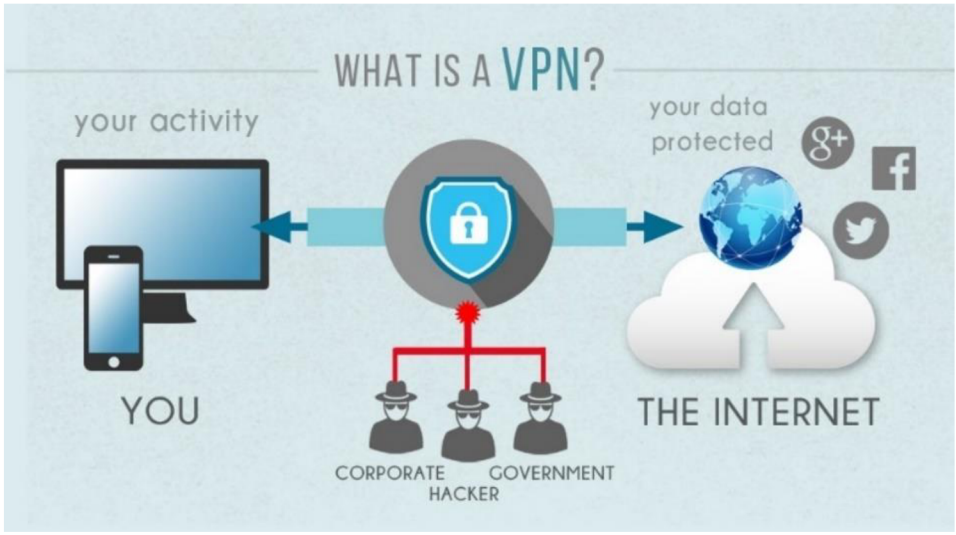
Obrázek 13 – Princip fungování DLP

Zdroj: https://www.aec.cz/cz/dlp

3.7.5.4. VPN

VPN neboli do českého překladu virtuální privátní síť je nástroj, vymoženost a technologie, která slouží k zabezpečení síťové komunikace. Velká část komunikace probíhá skrz internet. Internet se považuje za nezabezpečenou síť. VPN umožnuje vytvářet virtuální kanály pro komunikaci. Celá komunikace začíná navázáním a ověřením totožnosti obou účastníku pomocí certifikátů. Po úspěšné autentizaci dojde k zahájení komunikace.

Virtuální privátní síť si může organizace hostovat sama pomocí svých serverů. Pokud se jedná o uživatele, existují i velké množství poskytovatelů VPN služeb. Za určitou finanční částku má uživatel k dispozici servery, které může využívat k vlastní komunikaci. Servery jsou dedikovány po celém světě, aby zajistily maximální ochranu a možnost změny IP adresy dle potřeb. (35)(36)



Obrázek 14 – Princip fungování VPN

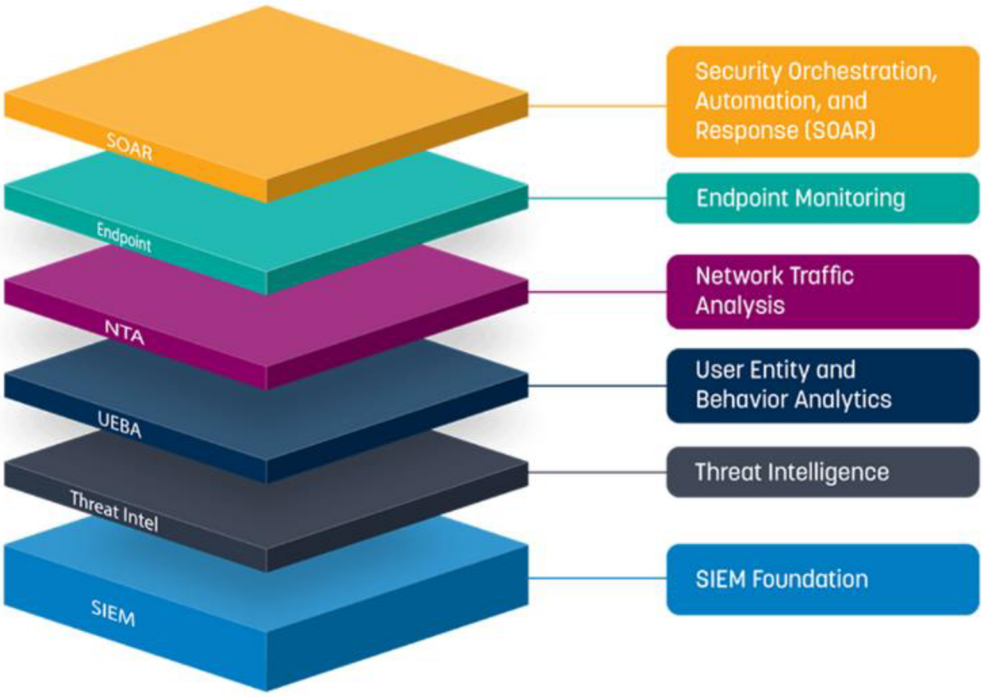
Zdroj: https://www.alza.cz/slovnik/co-je-vpn#definice

3.7.5.5. SIEM

SIEM systémy umožnují monitorování komunikace ve vnitropodnikové sítí, ukládání a generování logu s bezpečnostními aktivitami a analýzu bezpečnostních hrozeb. Na základě bezpečnostních politik dokáže tyto hrozby eliminovat či na ně včas upozornit. Tento systém slouží jako preventivní prvek v bezpečnostní, kdy dokáže zakročit vůči bezpečnostním hrozbám, tak aby se z nich nestaly bezpečnostní incidenty. (37)(38)

Systém poskytuje jak grafické prostředí, tak i příkazovou řádku. Umožnuje uživateli sledovat veškeré dění na sítí, nebo provoz na databázových a aplikačních serverech. Hlavním účelem SIEM systému je generování a uchovávání logů. Logy bývají následně použity pro dohledání bezpečnostních narušení nebo známky pokusů o narušení integrity. Tyto logy jsou hlavními podklady při provádění forenzní analýzy. Na základě logů se provádějí bezpečnostní audity. (38)

V dnešní době jsou SIEM systémy velmi populární a běžně používaný ve vnitropodnikovém prostředí. Nejedná se ovšem o levnou záležitost. Tyto systémy jsou velice složité. Jejich provoz a konfiguraci mají na starost kompetentní a certifikovaný personál. (37)(38)



Obrázek 15 – Princip fungování SIEM systému

Zdroj: https://www.comguard.cz/logrhythm

3.7.5.6. Anti-Spam

Jedná se o zařízení, které se opět může vyskytovat v podobě fyzického zařízení či softwarového agenta nainstalovaný na stanici. Hlavním úkolem tohoto zařízení je detekce, skenování a případná blokace nevyžádaných zpráv na základě definovaných pravidel či machine learningu[7]. (39)(40)

Anti-Spam by měl být instalován tak, aby viděl na všechny příchozí i odchozí emaily, které putují dovnitř a ven z podniku. Na základě toho lze docílit kompletní kontroly komunikace v podniku a tím omezovat, nebo nastavovat politiky či bezpečnostní pravidla. Anti-spam kontroluje obsah příchozích zpráv, reputaci odesílatele, předmět zprávy a další parametry. Na základě celkového skenu emailových hlaviček a obsahu udělí tomuto emailu trestné body. Také nazývané jako scóre. Pokud má email velký počet trestných bodů, je automaticky zablokován a přesunut do fronty na spam, kdy tento email nebude doručován a v nebližší době vymazán. Anti-spam loguje na stejném principu jako SIEM

[7] Jedná se o umělou inteligenci, která na základě události v historii použije stejný nebo podobný typ chování.

systém. Na základě logů poskytuje možnost dohledání v historii emailové komunikace, náznaky bezpečnostních hrozeb a mnoho dalších aspektů. (39)

Spamové odesílatele lze blokovat na základě blacklistu. Jedná se o listinu blokovaných odesílatelů. Pokud je zaslána zpráva pomocí emailové komunikace do podniku z adresy, která je na blacklistu, automaticky je přesunuta do fronty na vymazání. Proto byl vytvořen i whitelist. Jedná se o přesný opak, tedy listinu legitimních emailových adres a domén. Tyto emaily nepodléhají anti-spamové kontrole a jsou doručovány příjemci bez kontroly. (40)

Blokovací pravidla jsou opět velmi subjektivní a závisí jenom na podniku, jaká omezení nastaví. Tak jak anti spam může blokovat příchozí komunikaci, lze zde nastavit i pravidla pro odchozí komunikaci. Tímto úkonem bude zamezeno zaměstnancům podniku v používání vulgárních či jiných zakázaných slovních spojení.

3.7.6. Penetrační testování

Penetrační testování je způsob ověření stupně zabezpečení podniku či jiného subjektu na základě otestování jeho zranitelností a vyhodnocení dle patřičných analýz. Penetrační testy provádí kvalifikované osoby, kdy testují jak hardware, software, síťové i lokální prostředí podniku. Hlavním účelem testování je simulace průběhu předefinovaného útoku a zjištění, zdali dosavadní nasazené zabezpečení je dostačující. Hlavním úkolem testování je identifikovat potenciální hrozby, konzultace následného řešení, školení a demonstrace kritického scénáře napadení a vyřazení celé infrastruktury. Zadání penetračního testování se může lišit dle podnikových potřeb. (41)(42)

Testování lze rozdělit na interní a externí. Interní penetrační testy mají za úkol otestovat bezpečnost infrastruktury, pokud se útočník již dostal do vnitřní sítě a jaké škody by mohl napáchat. Externí penetrační testy se simulují z internetu. Útočník teprve snaží o proniknutí do perimetru. (42)

Nelze opomenout, že potenciální hrozby se neskrývají jen z vnějšího z prostředí internetu. Potenciálního útočníka lze nalézt i uvnitř podniku. Například v podobě rozzlobeného zaměstnance. I proti takovému scénáři může být penetrační testování účinné.

Testovací scénáře by měly zahrnout veškeré možné druhy hrozeb a následně poukázat na možný dopad bezpečnostních incidentů. (41)

Cena penetračního testování se pohybuje kolem 50.000 Kč až 5.000.000 Kč. Záleží na velikosti podniku a složitosti infrastruktury. (46)

4. Vlastní práce

Praktická část diplomové práce bude realizována na Ministerstvu spravedlnosti České republiky, dále jen MSP. Přesněji v odboru informatiky, v oddělení kybernetické bezpečnosti. Bude dodrženo zadání práce realizace vlastního řešení, přesněji vytvoření návrhu zabezpečené sítě LAN pro menší podnik či domácnost. Následuje použití odborných metodik a best practices postupů. Za účelem zabezpečení demonstrované sítě a připravení takzvaně k provozu. Úkolem této diplomové práce je pojednat a posloužit jakožto universálním materiálem při zabezpečení podnikových a domácích sítí LAN.

Autor diplomové práce podotýká, že se nemá jednat o návod či dokument podobný tomuto typu, ale o pomůcku sloužící s obeznámením s problematikou a jejího řešení v denním běžném provozu. Ve vnitropodnikové infrastruktuře ministerstva se používá hypervizor VMware. Vlastní návrh bude demonstrován právě pomocí tohoto hypervizoru.

Data použitá v praktické části nemusí být vždy pravdivá, v důsledku utajování a zveřejňování citlivých informací ministerstva.

V první polovině praktické části bude demonstrován vlastní návrh řešení, kdy bude vytvořen vlastní virtuální server a následně na něm budou zprovozněny a nakonfigurované potřebné služby. Ve druhé polovině praktické části následuje pojednání o technologiích a zařízeních, které slouží k zabezpečení sítě. Výsledky testování demonstrativní sítě se budou nacházet v závěru a diskusi.

4.1. Fyzické zabezpečení sítě

Jakožto prvním faktorem v ochraně počítačové sítě musí být fyzická ochrana sítě jako taková. Pokud se útočník dostane k přenosovým a komunikačním cestám, může jednoduše odposlouchávat komunikaci nebo ji zaměňovat za vlastní obsah. Trend fyzického vniknutí do datacenter výrazně opadá. Fyzické zabezpečení serveroven je v dnešní době velmi vyspělé. Obrané mechanismy mají i několik vrstev, přes které se útočník fyzicky jen tak nedostane. I když tento trend upadá, nesmí být podceněn žádný faktor. Špatně nastavený

server či switch, který nemá korektně nastavený device control[8] může mít fatální následky pro celý podnik.

Architekturu fyzického zabezpečení definuje podnik. Pokud organizace využívá služby Cloud computingu, má o jednu starost méně. Tak jak toto zabezpečení obstarává provozovatel cloudových služeb. Pokud ovšem se jedná o státní podnik, jak je tomu v našem případě, svá data ukládat do cloudu nesmí. Veškeré technologie a data musí mít uložené fyzicky, takzvaně on premise[9].

4.1.1. Zabezpečení budovy

Jako první vrstvou fyzické ochrany, kterou by měl útočník překonat, je vstup do budovy podniku. Opět nutno podotknout, že každý zabezpečovací systém se může lišit dle individuální architektury. Uváděný příklad nemusí sloužit jako obecným standardem fyzického zabezpečení sítě.

V tomto případě, kdy se jedná o Ministerstvo spravedlnosti ČR, se musí osoba, která chce přistoupit do datového centra, projít fyzickou kontrolou přes justiční stráž a následně se validovat zaměstnaneckou přístupovou kartou. Budova je pod neustálým dohledem justiční stráže, která vykonává obraný prvek. Veškeré prostory jsou monitorovány kamerovým systémem, v některých místnostech signalizačními čidly a dalšími prvky zabezpečení. Typické obrané prvky jako bezpečnostní dveře a okna budovy jsou samozřejmostí.

Každá návštěva či osoba, která není zaměstnancem ministerstva, projde důkladnou kontrolou. Jedná se o kontrolu zavazadel, detektorem kovu, ověření a evidencí dle občanského průkazu. Následně osoba dostane návštěvnický průkaz. Tento průkaz musí návštěva nosit na viditelném místě a vyčká na doprovod ze strany ministerstva. Tímto postupem je zamezeno vstupu neoprávněné osoby do budovy.

---

[8] Jedná se o softwarovou či fyzickou ochranu zařízení před nepovoleným použití přenosných datových uložišť a jiných vstupních zařízení, například jako flash disky atd.

[9] Interní infrastruktura a krabicové řešení. Všechna data jsou uložena lokálně, nic neputuje do cloudu.

4.1.2. Zabezpečení serveroven

Přístup do serveroven je striktně kontrolován a jen oprávněné osoby zde mají přístup. Ke vstupu do serverovny je vyžadován speciální přístup ve formě fyzické certifikační karty. Osoby, které sem mají přístup jsou evidovány ve speciálním rejstříku. Každá osoba žádající o vstupní oprávnění musí projít bezpečnostním školením a prověrkou. Na základě uvážení bezpečnostního sboru jsou tyto oprávnění vydána.

Přístup do serveroven je hlídán pomocí bezpečnostních kamer. Na kamerový systém dohlíží justiční stráž daného ministerstva, soudu či státního zastupitelství. Serverovny jsou také opatřeny signalizačním alarmem, který musí být před vstupem do serveroven vypnut pomocí přístupového hesla. Každý administrátor či technik přistupující do serveroven má vlastní přístupové údaje. Tímto krokem je docílena dohledatelnost osoby, která přistupovala do serverovny jako poslední.

4.1.3. Zabezpečení fyzických strojů

Jak již bylo zmíněno v předešle časti praktické části. Do serveroven a k fyzickým strojům mají přístup jen administrátoři a technici, kteří jsou odborně vyškolení. Pokud by se útočník dostal přes všechny zmíněné vrstvy ochrany, fyzické stroje (servery, switche, disková pole) jsou opatřeny bezpečnostními mechanismy, které zamezují kompromitaci stroje. To znamená, že pokud se uživatel chce přihlásit napřímo do daného zařízení, musí zadat přístupové heslo. Heslo je sděleno jen správcům provozu.

Veškeré porty, které se na switchi nevyužívají jsou z pravidla deaktivované. Na serverech bývá nastavený device control, který zakazuje připojení externího zařízení přes USB. Pokud by se útočník dostal fyzicky k serveru a snažil se o nainstalování škodlivého malwaru ze svého USB přenosného uložiště, neuspěl by. Musel by se přihlásit pomocí administrátorského hesla a tento device control vypnout.

4.2. Návrh architektury sítě

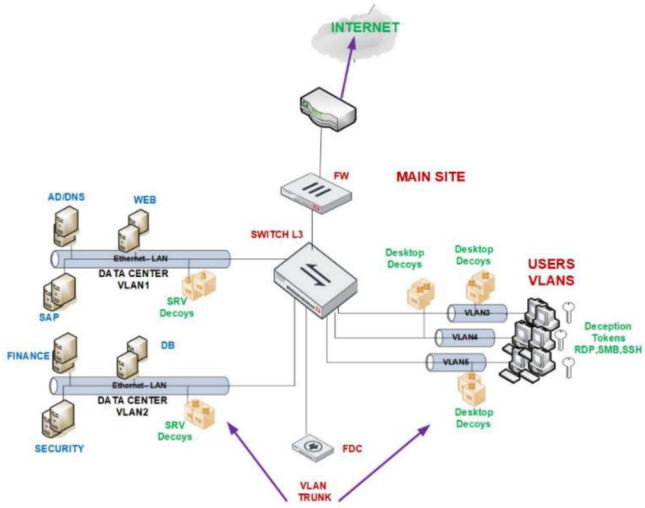
Velikou roli v zabezpečení lokální sítě tvoří její architektura a způsob rozložení. Síť by měla být z velké části decentralizovaná, redundantní, a hlavně odolná vůči výpadkům

jednotlivých uzlů. Samotná síť by měla připomínat tvar bludiště, kdy se jednotlivé sektory v případě útoku dají odříznout od běžného provozu.

Hlavní páteřní síť by měla být tvořena centrálními prvky, jako jsou corové switche, servery a routery. Tento druh zapojení by měl následně připomínat tvar kruhu. Každé zařízení z páteřní sítě by mělo být propojené s každým. V případě výpadku se využije náhradní komunikační cesta.

Pokud vypadne jeden či vícero uzlů, síť by měla zůstat aktivní a nedotčená. Z důvodu zachování vysoké dostupnosti služeb. Samotný provoz a špičky provozu se dají monitorovat. V případě nutnosti nastavit balancery sítě, aby balancovaly zátěž na příslušných uzlech. V kritickém scénáři by se zapojovaly neaktivní síťové prvky do komunikace, které by tuto dočasnou zátěž dokázaly překonat.

Každá síťová architektura by měla počítat se základním problémem v IT. To je obávaný výpadek elektřiny. V tomto případě by měl být každý uzel vybaven náhradním zdrojem elektřiny v podobě UPS. Jedná se o zařízení, které dokáže pohánět zařízení na potřebnou dobu, většinou se jedná o řády desítek minut. Cílem je zajištění náhradního zdroje elektřiny či k řádnému ukončení procesů na strojích a přepojení komunikace na jinou lokaci. Pokud se jedná o větší serverovny a pracovní stanoviště, používají se diesel agregáty. Toto zařízení je poháněné naftou a produkuje elektřinu. Jedná o se takzvaný generátor.



Obrázek 16 – Návrh architektury sítě

Zdroj: https://docs.fortinet.com/document/fortideceptor/4.0.0/best-practices/557405/network-topology-best-practices

4.3. Bezpečnostní protokoly na linkové vrstvě

4.3.1. 802.1X

802.1X je bezpečnostní protokol na linkové vrstvě. Celý princip fungování spočívá v ověřování portů pomocí autentizace. Základní stav portu či připojovací zásuvky je ve stavu disabled. Tedy lze říci, že nečinný. Uživatel po připojení k zásuvce je vyzván k autentizaci pomocí přihlašovacích údajů. Odpověď je následně odeslána autentizačnímu serveru, nazývaný jako Radius. Server na základě porovnání s údaji v databázi přístup povolí či zamítne. Po úspěšné autentizaci se port nastaví dle dané konfigurace sítě. Nastavení portu je definováno na celkové architektuře sítě v souladu bezpečnostními politikami podniku.

Bezpečnostní protokol je výbornou pomůckou při řízení neoprávněných přístupů do sítě. Každý uživatel přistupující přes port se autentizuje. Bez této autentizace není navázaná komunikace, ani připojení do interní sítě.

Velkou nevýhodou protokolu může být například náročnost na provedení a celkové zavádění do podniku. Jedná se o poměrně složitý autentizační systém, který musí být nakonfigurován korektně. Další z nevýhod protokolu je přístup přes vzdálenou plochu, naplánované aktualizace a zálohy. Stanice je probuzena pomocí wake on lan paketu, například v nočních hodinách. Po úspěšné akci je počítač opět vypnut či uveden do původního stavu. Je zapotřebí tento údržbový úkon korektně nastavit, tak jak protokol 802.1X může akci zcela omezit, jelikož se stanice neautentizuje. [43]

4.3.2. ARP

ARP protokol zaujímá charakter komunikačního i bezpečnostního protokolu. Protokol má za úkol přiřazení každému zařízení na základě jeho MAC adresy příslušnou IP adresu. Tento záznam si vede ve své ARP tabulce. Pomocí ARP tabulky je komunikace v sítí o hodně rychlejší a snazší. Pokud zařízení A chce kontaktovat zařízení B ve stejné sítí, potřebuje k tomu jeho MAC adresu. Pokud tento záznam o MAC adrese chybí, doptá se pomocí IP adresy. Následně si tyto dva záznamy, jak MAC, tak i IP, spojí. Pro následující komunikaci již není zapotřebí doptávání se pomocí ARP funkce.

ARP protokol pomáhá evidovat zařízení v sítí pomocí jejich MAC adres a přiřazeným IP adresách. Pokud by útočník v síti podvrhl svoje zařízení, které by obsahovalo stejnou IP adresu, ale jinou MAC adresu. ARP protokol dokáže tuto změnu rozpoznat. (44)

4.4. Virtualizace

Virtualizace se na první pohled jeví jako nová technologie prosperující v poslední dekádě. První zmínky o virtualizace sahají do 60. let minulého století. Nejednalo se o virtualizaci, jak jí známe dnes, ale jen o virtualizovaní jednolitých komponentů. Dnes však tuto technologii využíváme denně. Aniž bychom poznali, že se vůbec o virtualizaci jedná. Dnes lze virtualizovat celé servery, desktopy či samotné aplikace.

Díky virtualizaci a takzvané škálovatelnosti může podnik ušetřit značné náklady na provozu. Nemusí pro každou službu či aplikaci zřizovat fyzický server. Bezpečnostní politika udává povinnost provozovat každou službu odděleně na svém serveru. Hlavní příčinou je již zmíněná bezpečnost, ale také prevence vůči výpadkům nebo jeho pravidelná údržba v reálném čase.

Na současném trhu se vyskytují tři největší hypervizory. Jedná se o produkt Hyper-V od firmy Microsoft, VMware od firmy VMware a hypervizor Citrix od společnosti Citrix Systems. Každý hypervizor je jedinečný a hodí se pro jiný druh virtualizace. Nelze tedy definovat, který je nejlepší. Závisí na celkové architektuře sítě podniku a samotném účelu virtualizace.

Jelikož v našem případě MSP využívá a má zakoupené licence pro VMWare, bude použit tento hypervizor. Osobně ho autor práce upřednostňuje před ostatními virtualizačními produkty. Primárně z důvodu velké popularity, žádané certifikace na trhu a kompatibility s ostatními vendory.

4.4.1. Instalace virtuálního stroje

Před instalací virtuálního stroje je důležité určit hosta, na kterém celá virtualizace bude provozována. Mělo by se jednat o výkonný server či stanici s dostatečným obsahem

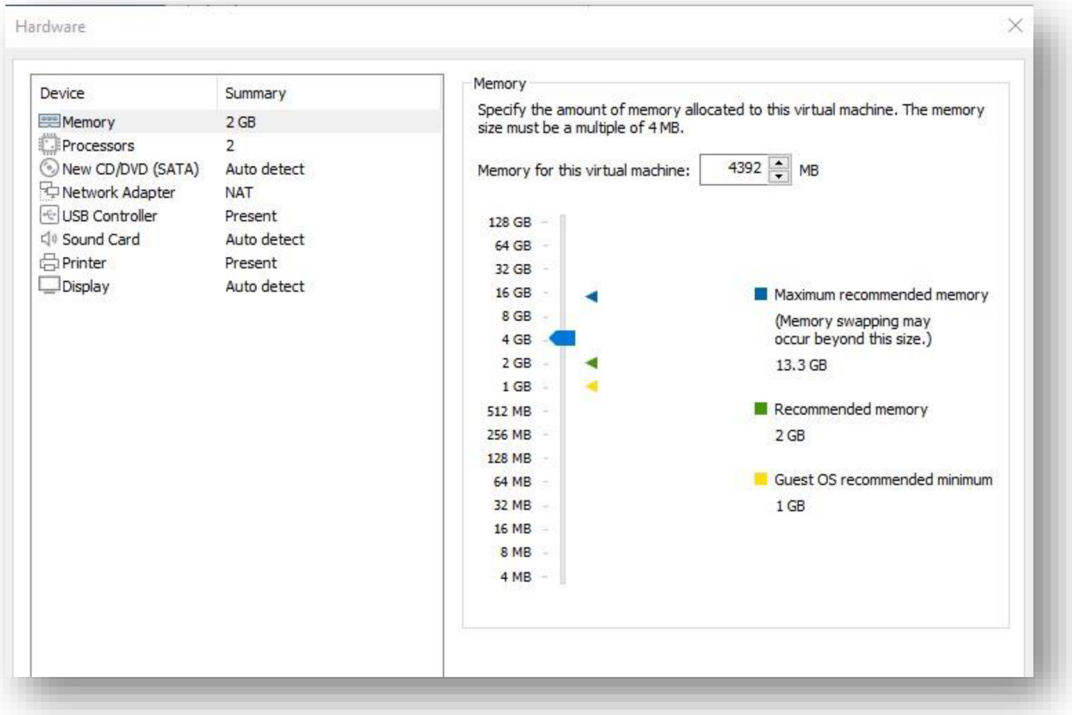
RAM paměti, procesorem a datovém uložišti. Tak jak data budou jen přibývat, je moudré alokovat zdroje hned ze začátku, z důvodu možného vyčerpání volných kapacit a nutnosti migrace na jiného hostitele.

Po instalaci vybraného hypervizoru přichází na řadu vytvoření a konfigurace virtuálního stroje. Bude demonstrován návrh praktické části pomocí Windows Serveru 2016 – Standart Edition. K instalaci bude zapotřebí ISO soubor tohoto operačního systému. ISO soubor je dostupný ke stažení na oficiálních stránkách Microsoftu či všude jinde na internetu. ISO soubor je zdarma ke stažení, ovšem hned po instalaci je uživatel vyzván k zadání sériového čísla produktu, z důvodu zabránění používání neautorizovaného produktu a porušení licenčních práv.

Prvním krokem při vytváření virtuálního stroje je alokace zdrojů. Zdroje jsou přebírané z hostitelského zařízení, na kterém bude virtuální stroj provozován. V tomto případě se bude jednat o běžný server se dvěma procesory, 4 GB RAM pamětí a základní síťovou kartou. Pro demonstraci bude plně dostačovat datové uložiště o kapacitě 100 GB.

Po úspěšném vytvoření virtuální stroje přichází na řadu instalace operačního systému. K tomuto kroku bude použit zmíněný ISO soubor. Jazyk systému ve většině případech bývá angličtina s českou klávesnicí pro usnadnění vstupu. Následuje instalace operačního systému. Pokud vše proběhlo úspěšně, uživatel je vyzván k zadání hesla od administrátorského účtu, pod kterým bude zpočátku operovat a konfigurovat server.

Heslo od administrátorského účtu musí být pečlivě vybíráno. Obsah hesla by měl dle bezpečnostních politik obsahovat nejméně 12–20 znaků, malá či velká písmena a speciální znaky. Pokud instalace proběhla korektně, lze se přihlásit do systému. Přichází řada na konfiguraci vytvořeného virtuálního serveru.



Obrázek 17 - Vytvoření virtuálního stroje

Zdroj: Autor

4.5. Základní konfigurace serveru

Pokud bylo docíleno úspěšně instalace hypervizoru a virtuálního stroje s operačním systémem, lze na něm začít operovat. Nyní budou demonstrovány základní technické a bezpečnostní postupy, které by se měly provést pokaždé na nově instalovaném serveru. Jedná se o soubor metod a postupů, které fungují běžně v praxi. Lze to nazvat obecným know-how, které se zaučuje v organizacích na pozicích juniora. Obecné základní znalosti při práci se serverovou infrastrukturou. Odborné postupy a konfigurace mají zabránit neoprávněnému přístupu na server. Nově nainstalovaný server nemusí zpočátku disponovat pokročilou zabezpečovací technologií, například firewallem či antivirem. Lze o něm tvrdit, že je holý a zranitelný.

Zmíněná konfigurace nemusí být prováděna ve stejném pořadí, jak udává diplomová práce. Konfigurační kroky lze provádět náhodně, avšak finální konfigurace serveru by měla zahrnovat všechny zmíněné postupy z důvodu docílení maximálního zabezpečení stroje a připravení k běžnému provozu.

4.5.1. Přejmenování serveru

Jedním z prvních kroků při konfiguraci serveru je jeho přejmenování. Server se uvnitř infrastruktury prezentuje pomocí hostname neboli jména. Je důležité pojmenovávat servery dle obecných a vnitropodnikových směrnic. Podnik může disponovat desítkami či stovkami serverů. Je zapotřebí je mezi sebou identifikovat. Samotný název by měl napovídat o jaký server se jedná, kde je uložen nebo jaká aplikace je na něm provozována. Často se při pojmenování serverů používají zkratky jako AP, která stojí za aplikačním serverem či DB, jakožto databázový server.

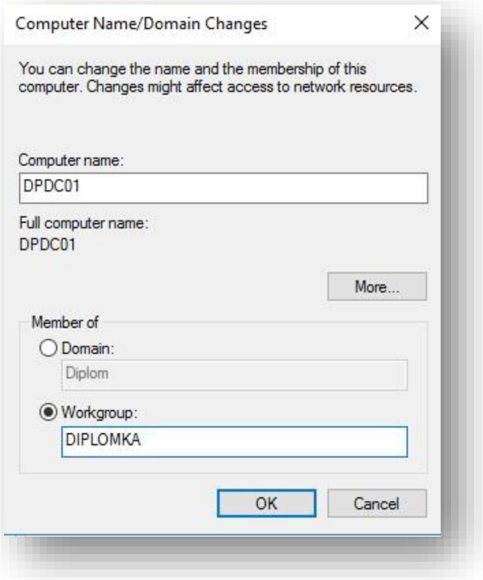
V demonstrovaném případě se bude jednat o doménový centrální řadič, na kterém budou provozovány další služby. Bude pojmenován DPDC01, kdy DP zaujímá název diplomové práce, DC je pojmenování pro domain controler neboli doménový řadič. Jelikož se jedná o první a zatím jediný server, náleží mu očíslování 01.

4.5.1.1. Přidání do domény

Při přejmenování serveru bude uživatel vyzván k zadání domény. Pomocí domény lze hromadně spravovat počítače a uživatele v organizaci.

Pokud podnik má zaregistrovanou doménu – následuje přidání počítače do domény. Uživatel je vyzván k zadání přihlašovacích údajů od správcovského účtu dané domény. Pokud je autentizace úspěšná, stanice se přidá do domény a je vyžadován restart stanice pro úspěšné dokončení změn.

Pokud podnik nemá zaregistrovanou doménu – nejedená se o velké omezení. Dočasně řešení může být používání workgroup. Také nazývané jako pracovní skupiny. Pracovní skupiny zastupují lokální domény v síti. Při instalaci DNS serveru si lze vytvořit vlastní lokální doménu, která bude jen v lokální síti.



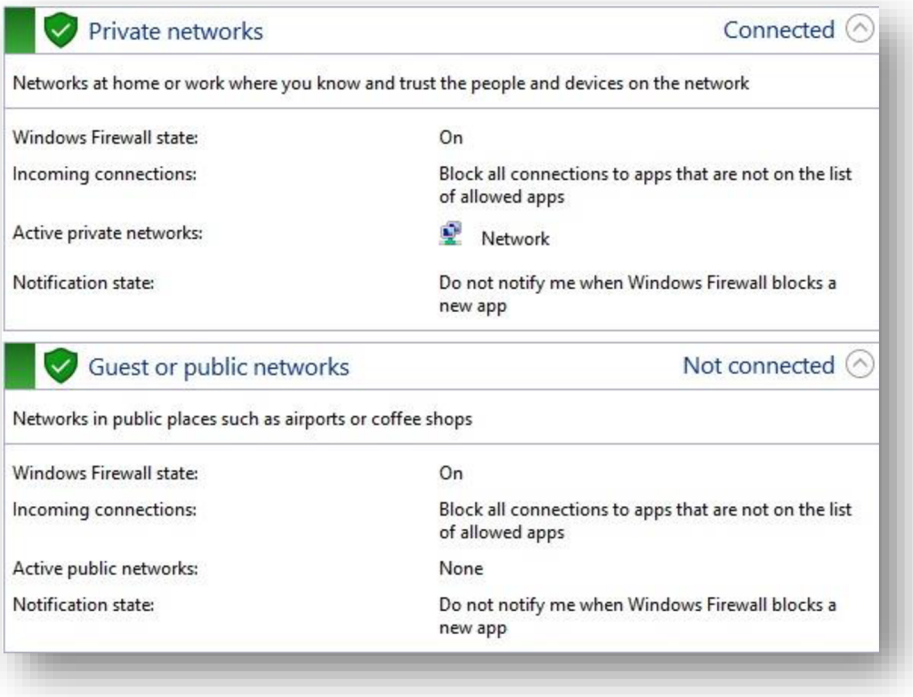
Obrázek 18 - Přejmenování pracovní stanice nebo serveru

Zdroj: Autor

4.5.2. Windows firewall

Operační systém Windows nabízí základní firewall v podobě softwarového řešení. Často se může stát, že při špatné instalaci serveru nebo na základě doménových politik může být tento firewall při prvotní instalaci vypnut.

Je důležité tento faktor zkontrolovat. Pokud podnik disponuje externím, již nasazeným a korektně nakonfigurovaným firewallem, může tento krok přeskočit. Avšak pokud neexistuje žádný jiný firewall než tento základní, je velmi důležité ho zapnout a průběžně kontrolovat jeho stav. Firewall je hlavním defensivním prvkem v síti, který brání před vnějšími útoky z internetu.



Obrázek 19 - Windows firewall

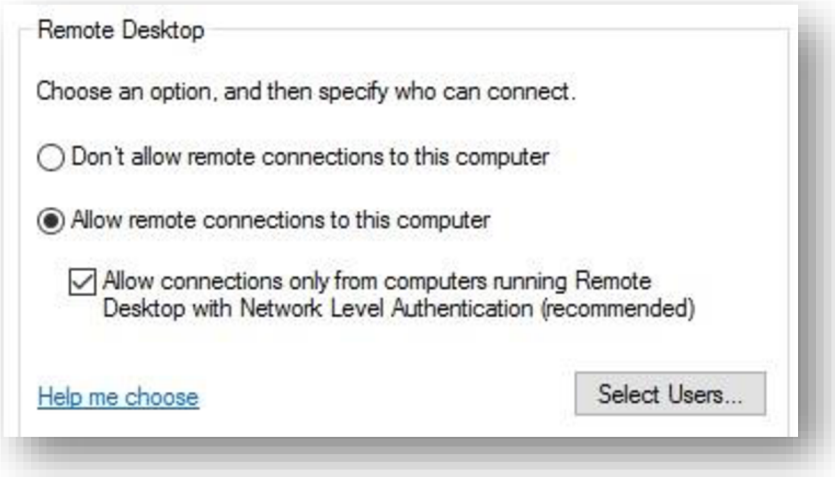
Zdroj: Autor

4.5.3. Vzdálená plocha – RDP

RDP – remote desktop protocol neboli v překladu přístup přes vzdálenou plochu, je funkce, kterou Windows nabízí k ovládání stanic či serveru vzdáleně. To znamená, že pomocí IP adresy se lze na danou stanici napojit, přihlásit a následně na ni operovat. Stejně jak kdyby uživatel pracoval se stanicí fyzicky.

Je potřeba si uvědomit, jakou roli a účel bude daný server zastávat. Zdali se na něj budou uživatelé a dodavatelé připojovat vzdáleně, nebo se bude jednat o virtuální stroj. Přístup na virtuální server lze taktéž realizovat pomocí hypervizoru. Jestli se RDP funkce na stanici povolí, server je vystaven většímu riziku neoprávněného přístupu.

Pokud má server RDP funkci vypnutou, jediným způsobem, jak na něm lze operovat je skrz hypervizor nebo fyzicky.



Obrázek 20 - RDP funkce

Zdroj: Autor

4.5.4. Nastavení statické IPv4 adresy

Každý server by měl mít nastavenou statickou IP adresu, pokud se nejedná o dočasné zařízení. Toto pravidlo ulehčuje administraci zařízení v podniku, evidenci a bezpečnostní audity.

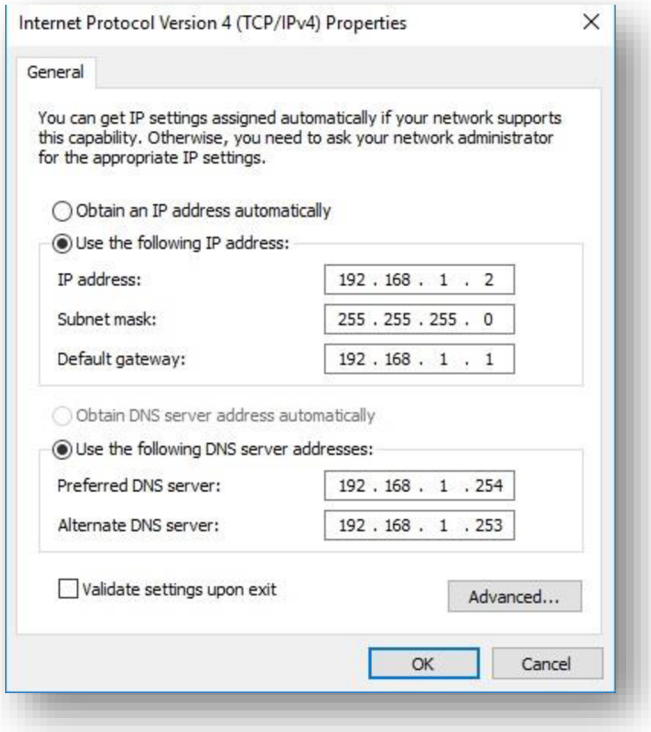
Server disponuje oprávněními, kam může přistupovat. Je členem skupin v Active Directory anebo má nastavené prostupy na firewallu. Tyto vlastnosti souvisí s jeho IP adresou. Pokud by server dostával pokaždé novou IP adresu od DHCP serveru, udělené přístupy by byly ztraceny. Každý podnik by si měl vést evidenci zařízení v podniku a jejich statických IP adres.

Demonstrovaný server nebudete výjimkou. Následuje konfigurace statické IP adresy. Uživatel se naviguje do nastavení síťového rozhraní a zvolí IP verzi 4 – IPv4. Pokud by měla být demonstrována reálná ukázka z praxe, administrátor v podniku by se nejdřív podíval do evidence volných pozic v subnetu. Na základě tohoto faktu by byla vybrána volná IP adresa. Adresa by se přiřadila danému zařízení a volné místo v evidenci by bylo přepsáno názvem serveru.

Jelikož se jedná o testovací prostředí, IP adresu si může uživatel zvolit libovolně. Pro demonstrativní účely bude zvolena IP adresa 192.168.1.2/24 s maskou C, tedy

255.255.255.0. Číslování začíná od dvojky, jelikož zpravidla na první pozici je vždy gateway. Gateway bude mít adresu 192.168.1.1/24. Pokud by existoval již vytvořený DNS server a jeho alternativní náhrada, pole pro DNS by obsahovaly reálné IP adresy. V ukázkovém příkladě budou pro DNS servery zvoleny testovací IP adresy 192.168.1.254 a 192.168.1.253.

Po této konfiguraci má demonstrativní server nastavenou statickou IP adresu a je připravený k dalším konfiguracím.



Obrázek 21 - Nastavení statické IPv4 adresy

Zdroj: Autor

4.5.5. Windows Defender

Stejně jako u předešlého odstavce s firewallem i zde bude zpočátku operováno se základním antivirem Defender, který je předinstalovaný v operačním systému Windows. Tento antivirus prošel významnou změnou za posledních pár let. Společnost Microsoft se na Defender velmi zaměřila a vyvinula antivirus, který je zdarma, již před implementován a schopný konkurovat komerčním antivirům. Autor diplomové práce taktéž využívá tento

antivirus pro své soukromé potřeby a musí podotknout absolutní spokojenost s tímto bezpečnostním prvkem.

Placená verze antiviru pro podniky se jmenuje Microsoft Defender pro firmy. Tento produkt je nadstavbou klasického Microsoft Defenderu. Umožnuje dodatečné funkce a možnost nasazení do infrastruktury jakožto plnohodnotný antivirus.

Vrátíme se zpět k základnímu Defenderu. Na testovacím serveru je zapotřebí zkontrolovat, zdali je antivirus aktivní. Nesmí se opomenout aktualizace virové databáze.

4.5.6. Windows Updates

Na základě instalačního ISO souboru se může stát, že nainstalovaný operační systém může být zastaralý. Je zapotřebí server aktualizovat na nejnovější verzi a nastavit pravidelné aktualizování dle podnikových směrnic. Windows aktualizace se nachází v ovládacím panelu operačního systému. Pokud systém nenabízí žádné aktualizace, lze je takzvaně vynutit a zaktualizovat na nejnovější verzi.

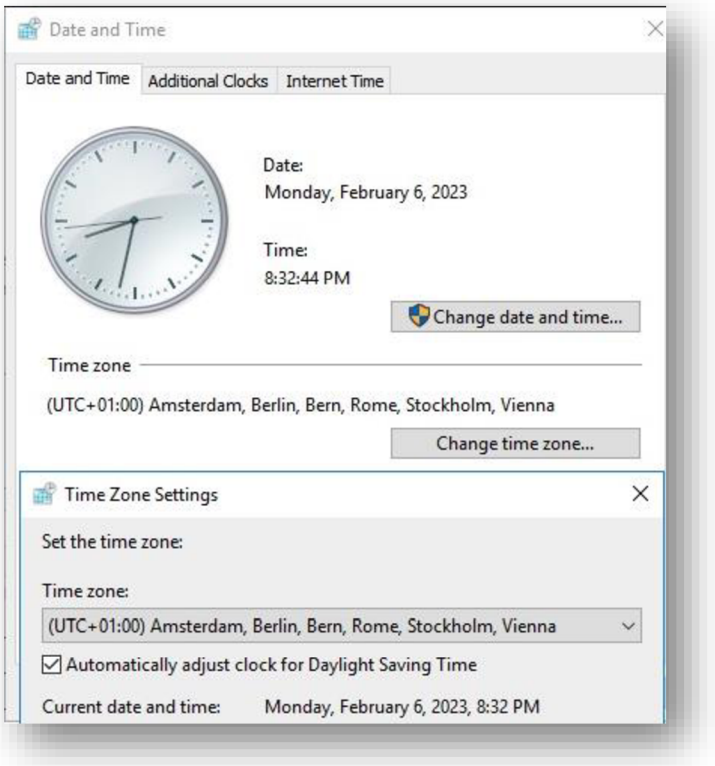
Pokud bude daný podnik v budoucnu disponovat více stanicemi a servery. Nezbytným krokem bude zřízení aktualizačního serveru. Tento server vykonává funkci přístupového bodu. V případě, že vyjde nová aktualizace, aktualizační server si tuto aktualizaci stáhne k sobě. Následně pomocí LAN sítě aktualizaci rozdistribuuje dál do podniku pomocí komunikačních linek bez nutnosti zatěžování internetové přípojky.

Ve Windows Updates lze zvolit i dobu aktivního používání. To znamená časové rozmezí, kdy se nemají provádět aktualizace z důvodu práce na těchto stanicích.

4.5.7. Nastavení času a časové zóny

Jako poslední základní konfigurací na serveru je nastavení času a časové zóny. I když se to může zdát jako triviální věc, všechny servery a stanice by měly být časově synchronizované. Společná synchronizace je důležitá kvůli plánovaným aktualizacím, odstávkám a dalším úkonům. Pokud bude mít server nesprávně nastavený čas, může docházet k nestabilnímu chodu aplikací na něm a dalším drobným výpadkům, které mohou být pro provoz rizikové.

Pro demonstrativní účel bude zvolen evropský čas, tedy UTC +1:00 (Amsterdam, Berlín, Řím, Vídeň).



Obrázek 22 - Nastavení času a časové zóny

Zdroj: Autor

4.6. Instalace doménového řadiče

4.6.1. Základní informace

Doménový řadič, jak již název napovídá, řídí celou doménu. To znamená, že se jedná o centrální prvek, který bude spravovat všechny služby provozované uvnitř domény. Doménových řadičů může být více záleží dle architektury podnikové sítě. Pro demonstraci bude realizován návrh řešení pomocí jednoho centrálního řadiče.

Nutno podotknout, že ne každý server je ihned doménovým řadičem. Musí se takzvaně povýšit na tuto funkci. Aby server byl připravený na tuto promoci, musí splňovat

všechny předešle konfigurační kroky, které byly uvedeny v předešlých částech diplomové práce.

Po instalaci doménového řadiče bude administrátor spravovat doménu právě pomocí tohoto centrálního prvku. To znamená, pokud bude chtít přidávat uživatele, počítač do domény či upravit bezpečnostní politiku, musí se přihlásit na doménový řadič a tyto změny provádět zde.

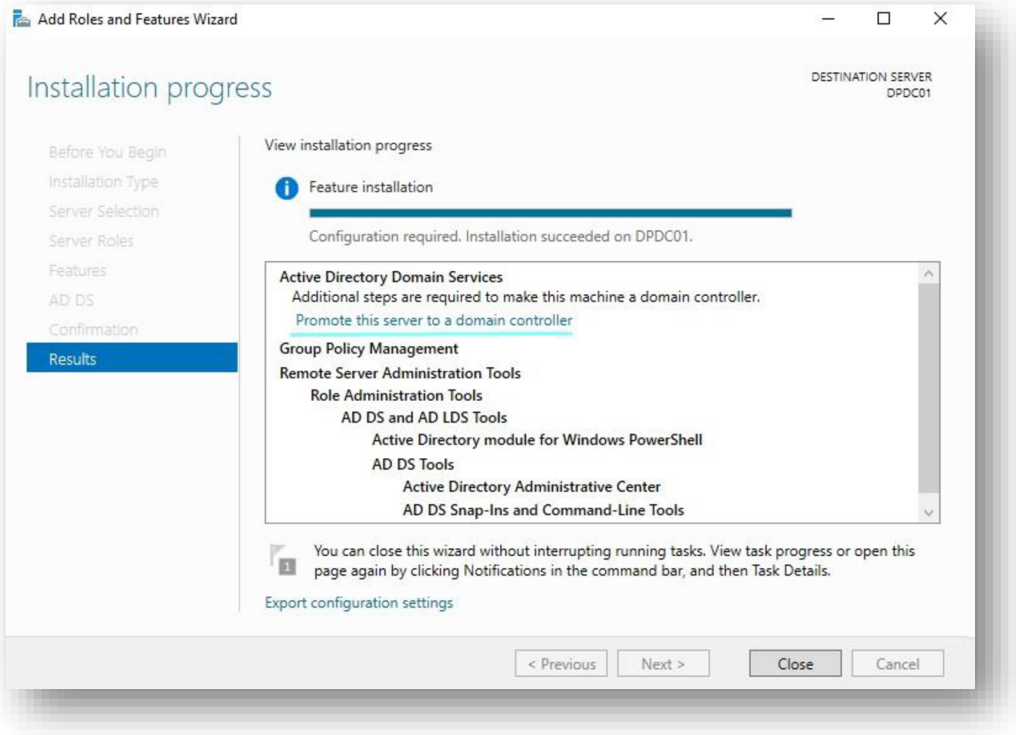
Autor diplomové práce by rád podotknul, že následující postup instalace řadiče lze také provádět v příkazové řádce PowerShell. Všechny úkony mohou být prováděny přes speciální příkazy. V praxi to tak i běžně funguje. Dodavatelé služeb či kompletních řešení mají již předpřipravené scripty a příkazy, které jen aplikují. Jedná se o velmi efektivní práci z hlediska časové náročnosti. V tomto případě bude instalace prováděna pomocí grafického rozhraní.

4.6.2. Instalace Active Directory a povýšení na doménový řadič

Pokud server prošel základní konfigurací, je připravený. Veškeré konfigurační prvky nebo dodatkové služby lze instalovat pomocí lokálního nastavení serveru. Instalace hlavních a dodatkových služeb je poměrně jednoduchá, tak jak veškerý proces instalovaní řídí průzkumník instalací.

Pro základní demonstraci bude dostačovat instalace *Active Directory Domain Services*. Průzkumník instalací nabídne další doplňkové služby, které mohou být v doprovodu s touto službou nainstalovány. Prozatím tento krok lze přeskočit a dokončit instalaci Active Directory.

Po úspěšné instalaci systém vyzve uživatele k možnosti povýšení daného serveru na doménový řadič. K docílení povýšení doménového řadiče je zapotřebí potvrzení volby. Následuje povýšení serveru.



Obrázek 23 - Instalace AD a povýšení doménového řadiče

Zdroj: Autor

Pokud povýšení serveru proběhlo úspěšně, systém vyzve uživatele k vytvoření hesla od *DSRM – Directory Services Restore Mode* neboli služby obnovy celého Active Directory. Jedná se o bezpečnostní prvek, který umožnuje obnovit nastavení celého AD v případě, že dojde ke kompromitaci, ztrátě dat či obnově po hackerském útoku.

4.6.3. Active Directory

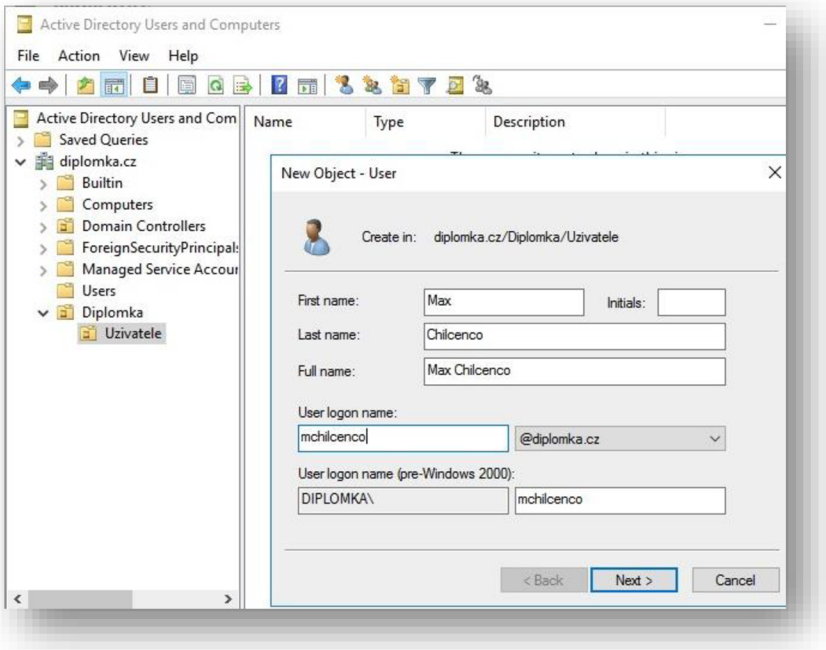
Active Directory, ve zkratce AD, je nástroj v operačním systému Windows pro správu domény, oprávnění a členů uvnitř domény. Při prvotní instalaci AD se průzkumník doptá uživatele, zdali již existuje organizační doména či bude vytvořena nová.

Pro demonstraci bude vytvořena nová doména s názvem diplomka.cz. Název by měl být objektivní a identifikovatelný. Pro přesvědčení o úspěšné instalaci se může uživatel sám podívat na volbu – Active *Direcory Users and Computers*. Služba je umístěna v nastavení lokálního serveru.

Pokud by se jednalo o reálný podnik v praxi, prvním krokem by bylo vytvoření stromové struktury adresářů s uživateli, kterým by se následně přiřadily skupiny a patřičná oprávnění. V tomto případě bude plně dostačovat testovací adresář a jeden testovací uživatel.

Pomocí pravého kliku na doménu v oblasti AD lze zvolit možnost New, Organizational Unit. Tímto úkonem se vytvoří adresář. Nyní přichází na řadu vytvoření uživatele. Proces vytvoření lze duplikovat až na poslední krok. Jelikož probíhá vytvoření uživatele, je nutné zvolit v tomto případě New, User. Po úspěšném vytvoření testovacího uživatele je nezbytné vyplnit dodatečné informace o subjektu za účelem lepší identifikace v AD.

Atributy jména a příjmení jsou jasné. Ovšem uživatelský login a jeho tvar jsou většinou v podniku udávaný předefinovanou syntaxí. Pomocí tohoto loginu se bude uživatel později přihlašovat do domény. Ve většině případů se jedná o jednoduchou syntaxi jakožto první písmeno ze jména a celé příjmení. Avšak každý podnik má svá pravidla a jiné potřeby. V našem případě bude použita klasická syntaxe. Jméno Maximilian Chilcenco bude po aplikovaní syntaxe přeměněno na mchilcenco.



Obrázek 24 - Vytvoření uživatele v AD

Zdroj: Autor

4.6.4. DNS – Domain Name System

Spolu s Active Directory a povýšení serveru na doménový řadič se v instalačním balíčku služby nainstalovala i služba DNS – Domain Name Systém neboli v českém překladu služba pro překlady jmen. Tato služba umožnuje převádět IP adresy na doménová jména a zpětně.

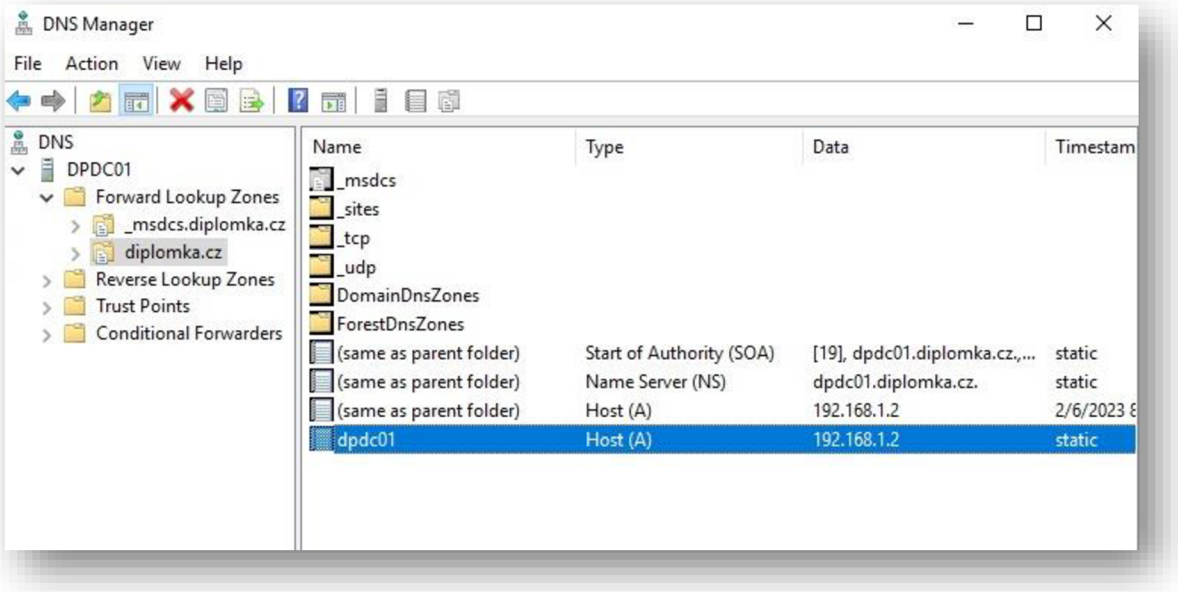
Pro příklad, pokud uživatel zadá adresu 77.75.79.222 do webového prohlížeče, dostane se na odkaz www.seznam.cz. Pro lidský mozek je lépe zapamatovatelný text nežli dlouhé číselné řetězce. Celý princip funguje následovně. Pokud uživatel zadá do vyhledávače www.seznam.cz, prohlížeč odešle dotaz na centrální DNS server doptávající se po IP adrese této webové stránky. Server odpoví a zašle prohlížeči IP adresu. Webový prohlížeč odpověď přijme a zobrazí obsah webové stránky.

V demonstrativním případě se bude jednat o podobný scénář. V podniku se běžně provozují interní webové stránky, systémové služby dostupné přes webové rozhraní a tak dále. Je nezbytnou součástí mít DNS službu implementovanou v doméně z důvodu zajištění validních překladů adres. Do DNS konfigurace se lze dostat přes nastavení lokálního serveru.

Práce s DNS službou je poměrně jednoduchá. V ukázkovém případě lze najít jen jeden překlad. Jedná se o hostname DPDC01 na adresu 192.168.1.2, což odpovídá IP adrese serveru. Pokud by jakákoliv služba pracovala napřímo s MAC adresou zařízení a nevěděla by IP adresu daného zařízení. Služba by se doptala DNS serveru. Na základě tohoto dotazu DNS server zprostředkuje odpověď spolu s doptávanou IP adresou.

Existuje 2 typy překladů, jedná se o:

Forward Lookup Zone – Překlad z hostname na IP adresu
Reverse Lookup Zone – Překlad z IP adresy na hostname



Obrázek 25 - Konfigurace DNS

Zdroj: Autor

4.7. DHCP – Dynamic Host Configuration Protocol

Služba DHCP umožnuje automaticky přidělovat a zapůjčovat volné IP adresy z rozsahu. Tato služba nepřiděluje jenom IP adresy, ale kompletní síťovou konfiguraci dané sítě. To znamená, že nastaví nově připojenému klientovi IP adresu, masku sítě, gateway bránu a adresu DNS serveru. Tyto základní informace potřebuje nově připojený klient, aby byl schopný komunikace v dané síti.

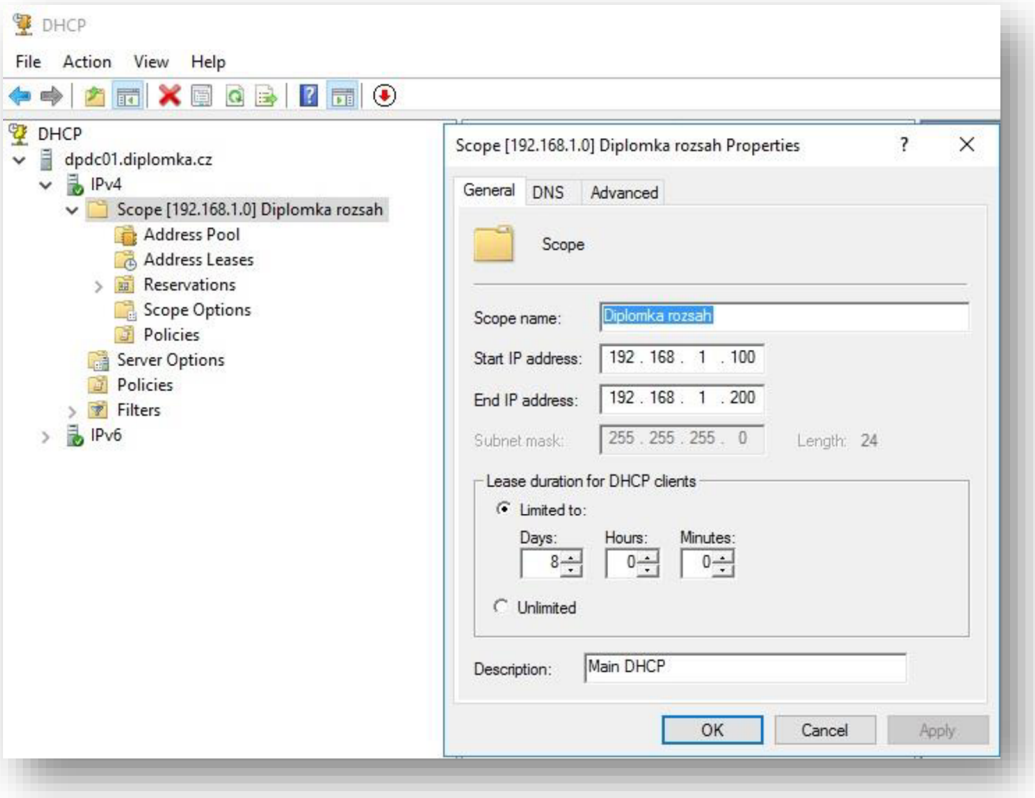
Jelikož se služba nenachází v základním balíčku instalace Windows Serveru, musí jí uživatel doinstalovat, tak jak tomu předcházelo u předešlých služeb. Instalační průzkumník se nachází jako vždy v lokálním nastavení daného serveru. Po úspěšné instalaci dodatkové služby na server lze přistoupit ke konfiguraci.

DHCP služba nabízí konfiguraci dvou typů adres. Jedná se o IPv4 a IPv6. Pro demonstraci bude použita IP adresa verze 4. Pro přidání nového rozsahu je nutné zvolit možnost – *New Scope*.

Ukázkový server disponuje statickou IP adresu 192.168.1.2/24, gateway brána se nachází na IP adrese 192.168.1.1/24. Následně bude prezentován reálný příklad z praxe.

Prvních 100 IP adres v rozsahu budou přidělena stanicím, serverům, tiskárnám a dalším síťovým zařízením. Na adresách 192.168.1.253/24 a 192.168.1.254/24 by se nacházely DNS servery. Takže tyto IP adresy jsou také obsazeny. Pomocí hrubého odhadu bude zvolen dostupný rozsah pro přidělování adres novým zařízením v rozsahu 192.168.1.100 – 192.168.1.200/24.

Pokud se do podnikové sítě LAN připojí nové zařízení, které nebude mít nastavené statickou IP adresu a doptá se DHCP serveru pro přidělení adresy. DHCP server mu přidělí IP adresu z rozsahu 192.168.1.100 – 192.168.1.200/24.



Obrázek 26 - Konfigurace DHCP

Zdroj: Autor

4.8. BitLocker

Jedná se o kryptografickou funkci implementovanou v každé verzi operačního systému Windows. Tato služba, či chceme-li funkce, slouží k šifrování systémových disků

a diskových svazků. Funkci lze využívat na stanicích a serverech k prevenci neoprávněného přístupu k daty. Po aktivování BitLocker funkce se disk zašifruje speciálním šifrovací algoritmem. Aby byl uživatel schopen používat data uložená na zašifrovaném disku, je nutná autentizace pomocí hesla.

Následuje demonstrace zprovoznění a konfigurace BitLocker šifrovací funkce. Doplňkovou funkci opět lze nainstalovat pomocí průzkumníka v lokálním nastavení serveru. BitLocker se ve většině případech, je tak i nastavený v základní konfiguraci, využívá společně s TPM čipem. Jedná se o kryptografické uložiště buď na základní desce počítače nebo na přenosném uložišti v podobě tokenu.

Pro efektivní ukázku je zapotřebí nutnost TPM čipu vypnout pomocí politiky. V nastavení doménových politik se nachází sekce s BitLocker funkcí. Nutno zvolit možnost – Require additional authentication at startup, v překladu vyžadovat dodatečné ověření při spuštění. Základní stav této politiky je nenastaven, tedy zakázán. Pokud chce uživatel využívat služby BitLockeru bez TPM čipu, musí tuto politiku aktivovat.

V rámci demonstrace bude zvolená politika aplikovaná na celou doménu diplomka.cz. Administrace BitLocker se nachází v ovládacích panelů serveru, záložka systém a zabezpečení. Po zapnutí BitLocker funkce systém vyzve uživatele k vytvoření přístupového hesla, díky kterému se bude autentizovat. Instalační průzkumník nabídne, jakým způsobem má být uložen náhradní přístupový klíč, pokud dojde ke ztrátě primárního hesla. Záložní klíč nelze uložit na stejnou stanici či server, kde bude aplikován BitLocker z důvodu zašifrování celého uložiště. BitLocker nabízí dvě možnosti šifrování. Kompletní šifrování celého disku nebo jen zapsaných dat. Posledním krokem uživatel potvrdí zvolenou volbu a zahájí šifrování disku. Pokud šifrování disku proběhlo úspěšně, instalační průvodce bude vyžadovat restart operačního systému.

Po provedeném restartu si lze ihned všimnout zásadních změn. Uživatel je vyzván funkcí BitLocker k zadání přístupového hesla, díky kterému se autentizuje. Teprve po autentizaci dojde ke spuštění operačního systému se zašifrovaným diskem.

Obrázek 27 - Konfigurace BitLockeru

Zdroj: Autor

4.9. Antivirus – Trend Micro Apex One

K zajištění bezpečného chodu organizace je nezbytnou součásti provozovat antivirovou ochranu na vnitropodnikových stanicích a serverech. Útoky na zařízení mohou přicházet odkudkoliv. Kybernetické útoky mohou být směřovány z internetu nebo dokonce z interního perimetru. Neproškolený uživatel může přinést zavirované zařízení z domova. Z důvodu přebytečně vysokých oprávnění mu bude umožněno použíti přenositelných flash disků v interní sítí. Jedná se o otázku času, než dojde k bezpečnostnímu incidentu. Ideální scénář, který je bohužel běžný v praxi. I kdyby daný podnik disponoval bezpečnostními prvky za miliony korun, tím nejslabším článkem v bezpečnosti bude vždy uživatel.

Antivir by měl všechny tyto hrozby odrazit a být schopen preventivně zabezpečit zařízení. Efektivně hrozbu eliminovat a následně provést kontrola systému, zdali se v systému nevyskytuje škodlivý kód. Technologické standarty na zabezpečení sítí a stanic se neustálé zvyšují. Dnešní antiviry, komerční či enteprise, neposkytují pouze antivirovou ochranu ale i další funkce, které jsou v produktu zahrnuty.

Pro demonstraci bude využit enterprise antivirový produkt Trend Micro Apex One od firmy Trend Micro. Tato firma se primárně soustředí na podniky velkého rozsahu. Běžný

uživatel se s tímto produktem často nesetká. Trend Micro Apex One antivir nabízí pokročilou antivirovou ochranu a další funkce, které nebývají součásti základních balíčků antivirů. Jako doplňkové služby můžeme zmínit funkci device control, která umožnuje spravovat všechna připojená nebo nově připojená zařízení na stanicích a serverech. V antivirovém rozhraní lze zakázat připojení jakýkoliv přenosných zařízení, pokud se jedná o běžného uživatele a dotyčný nebude disponovat příslušnými oprávněními.

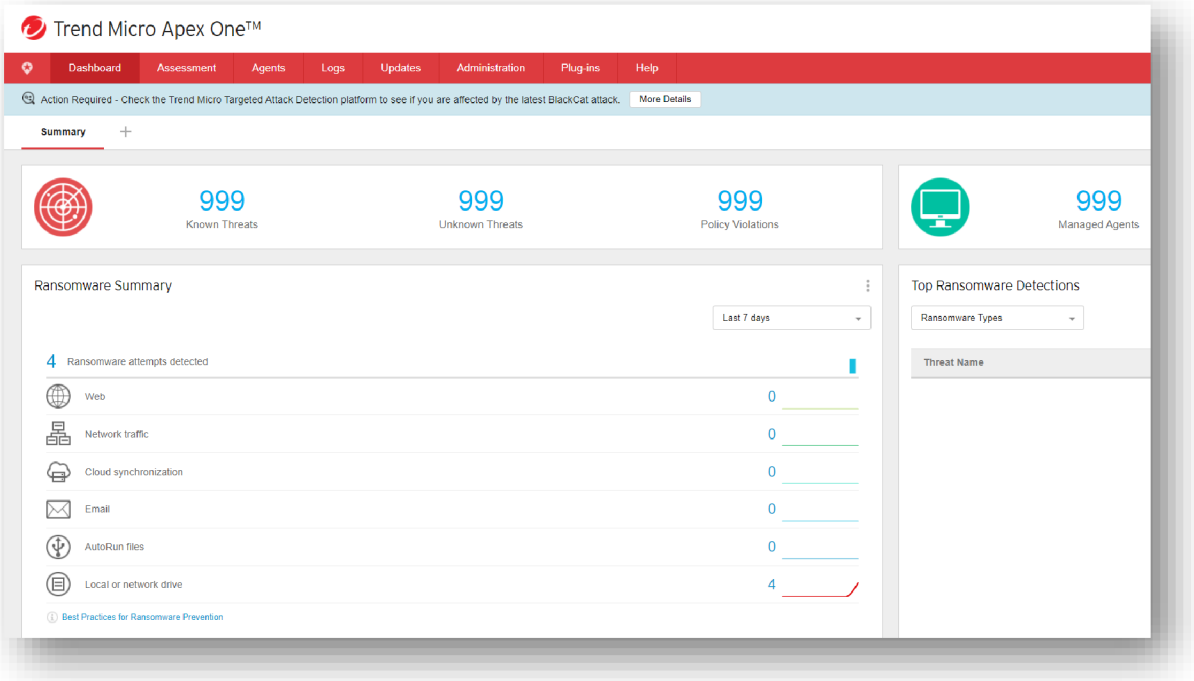
Další funkcí, kterou je důležité zmínit je Data Lose Protection, ve zkratce DLP. Jedná se o funkci, která má za úkol kontrolovat citlivá data, aby nebyla zneužita, odeslána skrz email či fyzicky vynesena ven z podniku. Hlavním principem je definování citlivých dat a informací. Může se jednat například o rodná čísla, číslo objednávek atd. Citlivá data jsou relevantním údajem, musí je každý podnik stanovit sám. Jedná se o subjektivní záležitost. Tato služba funguje na pozadí stanice. Hlavním úkolem je monitorovaní vymezené skupiny citlivých dat. Pokud dojde k narušení či nekorektnímu zacházení s těmito daty, daný proces se ukončí a odešle bezpečnostní hlášení příslušnému správci.

Trend Micro Apex One antivir funguje na agentovým principu. Na každé stanici či serveru je nainstalovaný agent, který zařízení monitoruje. Všechny agenty mezi sebou komunikují přes centrální server, který lze konfigurovat pomocí webového rozhraní. Veškeré antivirové změny, aktualizace virové databáze a konfigurace se provádějí na centrálním prvku. Po provedených změnách centrální prvek rozdistribuuje informace o novém nastavení na jednotlivé agenty.

4.9.1. Náklady na nákup a provoz antiviru

Název produktu	*Počet ks*	*Typ*	*Cena za kus*	*Cena podpory na rok*	*Celkový náklad na první rok provozu v Kč*
Antivir – Trend Micro	1	SW	x	3 000 000,-	3 000 000,-

Tabulka 1 - Náklady na nákup a provoz antiviru



Obrázek 28 - Antivirus Trend Micro Apex One

Zdroj: Autor

4.10. Next-Generation Firewall – Fortigate

Na začátku praktické části diplomové práce byl představen softwarový firewall, zabudovaný v operačním systému Windows. Tento firewall poskytuje základní ochranu v sítové komunikaci. Pro demonstrativní účely a testování bude představen fyzický Next-Generation firewall od firmy Fortigate, který poskytuje širší spektrum zabezpečení. Fyzický prvek bude vždy lepší, spolehlivější, a hlavně výkonnější než softwarový klient.

Next-Generation Firewall od firmy Fortigate představuje jedno z nejlepších fyzických firewall řešení na aktuálním trhu. Firma Fortigate se zaměřuje jak na velké enterprise podniky, tak i na začínající malé firmy či soukromé domácnosti. Next-Generation firewall, jak bylo již pojednáno v teoretické části, obsahuje spoustu defenzivních prvků a umožnuje kompletní zabezpečení síťového provozu. V ukázkové demonstraci lze simulovat vlastní scénáře užití a bezpečnostní protokoly, které firewall poskytuje. V tomto případě se bude jednat o návrh řešení, při kterém bude firewall uveden do provozu při prvotním fyzickém zapojení do sítě. Následuje základní konfigurace a připravení na běžný

provoz v podniku. Hlavním úkolem demonstrace je zajistit, aby se uživatele v podnikové síti dostali bezpečně na internet. Veškeré konfigurační kroky, které budou následovat lze opět provádět jak v grafickém prostředí, tak i příkazové řádce.

Při prvotním zapojení Fortigate firewallu do vnitropodnikové sítě je nezbytné nastavit statickou IP adresu, masku sítě a základní gateway bránu. Nutno podotknout, že stavebním kamenem celé sítové infrastruktury je právě firewall. Pokud bude tento prvek špatně nakonfigurován, neprojde žádná síťová komunikace do podniku ani ven z podniku. Je důležité promyslet, kde v síťové topologii se bude firewall nacházet a přenechat konfiguraci na odborném personálu. V demonstraci se budou vyskytovat 2 interface rozhraní. První interface pro síť WAN, který bude komunikovat ven do internetu. Druhý pro vnitropodnikovou síť LAN, kde se budou nacházet všechna ostatní zařízení v podniku.

Při konfigurování interfacu je nezbytné pojmenovávání pomocí aliasu, z důvodu lepší organizace a pozdější manipulace v rozhraní. Každý z interfacu musí mít vlastní IP adresu. WAN interface bude disponovat adresou 192.168.1.252/255.255.255.0, totožná s adresou routeru. V LAN interfacu bude obsažen rozsah z interní sítě, tedy IP adresa 192.168.1.3/255.255.255.0. Každému interfacu lze konfigurovat administrátorské funkce, jako například protokoly HTTPS, ICMP, SSH, SNMP a tak dále. Je důležité určit jaké protokoly budou povoleny z důvodu možného zneužití a zahlcení síťového provozu. Například pomocí protokolu ICMP, tedy ping.

Pokud jsou interfacy připravené a nakonfigurované, lze postoupit k routovacím pravidlům. Účelem demonstrace je povolení přístupu uživatelům na internet. Pro tento typ příklad bude zvoleno universální pravidlo pro routování. To znamená, že routovací destinace bude mít hodnoty 0.0.0.0/0.0.0.0. Nutno připomenout nastavení gateway brány, která má adresu v síti 192.168.1.1/255.255.255.0. Tímto krokem bylo docíleno, kam má firewall routovat neboli směřovat při komunikaci ven ze sítě.

V neposlední řadě je důležité definovat firewall politiky. Ty udávají takzvané prostupy. To znamená, z jaké adresy či interfacu je umožněna komunikace a kam. Tato politika bude z důvodu korektní administrace pojmenována jako – internet přístup. V konfiguraci firewallu je nutné nyní propojit oba interfacy. To znamená příchozí

interface z LAN sítě a odchozí interface z WAN sítě. V tomto kroku lze definovat pro jaká zařízení bude politika aplikována, lze nastavit i výjimky. Pro demonstraci bude použito základní nastavení tedy pro všechna zařízení. V posledním kroku konfigurace se uživatel setká se defenzivními prvky firewallu. Pomocí politiky lze nastavit jaká kontrola má být prováděna při vykonání dané politiky. Firewall nabízí tyto defenzivní služby:

- Antivirus – Antivirová kontrola
- Web Filter – Kontrola webu na základě jeho scóre
- DNS Filter – DNS kontrola
- Aplikační kontrola – Kontrola aplikace na základě scóre, certifikátu dalších hodnot
- IPS – Virtualizace paketů, rozebraní komunikace na pakety
- SSL Inspection – Kontrola na základě SSL

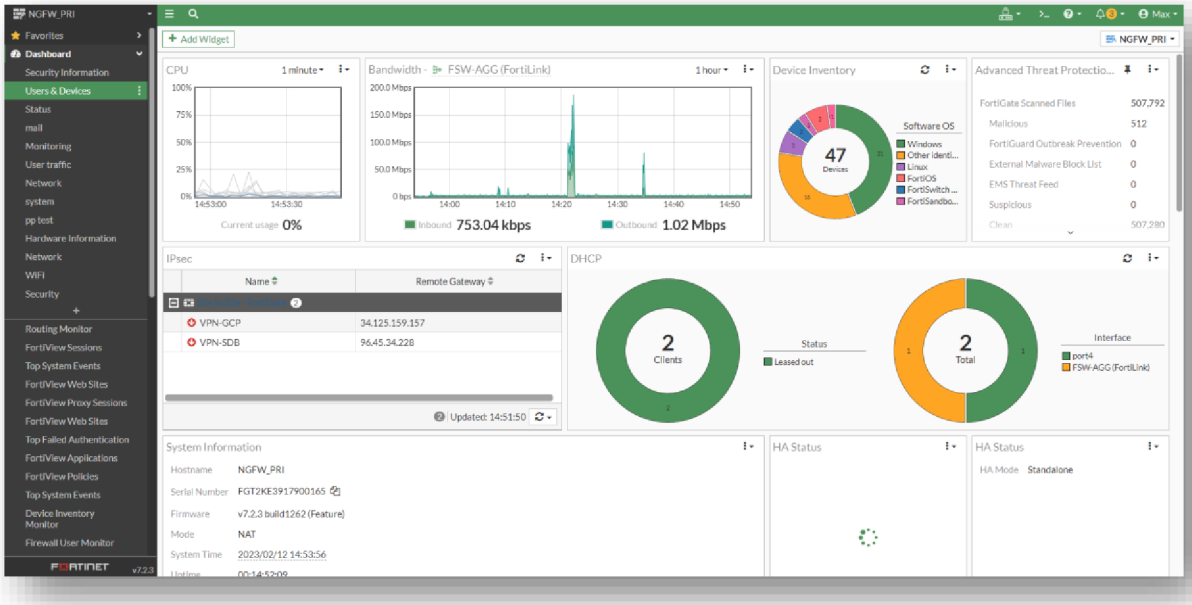
Posledním krokem konfigurace bývá volba překladu adres pomocí NAT funkce, která má za úkol překládat vnitřní IP adresy na veřejné. Důležitým aspektem, který by neměl uživatel vynechat je zapnutí logování firewallu pro případné auditování či řešení provozních výpadků.

Demonstrativním postupem bylo docíleno konfigurace Fortinet Firewall při prvotním zapojení do vnitropodnikové sítě. Konfigurace obnášela nastavení statické IP adresy pro administraci zařízení, definice a vytvoření síťových interfacu, nastavení routovacího pravidla a tvorbu bezpečnostních politik, které umožnují přistupovat a komunikovat z lokální sítě do internetu.

4.10.1. Náklady na nákup a provoz firewallu

Název produktu	*Počet ks*	*Typ*	*Cena za kus*	*Cena podpory na rok*	*Celkový náklad na první rok provozu v Kč*
Firewall – Fortigate 1500D	2	HW	39 570,-	18 000,-	97 140,-

Tabulka 2 - Náklady na nákup a provoz firewallu



Obrázek 29 – Next-Generation Firewall Fortigate

Zdroj: Autor

4.11. Proxy Server – Trend Micro IWSVA

Jelikož má MSP zakoupené hromadné enteprise licence na Trend Micro produkty, spadá sem i licence na proxy server a poštovní antivirus. Proxy server je defenzivní prvek umístěn v síti, který má za úkol zprostředkovávat požadavky zasílané ze strany uživatele. Proxy server může mít spoustu účelů. Například uchovávat nejčastěji navštěvované internetové stránky do své cache paměti, aby nedocházelo k opakovanému doptávání se DNS serveru a zahlcování komunikační linky.

Hlavním prvek je bezpečnost, který proxy server umožnuje. Pokud uživatel komunikuje směrem do internetu, komunikace probíhá skrz proxy server. To znamená, že identita, lokace a další citlivá informace o klientovi zůstávají v utajení. Pokud by došlo ke kybernetickému útoku na uživatele, útočník by musel nejdřív cílit svůj útok na proxy server. Následně pokračovat přes další bezpečnostní prvky. Na závěr směřovat útok na samotného uživatele.

MSP je vybaveno několika proxy servery, které mezi sebou komunikují a sdílí konfigurace. Tyto proxy servery jsou následně korigovány balancery F5, které přehazují

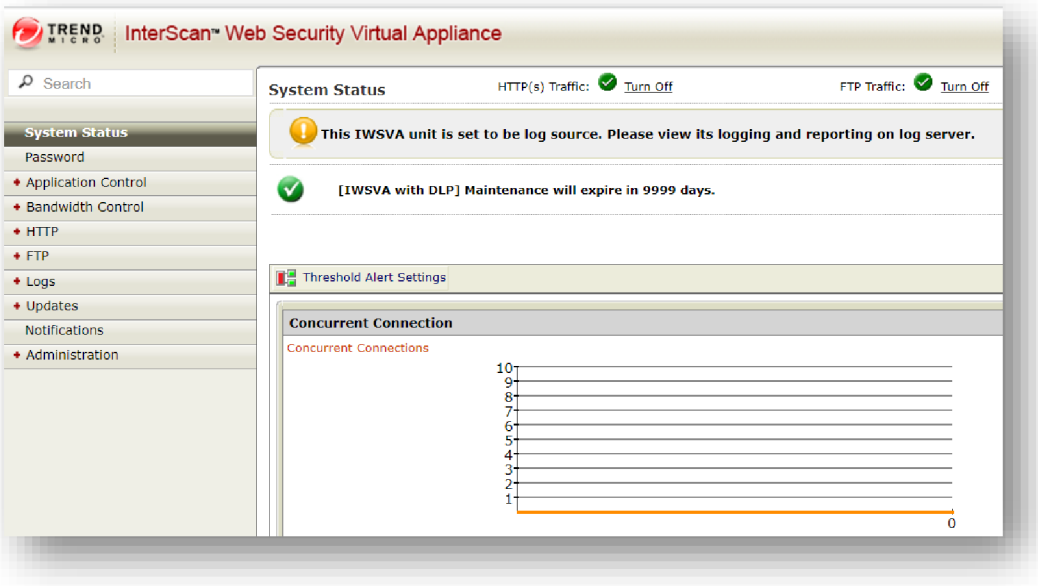
technickou zátěž mezi servery a řídí celkovou komunikaci za účelem vzájemné spolupráce. Proxy server v tomto případě zaujímá roli bezpečnostního a kontrolního prvku. Síťová architektura je postaveny tak, aby veškerá komunikace směřována do internetu putovala právě přes tyto proxy servery. Díky této architektuře lze monitorovat uživatelskou aktivitu na internetu. Na základě toho faktu přijímat vnitropodniková opatření jako povolování či blokování webových stránek.

Proxy server od firmy Trend Micro je vybavený poštovním antivirem IWSVA, který má za úkol blokovat nevyžádané či virové zprávy ještě před ním, než dorazí na poštovní servery a samotným uživatelům.

4.11.1. Náklady na nákup a provoz proxy serveru

Název produktu	*Počet ks*	*Typ*	*Cena za kus*	*Cena podpory na rok*	*Celkový náklad na první rok provozu v Kč*
Proxy Server – Trend Micro IWSVA	6	SW	x	65 000,-	390 000,-

Tabulka 3 - Náklady na nákup a provoz proxy



Obrázek 30 - Proxy server Trend Micro

Zdroj: Autor

4.12. Antispam – Barracuda Email Security Gateway

Antispam zaujímá pozici bezpečnostního prvku v sítí, který má za úkol monitorovat poštovní provoz v podniku. Umístění tohoto zařízení v síti se doporučuje těsně za firewallem ale ještě před poštovním serverem, aby veškerá komunikace směřovala právě přes tento prvek. To znamená kompletní monitorování a řízení příchozí i odchozí emailové komunikace.

Kybernetické útoky se neustále vyvíjí. Dnešním trendem již není fyzické napadání zařízení či pronikání do vnitropodnikových sítí na základě hrubé síly. Obrané prvky jakožto firewally a antiviry jsou velmi pokročilé a jejich zabezpečení jsou efektivní. Velkým trendem dnešní doby jsou phishingové útoky a sociální inženýrství, kdy útočníka pustí do podnikové sítě samotný uživatel. Antispam od firmy Barracuda je fyzické zařízení, které monitoruje poštovní provoz. Zařízení disponuje svojí databází a filtračními prvky. Na základě, kterých dokáže samovolně blokovat škodlivé odesílatele. K blokování dochází pomocí takzvaného score. Jedná se o subjektivní vyhodnocovací systém. Čím větší má odesílatel score, tím větší šance, že bude daná zpráva zablokována.

Pomocí antispamu lze blokovat odesílatele na základě domén, provádět blokace emailů pomocí klíčových slov nebo předmětu zprávy. Pokud se jedná o aktivního útočníka, který neustále mění domény a zasílané zprávy, lze blokovat konkrétní poštovní server dle IP adresy. Antispam Barracuda umožnuje logování emailů po nezbytně dlouhou dobu. Tento časový horizont si podnik libovolně nastavuje a upravuje dle vlastních potřeb na základě vnitropodnikových politik a zákonných dob pro ukládání logů v organizaci.

4.12.1. Náklady na nákup a provoz antispamu

Název produktu	*Počet ks*	*Typ*	*Cena za kus*	*Cena podpory na rok*	*Celkový náklad na první rok provozu v Kč*
Antispam – Barracuda Email	1	SW	x	1 450 000,-	1 450 000,-

Tabulka 4 - Náklady na nákup a provoz antispamu

Obrázek 31 - Antispam Barracuda

Zdroj: Autor

4.13. Vulnerability management – Nessus

Vulnerability managment, v překladu řízení zranitelností, je proces, který má za úkol identifikovat a včasně eliminovat bezpečnostní zranitelnosti v infrastruktuře. Tato analýzy probíhá na hardwarové, softwarové a sítové vrstvě. Hlavním cílem je detekovat bezpečnostní zranitelnosti dřív než útočník, který je může potenciální využít ve svůj prospěch.

Tento proces by měl být pravidelně vykonáván na základě bezpečnostního auditu. Každý týden vycházejí aktualizace na informační systémy, aktualizace virových databází

a další preventivní úkony za účelem omezení kybernetické aktivity. Organizace, která provádí bezpečnostní kontroly za účelem odhalení zranitelnosti si musí být jistá, že její opatření opravdu fungují.

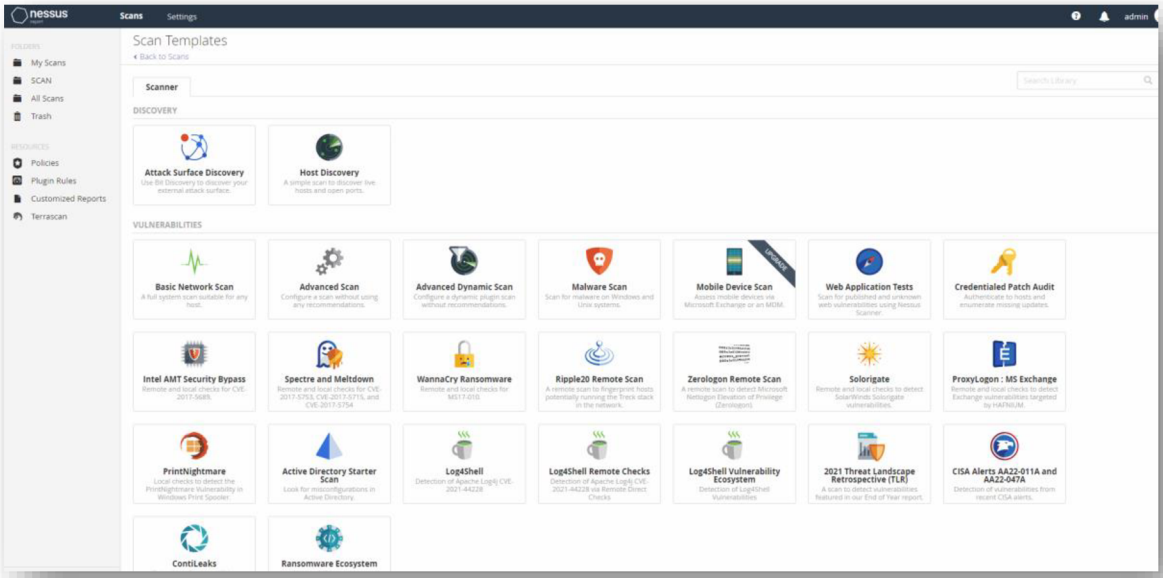
Zatím co vulnerability management je jen sada metod a postupů, jak tyto bezpečnostní rizika hledat a eliminovat na teoretické úrovni. Byl k tomu vytvořen i aktivní prvek používající v praxi. Jedná se o vulnerability scanner. Tento nástroj má za úkol vyhledávat zranitelnosti pomocí skenovacího mechanismu a odhalování obecně známých zranitelnosti. Může se jednat například o otevřené porty, které nejsou využívané. Používání zastaralé verze šifrování či dokonce provozování aplikací na již nepodporovaném operačním systému.

Demonstrace bude probíhat ve vulnerability skeneru Nessus od firmy Tenable Inc. Jedná se o komerční produkt, který funguje na klasické licenční politice. Pro testovací účely lze využít demo verzi. Ta je na 7 dní pro testovací účely zdarma. Vulnerability skener Nessus byl aplikován pro účely demonstrace na testovací lokální sít. Na základě skenovacího výstupu lze zjistit, zdali bezpečnostní konfigurace, o které tato diplomová práce pojednává je dostačující a efektivní.

4.13.1. Náklady na nákup a provoz vulnerability skeneru

Název produktu	*Počet ks*	*Typ*	*Cena za kus*	*Cena podpory na rok*	*Celkový náklad na první rok provozu v Kč*
Vulnerability mng. Nessus	1	SW	53 200,-	7 000,-	60 200,-

Tabulka 5 - Náklady na nákup a provoz vulne. man. Nessus



Obrázek 32 - Vulnerability management Nessus

Zdroj: Autor

4.13.2. Užití vulnerability skeneru

Základní demoverze produktu je ke stažení na oficiálních stránkách prodejce. Vulnerability skener Nessus nabízí velké množství analýz a podrobných skenů. Každý skenovací scénář se zaměřuje na odlišné zranitelnosti a bezpečnostní sektory. V ukázkovém případě se bude jednat o základní skenování. Cíleným výstupem skeneru je kompletní výpis zranitelností v testovací síti.

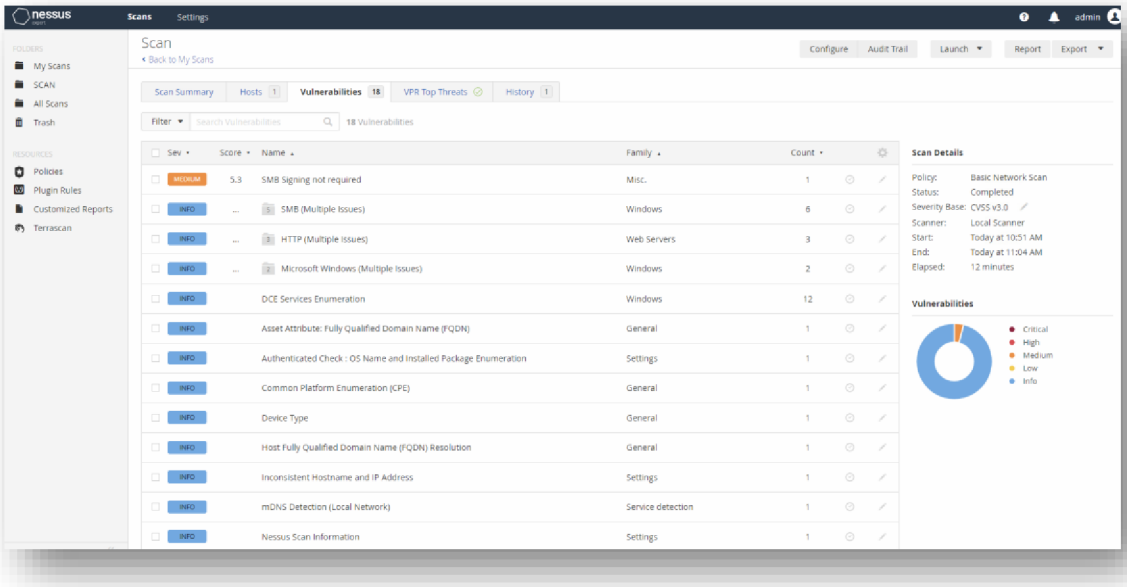
Po zadání rozsahu IP adres, na kterém bude prováděn sken, lze započít skenování. V ukázkovém případě se bude jednat o testovací stanici DPDCO1, která má IP adresu 192.168.1.2/24. Zvolený druh skenu zkontroluje zranitelnosti na stanici a v síti, kde se stanice nachází. Se skenerem lze interakčně pracovat po čas skenování, avšak primárním cílem je finální výstup skeneru.

Po dokončení skenu a vyhotovení analýzy má uživatel k dispozici kompletní výstup o provedené akci i se zjištěnými zranitelnostmi. Na výstupu lze vidět, že testovací stanice v testovací síti nedisponuje žádnými kritickými zranitelnostmi. Veškeré zranitelnosti až na jeden případ mají status – INFO. Vulnerability skener v této kategorii jen pojednává

o nedostatcích a možných zranitelnostech. Avšak se o zranitelnost jako takovou nejedná. Kategorie INFO slouží jen k informování uživatele.

Skener zjistil na základně vygenerovaného výstupu jednu zranitelnost z kategorie MEDIUM pod názvem – SMB Signing not required. Zkratka SMB zastupuje Server Mesage Block. Jedná o souborový protokol v operačním systému Windows. Tento protokol slouží k odesílání a sdílení souborů v rozhraní operačního systému. Z důvodu stáří tohoto protokolu se již nedoporučuje jeho používání. Protokol je přednastavený v group policy aby byl obecně zapnutý. Nastavení se aplikuje na všechny nově nainstalované servery a stanice. Je zapotřebí tento protokol manuálně vypnout.

Díky výstupu ze skenovacího nástroje Nessus byla úspěšně odhalena jedna potenciální bezpečnostní zranitelnost z kategorie MEDIUM. Zranitelnost byla včas odstraněna a tím pádem došlo k eliminaci bezpečnostního rizika. Testovací server provozovaný v demonstrativní síti již nedisponuje žádnými dalšími zranitelnostmi. Na základě tohoto faktu lze konstatovat, že veškeré bezpečnostní kroky, o kterých bylo pojednáno v předešlých částech diplomové práce jsou efektivní. Díky zmíněné konfiguraci bylo docíleno základního zabezpečení v sítovém provozu.



Obrázek 33 - Výsledky scanu Nessus

Zdroj: Autor

4.14. Dohledové systémy

Dohledové systémy slouží k monitorování provozu v síti. Pokud podnik disponuje nakonfigurovanou a funkční sítí, má jí zabezpečenou pomocí bezpečnostních prvků, může přistoupit k monitorování provozu. Na základě monitorovacích technologií lze určit technické poruchy, chystané nebo již proběhlé kybernetické útoky či narušování vnitřních bezpečnostních politik.

Monitorovacích technologií je celé spektrum. V dnešní době se na trhu vyskytují velké množství prodejců neboli vendorů, kteří nabízí takzvaně all-in-one řešení. V následujících kapitolách se bude jednat sadu monitorovacích technologií.

Každý monitorovací prvek funguje nezávisle na ostatních zařízeních a slouží výhradně ke svému účelu. Spojení těchto technologií lze docílit k universálnímu řešení, které pokrývá všechny sektory sítě.

4.14.1. SIEM – Elisa Security Manager

SIEM – Elisa Security Manager je zařízení poskytující kompletní přehled o událostech ve vnitropodnikové infrastruktuře. Jedná se o logovací nástroj, který dokáže v reálném čase rozpoznat hrozby, upozornit na ně a v některých případech dokonce je sám eliminovat. Pomocí SIEMu lze monitorovat vnitropodnikovou síť, shromažďovat data a následně je analyzovat. Jedná se o centrální monitorovací prvek, na který lze napojit další podnikové aplikace či systémy. Do SIEMu lze napojit zasílané oznámení z firewallu, antispamu, proxy serverů, antiviru a mnoho dalších. Všechny tyto eventy neboli události budou soustředěny centrálně na jednom místě, kde k nim bude administrátor sítě přistupovat.

Administrátor již nemusí sledovat všechny tyto zařízení jednotlivě, stačí mu jediný účinný nástroj. Díky filtrům a dalším selekcím lze se SIEM technologií pracovat velmi efektivně. Vybírat časové úseky v minulosti, sledovat poklesy výkonů zařízeních a dalších potřebné informace.

Elisa Security Manager je kompletní SIEM řešení, které všechny výše uvedené funkce nabízí. Obsahuje přívětivé GUI grafické rozhraní pro uživatele a rychlejší

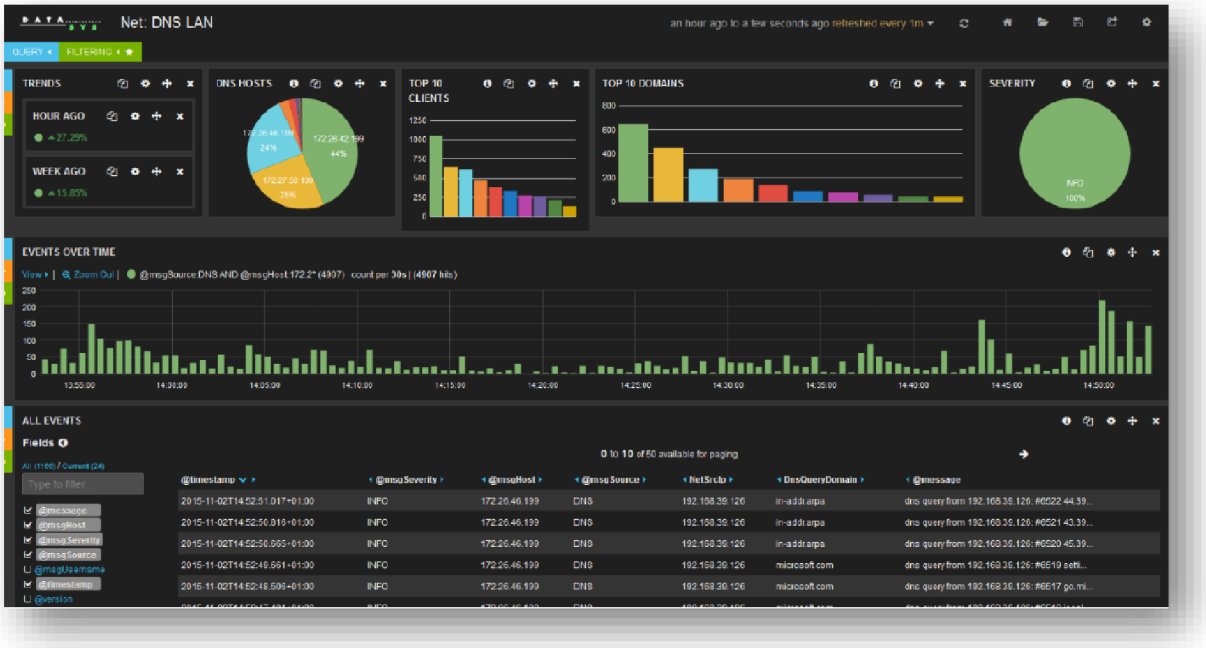
orientaci v rozhraní. Systém Elisa se neustále učí. To znamená, že SIEM zařízení obsahuje základní metody a postupy, jak detekovat hrozby v síti. Avšak postupem času provádí na pozadí analýzy a monitoring sítě, snižuje false positive poplachy a snaží se co nejvíce přizpůsobit dané infrastruktuře.

Na dnešním trhu práce v oblasti kybernetické bezpečnosti je velká poptávka po lidech, kteří SIEM zařízením rozumí a dokážou je ovládat na agendové úrovni. Efektivní auditování, logování a následně selekce událostí je klíčovým faktorem všech podniků. Jedná se o velký trend a vymoženost, jak se efektivně bránit pomocí včasné predikce hrozeb a jejich eliminace.

4.14.1.1. Náklady na nákup a provoz SIEM systému

Název produktu	*Počet ks*	*Typ*	*Cena za kus*	*Cena podpory na rok*	*Celkový náklad na první rok provozu v Kč*
SIEM – Elisa Security Manager	1	SW	x	109 000,-	109 000,-

Tabulka 6 - Náklady na nákup a provoz SIEM



Obrázek 34 – SIEM Elisa

Zdroj: https://docplayer.cz/36323951-Datasys-elisa-log-management-rizeny-zabbixem-lukas-maly-dis-it-konzultant-bezpecnost-a-monitoring.html

4.14.2. Monitoring privilegovaných účtů – Ekran System

Vnitropodnikové procesy a služby lze v dnešní době outsourcovat, tedy přenechat dodavateli. Pro podnik se to může zdát být výhodnější. Ušetří finanční náklady a nemusí disponovat zaučeným personálem k výkonu dané činnosti. Pokud si organizace objedná službu od dodavatele, musí mu umožnit přístup do své infrastruktury. I když je dodavatel vázán na smlouvy a SLA – Service Level Agreement, stále je zde možný výskyt bezpečnostního rizika. Může dojít k uniku dat, poškození organizace či jiných nekalých činností. Dodavatel se může tvářit přátelsky, avšak zdání klame.

Poskytovatel služby by měl disponovat jen oprávněními nezbytné pro výkon jeho práce. To znamená přístupy od aplikací, které nutně potřebuje. Oprávnění vytvářet, mazat a nahlížet jen kam mu jeho agenda dovoluje. Ve většině případech dodavatel pracuje uvnitř podniku pomocí vzdáleného plochy či zabezpečeného VPN kanálu. Z důvodu možného vykonávání pracovní agendy vzdáleně bez nutnosti fyzické přítomnosti na pracovišti. Pokud se jedná o větší organizaci či státní podnik, jak je tomu na MSP, organizace má vlastní VPN

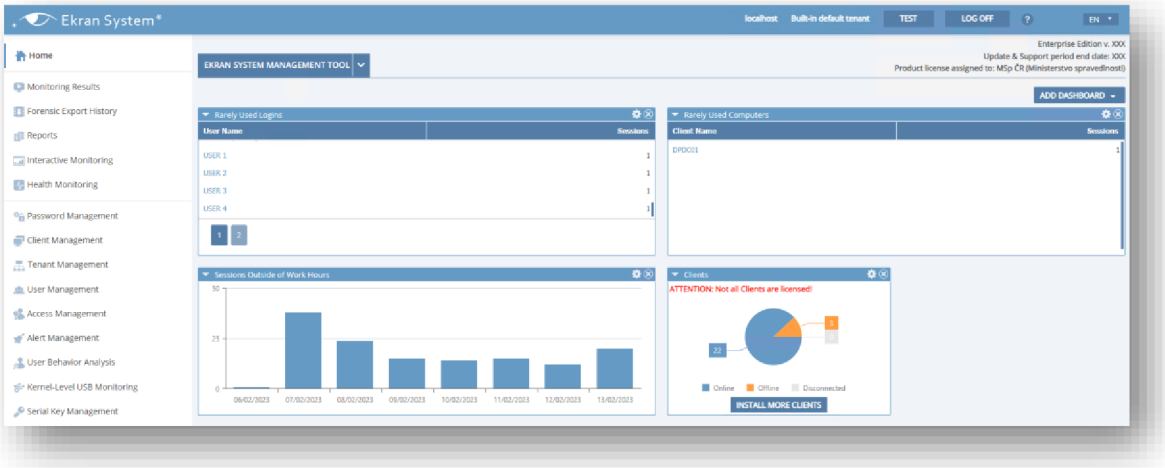
zabezpečené kanály a způsoby šifrování komunikace. Dodavatel se připojuje na terminálové servery, ze kterých dále operuje.

Systém Ekran umožnuje monitorování plochy a události na serverech. Ideálním případem užití této technologie je monitorování dodavatelů. Avšak lze ho použít i za účelem monitorování běžných uživatelů a jejich pracovních ploch. I když by dodavatel měl disponovat potřebnými oprávněními ke své činnosti, hraje zde velkou roli lidský faktor. Dodavatel může disponovat většími oprávněními, než mu bylo předurčeno. Kupříkladu vidět adresáře, která nemá a další případy převyšujících oprávnění. Monitorovací zařízení Ekran funguje na klasickém principu klienta. Software funguje po celou dobu na pozadí stanice. Systém monitorování se spouští sám automaticky při prvotním přihlášení na danou stanici. Na základě konfigurace lze nastavit, jak dlouho budou nahrávky v systému uloženy a po jaké době dojde k samovolnému výmazu z uložiště.

4.14.2.1. Náklady na nákup a provoz Ekran Systems

Název produktu	*Počet ks*	*Typ*	*Cena za kus*	*Cena podpory na rok*	*Celkový náklad na první rok provozu v Kč*
Monitoring účtů Ekran System	1	SW	x	14 450,-	14 450,-

Tabulka 7 - Náklady na nákup a provoz Ekranu



Obrázek 35 - Monitoring privilegovaných účtu Ekran

Zdroj: Autor

4.14.3. Monitoring sítě – Flowmon sondy

Podnik nebo organizace, které nejsou na startupové úrovni mají zpravidla více poboček či pracovišť. Jedná se sice o rozdílné lokace, ale používané informační systémy, podnikové politiky a data jsou stejná. Jeden celek, který je decentralizován. Stejně je tomu i u státního podniku, jako v případě MSP. Ministerstvo je obsaženo z několika desítek krajských složek, soudů, státních zastupitelství a dalších subjektů justičního resortu.

Pokud je zapotřebí zabezpečit kompletní organizaci jako celek, je nezbytné monitorovat a řídit její decentralizované části. Organizační celek může působit z vnějšího pohledu jako zabezpečená a nedobytná pevnost, avšak její menší části mohou být bezpečnostním rizikem. Některé subjekty organizační struktury nemusí dosahovat stejných standartu v zabezpečení jako centrální. Nedostačující vymezené finančních prostředky pro podřízené subjekty na zabezpečovací technologie mohou ovlivnit celou organizaci.

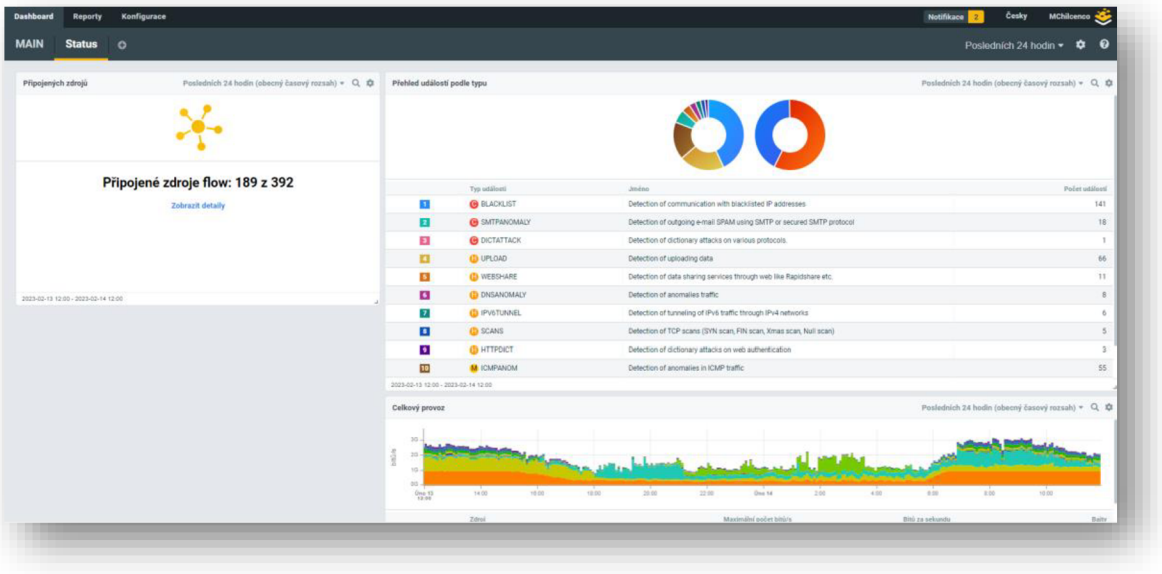
Pro tento případ byly vytvořeny monitorovací sondy a kolektory. Jedná se o aktivní síťový prvek, který monitoruje komunikaci v síti. Pomocí sond lze získávat ze sítě data. Například nedostupnost sítě, opakující se požadavky se stejné IP adresy, skenování portů a mnoho dalších bezpečnostních rizik, které jsou zapotřebí řešit v reálném čase.

Sonda od firmy Flowmoon slouží primárně k monitorování síťového provozu. Zatím co kolektor, jak jeho název napovídá, všechny tyto události a logy zaznamenává a generuje uživatelsky přívětivý výstup. Pro uvedení reálného příkladu zapojení, bude pojednáno o způsobu zapojení na MSP a resortních složkách. Každá resortní složka disponuje sondou ve své doméně či instituci. Sonda monitoruje veškerý provoz v sítí dané složky. Tyto informace jsou přeposílány do centrálního kolektoru, který je umístěn na MSP. Na základě těchto informací má MSP shromážděné potřebné informace a podklady k řízení bezpečnostních rizik napříč celým resortem.

4.14.3.1. Náklady na nákup a provoz Flowmoon sond

Název produktu	*Počet ks*	*Typ*	*Cena za kus*	*Cena podpory na rok*	*Celkový náklad na první rok provozu v Kč*
Monitoring sítě Flowmon sondy	4	SW	x	450 000,-	1 800 000,-

Tabulka 8 - Náklady na nákup a provoz Flowmoonu



Obrázek 36 - Monitoring sítě Flowmoon sonda

Zdroj: Autor

4.14.4. Monitoring infrastruktury – Zabbix

Podniková infrastruktura může být tvořena velkým počtem výpočetních zařízení, které je nebytné monitorovat a mít přehled o jeho aktuálním stavu. Pokud se jedná o klasický podnik, který si provozuje své technologie takzvaně on premise, tedy fyzicky na svých strojích. Může se dostat na hodnoty desítek až stovek fyzických a virtuálních serverů. Všechny tyto stanice je zapotřebí monitorovat. K zajištění stabilního provozu je nutné sledovat jejich stav. Zdali je stanice dostupná, zdali u nich nedochází k zaplnění disku a mnoho dalších důležitých událostí.

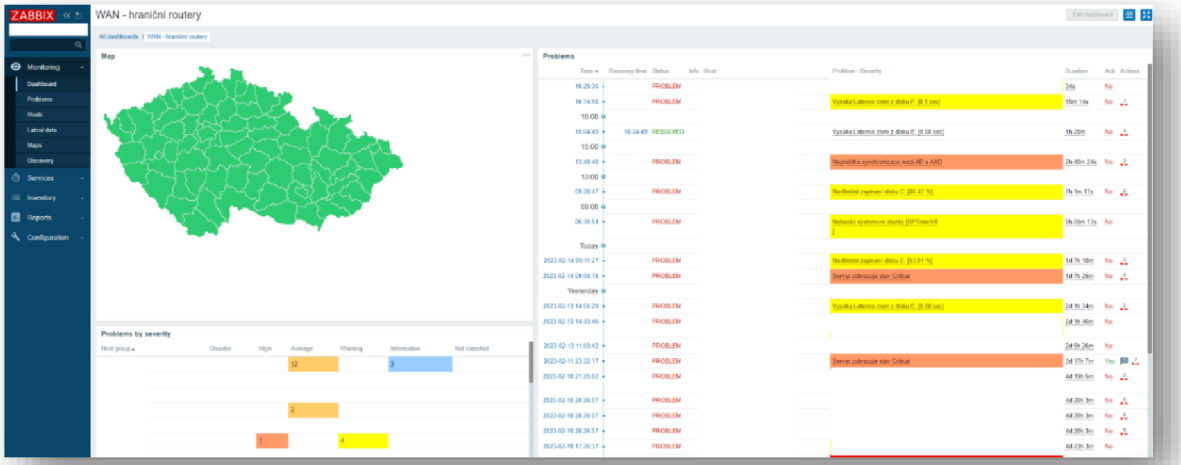
Pro tento druh monitorování existuje monitorovací systém Zabbix. Tento produkt je zdarma a open source. Jediné, co je placené, je podpora a konzultace, které poskytují externí dodavatelé. Zabbix je postaven na linuxovém jádru. Jedná se o agentový systém snímající potřebné informace z daných zařízeních. Instalace Zabbix agenta na čerstvě nainstalovaný server patří mezi základní kroky při konfiguraci nového zařízení. Pomocí template vzoru a šablon lze předvolit snímané hodnoty, které budou centrálně odesílány do uživatelského rozhraní. V praxi také nazýváno jako dashboard.

Snímané hodnoty, které by podnik mohl sledovat jsou například: doba odezvy serveru, nedostupný příkaz ping, zaplněný disk, restartovaní serveru, vysoká teplota zařízení.

4.14.4.1. Náklady na nákup a provoz Zabbixu

Název produktu	*Počet ks*	*Typ*	*Cena za kus*	*Cena podpory na rok*	*Celkový náklad na první rok provozu v Kč*
Monitoring infra. Zabbix	1	SW	x	186 000,-	186 000,-

Tabulka 9 - Náklady na nákup a provoz Zabbix



Obrázek 37 - Monitoring infrastruktury Zabbix

Zdroj: Autor

5. Výsledky a diskuse

Pokud budou shrnuty veškeré poznatky, kterými tato diplomová práce disponuje, lze docílit efektivního zabezpečení domácí či vnitropodnikové sítě malého rozsahu. Odborné postupy, konfigurace a know-how obsažené v teoretické a praktické části reflektují reálné zkušenosti autora diplomové práce z výkonů pracovní činnosti v odboru kybernetické bezpečnosti, kdy se s konkrétní problematikou potýká na denní bázi. Lze konstatovat, že uvedené příklady a konfigurace jsou převzaty z praxe, na kterých je možné bazírovat při tvorbě vlastního řešení.

Teoretická část diplomové práce disponuje širokým spektrem zabezpečovacích technologií. Autor diplomové práce je si vědom, že je nemožné pojednat o veškerých bezpečnostních technologiích v jednom dokumentu. Nicméně se v teoretické části lze dočíst základní principy fungování počítačových sítí, informace o referenčním modelu ISO/OSI, model TCP/IP, nejčastější typy útoků, rozdíly mezi jednotlivými útočníky a okrajově shrnuty základní zabezpečovací technologie.

V praktické části je obsažena universální metodika, jak by měl podnik postupovat při tvorbě nové podnikové sítě, její základní konfigurace a zabezpečení. Následuje tvorba vlastního řešení pomocí virtualizační technologie VMware, nasazení reálných produktů z praxe, jakožto Fortigate firewall a vulnerability scanner Nessus. Praktická část taktéž obsahuje ceny jednotlivých systémů a bezpečnostních technologií.

Pomalu ale jistě se velká část uživatelů snaží o digitalizaci. To znamená konvertování pracovních činností, volnočasových aktivit a veškerých procesů spojené s běžným životem do digitálního prostředí. Uživatelé nebo organizace používají síťové technologie ke komunikaci, sdílení a ukládání dat, poskytování či získávání služeb. Internet jako takový se považuje za nezabezpečenou síť. Veliká část uživatelů s nekalými úmysly, nazývané jako hackeři, usilují o získání podnikových dat. Pokud se jim podaří tyto data ukrást či zašifrovat, požadují po napadaném podniku výkupné, takzvaný ransom. Pokud útočník s vydíráním neuspěje, zvolí možnost prodeje dat na Dark Webu. Ostatní uživatelé či konkurenční podniky za citlivé informace rádi zaplatí. Hackeři neodmítnou ani data běžného uživatelé. Žádný subjekt není v bezpečí, pokud se připojuje na internet.

Kybernetická bezpečnost je odvětví v IT, které se zabývá zabezpečování informací a majetku před zneužitím. Tento IT sektor v sobě zahrnuje právě i síťové bezpečnostní technologie a veškerou problematiku, o které diplomová práce pojednává. Jedná se o velký trend na trhu práce a služeb. Pokud podnik, který není na startovní úrovni, nedisponuje oddělením pro kybernetickou bezpečnost, měl by tento faktor rychle napravit. Finance vyčleněné na zabezpečovací technologie a zaškolení personálu by měly být ve stejné výši jako náklady na ostatní provozní oddělení. Velká část organizací si není vědoma podstaty a klíčové role kybernetické bezpečnosti v běžném podnikání. Pokud dojde ke zkompromitování dat a pošpinění pověsti organizace, ztratí důvěru na světovém trhu. Pro některé podniky to může mít fatální následky.

Jakékoliv zařízení v dnešní době komunikuje do internetu. Veškeré aplikace, kompletní systémy či sítě jsou zranitelné, pokud byly a budou navržené člověkem. Nelze opomenout lidský faktor, který hraje v bezpečnostních zranitelnostech klíčovou roli. Neexistuje dodavatel, který by poskytl kompletní ochranu a zaručil bezpečný chod organizace. Je důležité, aby se podnik či uživatel včas připravil na ten nejhorší scénář. I kdyby došlo k zašifrování dat či napadení. Je důležité obnovit infrastrukturu ze záloh, oddělit napadenou část od té produkční a jednat dle kritického plánu obnovy. Reagovat na již proběhlé kybernetické útoky je nedostačující. Hlavním smyslem kybernetické bezpečnosti, zabezpečovacích či síťových technologií je prevence. To znamená zamezení možného výskytu bezpečnostních zranitelnosti ještě před tím, než se z nich stanou bezpečnostními událostmi či incidenty.

6. Závěr

Hlavním cílem diplomové práce bylo pojednat o bezpečnostních technologiích v počítačových sítích, uvést a zhodnotit technologii, představit aktuální situaci v tomto odvětví a následně demonstrovat vlastní návrh řešení pomocí virtualizační technologie VMware.

Teoretická východiska a poznatky jsou shrnuta v jednotlivých kapitolách diplomové práce. V teoretické části bylo shrnuté široké spektrum přínosů a záporů, která technologie přináší. Z počátku byla představena technologie počítačových sítích jako taková, následoval referenční model ISO/OSI. Nutno podotknout, že se jedná o teoretický model. Co se praktického modelu týče, byl představen model TCP/IP. Nesmí chybět síťové prvky a samotné topologie sítí. Taktéž byly představeny typy kybernetických útoků, například různé druhy malwaru, SQL Injection či DDoS. Následovaly typy útočníků, které dělíme především na hackery, tedy osoby s nekalými úmysly a etickými hackery. Jedná se o osoby používající své dovednosti a schopnosti v legitimním směru. Jakožto kontrolním a defenzivním prvkem v oblasti kybernetické bezpečnosti v České republice zaujímá pozici NÚKIB, v celém znění Národní úřad pro kybernetickou a informační bezpečnost. Nesmí se opomenout pojednání o kryptografických a bezpečnostních certifikátech, symetrickém a asymetrickém šifrování, elektronickém podpisu a jeho principu fungování. Okrajově byly shrnuty zabezpečovací technologie kupříkladu firewall, proxy server či SIEM systém. Závěr teoretické části obsahuje informace o penetračním testování, k čemu takové testování slouží a v jakých částkách se služba pohybuje.

Praktická část obsahovala dvě části. V první části byl realizován vlastní návrh řešení pomocí virtualizační technologie a VMware hypervizoru. Následovala základní konfigurace virtuálního stroje, která se řídí odbornými postupy využívané v denní praxi pomocí takzvaných best practise. Taktéž byl demonstrován vlastní návrh na zabezpečení lokální sítě malého rozsahu. Pomocí vulnerability scanneru od firmy Nessus proběhlo otestování vlastního návrhu, kdy návrh úspěšně prošel základním testovacím scénářem. Testovací síť se zmíněnou konfigurací neobsahovala žádné kritické zranitelnosti. Díky demoverzi firewallu, která firma Fortigate poskytuje, byl uskutečněn navržený testovací scénář. Demonstrace spočívala v základní konfiguraci firewallu při prvotním zapojení nebo

pořízení daného zařízení, vytvoření síťových interfaců, routovacích pravidel a následné vytvoření zabezpečeného prostupu na internet. Ve druhé části byly představeny reálné bezpečnostní technologie a systémy, které se využívají v praxi, přesněji na MSP. Představení technologií obsahovalo princip jejich fungování, případy užití a kalkulace počátečních nákladů na zavedení technologie do podniku. Zmíněné cenové náklady jsou subjektivní a nemusí být pro každou organizaci totožné. Běžný uživatel nemá přístup k těmto cenovým údajům, z důvodu vytváření subjektivních cenových nabídek přímo pro daný podnik.

Na závěr lze konstatovat, že byly docíleny hlavní a dílčí cíle diplomové práce dle zvolené metodiky. Vlastní návrh řešení v praktické části byl vytvořen pomocí vlastních zkušeností autora, které jsou bazírovaný na světových, uznávaných postupech a best practise metodách. Byl vytvořen universální postup pro domácnosti či podnik malého rozsahu, díky kterému lze vytvořit vlastní síť, provést základní konfiguraci, spolu se zabezpečením a tím uvést síť do provozu. Demonstrativní postup byl otestován pomocí komerčního nástroje Nessus, který potvrdil, že zmíněná konfigurace a stupeň zabezpečení jsou dostačující.

7. Seznam použitých zdrojů

Knižní zdroje

1. BEJTLICH, Richard. *The practice of network security monitoring: understanding incident detection and response*. San Francisco: No Starch Press, 2013. ISBN 978-159-3275-099.

2. CARTHERN, Chris, William WILSON, Richard BEDWELL a Noel RIVERA. *Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA,* 2015. ISBN 0306465604

3. DARAS, Nicholas J. *Computation, Cryptography, and Network security*. New York, NY: Springer Science Business Media, 2015. ISBN 978-331-9182-742

4. MCMILLAN, T. -- EBRARY, INC. *Cisco networking essentials : e-book. Indianapolis*, Ind.: John Wiley & Sons, Inc., 2012. ISBN 978-1-118-09759-5.

Internetové zdroje

5. Khanacademy.org [online], *Počítačové sítě* [cit. 2022-10-22] Dostupné z: https://cs.khanacademy.org/computing/informatika-pocitace-a-internet/x8887af37e7f1189a:internet/x8887af37e7f1189a:site-a-jejich-propojovani/a/computer-networks-overview

6. Muni.cz [online], *Historie rozlehlých počítačových sítí* [cit. 2022-10-22] Dostupné z: https://www.fi.muni.cz/usr/jkucera/pv109/xsmysit.html

7. Zamekkurim.cz [online], *Inovace a vznik počítačových sítí* [cit. 2022-10-23] Dostupné z: https://www.zamekkurim.cz/security/Dum%20-%20Digitalni%20ucebni%20materialy/05_Sada_Pocitacove_site_1/VY_32_INOVACE_05_03_VZNIK%20POCITACOVYCH%20SITI%20.pdf

8. 8U.cz [online], *Referenční model ISO/OSI* [cit. 2022-10-23] Dostupné z: http://ijs2.8u.cz/index.php?option=com_content&view=article&id=13&Itemid=119

9. eArchiv.cz [online], *Referenční model ISO/OSI – sedm vrstev* [cit. 2022-10-26] Dostupné z: https://www.earchiv.cz/a92/a213c110.php3

10. Sspbrno.cz [online], *Sada protokolů TCP/IP* [cit. 2022-10-26] Dostupné z: https://moodle.sspbrno.cz/pluginfile.php/6413/mod_resource/content/1/tcpip.pdf

11. Techtarget.com [online], *What is TCP/IP and How Does it Work* [cit. 2022-10-26] Dostupné z: https://www.techtarget.com/searchnetworking/definition/TCP-IP

12. Khanacademy.org [online], *IP Pakety* [cit. 2022-11-03]
Dostupné z: https://cs.khanacademy.org/computing/informatika-pocitace-a-internet/x8887af37e7f1189a:internet/x8887af37e7f1189a:ip-adresy/a/ip-packets

13. Samuraj-cz.com [online], *TCP/IP – model, encapsulace, paket vs. rámec* [cit. 2022-11-03]
Dostupné z: https://www.samuraj-cz.com/clanek/tcpip-model-encapsulace-paketu-vs-ramec/

14. Samuraj-cz.com [online], *Adresování v IP sítích* [cit. 2022-11-06]
Dostupné z: https://www.samuraj-cz.com/clanek/adresovani-v-ip-sitich/

15. Cvut.cz [online], *Základy adresace v počítačových sítích* [cit. 2022-11-06]
Dostupné z: https://dsn.felk.cvut.cz/projects/psitest/docs/zaklady-adresace.pdf

16. 8U.cz [online], *Pasivní síťové prvky* [cit. 2022-11-06] Dostupné z: http://ijs2.8u.cz/index.php?option=com_content&view=article&id=19&Itemid=124

17. Educba.com [online], *Types of Network Topology* [cit. 2022-11-06]
Dostupné z: https://www.educba.com/types-of-network-topology/

18. Pepa.zvonicek.info [online], *Topologie sítí* [cit. 2022-11-22]
Dostupné z: http://pepa.zvonicek.info/inf/topologie.html

19. Docplayer.cz.cz [online], *Bezpečnost počítačových sítí* [cit. 2022-11-22]
Dostupné z: https://docplayer.cz/2694031-Bezpecnost-pocitacovych-siti.html

20. VSB.cz [online], *Počítačové sítě a ochrana dat* [cit. 2022-11-22]
Dostupné z: https://fbiweb.vsb.cz/~sen76/data/uploads/skripta/poitaove-sit-a-ochrana-dat.pdf

21. Datasys.cz [online], *10 nejčastějších typů kybernetických útoků* [cit. 2022-11-22]
Dostupné z: https://www.datasys.cz/10-nejcastejsich-typu-kybernetickych-utoku/

22. Kybez.cz [online], *Jaké jsou nejčastější typy kybernetických útoků?* [cit. 2022-11-22] Dostupné z: https://www.kybez.cz/jake-jsou-nejcastejsi-typy-kybernetickych-utoku/

23. Pixman.cz [online], *Kybernetická bezpečnost: Typy útoků a prozíravý vývoj aplikací* [cit. 2022-11-22]
Dostupné z: https://www.pixman.cz/blog/kyberneticka-bezpecnost-typy-utoku-a-proziravy-vyvoj-aplikaci

24. Avast.com [online], *Hacker* [cit. 2022-11-25]
Dostupné z: https://www.avast.com/cs-cz/c-hacker

25. Cnws.cz [online], *Základy hackingu: kdo je etický hacker a jak se jím stát?* [cit. 2022-11-25]
Dostupné z: https://www.cnews.cz/zaklady-hackingu-jak-se-stat-etickym-hackerem

26. Sciencedirect.com [online], *Hacktivist* [cit. 2022-11-25]
Dostupné z: https://www.sciencedirect.com/topics/computer-science/hacktivist

27. Nukib.cz [online], [cit. 2022-11-27]
Dostupné z: https://www.nukib.cz/

28. Sands.cz [online], *Next Generation Firewall* [cit. 2022-11-27]
Dostupné z: https://www.sands.cz/sluzby-produkty/kyberneticka-bezpecnost/next-generation-firewall/

29. Cisco.com [online], *What Is a Next-Generation Firewall?* [cit. 2022-11-27]
Dostupné z: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html

30. Safetydetectives.com [online], *Co je firewall a může zcela ochránit Váš počítač v roce 2023?* [cit. 2022-11-29]
Dostupné z: https://cs.safetydetectives.com/blog/co-je-firewall-a-muze-zcela-ochranit-vas-pocitac/

31. Fortinet.com [online], *What is a Proxy Server? How does it work?* [cit. 2022-12-02]
Dostupné z: https://www.fortinet.com/resources/cyberglossary/proxy-server

32. Javapoint.com [online], *What is a proxy server and how does it work?* [cit. 2022-12-02]
Dostupné z: https://www.javatpoint.com/what-is-a-proxy-server-and-how-does-it-work

33. Autocont.cz [online], *Technologie DLP pro ochranu před únikem dat* [cit. 2022-12-05]
Dostupné z: https://www.autocont.cz/produktlisty/technologie-DLP#

34. Diit.cz [online], *Ochrana před ztrátou dat, aneb co je to DLP?* [cit. 2022-12-05]
Dostupné z: https://diit.cz/clanek/ochrana-pred-ztratou-dat-aneb-co-je-to-dlp

35. Alza.cz [online], *Co je VPN?* [cit. 2022-12-05]
Dostupné z: https://www.alza.cz/slovnik/co-je-vpn#definice

36. Kaspersky.com [online], *What is VPN? How It Works, Types of VPN* [cit. 2022-12-05]
Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

37. Newps.cz [online], *Systém SIEM – nástroj pro správu a monitoring IT infrastruktury* [cit. 2022-12-08]
Dostupné z: https://www.newps.cz/novinka/82-system-siem-nastroj-pro-spravu-a-monitoring-it-infrastruktury

38. IBM.com [online], *What is SIEM?* [cit. 2022-12-12]
Dostupné z: https://www.ibm.com/topics/siem

39. Mimecast.com [online], *What is anti-spam?* [cit. 2022-12-15]
Dostupné z: https://www.mimecast.com/content/anti-spam-software/

40. Avonet.com [online], *Zabezpečení elektronické pošty* [cit. 2022-12-17]
Dostupné z: https://avonet.cz/24879-zabezpeceni-elektronicke-posty

41. Eset.com [online], *PENETRAČNÍ TESTY* [cit. 2022-12-20]
Dostupné z: https://www.eset.com/cz/firmy/eset-services/penetracni-testy/

42. Cesnet.cz [online], *Penetrační testování – co to je, jak na ně* [cit. 2022-12-20]
Dostupné z: https://hsoc.cesnet.cz/_media/cs/dokumenty/tech/penetracni_testovani-summary.pdf

43. Muni.cz [online], *802.1X – autentizace v počítačových sítích* [cit. 2022-12-22]
Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/590.html

44. Samuraj-cz.com [online], *TCP/IP – nalezení MAC adresy k IP – ARP* [cit. 2022-12-22]
Dostupné z: https://hsoc.cesnet.cz/_media/cs/dokumenty/tech/penetracni_testovani-summary.pdf

Ostatní zdroje

45. Poznámky z předešlých let studia

46. Interní materiály MSP

8. Seznam obrázků, tabulek, grafů a zkratek

8.1. Seznam obrázků

8.2. Seznam tabulek