Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Monitoring sítě, implementace bezpečnostních systémů ve firmě

Ladislav Routner

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Ladislav Routner

Informatika

Název práce

Monitoring sítě, implementace bezpečnostních systémů ve firmě

Název anglicky

Network monitoring, implementation of security systems in the company

---

Cíle práce

Cílem bakalářské práce je navrhnout řešení pro zlepšení zabezpečení sítě ve firmě.
V bakalářské práci bude dále popsáno, jakým způsobem jsou ve firmě implementovány bezpečnostní systémy a jakým způsobem jsou využívány různé nástroje pro monitoring sítě. Dále bude v práci diskutováno o výzvách, kterým čelí IT specialisté v oblasti monitoringu a bezpečnosti.

Metodika

Bakalářská práce bude sestavena z teoretické a praktické části. Teoretická část bude věnována teoretickému základu monitorování sítě jako prvku bezpečnostního systému. K této části proběhne analýza odborné literatury, metoda vyhledávání výzkumů a internetové zdroje. Ve druhé části se bude práce věnovat analýze informační bezpečnosti na jejímž základě bude vytvořen návrh na implementaci bezpečnostního systému. Po implementaci budou sledovány výsledky, na jejichž základě bude vytvořeno hodnocení tohoto systému.

Doporučený rozsah práce

35-45s.

Klíčová slova

monitorování, síť, systém, bezpečnost, infrastruktura, software, kybernetický útok

---

Doporučené zdroje informací

ADAMS, Niall M., Nicholas HEARD. Data analysis for network cyber-security. London, UK: Imperial College Press, 2014. ISBN 9781783263745.

KUROSE, James F.; ROSS, Keith W. *Počítačové sítě.* Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

LUDVÍK, Miroslav; ŠTĚDROŇ, Bohumír. *Teorie bezpečnosti počítačových sítí.* Kralice na Hané: Computer Media, 2008. ISBN 978-80-86686-35-6.

SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

TRULOVE, James. Sítě LAN: hardware, instalace a zapojení. Praha: Grada, 2009. Profesionál. ISBN 978-80-247-2098-2.

WILSON, Ed. Network monitoring and analysis : a protocol approach to troubleshooting. New Jersey: Prentice Hall PTR, Upper Saddle River, 2000. ISBN 0-13-026495-4.

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Martin Havránek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 4. 9. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 14. 03. 2024

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Monitoring sítě, implementace bezpečnostních systémů ve firmě " jsem vypracoval samostatně pod vedením vedoucího bakalářské 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 uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14.3.2024 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Martinu Havránkovi, Ph.D. za jeho odbornou pomoc a cenné rady.

Monitoring sítě, implementace bezpečnostních systémů ve firmě

Abstrakt

Tato bakalářské práce se zabývá monitorováním sítě a implementací bezpečnostního systému ve firmě. V teoretické části práce je popsán koncept monitorování sítě, jeho význam pro zajištění bezpečnosti a dostupnosti sítě, také nástroje a metody, které se používají pro monitorování sítě. V praktické části práce je popsán postup realizace segmentace sítě ve vybrané firmě, která poskytuje služby v oblasti nemocničního vybavení. Segmentace sítě je způsob, jak rozdělit síť na menší části, které mají různé úrovně přístupu a zabezpečení. Cílem segmentace je zvýšit její bezpečnost, snížit riziko útoků a zlepšit výkon. V práci je popsán proces analýzy současného stavu sítě, příprava na implementaci segmentace sítě podle požadavků firmy a implementace segmentace sítě pomocí vhodných nástrojů a zařízení. V závěru práce je zhodnocen přínos této práce pro bezpečnost a monitorování sítě ve firmě.

Klíčová slova: monitorování, síť, systém, bezpečnost, infrastruktura, software, kybernetický útok, segmentace, firewall

Network monitoring, implementation of security systems in the company

Abstract

This bachelor thesis deals with network monitoring and implementation of a security system in a company. The theoretical part of the thesis describes the concept of network monitoring, its importance in ensuring network security and availability, and the tools and methods that are used for network monitoring. In the practical part of the thesis, the procedure for implementing network segmentation in a selected company that provides hospital equipment services is described. Network segmentation is a way to divide a network into smaller parts that have different levels of access and security. The goal of network segmentation is to increase network security, reduce the risk of attacks and improve network performance. This paper describes the process of analyzing the current state of the network, preparing to implement network segmentation according to the company's requirements, and implementing network segmentation using appropriate tools and equipment. The paper concludes by evaluating the contribution of this work to the security and monitoring of the network in the company.

Keywords: monitoring, network, system, security, infrastructure, software, cyberattack, segmentation, firewall

Obsah

1 Úvod **10**

2 Cíl práce a metodika **11**

2.1 Cíl práce 11

2.2 Metodika 11

3 Teoretická východiska **12**

3.1 Počítačová síť 12

3.1.1 Síť z pohledu firmy 12

3.1.2 Síť z pohledu běžného uživatele 12

3.1.3 ARPANET 13

3.1.4 TCP/IP 13

3.1.5 OSI 16

3.2 Monitoring sítě 17

3.2.1 Freeware 20

3.2.2 Komerční použití 22

3.3 Bezpečnostní systémy 25

3.3.1 Narušení bezpečnosti 26

3.3.2 Typy síťové bezpečnosti 28

4 Vlastní práce **37**

4.1 Úvod do praktické části 37

4.2 Analýza prostředí 37

4.3 Příprava implementace 38

4.3.1 Revize DHCP serveru 38

4.3.2 Předělání rezervací na FQDN rezervace 38

4.3.3 Statické IP adresy v LAN 39

4.3.4 Příprava nového DHCP serveru 40

4.3.5 Optimalizace firewallových pravidel 41

4.3.6 Vytvoření nových VLAN 41

4.3.7 Domluva výpadku LAN a serverů 42

4.4 Implementace 42

4.4.1 Úprava DHCP lease time 42

4.4.2 Odpojení síťového adaptéru na VMs 43

4.4.3 Konfigurace brány firewall FortiGate 43

4.4.4 Transformace rozhraní LAN 43

4.4.5 Přeskupení virtual machines 44

5 Výsledky a diskuse **45**

6 Závěr **48**

7 Seznam použitých zdrojů 49

8 Seznam obrázků, tabulek, grafů a zkratek 50

8.1 Seznam obrázků 50

8.2 Seznam tabulek 50

8.3 Seznam grafů 50

8.4 Seznam použitých zkratek 50

1 Úvod

Oblast správy a ochrany informačních systémů je významně ovlivněna klíčovými oblastmi monitorování sítě a implementace bezpečnostních systémů. Tyto aspekty hrají klíčovou roli při ochraně integrity a důvěrnosti citlivých dat v rámci organizačních sítí. Zkoumání těchto oblastí je základem této bakalářské práce, která se zabývá složitostmi monitorování sítě i implementací bezpečnostních systémů, přičemž se zaměřuje zejména na princip implementace segmentace sítě jako účinného nástroje pro zvýšení celkové bezpečnosti sítě.

Úvodní část práce se soustředí na teoretické základy monitorování sítě, zahrnující komplexní analýzu jeho cílů, metodik a používaných nástrojů, kterým čelí v dynamickém prostředí informačních systémů. Toto teoretické zkoumání připravuje půdu pro diferencované pochopení mnohostranné povahy monitorování sítí a poskytuje základ, na němž lze účinně stavět praktické aspekty práce.

Další část práce přechází do praktické oblasti a objasňuje reálnou implementaci segmentace sítě v konkrétním prostředí. Zvolený přístup zahrnuje návrh a implementaci řešení založeného na virtuálních lokálních sítích (VLAN). Tento praktický pokus slouží jako hmatatelný projev dříve získaných teoretických poznatků a nabízí praktický plán pro ty, kteří chtějí posílit své síťové zabezpečení prostřednictvím strategické aplikace segmentace sítě.

Zastřešujícím cílem této práce je nejen objasnit teoretické a praktické aspekty monitorování sítě a implementace bezpečnostních systémů, ale také sloužit jako příručka pro osoby pověřené implementací takového bezpečnostního systému. Poskytnutím komplexního zkoumání segmentace sítě jako účinného nástroje si tato práce klade za cíl vybavit čtenáře znalostmi a poznatky potřebnými k tomu, aby se mohli orientovat ve složitostech zavádění robustních bezpečnostních opatření v rámci svých síťových infrastruktur. Tímto komplexním zkoumáním se tato práce snaží přispět k širší diskusi o bezpečnosti informačních systémů a usnadnit informovanější, strategičtější přístup ke správě i ochraně sítí.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem bakalářské práce je navrhnout řešení pro zlepšení zabezpečení sítě ve firmě. V bakalářské práci bude dále popsáno, jakým způsobem jsou ve firmě implementovány bezpečnostní systémy a jakým způsobem jsou využívány různé nástroje pro monitoring sítě. Dále bude v práci diskutováno o výzvách, kterým čelí IT specialisté v oblasti monitoringu a bezpečnosti.

2.2 Metodika

V teoretické části se práce věnuje podrobnému rozboru principů monitoringu sítě, přičemž zdroje byly vybírány velmi pečlivě, aby byla zajištěna vysoká kvalita informací.

Kybernetická bezpečnost, jako klíčový prvek celkového bezpečnostního systému, byla v teoretické části této práce podrobně prozkoumána. Tato práce se zabývá nejen koncepty a teoretickými základy, ale také se zaměřuje na praktické příklady a studie případů, které ilustrovaly výzvy a úspěchy v oblasti kybernetické bezpečnosti.

Praktická část práce je věnována detailnímu popisu implementace segmentace sítě, což představuje klíčový prvek pro zajištění efektivní kybernetické bezpečnosti. Tato část je systematicky strukturována do dvou fází. V první části se podrobně věnuje přípravě na implementaci, analyzující nezbytné kroky a předpoklady pro úspěšné provedení segmentace sítě. Zahrnula také optimalizaci nastavení a konfigurace sítě na základě hloubkového průzkumu aktuálních trendů a osvědčených postupů.

Druhá část praktické implementace poskytuje podrobný náhled na samotný proces implementace segmentace sítě. Zde jsou prezentovány technické detaily, specifické postupy a případné výzvy, které vznikly v průběhu implementace. Tato fáze nabízí praktický přehled o aplikaci teoretických poznatků do reálného prostředí, což přináší konkrétní hodnotu pro odbornou i laickou veřejnost.

V závěrečné části práce jsou důkladně zhodnoceny dosažené výsledky a účinnost implementované segmentace sítě. Diskutují se zde přínosy a navrhují možná vylepšení, která by mohla přispět k dosažení optimálního stavu bezpečnostního systému. Celkové shrnutí v závěru práce reflektuje na teoretickou i praktickou část, zdůrazňuje klíčové aspekty a význam dosažených poznatků pro oblast kybernetické bezpečnosti a monitorování sítě.

3 Teoretická východiska

3.1 Počítačová síť

3.1.1 Síť z pohledu firmy

Síť je soubor překrývajících se vazeb mezi jednotlivci nebo skupinami, které mohou být formální nebo neformální. V kontextu organizací mají sítě zásadní význam pro rozvoj strategické konkurenční výhody. Autoři tvrdí, že organizace jsou vysoce dynamické sociální entity, které jsou souborem jednotlivců, kteří spolupracují, aby vytvořili něco, co by žádný z jednotlivců sám o sobě vytvořit nemohl. Proto je pro efektivní řízení a inovace zásadní porozumět sítím, které v organizaci existují, a jejich vzájemné interakci (Aalbers, a další, 2015).

Autoři diskutují, že sociální sítě jsou důležité pro inovace v organizacích, protože usnadňují přenos znalostí a informací mezi zaměstnanci. Sociální sítě mohou také pomáhat vytvářet, rozptylovat, prověřovat a zlepšovat informace. Autoři upozorňují, že existují různé typy sociálních sítí, včetně sítí formálních a neformálních, a že tyto sítě mohou mít na inovace různý vliv. Zabývají se také pojmem "uzavřenost sítě", který označuje míru, do jaké jsou jednotlivci v síti vzájemně propojeni. Tvrdí, že uzavřenost sítí může mít v závislosti na kontextu jak pozitivní, tak negativní vliv na inovace. Autoři se rovněž zabývají významem pozice v síti, tedy umístěním jednotlivce nebo skupiny v rámci sítě, pro inovace. Poznamenávají, že jednotlivci na centrálních pozicích v síti mohou mít lepší přístup k informacím a zdrojům a mohou být schopni lépe koordinovat a usnadňovat inovace. Autoři však upozorňují, že pozice v síti není vždy prediktorem inovací a že roli hrají i další faktory, jako je kreativita a motivace jednotlivce. Na závěr autoři diskutují o významu řízení sítí pro inovace a uvádějí některé strategie pro využití sociálních sítí k podpoře inovací v organizacích (Aalbers, a další, 2015).

3.1.2 Síť z pohledu běžného uživatele

Počítačová síť je soubor propojených zařízení, která spolu komunikují prostřednictvím výměny dat a prostředků. Tato připojení mohou být drátová nebo bezdrátová a komunikace v síti se opírá o protokoly jako TCP/IP, SMTP a HTTP. První počítačová síť, síť ARPANET (Advanced Research Projects Agency Network), byla založena americkým ministerstvem obrany na konci 60. let 20. století. Počítačové sítě mohou být různého rozsahu, od dvou notebooků propojených ethernetovým kabelem až po rozsáhlý globální systém vzájemně propojených sítí známý jako internet (Kinza, a další, 2023).
Dá se také rozdělit dle geografického rozsahu na:

• LAN (místní sítě) - jsou sítě, které pokrývají malou oblast, jako je kancelář nebo domov
• WAN (rozlehlé sítě) - pokrývají velké oblasti, jako je město nebo stát.
• GAN (globální sítě) - jsou obvykle složeny z několika WAN, které jsou propojeny pomocí mezinárodních spojů.
• PAN (sítě veřejného přístupu) - malé sítě, které jsou určeny pro osobní použití.
• MAN (sítě městské oblasti) - pokrývají malé až střední oblasti, jako je město nebo okres.
Či dle jiných specifik:
• WAP (Sítě bezdrátových přístupových bodů) - používají bezdrátové připojení k internetu.
• VPN (Sítě virtuální privátní sítě) - používají šifrování k vytvoření privátní sítě přes veřejnou síť, jako je internet (Trulove, 2009).

3.1.3 ARPANET

Síť ARPANET byla vytvořena v USA v 60. letech a měla sloužit k výzkumu způsobu komunikace v případě jaderné války. Tato síť byla prvním experimentem vytváření rozsáhlé sítě propojující hostitelské počítače a terminálové servery. Postupně vznikly protokoly pro provoz sítě, a vznikla síťová vrstva známá jako Internet Protocol (IP). Další sítě se začaly rozvíjet na základě protokolu IP, a tím vznikl základ dnešního internetu.

ARPANET se vyvíjela a stala páteřní sítí, přes kterou procházela většina provozu internetu. Další sítě, jako NSFNET, se k ARPANETu přidávaly, což rozšířilo internet a umožnilo široké použití pro vědecký a akademický výzkum. Později se síť NSFNET stala dominantním prvkem, který zajišťoval spojení a růst internetu.

Přechod k protokolům TCP/IP byl klíčovým krokem v rozvoji internetu. Tyto protokoly umožnily efektivní komunikaci mezi různými počítači a sítěmi a staly se tak základem internetu. Původně se v ARPANETu používal protokol NCP, ale přechod na TCP/IP se stal klíčovým momentem v historii internetu.

Internet se postupně šířil po celém světě, propojoval různé sítě a umožnil komunikaci mezi lidmi a počítači na celém světě. Díky své otevřenosti a schopnosti růst se internet stal základem moderní komunikace, a to i pro komerční účely (Peterka, 1995).

3.1.4 TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) je soubor síťových protokolů, který tvoří základní stavební kámen internetu a většiny současných počítačových sítí. Tyto protokoly umožňují komunikaci mezi různými zařízeními připojenými k síti a

zajišťují přenos dat tak, aby byl spolehlivý a efektivní. TCP/IP byl vyvinut v 70. a 80. letech 20. století a od té doby se stal standardem pro většinu světové sítě.

Vývoj TCP/IP začal v USA v rámci projektu ARPANET, což byla první datová síť používající technologii "packet switching". Na ARPANETu byly původně používány experimentální protokoly, ale v 70. letech začalo být jasné, že je potřeba standardizovaný a efektivní protokol pro komunikaci v síti. Pro představu je přiložena tabulka s přenosovými rychlostmi z roku 1994 viz Tabulka 1.

Tabulka 1: Srovnání relativních cen mezinárodních pevných okruhů v roce 1994

Přenosová rychlost	Kolikrát je vyšší přenosová rychlost (vůči 64kbs)	Kolikrát je vyšší cena
64 kbps	1	1
128 kbps	2	1,8
256 kbps	4	3
512 kbps	8	5
1 mbps	16	7,5
2 mbps	32	10

Zdroj: (Peterka, 1995)

TCP/IP je hierarchický systém s několika vrstvami, které mají specifické funkce. Základními vrstvami jsou:

Síťová vrstva (Network Layer): Tato vrstva řídí směrování dat mezi různými sítěmi. Používá IP (Internet Protocol) adresy k určení cesty, kterou data mají putovat k cíli. IPv4 (verze 4) a IPv6 (verze 6) jsou nejznámějšími protokoly této vrstvy.

Transportní vrstva (Transport Layer): Tato vrstva zajišťuje spolehlivý přenos dat mezi koncovými zařízeními. Dva hlavní protokoly této vrstvy jsou TCP (Transmission Control Protocol) a UDP (User Datagram Protocol). TCP zajistí, že data dorazí bez ztráty a v daném pořadí, zatímco UDP poskytuje rychlejší, ale méně spolehlivý přenos.

Aplikační vrstva (Application Layer): Toto je vrstva, na které běží konkrétní aplikace, jako jsou webové prohlížeče, e-mailové klienty a další. Protokoly této vrstvy určují, jak aplikace komunikují a jakým způsobem jsou data zpracovávána.

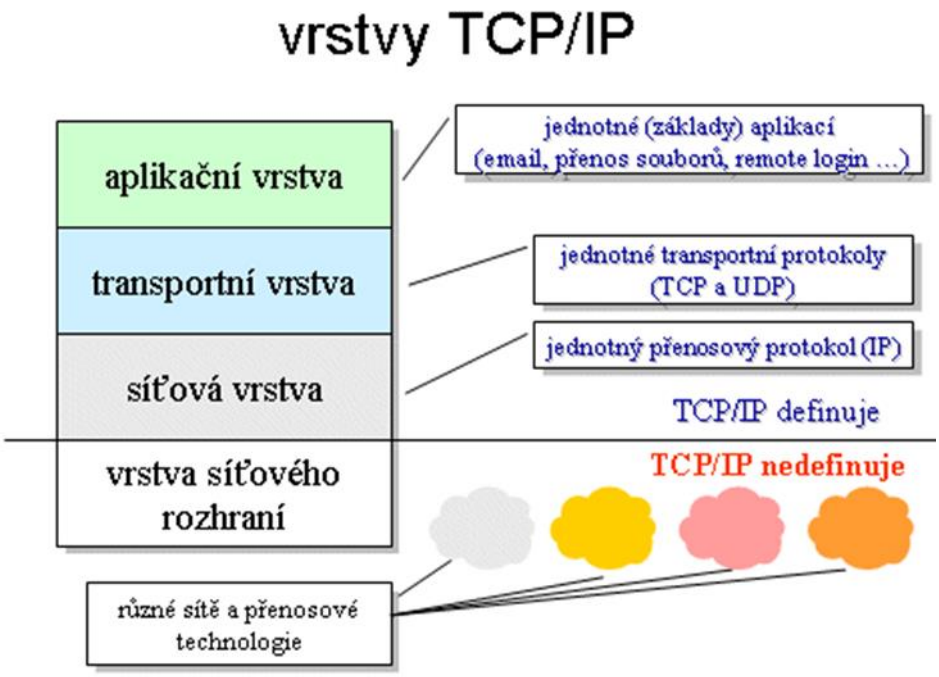
Linková vrstva (Link Layer): Tato nejnižší vrstva řídí fyzický přenos dat po síti. Zahrnuje hardwarové technologie, jako jsou Ethernet nebo Wi-Fi, a definuje způsob, jakým se data přenášejí na konkrétní médium.

TCP a UDP jsou dva nejdůležitější protokoly transportní vrstvy (Ludvík, a další, 2008). TCP je spojově orientovaný protokol, což znamená, že zajišťuje spolehlivý a řízený přenos dat. Používá potvrzovací mechanismus, kontrolní součet a řízení toku k dosažení spolehlivosti. Naopak UDP je nespojově orientovaný protokol, který je rychlejší, ale neposkytuje takovou spolehlivost. UDP se často používá pro aplikace, které tolerují určitou míru ztráty dat, jako jsou hlasové zprávy a videohovory.

Síťová vrstva používá IP adresy k identifikaci zařízení v síti. Původně byly používány IPv4 adresy, ale kvůli omezenému počtu dostupných adres byla vytvořena nová verze, IPv6. IPv6 používá 128bitové adresy, což umožňuje jejich astronomický počet a řeší problém s jejich vyčerpáním.

TCP/IP protokoly jsou základním kamenem moderního internetu a datových sítí. Jejich hierarchická struktura a rozmanité vrstvy umožňují spolehlivou a efektivní komunikaci na celém světě. TCP/IP je výsledkem desítek let vývoje a standardizace a zůstává klíčovým prvkem v digitálním světě. Autor Peterka znázornil vrstvy TCP/IP protokolu viz. Obrázek 1 (Kurose, a další, 2014).

Obrázek 1: Vrstvy TCP/IP protokolu



Zdroj: (Peterka, 1995)

3.1.5 OSI

Referenční model OSI je systematický přístup k nastínění služeb protokolů, které definují síťovou architekturu. Jedná se o sedmivrstvý model, který popisuje, jak jsou data přenášena po síti. Každá vrstva v rámci modelu spolupracuje s vrstvami nad a/nebo pod ní, aby sloužila k přenosu dat.

Sedm vrstev referenčního modelu OSI je následujících:

1. Fyzická vrstva: Zodpovědná za přenos surových datových bitů přes fyzické médium, jako je měděný vodič nebo optický kabel.

2. Vrstva datového spoje: Zodpovídá za přenos datových rámců přes fyzické médium. Zajišťuje také detekci a opravu chyb.

3. Síťová vrstva: Má na starost směrování datových paketů mezi různými sítěmi. Zajišťuje také logické adresování a řízení přetížení.

4. Transportní vrstva: Musí zajistit spolehlivé doručování dat mezi koncovými body. Zajišťuje také řízení toku a obnovu chyb.

5. Relační vrstva: Je zodpovědná za vytváření, udržování a ukončování relací mezi aplikacemi.

6. Prezentační vrstva: Překládá data mezi různými formáty, například ASCII a EBCDIC.

7. Aplikační vrstva: Vrstva pro přenos dat (Application layer): Tato vrstva zodpovídá poskytování služeb aplikacím, jako je e-mail, přenos souborů a prohlížení webových stránek.

Referenční model OSI je důležitý, protože poskytuje společný jazyk pro dodavatele, kteří vytvářejí produkty pro prostředí s více dodavateli. Pomáhá také správcům sítí při řešení problémů, protože poskytuje jasnou představu o tom, jak jsou data v síti přenášena (Edwards, a další, 2009).

3.2 Monitoring sítě

Monitoring sítě představuje klíčový prvek pro udržení stability a bezproblémový chod moderních podnikových sítí. Jedná se o systematický proces, kde softwarové a hardwarové nástroje pracují v harmonii, neustále hlídají zdraví a výkonnost všech připojených zařízení. Jeho hlavním cílem je zachytit potenciální problémy dříve, než se stihne projevit jejich negativní vliv na běžné operace firmy.

Zakoupení, instalace a konfigurace těchto monitorovacích systémů může představovat zásadní investici, ale v dlouhodobém horizontu se tato investice mnohonásobně vrátí. Monitoring totiž plní několik klíčových funkcí, které jsou pro moderní podnikovou síť nepostradatelné.

Monitoring umožňuje odhalit nejen aktuální potíže, ale i potenciální hrozby, jako je zařízení blížící se konci své životnosti nebo časté výkyvy v síťovém provozu. Díky tomu je možné podniknout preventivní kroky a minimalizovat výpadky sítě, to je zejména v kritických odvětvích jako zdravotnictví a finance naprosto nezbytné.

Zároveň výrazně přispívá ke zlepšení výkonu sítě. Také poskytuje důležité informace o tom, kde a jakým způsobem lze síť optimalizovat. To může znamenat například rozšíření šířky pásma na konkrétních linkách nebo optimalizaci datového toku. Díky tomu mohou uživatelé v síti zažívat rychlejší a spolehlivější připojení, což má pozitivní vliv na produktivitu práce a celkovou uživatelskou spokojenost.

Závěrem, monitoring je často klíčovým prvkem pro dodržování přísných regulačních požadavků. V některých odvětvích, jako jsou finance nebo zdravotnictví, jsou podniky povinny monitorovat své sítě a uchovávat data o provozu. Tyto informace mohou být důležité pro audity a zajištění souladu se zákony a předpisy (Wilson, 2000).

SNMP

Protokol SNMP (Simple Network Management Protocol) je standardní protokol používaný ke správě a monitorování síťových zařízení, jako jsou směrovače, přepínače a servery. Umožňuje těmto zařízením sdílet informace o jejich výkonu a stavu s centrálním systémem správy, což z něj činí důležitý nástroj pro správce sítě.

Protokol SNMP používá model klient – server a má několik klíčových částí. Spravovaná zařízení, jako jsou směrovače nebo servery, jsou zařízení, která je potřeba monitorovat. Agenti, kteří jsou softwarové moduly ve spravovaných zařízeních, shromažďují údaje o výkonu zařízení a odpovídají na požadavky. Správci SNMP jsou systémy, které monitorují a spravují zařízení. Žádají agenty o data a v případě problémů odesílají oznámení. Databáze informací o správě (MIB) je jako databáze se strukturou spravovaných objektů. Každý objekt má jedinečný identifikátor (OID) a uchovává informace o specifických aspektech spravovaného zařízení.

Protokol SNMP funguje prostřednictvím standardizovaných zpráv a systému požadavek – odpověď. Správci SNMP posílají agentům SNMP na spravovaných zařízeních požadavky, v nichž požadují konkrétní informace o stavu, výkonu nebo konfiguraci zařízení. Agenti SNMP tyto požadavky zpracovávají, získávají potřebná data z MIB a posílají je zpět manažerům. Kromě toho mohou agenti SNMP odesílat správcům výstrahy, když zjistí problémy bez předchozího požadavku (Mauro, a další, 2001).

Ping a Traceroute

Ping a traceroute jsou základní diagnostické nástroje sítě, které pomáhají pochopit síťové připojení a řešit problémy. Jsou neocenitelné jak pro správce sítě, tak pro běžné uživatele, protože nabízejí přehled o výkonu sítě a připojení.

Ping, odvozený z anglického "Packet Internet Groper", je jednoduchý nástroj, který odešle paket dat na cílové zařízení, obvykle jiný počítač nebo server, a změří čas, za který paket dorazí k cíli a zpět. Určuje, zda je cíl dosažitelný, a jak dlouho trvá cesta dat tam a zpět.
Ping se běžně používá k ověření síťového připojení, testování doby odezvy zařízení a identifikaci problémů s latencí. Úspěšný ping znamená, že cíl je dosažitelný, zatímco neúspěšný ping může znamenat problémy se sítí.

Traceroute je pokročilejší nástroj, který sleduje cestu paketu k cíli. Odhalí všechna mezilehlá zařízení (směrovače), která paket na své cestě k cíli potká. Traceroute také poskytuje informace o době, kterou zabere každý "skok".

Tento nástroj je užitečný zejména při diagnostice problémů v síti. Pokud traceroute ukáže nadměrné zpoždění nebo ztrátu paketů na určitém skoku, může přesně určit, kde v síti je problém. Traceroute také pomáhá identifikovat špatně nakonfigurované nebo nefunkční směrovače (Wilson, 2000).

Analýza logů

Analýza protokolů je postup, při kterém se zkoumají soubory protokolů generované síťovými zařízeními, servery a aplikacemi. Tyto protokoly jsou záznamem síťových aktivit, bezpečnostních událostí, chyb a výkonnostních metrik. Slouží jako malé části zanechané síťovými zařízeními, operačními systémy a aplikacemi. Porozumění těmto protokolům je pro správu sítě klíčové.

Různé typy protokolů, včetně protokolů zabezpečení, systémových protokolů a aplikačních protokolů, mají každý svůj specifický účel. Bezpečnostní protokoly pomáhají odhalovat narušení a podezřelé aktivity, zatímco systémové protokoly poskytují historický kontext pro řešení problémů a diagnostiku. Aplikační protokoly mohou být užitečné při sledování databázových transakcí.

Pro využití potenciálu dat protokolů jsou nezbytné nástroje pro analýzu protokolů. Tyto nástroje přijímají a analyzují soubory protokolů a prezentují data ve strukturovaném a uživatelsky přívětivém formátu. Analýza protokolů je neocenitelná pro zabezpečení, optimalizaci výkonu, řešení problémů a dodržování předpisů v různých odvětvích, což z ní činí nepostradatelnou praxi pro správce a manažery sítí (Wilson, 2000).

Monitorování na základě prahových hodnot

Monitorování založené na prahových hodnotách je důležitým přístupem při správě sítě. Zahrnuje nastavení předem definovaných prahových hodnot výkonu pro různé aspekty sítě, jako je využití šířky pásma, vytížení procesoru nebo doba odezvy. Při překročení těchto prahových hodnot monitorovací systém generuje výstrahy nebo oznámení, která signalizují, že určitý parametr sítě překročil přijatelné meze.

Tato monitorovací technika je velmi účinná při proaktivním řešení problémů v síti. Definováním konkrétních prahových hodnot mohou správci sítě dostávat včasná varování o potenciálních problémech dříve, než dojde k jejich eskalaci. Pokud například využití procesoru na kritickém serveru překročí předem definovanou mezní hodnotu, spustí se upozornění, které správcům umožní problém prozkoumat a okamžitě řešit.

Monitorování založené na prahových hodnotách je univerzální a lze jej použít pro různé síťové metriky, včetně latence, ztráty paketů a využití zdrojů. Zajišťuje, že správci jsou stále informováni o výkonu síťových komponent a mohou včas přijmout opatření, aby zabránili přerušení služeb nebo snížení výkonu. Tento přístup pomáhá udržovat stabilitu sítě a optimalizovat přidělování zdrojů, což z něj činí základní postup při správě sítě (Wilson, 2000).

3.2.1 Freeware

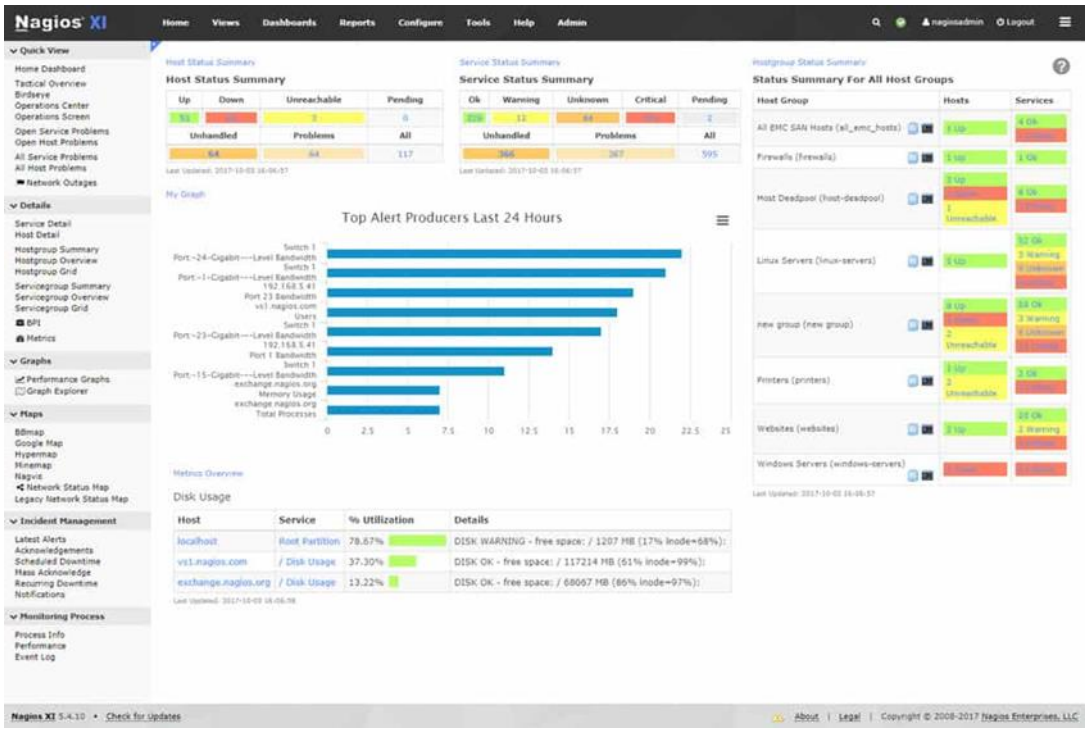
Nagios

Nagios Core, open-source aplikace pro monitorování systémů a sítí (Obrázek 2), je navržena tak, aby monitorovala určené hostitele, služby a poskytovala upozornění na problémy i zlepšení. Ačkoli je jeho původní návrh určen pro Linux, lze jej přizpůsobit většině systémů podobných Unixu.

Mezi klíčové vlastnosti Nagios Core patří monitorování síťových služeb a prostředků hostitelů, jednoduchý návrh zásuvných modulů pro vlastní kontroly služeb, paralelizované kontroly služeb a možnost definovat hierarchii síťových hostitelů. Umožňuje kontaktní oznámení prostřednictvím e-mailu, pageru nebo vlastních metod při vzniku nebo řešení problémů a lze konfigurovat obsluhy událostí pro proaktivní řešení problémů.

Nagios Core navíc podporuje automatickou rotaci souborů protokolů, implementaci redundantních monitorovacích hostitelů a nabízí volitelné webové rozhraní pro zobrazení stavu sítě v reálném čase, historie oznámení a další (Keary, 2023).

Obrázek 2: Nagios Core



Zdroj: (Keary, 2023)

Zabbix

Zabbix je vysoce uznávané open-source řešení pro monitorování a správu sítě (Obrázek 3), které je známé svou všestranností při monitorování různých aspektů síťových systémů, aplikací a služeb. Podporuje monitorování v reálném čase, což uživatelům umožňuje sledovat stav a výkonnost síťových prostředků v okamžiku, kdy dojde k událostem, a shromažďuje různá data včetně systémových metrik a protokolů, aby poskytl komplexní pohled na síť.

Jednou z význačných funkcí Zabbixu jsou jeho robustní funkce upozorňování a oznamování. Uživatelé mohou nastavit spouštěče a prahové hodnoty pro příjem upozornění při splnění konkrétních podmínek nebo při výskytu problémů a tato upozornění lze doručovat prostřednictvím kanálů, jako jsou e-mail, SMS a vlastní skripty, aby bylo možné zajistit včasnou reakci (Keary, 2023).

Architektura Zabbixu je modulární a rozšiřitelná, takže nabízí flexibilitu při vytváření vlastních zásuvných modulů a integrací pro splnění konkrétních požadavků na monitorování. Komunita Zabbix neustále vyvíjí širokou škálu zásuvných modulů a šablon, které mohou uživatelé snadno nasadit.

Dalším důležitým aspektem systému je ukládání historických dat, které umožňuje analýzu a vizualizaci výkonu sítě v čase. Tato historická data jsou nezbytná pro plánování kapacity, analýzu trendů a identifikaci dlouhodobých problémů.

Také nabízí intuitivní webové rozhraní pro konfiguraci, monitorování a vytváření zpráv s pokročilými možnostmi vizualizace map, obrazovek a zjišťování sítě. Lze jej škálovat tak, aby vyhovoval velkým a složitým síťovým prostředím, a podporuje možnosti vysoké dostupnosti pro zajištění nepřetržitého monitorování.

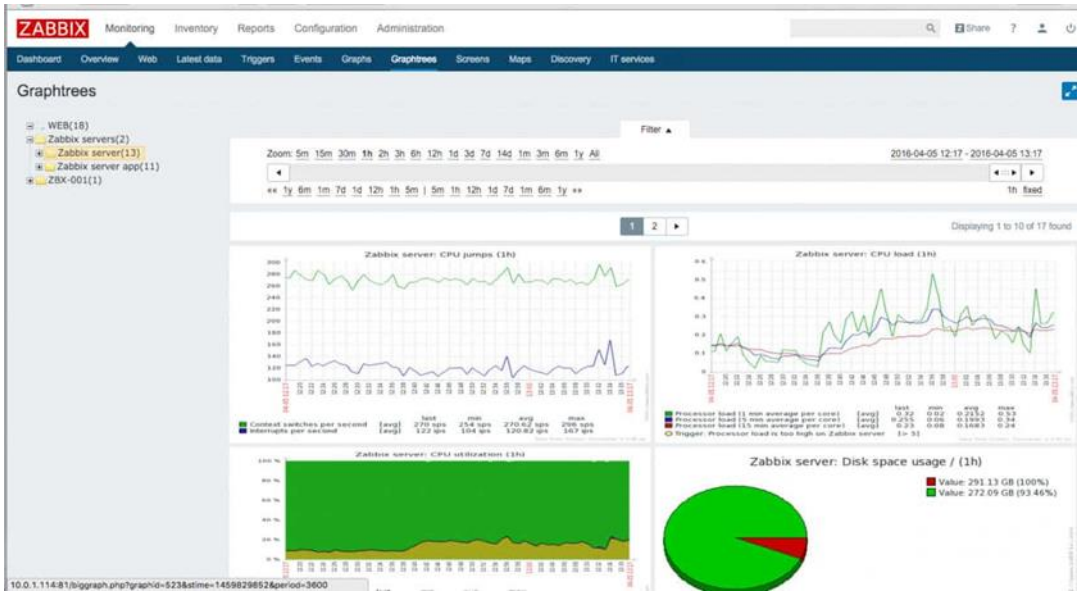
Obsahuje také nástroje pro vytváření zpráv a analýz, které uživatelům umožňují vytvářet vlastní zprávy a panely pro vizualizaci dat. Funkce reportování je nezbytná pro optimalizaci výkonu, analýzu trendů a vykazování shody s předpisy.

Zabbix je k dispozici v bezplatné komunitní verzi s otevřeným zdrojovým kódem i v komerční podnikové verzi, přičemž podniková verze nabízí další funkce a profesionální podporu. Nástroj těží z aktivní a živé komunity uživatelů, která neustále přispívá k jeho vývoji a poskytuje množství zdrojů, šablon a zásuvných modulů.

Zabbix je navržen s ohledem na bezpečnost a lze jej používat v různých odvětvích, včetně zdravotnictví a finanční sféry, aby splňoval požadavky na shodu s předpisy. Vývojový tým se i nadále věnuje inovacím a zajišťuje, aby Zabbix zůstal relevantní a připravený na budoucnost v neustále se vyvíjejícím prostředí IT. Jeho holistický přístup umožňuje správcům sítě udržovat výkon sítě, proaktivně identifikovat problémy a optimalizovat přidělování zdrojů,

což z něj činí špičkovou volbu pro organizace všech velikostí, které hledají robustní možnosti monitorování sítě (Liefting, a další, 2022).

Obrázek 3: Zabbix



Zdroj: (Keary, 2023)

3.2.2 Komerční použití

SolarWinds Network Performance Monitor

SolarWinds Network Performance Monitor (viz Obrázek 4) je komplexní nástroj pro monitorování výkonu sítě, který dokáže sledovat stav zařízení pomocí protokolu SNMP. Dokáže automaticky zjišťovat síťová zařízení připojená k síti.

Klíčové funkce:

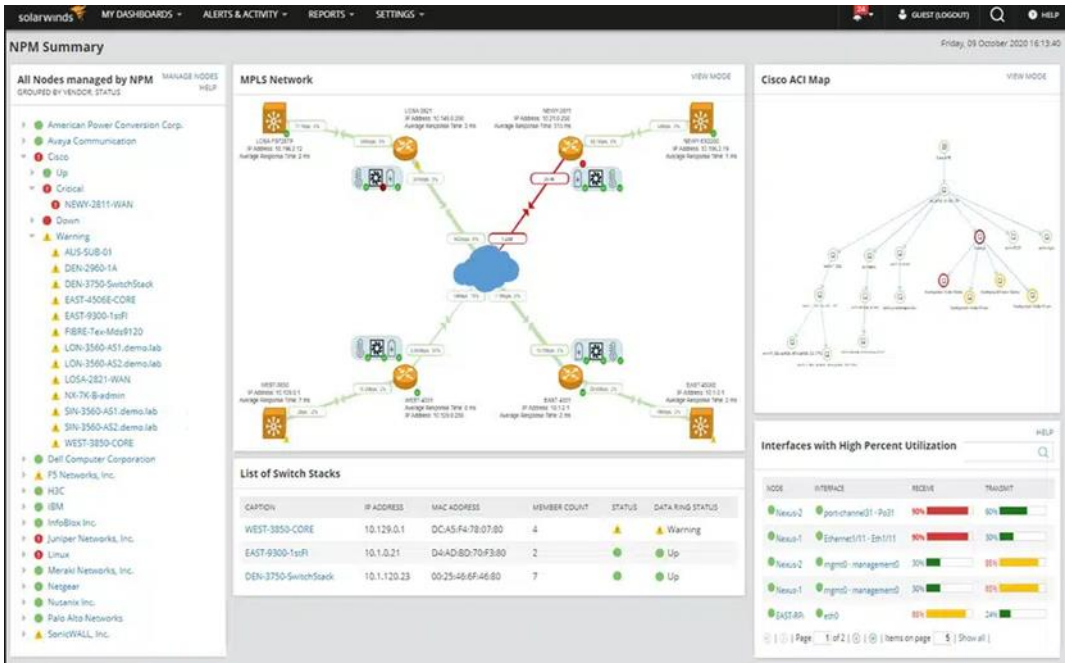
- Monitorování SNMP
- Automaticky zjišťuje připojená síťová zařízení
- Analýza síťových paketů
- Inteligentní síťové mapy s funkcí NetPath
- Vytváření tepelných map WiFi
- Systém výstrah
- Systém hlášení
- Unikátní funkce

Jedinečnou funkcí systému SolarWinds je nástroj NetPath. Jedná se o obdobu funkce traceroute, která je k dispozici v jiných nástrojích na tomto seznamu, jako jsou PRTG a Site24x7. Nástroj NetPath však zobrazuje trasu jako vizuální zobrazení.

Nabízí možnosti mapování pro vizualizaci struktury sítě a proaktivně odhaluje problémy s výkonem. Při výskytu problémů tento systém okamžitě vydává upozornění a oznámení. Objevená zařízení, aplikace a služby lze navíc vizualizovat na mapě topologie sítě a získat tak přehled o propojení celé infrastruktury. Funkce NetPath nabízí možnost sledovat přenosy paketů hop po hopu, a to napomáhá efektivní diagnostice problémů s výkonem sítě.

Pro monitorování na míru umožňuje systém vlastních výstrah uživatelům stanovit spouštěcí podmínky pro výstrahy. Jakmile jsou tyto podmínky splněny, software doručuje oznámení e-mailem nebo SMS, čímž zajišťuje, že jsou uživatelé okamžitě informováni o významných událostech. Komplexní seznam výstrah, rozdělený podle závažnosti, je přístupný na stránce „Všechny aktivní výstrahy“, což uživatelům umožňuje sledovat stav sítě a včas řešit problémy (Kinza, a další, 2023).

Obrázek 4: SolarWinds Network Performance Monitor



Zdroj: (Keary, 2023)

PRTG Network Monitor

PRTG Network Monitor (viz Obrázek 5), vyvinutý společností Paessler, je univerzální sada pro monitorování sítě, která kombinuje protokol SNMP, sniffing paketů a rozhraní WMI

pro komplexní dohled nad sítí. Zjednodušuje proces monitorování tím, že nabízí funkce, jako je skenování síťových segmentů pro zjišťování a přidávání zařízení pro monitorování. Uživatelé si mohou vybrat z řady senzorů pro sledování konkrétních aspektů sítě. Mezi tyto senzory patří mimo jiné senzory pro sledování šířky pásma, senzory hardwarových parametrů, měřiče využití síťových dat, senzory SNMP, senzory VOIP a QoS.

Klíčové funkce:

- Monitorování SNMP
- Monitorování šířky pásma
- Zjišťování síťových zařízení pomocí skenování segmentů IP
- Přizpůsobitelné ovládací panely
- Systém výstrah založený na prahových hodnotách
- Funkce pro vytváření zpráv
- Přizpůsobitelné mapy sítě
- Jedinečné funkce

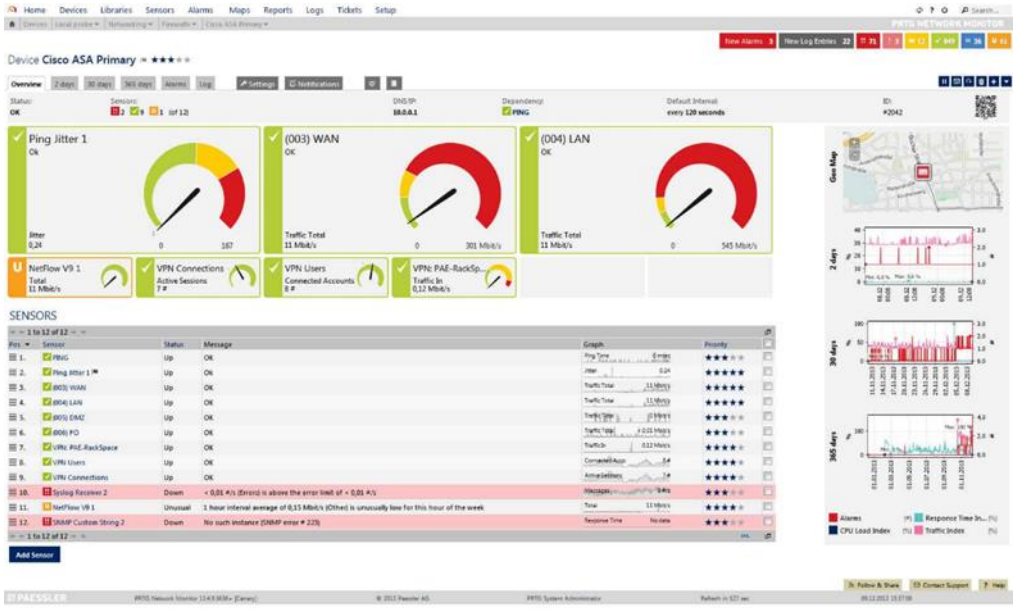
Jednou z charakteristických vlastností nástroje PRTG Network Monitor je výjimečné sledování doby odezvy webových stránek. Obsahuje senzor webových stránek pro záznam doby jejich načítání, který lze spustit na vyžádání nebo naplánovat. Balíček navíc zahrnuje monitor dostupnosti webových stránek založený na protokolu ping a tyto senzory pro monitorování jsou k dispozici i v bezplatné edici PRTG.

Tato aplikace je vysoce flexibilní a umožňuje uživatelům aktivovat a přizpůsobit senzory podle jejich specifických požadavků na monitorování sítí, serverů a aplikací.

Pro lepší vizualizaci poskytuje nástroj přizpůsobitelný řídicí panel, který usnadňuje vytváření síťových map infrastruktury v reálném čase. Obsahuje editor pro přetahování a více než 300 mapových objektů pro tvorbu map. Uživatelé mohou dokonce navrhovat vlastní mapové objekty pomocí jazyka HTML.

Systém výstrah založený na prahových hodnotách zajišťuje, že jsou uživatelé okamžitě informováni o změně stavu snímače, kolísání hodnot nebo překročení prahových hodnot. Upozornění jsou k dispozici v různých formátech, včetně e-mailu, push upozornění, SMS, zpráv na Slacku, zpráv Syslog, pastí SNMP, akcí HTTP, spuštění programu a dalších (Keary, 2023).

Obrázek 5: PRTG Network Monitor



Zdroj: (Keary, 2023)

3.3 Bezpečnostní systémy

Zabezpečení sítě zahrnuje strategická opatření zavedená za účelem ochrany dat a síťových zdrojů organizace. Slouží jako robustní obrana proti potenciálním hrozbám a neoprávněnému přístupu a poskytuje ochranu v širokém spektru odvětví bez ohledu na velikost organizace nebo její infrastrukturu.

Oblast zabezpečení sítí zahrnuje celou řadu technologií, zařízení a procesů, které jsou určeny k zajištění ochrany počítačových sítí a jejich dat. Tato bezpečnostní infrastruktura je určena k zajištění integrity, důvěrnosti a dostupnosti počítačů. "Triáda CIA" je zkratka pro důvěrnost, integritu, dostupnost a představuje základní komponenty, které označují bezpečnou síť. Tvoří základ pro vytváření zásad zabezpečení sítí v organizacích.

V době, kdy je internet věcí (IoT) novou normou, je síťová architektura stále složitější. Vyvíjející se prostředí představuje neustálou výzvu, protože hackeři neúnavně hledají a využívají zranitelnosti napříč zařízeními, daty, aplikacemi, uživateli a lokalitami. Důsledky i toho nejkratšího výpadku sítě mohou být finančně značné, což podtrhuje zásadní význam robustních opatření pro zabezpečení sítě (Prabhu, 2021).

Zabezpečení sítě představuje komplexní rámec technologií, zařízení a procesů pečlivě navržených tak, aby chránily síťovou infrastrukturu organizace před neoprávněným přístupem,

potenciálním zneužitím podnikových zdrojů, neúmyslným prozrazením a rušivým odepřením služeb.

Konkrétní metody, které organizace používá k posílení své sítě, se mohou lišit a jsou přizpůsobeny jejím jedinečným požadavkům a okolnostem. Základní cíl zabezpečení sítě však zůstává jednotný napříč celým podnikatelským prostředím. Tím je zajistit důvěryhodnost podnikových informací, zachovat integritu dat a zaručit nepřetržitý přístup k podnikovým zdrojům.

Zabezpečení sítě je pro každou organizaci nepostradatelným pilířem, který slouží jako ochranný štít chránící její zájmy a usnadňující efektivní provoz.

V dnešním dynamickém podnikatelském prostředí již finanční úspěch organizace nezávisí pouze na chytrých marketingových strategiích a zdravých peněžních tocích. Rychlý vývoj internetu přinesl okamžitou komunikaci a vysokorychlostní transakce, které tvoří základ moderních obchodních operací.

Naopak kyberzločinci a hackeři neustále zdokonalují své taktiky a snaží se narušit, odcizit a ohrozit tok dat procházející informační superdálnicí. Zabezpečení sítě je proto nezbytnou součástí, která pomáhá chránit digitální zájmy organizace a zajišťuje nepřerušený tok obchodních operací ve stále propojenějším světě (Swanagan, 2023).

3.3.1 Narušení bezpečnosti

Zranitelnosti sítě

Pro pochopení významu zabezpečení sítě a jeho úlohy při prevenci bezpečnostních útoků je zásadní identifikovat zranitelnosti, které hackeři využívají k získání neoprávněného přístupu, nasazení malwaru, manipulaci s daty nebo dokonce k jejich zničení. Tyto zranitelnosti mohou být slabými místy v infrastruktuře sítě:

- **Chybějící šifrování dat:** V některých případech jsou citlivá data přenášena nebo ukládána bez odpovídajícího šifrování nebo bezpečnostních opatření. Toto nedopatření může potenciálně vystavit data odposlechu nebo krádeži během přenosu.
- **Operating System Command Injection(OSCI):** Prostřednictvím této chyby mohou záškodníci provádět libovolné příkazy operačního systému. Tento průnik může ohrozit integritu a funkčnost serverů, na kterých běží aplikace, což může mít vážné následky.
- **SQL Injection:** Hackeři používají techniky SQL injection k zachycení a manipulaci s dotazy, které aplikace zadává svému serveru. Tato zranitelnost může vést k neoprávněnému přístupu k databázím a citlivým datům.

• **Chybějící ověření:** Některé softwary neimplementují správné ověřování uživatelů nebo prostředků, takže systém je náchylný k neoprávněnému přístupu.

• **Neomezené nahrávání nebezpečných typů souborů:** Tato zranitelnost vzniká, když softwarová aplikace umožňuje neomezené nahrávání potenciálně nebezpečných typů souborů. Škodlivé soubory mohou být nahrány a spuštěny v prostředí softwaru, což představuje významné bezpečnostní riziko.

Mezi další zranitelnosti patří slabá hesla, přetečení bufferu, chybějící autorizace, cross-site scripting a falšování, stahování kódů bez kontroly integrity, používání porušených algoritmů, přesměrování URL na nedůvěryhodné stránky, procházení cest a chyby.

Cílem účinných postupů zabezpečení sítě je řešit a zmírnit tyto zranitelnosti a chránit systémy, data a uživatele před potenciálními hrozbami a útoky. Používání robustních bezpečnostních opatření, jako jsou firewally, systémy detekce narušení a pravidelné hodnocení bezpečnosti, je zásadní pro ochranu před těmito a dalšími riziky zabezpečení sítě (Prabhu, 2021).

Typy útoků

Zranitelnosti v síti mohou organizace vystavit široké škále potenciálně ničivých útoků, jako jsou:

• **Viry:** Viry vyžadují k aktivaci interakci uživatele, často prostřednictvím podvodných e-mailů se škodlivými odkazy nebo přílohami. Jakmile se spustí, mohou obejít zabezpečení systému a narušit provoz zařízení a potenciálně poškodit zařízení uživatele.

• **Malware:** Malware je rychlým prostředkem pro škodlivé útoky, speciálně navržený k ohrožení a získání neoprávněného přístupu k systémům. Může se sám replikovat a rychle se šířit internetem a ovlivňovat všechny počítače připojené k síti, a dokonce i externí zařízení připojená k síti.

• **„Červ“ (worm):** Zranitelné síťové aplikace se mohou stát obětí útoků červa, které nevyžadují zapojení uživatele. Útočníci mohou odeslat malware přes stejné internetové připojení jako uživatel a vytvořit tak červa, který dokáže zneužít zranitelnosti sítě (Mareš, 2022).

> *„Nejzákeřnější jsou však nesmírně rychle se množící „počítačoví červy“, jako byl například ransomware vypuštěný pod názvem WannaCry, jenž v roce 2017 během prvních dvou týdnů od vydání zaviroval přibližně 400000 počítačů ve 150 zemích světa.“ (Mareš, 2022 str. 90)*

• **Phishing:** Phishingové útoky jsou běžně spojeny s narušením sítě. Uživatelé dostávají klamavé e-maily vydávající se za důvěryhodné zdroje. Interakce se škodlivými odkazy nebo přílohami v těchto e-mailech může způsobit zranitelnost sítě a ztrátu dat.

• **Botnet:** Při útoku botnetem je síť soukromých počítačů napadena a ovládána útočníkem bez vědomí jejich vlastníků. Útočník pak může tyto "zombie" počítače použít k infikování dalších zařízení nebo způsobení škody.

• **Odmítnutí služby (DoS) a distribuované odmítnutí služby (DDoS):** Útoky DoS mohou ochromit jednu síť nebo celou infrastrukturu a zabránit ověřeným uživatelům v přístupu ke zdrojům. Sofistikovanější forma útoků DDoS využívá k zacílení na oběti více napadených systémů, takže je obtížnější je odhalit a zmírnit.

• **Man-in-the-middle(muž uprostřed):** Při tomto typu útoku narušitel zachytí a odposlouchává komunikaci mezi dvěma uživateli sítě a může zachytit, sledovat nebo dokonce manipulovat s informacemi.

• **Sniffer paketů:** Pasivní přijímače umístěné v blízkosti bezdrátového vysílače kopírují každý přenášený paket, který často obsahuje důvěrná a citlivá data. Tyto přijímače se stávají paketovými čmuchaly a shromažďují všechny pakety ve svém dosahu.

• **DNS a IP Spoofing:** Při podvržení DNS hackeři poškozují tato data a zavádějí jejich mezipaměť, v důsledku čehož jmenný server při vyhledávání poskytuje nesprávné IP adresy. Při IP spoofingu se útočník vydává za jiného uživatele tím, že do internetu vkládá pakety s falešnými adresami.

• **Kompromitovaný klíč:** Útočníci mohou získat přístup k zabezpečené komunikaci kompromitací klíče, což je obvykle tajný kód nebo číslo používané k přístupu k citlivým informacím.

Řešení a zmírnění těchto zranitelností je zásadní pro ochranu bezpečnosti sítě a zajištění důvěrnosti, integrity a dostupnosti kritických dat a zdrojů. Při obraně proti těmto potenciálním hrozbám jsou klíčové důkladné bezpečnostní postupy a řešení (Prabhu, 2021).

3.3.2 Typy síťové bezpečnosti

Network Access Control

Řízení přístupu k síti (NAC) se stává stále důležitějším v souvislosti s tím, jak organizace zavádějí zásady BYOD (Bring Your Own Device). NAC poskytuje potřebnou viditelnost, řízení přístupu a funkce pro zajištění souladu s předpisy, které posilují infrastrukturu zabezpečení sítě (Adams, a další, 2014).

NAC neboli řízení přístupu k síti je síťové řešení navržené tak, aby umožňovalo přístup pouze vyhovujícím, ověřeným a důvěryhodným koncovým zařízením a zároveň zabraňovalo neoprávněnému přístupu k síťovým zdrojům a infrastruktuře.

Systémy NAC využívají kontrolu adres MAC a protokol SNMP k vynucení přísné kontroly přístupu. Nevyhovujícím zařízením je buď odepřen přístup k síti, jsou umístěna do karantény, nebo je jim udělen omezený přístup k výpočetním prostředkům. Tento přístup pomáhá chránit síť tím, že zabraňuje infikování sítě nezabezpečenými zařízeními.

Řešení NAC navíc dokáže oddělit hostovaná zařízení od interní sítě. Dokáže identifikovat všechna zařízení připojená k portům síťového přepínače, což umožňuje vzdáleně zakázat nepovolená zařízení bez nutnosti technické podpory, a tím dále zvýšit zabezpečení a kontrolu sítě (Swanagan, 2023).

Network Security Policies

Zásady zabezpečení sítě jsou klíčovým rámcem sestávajícím ze standardizovaných postupů a praktik. Slouží jako komplexní průvodce, který vymezuje pravidla pro přístup k síti, definuje síťovou architekturu a stanovuje parametry pro prosazování zásad.

Význam politiky zabezpečení sítě spočívá v tom, že dokáže vzdělávat a informovat zaměstnance organizace o základních požadavcích na ochranu aktiv v rámci síťové infrastruktury. Tato aktiva zahrnují široké spektrum, od kritických hesel a citlivých dokumentů až po servery, na nichž je provoz sítě založen.

Zásady zabezpečení sítě navíc stanoví jasný soubor pokynů, které upravují pořizování, konfiguraci a průběžný audit počítačových systémů a síťových prostředků. Dodržováním těchto zásad může organizace účinně snížit možnost náhodné i úmyslné ztráty dat, zmírnit riziko kybernetických útoků a udržet integritu svých podnikových dat. Dobře sestavené a snadno interpretovatelné zásady zabezpečení sítě jsou v podstatě impozantní ochranou, která posiluje síť proti hrozbám a zranitelnostem (Swanagan, 2023).

Application security

Bezpečnost aplikací představuje kritický proces zahrnující vývoj, integraci a důkladné testování bezpečnostních opatření v softwarových aplikacích. Hlavním cílem je posílit aplikace proti bezpečnostním zranitelnostem, které by mohly být zneužity hrozbami, včetně neoprávněného přístupu a modifikace dat.

Zpráva společnosti Veracode "State of Software Security" (Stav zabezpečení softwaru) upozorňuje na závažnost tohoto problému a uvádí, že ohromujících 83 % z 85 000 zkoumaných

aplikací vykazovalo alespoň jednu bezpečnostní chybu. Alarmujícím zjištěním bylo odhalení celkem 10 milionů bezpečnostních chyb v těchto aplikacích, přičemž 20 % z nich skrývalo alespoň jednu vysoce závažnou zranitelnost.

V této souvislosti je pro organizace nezbytné provádět rutinní testování zabezpečení aplikací. Tato praxe je zásadní pro identifikaci a následné zmírnění zranitelností kódu. Proaktivním řešením těchto nedostatků mohou organizace účinně odradit kybernetické útočníky od napadení nebo zneužití kritických webových aplikací a posílit tak svou digitální obranu proti potenciálním hrozbám (Swanagan, 2023).

Vulnerability Management

Správa zranitelností představuje trvalý a metodický postup zaměřený na identifikaci, stanovení priorit, nápravu a hlášení bezpečnostních zranitelností v počítačových systémech. Tento proces začíná odhalením, kategorizací a komplexním hlášením aktiv v síti. Tyto zprávy se používají jako základ pro zaměření a řešení bezpečnostních zranitelností v různých systémech.

Význam správy zranitelností je v současném digitálním prostředí obzvláště výrazný vzhledem k tomu, že škodliví aktéři neustále prohledávají internet a hledají zranitelnosti, které by mohli zneužít. Navíc aktivně využívají neřešených bezpečnostních chyb, a to i těch, které přetrvávají delší dobu. Důrazem na správu zranitelností mohou organizace tyto hrozby proaktivně řešit, čímž minimalizují rizika spojená s neopravenými zranitelnostmi a posilují svou pozici v oblasti kybernetické bezpečnosti (Swanagan, 2023).

Network Penetration Testing

Síťové penetrační testování představuje záměrné a systematické úsilí zaměřené na posouzení a zhodnocení bezpečnosti IT infrastruktury. Toto hodnocení se provádí metodickými pokusy o zneužití potenciálních zranitelností v síti při zachování bezpečného a kontrolovaného prostředí.

Tyto zranitelnosti se mohou projevovat v různých dimenzích, včetně operačních systémů, slabých míst služeb a aplikací, nesprávných konfigurací brány firewall nebo dokonce nejistého chování koncových uživatelů.

Význam penetračního testování v rámci kybernetické bezpečnosti organizace je mnohostranný. Zaprvé slouží jako neocenitelný vzdělávací nástroj, který poskytuje pracovníkům praktické zkušenosti s řešením kybernetických útoků pocházejících od škodlivých

subjektů. Tyto znalosti mohou být zásadní pro zvýšení celkové kybernetické odolnosti organizace.

Penetrační testování navíc plní důležitou funkci kontroly funkčnosti a účinnosti bezpečnostních politik organizace. Podrobením těchto zásad reálným testovacím scénářům mohou organizace zjistit jejich robustnost při odrazování a zmírňování potenciálních kybernetických hrozeb, a tím posílit své kybernetické zabezpečení (Swanagan, 2023).

Data Loss Prevention

Prevence ztráty dat (DLP) zahrnuje strategický přístup, jehož cílem je identifikovat a zmařit potenciální narušení dat nebo neoprávněný přenos citlivých informací. Toho se dosahuje prostřednictvím pečlivého monitorování, detekce a blokování citlivých dat v různých fázích, a to při jejich aktivním používání (při činnostech na koncových bodech), při přenosu (v síťovém provozu) a v klidovém stavu (v datovém úložišti).

Klíčový význam DLP podtrhuje jeho schopnost odhalit, a především zabránit neúmyslnému vystavení citlivých dat nechtěným příjemcům. Díky monitorování v reálném čase a automatickým mechanismům reakce hrají systémy DLP zásadní roli při ochraně datových aktiv organizace.

Řešení DLP nabízejí takovou úroveň přizpůsobení, která jim umožňuje okamžitě upozornit koncové uživatele prostřednictvím vyskakovacích oznámení nebo e-mailových zpráv v reakci na porušení zásad. Tento přizpůsobený přístup působí jako silný odrazující prostředek proti úniku dat, ať už je základní činnost náhodná, nebo škodlivá. V konečném důsledku slouží DLP jako robustní obranný mechanismus proti únikům dat a souvisejícím rizikům (Swanagan, 2023).

Antivirus software

Antivirový software je základní kategorií softwarových nástrojů, které slouží k prevenci, skenování, detekci a odstraňování virů z počítačových systémů.

Po instalaci většina antivirového softwaru pracuje tiše na pozadí a nabízí nepřetržitou ochranu v reálném čase před potenciálními virovými útoky. Tento proaktivní přístup je nepostradatelný tváří v tvář neustále rostoucímu náporu nově se objevujících virů, jejichž nesčetné varianty jsou objevovány každý den.

Dynamická povaha prostředí kybernetické bezpečnosti podtrhuje zásadní význam konfigurace antivirového softwaru tak, aby se automaticky aktualizoval na nejnovější soubory

s definicemi virů. Tím je zajištěno, že software zůstane dobře vybaven k boji proti množství škodlivých kódů kolujících po internetu.

Dnešní tvůrci škodlivého softwaru dobře vědí, jak zneužít zranitelnosti počítačových systémů, a antivirový software je proto první obrannou linií při ochraně těchto systémů před virovými infekcemi. Jeho proaktivní skenování a detekční funkce pomáhají zmírnit rizika, která představuje škodlivý software, a chrání tak integritu počítačových systémů (Swanagan, 2023).

Endpoint Detection and Response

Technologie EDR (Endpoint Detection and Response) hraje klíčovou roli v oblasti kybernetické bezpečnosti a je definována jako komplexní řešení, které průběžně zaznamenává systémové aktivity a události probíhající na jednotlivých koncových bodech v síti.

EDR poskytuje bezpečnostním týmům životně důležitou pomoc, protože jim poskytuje tolik potřebný přehled, který umožňuje odhalit bezpečnostní incidenty, které by jinak zůstaly skryty, a posiluje tak schopnosti organizace odhalovat hrozby a reagovat na ně.

Zásadní význam EDR podtrhuje jeho schopnost nabídnout grafické znázornění toho, jak se útočníkovi podařilo prolomit obranu systému, a následných akcí, které podnikl, když se dostal dovnitř. Toto grafické zobrazení zvyšuje hloubku analýzy incidentů a strategie reakce.
Jedním z nejvýznamnějších atributů EDR je jeho zdatnost při odhalování škodlivých aktivit probíhajících na koncovém bodě. Tato schopnost se rozšiřuje na identifikaci hrozeb pocházejících z exploitů nultého dne, pokročilých přetrvávajících hrozeb a zákeřných útoků bez souborů nebo malwaru, které postrádají rozeznatelné signatury, takže jsou schopny vyhnout se tradičním antivirovým řešením. EDR se svými pokročilými detekčními mechanismy tak představuje důležitou součást arzenálu kybernetické bezpečnostní obrany, která řeší vyvíjející se a nepolapitelnou povahu současných kybernetických hrozeb (Swanagan, 2023).

Email security

Zabezpečení e-mailu zahrnuje celou řadu postupů a technik navržených k ochraně e-mailových účtů, jejich obsahu a komunikace před neoprávněným přístupem, ztrátou dat nebo kompromitací.

E-mail slouží jako běžný vektor pro šíření škodlivého softwaru, nevyžádaného spamu a phishingových útoků, a proto je zabezpečení e-mailu prvořadým úkolem.

Organizace si uvědomují zásadní potřebu zavést robustní opatření pro zabezpečení e-mailů, aby se ochránily před různorodými kybernetickými hrozbami přenášenými prostřednictvím e-mailu. Kromě toho hraje klíčovou roli při zajišťování šifrování citlivých

zpráv při jejich cestě ze sítě k zamýšleným příjemcům. Toto šifrování slouží jako ochrana proti potenciálnímu zachycení a odhalení důvěrných informací, čímž je zachována důvěrnost a integrita komunikace v rámci organizace (Swanagan, 2023).

Wireless Security

Zabezpečení bezdrátových sítí představuje také ochranu Wi-Fi před neoprávněným přístupem a pokusy o záškodnické vniknutí.

Význam robustních opatření pro zabezpečení bezdrátových sítí v současné době vzrostl v důsledku rozšíření vzdálených pracovních úvazků, kdy se zaměstnanci připojují k internetu prostřednictvím bezdrátových sítí.

Bezdrátové sítě, včetně Wi-Fi, jsou ze své podstaty náchylné k hackerským útokům, pokud jsou povoleny nevhodné nebo slabé bezdrátové protokoly. Proto je nezbytné vybudovat a udržovat bezdrátovou síť opevněnou moderními protokoly bezdrátového zabezpečení, jako je WPA2. Takové protokoly slouží jako účinná ochrana proti kybernetickým útokům, posilují integritu sítě a chrání ji před možným narušením bezpečnosti (Swanagan, 2023).

IPS/IDS

V oblasti síťové bezpečnosti se systémy prevence narušení (IPS) a systémy detekce narušení (IDS) používají k identifikaci a zmírnění potenciálních bezpečnostních incidentů. Ačkoli se tyto pojmy často používají zaměnitelně, plní odlišné funkce.

Systém detekce narušení (IDS) slouží především jako bdělý pozorovatel v síti, který pečlivě monitoruje systém a síťové aktivity. Pokud identifikuje podezřelé události nebo vzorce naznačující potenciální narušení bezpečnosti, neprodleně odešle upozornění a informuje správce nebo bezpečnostní pracovníky.

Naproti tomu systém prevence narušení (IPS) je navržen tak, aby při zjištění probíhajících útoků okamžitě zasáhl. Jeho hlavním cílem je zmařit tyto útoky v reálném čase a zabránit tak ohrožení bezpečnosti cílových systémů a sítí.

IPS a IDS představují klíčové součásti bezpečnostní infrastruktury organizace. Zatímco systém IDS vyniká v identifikaci a hlášení bezpečnostních hrozeb, systém IPS proaktivně prosazuje bezpečnostní zásady a účinně zastavuje útoky v jejich počátku. Stojí za zmínku, že v moderních zařízeních pro zabezpečení sítě jsou tyto dvě technologie často integrovány do jediného zařízení pro jednotnou správu hrozeb (UTM), což zjednodušuje bezpečnostní operace a posiluje obranu sítě proti nesčetným hrozbám (Swanagan, 2023).

Network segmentation

Segmentace sítě je strategický architektonický přístup, který zahrnuje rozdělení sítě na několik samostatných segmentů nebo mikrosítí, čímž se efektivně vytvářejí izolované oblasti síťové aktivity.

Tato segmentace dává správcům sítě možnost pečlivě řídit tok provozu mezi těmito podsítěmi a prosazovat jemné zásady, které určují, jak se data v síti pohybují.

Význam segmentace sítě nelze přeceňovat. Zavedením tohoto přístupu mohou organizace dosáhnout několika cílů. Nejenže zvyšuje účinnost monitorování a zvyšuje výkonnost sítě, ale co je možná nejdůležitější – posiluje bezpečnost sítě.

Jednou z nejdůležitějších výhod segmentace sítě je její schopnost bránit šíření malwaru. Izolováním segmentů je možné omezit a zmírnit dopad narušení bezpečnosti v jednom segmentu a ochránit ostatní části před potenciálním ohrožením. Toto ochranné opatření působí jako robustní obrana a snižuje potenciální škody, které mohou bezpečnostní hrozby způsobit v celé síti (Swanagan, 2023).

SIEM

Systém správy bezpečnostních informací a událostí (SIEM) hraje klíčovou roli při pomoci organizacím s úkoly, jako je detekce hrozeb, zajištění shody s předpisy a efektivní správa bezpečnostních incidentů. Těchto cílů dosahuje shromažďováním, analýzou a zpracováním bezpečnostních událostí, a to jak v reálném čase, tak z minulých událostí. Kromě toho zpracovává různé zdroje dat o událostech a informace bohaté na kontext.

Systém SIEM je postaven na třech základních funkcích, které podtrhují jeho význam pro organizace:

- Detekce incidentů a vytváření časové osy útoků: SIEM vyniká při identifikaci bezpečnostních incidentů a vytváření časových os sekvencí útoků. Korelací dat a hloubkovou analýzou rychle rozpoznává hrozby a jejich chronologický průběh.
- Správa incidentů: SIEM poskytuje centralizovanou platformu pro správu bezpečnostních incidentů. To umožňuje bezpečnostním týmům koordinovat své reakce, důkladně vyšetřovat narušení bezpečnosti a efektivně řešit bezpečnostní problémy.
- Deník shody a regulace zdroje logů: SIEM slouží jako robustní zdroj protokolů, který organizacím umožňuje plnit jejich povinnosti v oblasti dodržování předpisů a regulací. Díky komplexnímu sběru a konsolidaci dat o událostech vytvářejí systémy SIEM rozsáhlé

auditní záznamy, které jsou neocenitelné pro hodnocení související s dodržováním předpisů a regulačním výkaznictvím.

Souhrnně lze říci, že řešení SIEM nabízejí organizacím nepostradatelné funkce, které jim pomáhají zlepšit jejich pozici v oblasti kybernetické bezpečnosti, zajistit shodu s předpisy a účinně reagovat na bezpečnostní incidenty (Swanagan, 2023).

Web security

Zabezpečení webu se týká zabezpečení webových aplikací, které jsou přístupné přes internet. Zahrnuje různá opatření, nástroje a prostředky, jejichž cílem je odhalovat kybernetické hrozby, předcházet jim a reagovat na ně.

V dnešním digitálním prostředí je pro firmy běžná přítomnost na internetu. Využívají webové stránky k propagaci služeb, usnadnění online plateb a výměně osobních informací s veřejností.

Zabezpečení webu má obrovský význam, protože chrání identitu a pověst organizace před možným poškozením. Strategie pro posílení zabezpečení webu zahrnují přijetí postupů bezpečného kódování, omezení webových aplikací tak, aby podporovaly pouze nejnovější protokoly SSL/TLS, pravidelné skenování zranitelností webových aplikací a provádění penetračních testů pro identifikaci a odstranění potenciálních slabých míst. Tato opatření společně přispívají k robustnějšímu a odolnějšímu rámci zabezpečení webu. (Swanagan, 2023)

Multifactor Authentication

Vícefaktorové ověřování (MFA), často označované jako MFA, je systém ověřování, který vyžaduje použití více než jednoho odlišného ověřovacího faktoru k úspěšnému ověření identity uživatele.

MFA lze provádět prostřednictvím vícefaktorového autentizátoru nebo kombinací různých autentizátorů, z nichž každý poskytuje různé autentizační faktory. Tyto faktory obecně spadají do tří kategorií: něco, co znáte, něco, co máte a něco, co jste.

Význam MFA spočívá v jeho schopnosti zvýšit bezpečnost. V situacích, kdy jsou uživatelské jméno a heslo uživatele kompromitovány, například v případě úniku dat, chybí kybernetickému útočníkovi další ověřovací faktor potřebný k dokončení procesu ověřování. Tato další úroveň zabezpečení pomáhá chránit uživatelské účty a citlivé informace (Swanagan, 2023).

Příklady ověřovacích faktorů zahrnují (Adams, a další, 2014):

- heslo nebo kód PIN.

• hardwarové nebo softwarové tokeny vydané organizací.

• biometrické identifikátory, jako jsou otisky prstů, skeny IRIS/retiny nebo rozpoznávání obličeje.

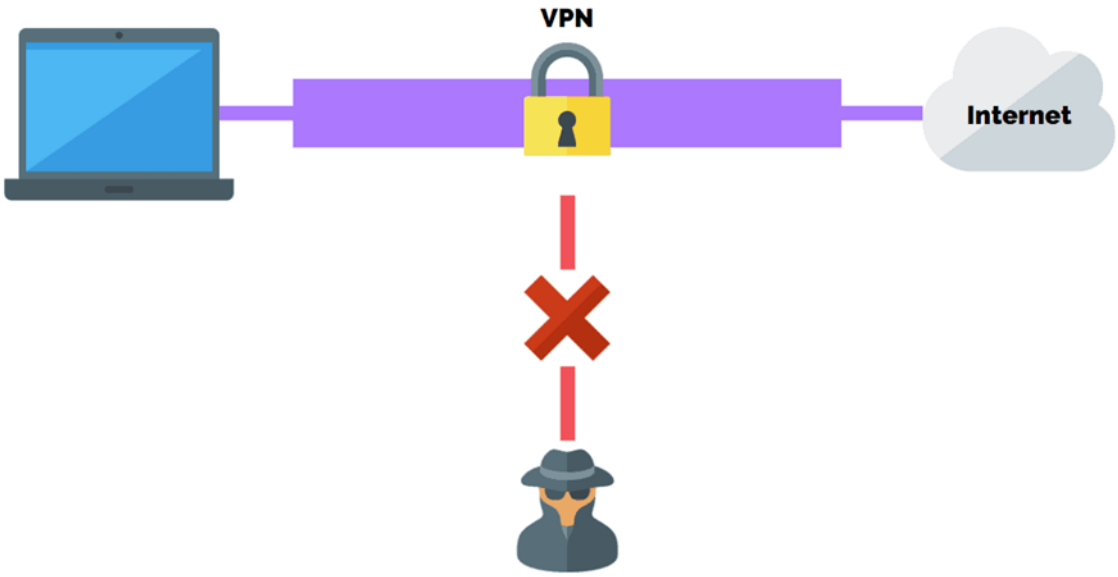
VPN

Virtuální privátní síť (viz Obrázek 6), často označovaná jako VPN, vytváří šifrované spojení přes internet mezi zařízením a sítí.

Toto šifrování zajišťuje bezpečný přenos citlivých dat a účinně brání neoprávněným osobám v zachycení nebo odposlouchávání síťového provozu. Sítě VPN jsou zvláště cenné pro usnadnění práce na dálku a zajištění soukromí a bezpečnosti dat.

VPN jsou důležité jak pro podniky, tak pro spotřebitele. Organizace často poskytují svým vzdáleným zaměstnancům standardní balíčky VPN, které jim umožňují připojit se ke kancelářské síti, jako by byli fyzicky přítomni v kanceláři. Toto připojení VPN vytvoří bezpečný tunel mezi klientem VPN a serverem VPN organizace, který účinně chrání citlivé informace před kybernetickými útočníky a neoprávněným přístupem (Swanagan, 2023).

Obrázek 6: VPN



Zdroj: (Swanagan, 2023)

4 Vlastní práce

4.1 Úvod do praktické části

Tato práce se zabývá problematikou segmentace sítě a bezpečnostních systémů ve firemním prostředí. Segmentace sítě je proces, který rozděluje síť na menší části, které jsou izolované od sebe pomocí firewallových pravidel. Tím se zvyšuje bezpečnost sítě, protože se snižuje riziko útoků a šíření malwaru mezi segmenty. Zároveň se zlepšuje výkon sítě, protože se redukuje množství provozu a kolizí na síťových zařízeních. Další výhodou segmentace sítě je snazší správa FW pravidel, protože se zjednodušuje jejich struktura a logika.

Cílem této práce je navrhnout a implementovat segmentaci sítě jako bezpečnostní systém, který splňuje požadavky nařízení NIS2 o kybernetické bezpečnosti. NIS2 je evropská směrnice, která stanovuje minimální úroveň kybernetické bezpečnosti pro poskytovatele esenciálních a digitálních služeb. V praktické části práce je popsána analýza současného stavu sítě, návrh segmentace sítě, implementace návrhu a testování funkčnosti a bezpečnosti řešení. V závěru práce jsou zhodnoceny dosažené výsledky a navrhnuty možná zlepšení pro budoucí rozvoj.

V následujících kapitolách se práce bude podrobněji věnovat jednotlivým úkolům, které byly stanoveny v rámci této práce. Tyto úkoly jsou: segmentace sítě, zvýšená bezpečnost, lepší výkon sítě, snazší správa firewallových pravidel a NIS2.

4.2 Analýza prostředí

Analýza prostředí byla provedena v prostředí firmy, která se zabývá výrobou a prodejem zdravotnických lůžek. Společnost má v České republice tři výrobní závody a kancelářské prostory v každém z nich. Celkem zaměstnává přes 2000 lidí, z toho cca 1500 pracuje na počítačích. Také využívá 112 tiskáren a 60 IoT zařízení pro monitorování a řízení výrobních procesů. Firma má dále 14 dceřiných společností v zahraničí.

Pro zajištění bezpečnosti a efektivity své činnosti společnost používá následující technologické řešení. Výroba je síťově oddělena od kancelářských prostor pomocí firewallů od společnosti Fortinet, které zabraňují neoprávněnému přístupu k citlivým datům a zařízením. Firma preferuje dodavatele Dell, který jí poskytuje notebooky, stolní počítače, switche i VXrail pro virtualizaci serverů. Původně byly počítače, IoT zařízení i WiFi ve stejném rozsahu IP adres jako servery (192.168.x.x), což způsobovalo problémy s přetížením sítě a kolizemi. Proto bylo potřeba implementovat segmentaci sítě.

4.3 Příprava implementace

V této části se práce bude věnovat přípravě pro implementaci tohoto bezpečnostního systému. Segmentace sítě je proces, který rozděluje síť na menší a logicky oddělené části, které se nazývají VLAN (Virtual Local Area Network). Tím se zvyšuje bezpečnost, výkon a efektivita sítě. Příprava pro implementaci segmentace sítě zahrnuje následující kroky:

4.3.1 Revize DHCP serveru

V rámci tohoto projektu bylo nezbytné provést podrobnou analýzu stávajícího stavu síťové infrastruktury se speciálním zaměřením na konfiguraci DHCP serveru. Tento server hraje klíčovou roli v síťovém prostředí tím, že zajišťuje dynamické přidělování IP adres zařízením připojeným k síti, a to umožňuje jejich snadnou správu a konektivitu. Během této analýzy byl objeven významný problém: značné množství IP adresních rezervací, které již neodpovídaly aktuálním potřebám a struktuře sítě.

V průběhu analýzy bylo zjištěno, že mnoho z těchto rezervací bylo zastaralých. Znamená to, že se vztahovaly k zařízením, která již nebyla součástí sítě, nebo byly přeřazeny do jiných segmentů. Kromě toho bylo identifikovány i duplicitní rezervace, kde jedna IP adresa byla přidělena více zařízením, což mohlo vést k potenciálním konfliktům a problémům s konektivitou. Dalším zjištěním bylo, že některé rezervace nebyly v souladu s danými plány na segmentaci sítě, tím došlo k neefektivnímu využití adresního prostoru a ke ztížení správy sítě.

Na základě těchto zjištění bylo nutné provést důkladnou revizi všech IP adresních rezervací na DHCP serveru. Cílem této revize bylo identifikovat a odstranit všechny nepotřebné, neplatné nebo konfliktní rezervace. Tento proces zahrnoval podrobnou kontrolu každé rezervace, s cílem zajistit, že všechny zachované rezervace budou odpovídat aktuálním a plánovaným potřebám sítě.

Tento krok se ukázal být klíčovým pro zajištění, že DHCP server bude schopen efektivně a bez problémů spravovat IP adresy v rámci nově segmentované sítě. Odstraněním zastaralých, duplicitních a nekonzistentních rezervací se zajistilo, že každé zařízení připojené k síti bude mít přidělenu správnou a unikátní IP adresu, což významně zvýšilo celkovou efektivitu a spolehlivost síťové infrastruktury.

4.3.2 Předělání rezervací na FQDN rezervace

Při přípravě na segmentaci této sítě bylo zásadním krokem přehodnocení a úprava strategie rezervace IP adres pro zařízení. Původní nastavení se spoléhalo na server DHCP (Dynamic Host Configuration Protocol), který přiděloval IP adresy na základě adres MAC

(Media Access Control) zařízení. Tento přístup byl sice funkční, ale byl zranitelný vůči bezpečnostním problémům, jako je například podvržení adresy MAC, kdy se útočník mohl vydávat za zařízení v síti a získat tak IP adresu neoprávněně. Navíc se tato metoda ukázala jako těžkopádná pro správu a organizaci IP adres v rámci konkrétních segmentů sítě, tím je toto pro plánovanou implementaci nezbytné.

Aby se tyto problémy vyřešily a zvýšila se bezpečnost i flexibilita, přešlo se na systém rezervování IP adres prostřednictvím plně kvalifikovaných doménových jmen. FQDN jednoznačně identifikuje zařízení v síti pomocí kombinace názvu hostitele a názvu domény. To nabízí bezpečnější přístup a lepší správu přidělování IP adres. Tato metoda zahrnuje přidělování IP adres serverem DHCP na základě názvů FQDN zařízení, které jsou ověřovány serverem DNS (Domain Name System). Tento proces ověřování zajišťuje, že IP adresy jsou přidělovány pouze ověřeným zařízením, čímž se účinně snižuje riziko zneužití IP adres prostřednictvím podvržení.

Přijetí FQDN pro rezervaci IP adres má několik klíčových výhod. Významně posiluje bezpečnost sítě zajišťováním toho, že IP adresy nelze získat podvodným způsobem. Také zjednodušuje správu IP adres. Protože je každému zařízení přiřazen jedinečný FQDN, mohou správci snadno změnit síťový segment zařízení aktualizací jeho záznamu DNS, aniž by museli měnit konfiguraci serveru DHCP. Tato úroveň flexibility je klíčová pro dynamické sítě, které vyžadují časté úpravy kvůli změnám rolí zařízení, umístění nebo zásad zabezpečení.

Tento přechod na rezervaci IP na základě FQDN je v souladu s širšími cíli segmentace sítě, což zvyšuje jak bezpečnost, tak i správu síťové infrastruktury. Zajištěním bezpečnějšího způsobu přidělování IP a usnadněním správy síťových segmentů je pokládán pevný základ pro robustnější a flexibilnější síťové prostředí. Tento přístup nejenže řeší bezprostřední problémy související se zabezpečením a segmentací, ale také nám umožňuje efektivněji spravovat a škálovat danou síť tak, aby splňovala budoucí požadavky.

4.3.3 Statické IP adresy v LAN

Jednou z hlavních překážek, které bylo potřeba překonat, bylo zjištění a úprava statických IP adres, které byly nastavené na některých zařízeních. Statické IP adresy jsou pevně přiřazené zařízením a nejsou ovlivněny změnami v konfiguraci sítě. Pokud by byl změněn rozsah IP adres pro segmentaci sítě, zařízení se statickými IP adresami by zůstala v původním rozsahu a nebyla by schopna komunikovat se zbytkem sítě. Proto bylo potřeba provést důkladnou analýzu sítě a identifikovat všechna zařízení se statickými IP adresami. V následujícím kroku se muselo převést co nejvíce zařízení na dynamické IP adresy, které jsou

automaticky přidělovány serverem DHCP podle aktuálního rozsahu. Tím se zajistilo, že zařízení budou schopna adaptovat se na změny v síti. Některá zařízení však vyžadovala statické IP adresy z důvodu bezpečnosti nebo specifických funkcí. Tato zařízení byla pečlivě zapsána a zaevidována, aby se mohly po změně rozsahu IP adres správně nakonfigurovat. Pro tato zařízení byly vytvořeny rezervace v serveru DHCP, který jim přiřadil nové statické IP adresy v novém rozsahu. Poté bylo nutné ručně změnit statické IP adresy na těchto zařízeních a ověřit jejich funkčnost. Tímto způsobem bylo vyhnuto možným problémům s kompatibilitou a dostupností zařízení se statickými IP adresami při segmentaci sítě.

4.3.4 Příprava nového DHCP serveru

Přechod ze zastaralé konfigurace serveru DHCP založené na systému Windows Server 2008 na modernější infrastrukturu využívající systém Windows Server 2022 byl strategickým krokem, jehož cílem bylo zvýšit výkon, zabezpečení a celkové schopnosti sítě. Vzhledem k tomu, že se vědělo o omezení a zranitelnosti spojené s nepodporovaným systémem Windows Server 2008, bylo rozhodnutí o upgradu klíčové. Systém Windows Server 2022, který je novější verzí, přináší pokročilé funkce, vylepšená bezpečnostní opatření a lepší výkonnostní ukazatele, což je v souladu s danými cíli pro robustní a efektivní síťovou infrastrukturu.

V procesu zřizování nového serveru DHCP byla provedena důkladná kontrola a audit stávajících rezervací IP adres na starém serveru. Tato kritická revize umožnila identifikovat a odstranit všechny rezervace, které byly zastaralé nebo již nebyly nutné. Vymazáním těchto zastaralých rezervací jsme nejen zefektivnili správu serveru DHCP, ale také uvolnili cenné IP adresy pro budoucí přidělování, čímž byly optimalizovány síťové zdroje.

Konfigurace nového serveru DHCP byla navíc pečlivě sladěna s danou strategií. Tím, že byl pro každý segment sítě navrhnut samostatný rozsah IP adres, které mohl server DHCP přidělovat, bylo dosaženo vyšší úrovně organizace a kontroly nad komunikací ve firemní síti. Tato segmentace usnadňuje řízení provozu a efektivnější využívání síťových zdrojů tím, že umožňuje přesnou kontrolu a přidělování IP adres v rámci segmentované síťové architektury.

Při této modernizaci a rekonfiguraci nešlo pouze o výměnu starého hardwaru nebo softwaru, ale o strategické úsilí, které mělo zajistit, aby tato síťová infrastruktura splňovala současné i budoucí požadavky. Přechod na systém Windows Server 2022 pro tuto infrastrukturu serverů DHCP je příkladem našeho odhodlání využívat pokročilá technologická řešení ke zvýšení výkonu, zabezpečení a možností správy sítě, čímž jsme vytvořili pevný základ pro další rozvoj a optimalizaci síťového prostředí.

4.3.5 Optimalizace firewallových pravidel

Jedním z dalších kroků při implementaci segmentace sítě je aktualizace firewallových pravidel. Firewall je zařízení, které kontroluje a filtruje síťový provoz podle definovaných kritérií. Pokud se změní struktura sítě, například rozdělením na menší subnety, je nutné zajistit, aby firewall odpovídal nové situaci. To znamená, že je třeba projít stará firewallová pravidla a zkontrolovat, zda jsou stále platná, nebo zda je potřeba je upravit nebo smazat. Také je třeba vytvořit nová pravidla pro nové subnety, aby bylo možné povolit nebo zakázat komunikaci mezi nimi a s ostatními částmi sítě. Tím se zvýší bezpečnost sítě a zabrání se nežádoucím únikům dat nebo útokům. Například pro LAN, kterou primárně využívají zaměstnanci v kancelářích byly zablokovány webové stránky s obsahem pro dospělé, či volné stahování .EXE souborů. Pro IoT zase bylo možné omezit přístup pouze na stránky pro updaty zařízení.

4.3.6 Vytvoření nových VLAN

Segmentace sítě je proces rozdělení na menší, logicky oddělené části, které se nazývají podsíť nebo VLAN.

Podsíť je část sítě, která má společnou síťovou adresu a masku. Umožňuje rozlišit mezi síťovou a hostitelskou částí adresy. Také definuje rozsah adres, které jsou v dané části sítě k dispozici.

VLAN je virtuální podsíť, která je vytvořena pomocí softwaru nebo hardwaru. Umožňuje seskupovat porty přepínače nebo zařízení do logických skupin bez ohledu na jejich fyzické umístění. Také používá značky (tagy) k identifikaci paketů, aby je mohl poslat tam, kam patří. Může být propojena s jinými podsítěmi pomocí trunkových linek a protokolů, jako je IEEE 802.1Q.

Při vytváření je třeba zvážit následující faktory:

- Počet a typy zařízení, která mají být součástí
- Požadavky na propustnost a prioritu pro různé typy provozu
- Požadavky na zabezpečení a soukromí pro různé typy dat
- Požadavky na správu a monitorování
- Požadavky na škálovatelnost a flexibilitu

Také je obvyklé použít následující kritéria pro seskupování zařízení:

- Funkce: Zařízení se stejnou funkcí nebo rolí jsou seskupena do jedné. Například servery, tiskárny, počítače, IoT atd.

- Geografie: Vybavení nacházející se ve stejné fyzické lokalitě jsou seskupena do jedné. Například v tomto případě jsou to zahraniční dceřiné společnosti nebo rozdělení závodů po ČR.
- Aplikace: Seskupit se dají také podle aplikace, kterou používají. Například VoIP.

4.3.7 Domluva výpadku LAN a serverů

Implementace segmentace sítě vyžaduje pečlivou přípravu a koordinaci se všemi zainteresovanými stranami, protože zahrnuje změny v konfiguraci zařízení a propojení sítě. Jedním z hlavních aspektů plánování implementace segmentace sítě je stanovení termínu, kdy bude provedena. Tento termín musí být dohodnut s vedením firmy, IT oddělením, provozními manažery a dalšími uživateli sítě, kteří by mohli být ovlivněni výpadkem internetu. Výpadek internetu je nevyhnutelným důsledkem implementace segmentace sítě, protože je nutné odpojit a znovu zapojit některé síťové prvky, jako jsou směrovače, přepínače, firewally a další. Délka výpadku závisí na složitosti a rozsahu segmentace sítě, ale obvykle se pohybuje od několika minut do několika hodin.

Výpadek internetu může mít negativní dopad na některé činnosti firmy, jako je například výrobní proces, komunikace se zákazníky nebo dodavateli, přístup ke cloudovým službám nebo interním aplikacím a tak dále. Proto je důležité si domluvit termín implementace segmentace sítě tak, aby se minimalizovaly tyto negativní dopady. Ideální termín by měl být v době, kdy je nejnižší provoz na síti, například o víkendech nebo v noci. Také je vhodné si vyhradit dostatečnou časovou rezervu pro případné komplikace nebo neočekávané problémy. Dále je nutné informovat všechny uživatele sítě o plánovaném výpadku internetu s dostatečným předstihem a poskytnout jim alternativní způsoby komunikace nebo práce během výpadku.

4.4 Implementace

Cílem implementace je systematické rozdělení sítě na rozeznatelné logické segmenty s vyhrazeným prostorem pro servery, respektive klienty a další jiné zařízení v síti. K dosažení tohoto cíle byla použita důmyslná kombinace virtuálních počítačů VMware a brány firewall FortiGate, čímž vzniklo integrované řešení pro efektivní správu sítě.

4.4.1 Úprava DHCP lease time

Prvním krokem byla strategická úprava DHCP lease time. Minimalizací doby trvání „pronájmu“ na minimální hodnotu byla snaha preventivně zmírnit případné konflikty IP adres

při přechodu mezi sítěmi VLAN. Toto preventivní opatření položilo pevný základ pro následné změny VLAN a podpořilo hladký proces restrukturalizace sítě.

Proaktivní řešení DHCP lease time je zásadní pro předcházení konfliktům, které mohou vzniknout při přechodu mezi sítěmi VLAN. Díky minimalizaci doby platnosti je síť lépe připravena na bezproblémové změny, a to zajišťuje efektivní komunikaci a přidělování prostředků.

4.4.2 Odpojení síťového adaptéru na VMs

Následně byly v rámci migrace virtuálních počítačů do nové VLAN systematicky odpojeny všechny přidružené síťové adaptéry. Cílem tohoto záměrného odpojení bylo vytvořit čistý štít pro nadcházející konfigurační kroky, a snížit tak pravděpodobnost rušení během procesu implementace VLAN.

Pečlivé odpojení síťových adaptérů slouží jako strategický manévr, který poskytuje kontrolované prostředí pro následné konfigurační kroky. Tento krok minimalizuje potenciální narušení, což přispívá k zefektivnění a zefektivnění procesu migrace VLAN.

4.4.3 Konfigurace brány firewall FortiGate

Klíčovým aspektem implementace bylo vytvoření nového rozhraní na bráně firewall FortiGate vyhrazeného pro serverovou VLAN. To vyžadovalo konfiguraci, včetně nastavení IP adresy v dohodnutém rozsahu. Kromě toho byla upravena pravidla brány firewall, aby byla umožněna bezproblémová komunikace mezi nově vytvořenou VLAN a širší internetovou infrastrukturou.

Konfigurace brány firewall FortiGate hraje ústřední roli při zajištění úspěšné implementace VLAN. Vytvoření vyhrazeného rozhraní pro serverovou VLAN spolu s přesným přiřazením IP adres a úpravami pravidel vytváří bezpečný a efektivní komunikační rámec mezi VLAN a internetem.

4.4.4 Transformace rozhraní LAN

V rámci dalšího rozšíření segmentace sítě byly provedeny úpravy stávajícího rozhraní LAN brány firewall FortiGate. IP adresa byla změněna na jinou, pečlivě vybranou z vyjednaného rozsahu. Toto rozhraní bylo následně přejmenováno na klientské rozhraní, čímž byla upevněna jeho vyhrazená role v rámci segmentované síťové architektury.

Transformace rozhraní LAN na bráně firewall FortiGate posiluje celkovou strategii segmentace sítě. Přiřazením samostatné IP adresy a jejím přejmenováním na klientské rozhraní

se posílí přehlednost a organizace, což přispívá k optimalizovanému a dobře strukturovanému síťovému prostředí.

4.4.5 Přeskupení virtual machines

Dále bylo v prostředí VMware provedeno pečlivé přeskupení virtuálních strojů. Každý virtuální počítač byl strategicky přepnut na odpovídající rozhraní brány firewall na základě své určené příslušnosti k síti VLAN. Následně se všechny virtuální počítače bez problémů znovu připojily k síti a byl proveden komplexní proces ověření, čímž se zajistila jejich optimální funkčnost v nově vytvořeném rámci VLAN.

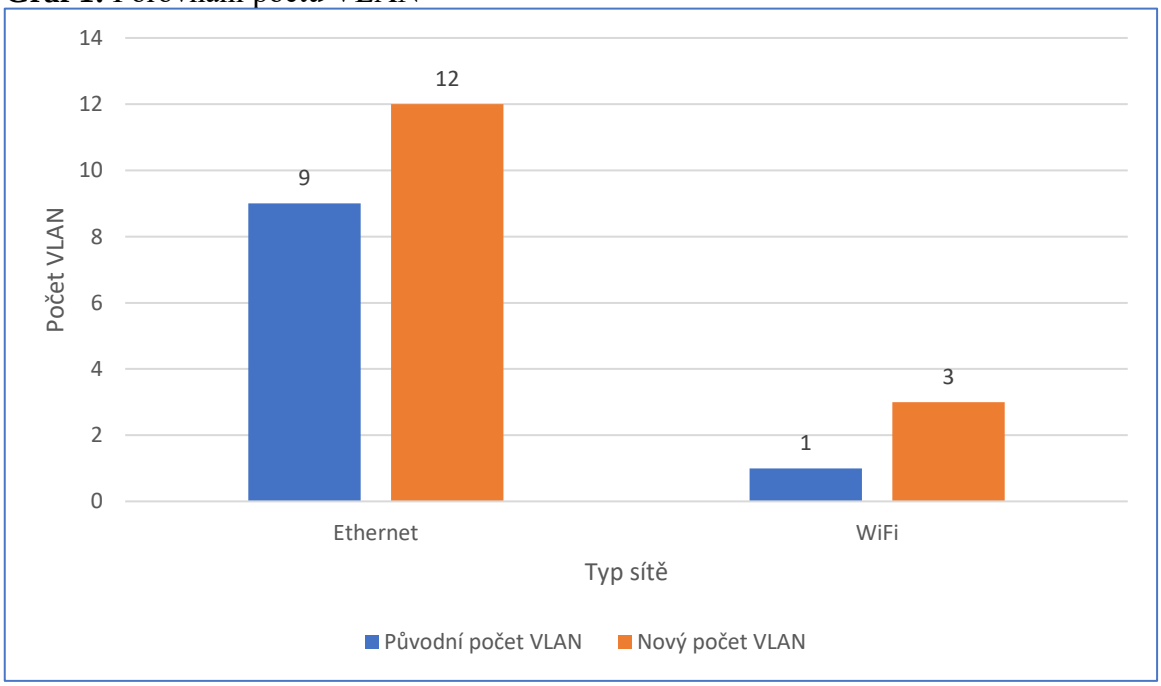
Proces přeřazení virtuálních strojů v prostředí VMware je kritickou fází implementace VLAN. Strategické přepínání a pečlivá příslušnost k určeným rozhraním brány firewall FortiGate zajišťují soudržnou a organizovanou strukturu sítě. Následný proces ověřování zaručuje bezproblémovou funkčnost virtuálních počítačů v rámci rekonfigurované sítě VLAN.

Tento komplexní přístup k segmentaci sítě nejen podtrhuje související technickou zdatnost, ale také zdůrazňuje strategické plánování a pečlivé provedení, které jsou nezbytné pro dosažení efektivní a bezpečné síťové architektury.

5 Výsledky a diskuse

Zde jsou shrnuty výsledky této bakalářské práce, která se zabývala implementací segmentace sítě v jedné velké firmě. Cílem segmentace bylo zvýšit výkon, bezpečnost a správu sítě. Tato implementace proběhla úspěšně a bez větších problémů. Pouze bylo nutno řešit otázku počítačů se statickou IP adresou, které jsou potřebné pro některé aplikace. S tímto problémem se ovšem počítalo. Dále bylo provedeno rozdělení sítě na několik logických segmentů viz Graf 1 podle funkce a typu zařízení. Například, z jedné VLAN pro kanceláře se vytvořily čtyři VLANy: jedna pro LAN, druhá pro servery, třetí pro IoT a čtvrtá pro pevné linky. Podobně se rozdělila i Wifi síť na tři segmenty: jedna pro doménové zařízení, druhá pro nedoménové zařízení a třetí pro IoT. Tímto bylo dosaženo větší bezpečnosti v dané síti, protože byla omezena komunikace mezi různými segmenty a zavedla se striktní pravidla firewallu. Zároveň se zlepšil výkon sítě, protože byla snížena broadcastová doména a zredukovaly se kolize a rušení. Na závěr může být konstatováno, že tato implementace segmentace sítě byla úspěšná a přinesla řadu výhod.

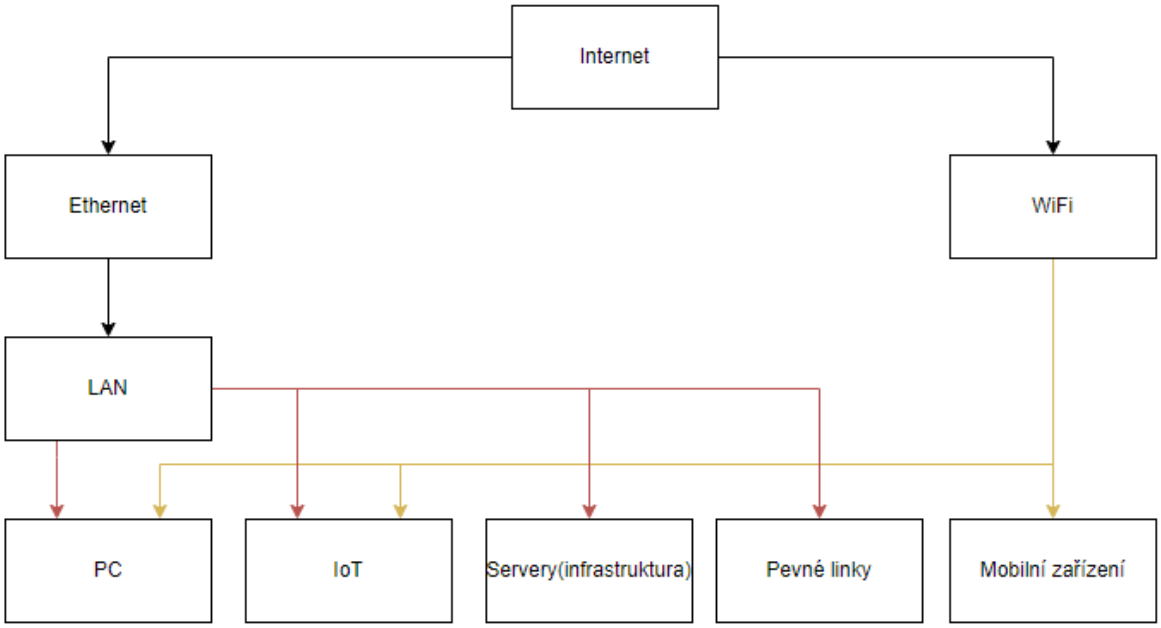
Graf 1: Porovnání počtu VLAN



Zdroj: Vlastní zpracování

Zde je na diagramu (viz Obrázek 7) zobrazena původní struktura sítě před provedením segmentace. Je patrné, že v rámci LAN (vyznačené červenou barvou) byly připojeny počítače, IoT zařízení, servery i pevné linky. V kontrastu s tím byla na WiFi (označené žlutou barvou) vytvořena pouze jedna síť, ke které se připojovaly všechny typy zařízení.

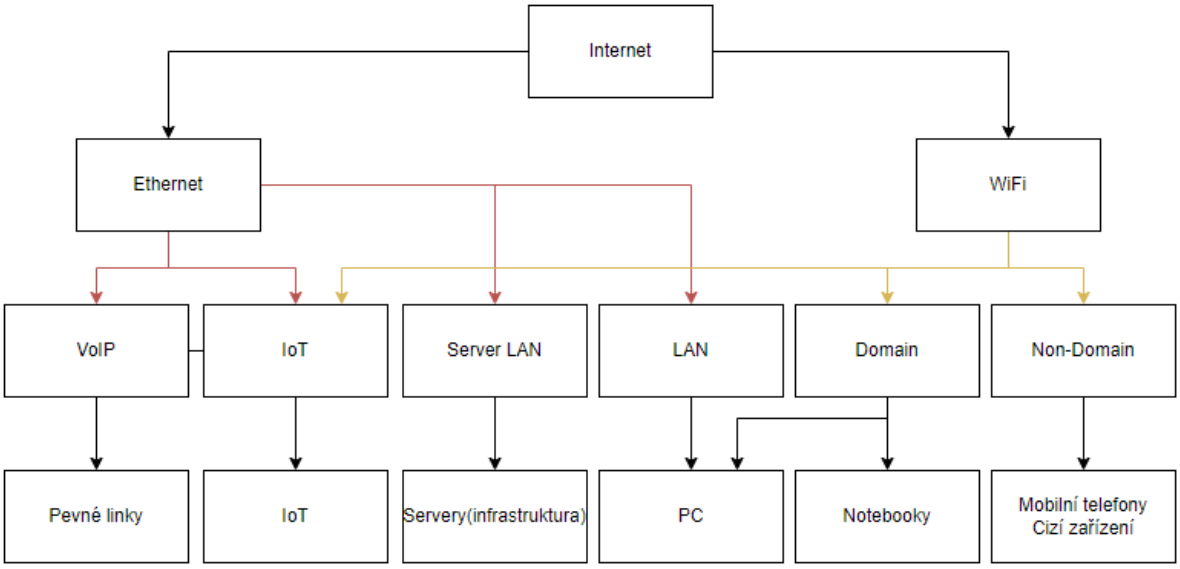
Obrázek 7: Schéma původní struktury sítě



Zdroj: Vlastní zpracování

Byla vytvořena nová struktura sítě po implementaci tohoto bezpečnostního systému. Na diagramu (viz Obrázek 8) je zřetelné, že v LAN síti (označené červenou barvou) došlo k vytvoření dalších podsítí pro LAN, IoT, servery a pevné linky. Dále je na diagramu vidět, že WiFi síť (označená žlutou barvou) byla rozdělena na tři podsítě: jednu pro IoT zařízení, druhou pro doménová zařízení a třetí pro nedoménová zařízení. Tato reorganizace sítě přináší lepší přehlednost, zvýšení bezpečnosti a efektivnější správu jednotlivých segmentů.

Obrázek 8: Schéma nové struktury sítě



Zdroj: Vlastní zpracování

6 Závěr

V závěru této bakalářské práce je provedena syntéza klíčových zjištění a výsledků z teoretické i praktické oblasti, která poskytuje ucelený přehled o přínosu studie. Teoretická část se zabývala složitostí monitorování sítí, zahrnující jeho význam, cíle, metody a nástroje. V praktické oblasti byla pečlivě navržena a provedena implementace segmentace sítě v konkrétní společnosti, jejímž cílem bylo zvýšit bezpečnost, výkonnost a stabilitu sítě.

Zkoumání monitorování sítě v teoretické části nejen objasnilo jeho mnohostrannou povahu, ale také zdůraznilo jeho klíčovou roli. Proniknutí do významu a cílů monitorování sítí spolu s rozsáhlou diskusí o různých metodách a nástrojích položilo pevný základ pro pochopení teoretických základů tohoto oboru.

Praktický aspekt této práce, soustředěný na návrh a implementaci segmentace sítě, představuje konkrétní aplikaci teoretických poznatků. Obsáhlé podrobné popsání postupu implementace nabízí cenné poznatky o provozních aspektech segmentace sítě.

Tento praktický počin, který se konkrétně zabývá otázkami bezpečnosti, výkonnosti a stability v reálném organizačním kontextu, přispívá k rozšíření znalostí o síťových technologiích.

Práce jako celek slouží jako významný doplněk o monitorování a segmentaci sítí. Její dvojí zkoumání teoretických konceptů a praktické implementace nejenže rozšiřuje naše chápání dané problematiky, ale také poskytuje diferencovaný pohled na průnik teorie a aplikace. Díky tomu může tato práce sloužit jako zdroj inspirace pro budoucí výzkumné snahy a praktické aplikace ve stále se vyvíjející oblasti síťových technologií. Poznatky získané z této práce přispívají nejen k akademickému snažení, ale mají také praktické důsledky a mohou být zdrojem informací o osvědčených postupech a strategiích v dynamickém prostředí správy sítí a kybernetické bezpečnosti.

7 Seznam použitých zdrojů

Aalbers, Rick a Dolfsma, Wilfred. 2015. *Innovation networks: managing the networked organization.* Abingdon : Routledge, 2015.
Adams, Niall a Heard, Nicholas. 2014. *Data analysis for network cyber-security.* London : Imperial College Press, 2014.
Edwards, James a Bramante, Richard. 2009. *Networking Self-Teaching Guide : OSI, TCP/IP, LANs, MANs, WANs, Implementation, Management, and Maintenance.* místo neznámé : John Wiley & Sons, Incorporated, 2009. ISBN: 9780470402382.
Keary, Tim. 2023. The Best Network Monitoring Tools of 2023. *comparitech.* [Online] 12. 10 2023. [Citace: 26. 10 2023.] https://www.comparitech.com/net-admin/network-monitoring-tools/.
Kinza, Yasar a Gillis, Alexander. 2023. TechTarget Networking. *TechTarget.* [Online] March 2023. [Citace: 28. Září 2023.] https://www.techtarget.com/searchnetworking/definition/network.
Kurose, James a Ross, Keith. 2014. *Počítačové sítě.* Brno : Computer Press, 2014.
Liefting, Nathan a Baekel, Brian Van. 2022. *Zabbix 6 IT Infrastructure Monitoring Cookbook: Explore the new features of Zabbix 6 for designing, building, and maintaining your Zabbix setup, 2nd Edition - Softcover.* místo neznámé : Packt Publishing, 2022. ISBN 9781803246918.
Ludvík, Miroslav a Štědroň, Bohumír. 2008. *Teorie bezpečnosti počítačových sítí.* Kralice na Hané : Computer Media, 2008.
Mareš, Petr. 2022. *Kyberkultura, hackeři a digitální revoluce: informace chce být svobodná.* Praha : Grada, 2022.
Mauro, Douglas a Schmidt, Kevin. 2001. *Essential SNMP.* [překl.] Autor. Sebastopol : O'Reilly, 2001. 0-596-00020-0.
Peterka, Jiří. 1995. Internet. *Computerworld.* 1995, 4/95.
Prabhu, Ruth Dsouza. 2021. What Is Network Security? Definition, Types, and Best Practices. *Spiceworks.* [Online] 24. 8 2021. [Citace: 23. 10 2023.] https://www.spiceworks.com/it-security/network-security/articles/what-is-network-security/.
Swanagan, Michael. 2023. What is network security? *Purplesec.* [Online] Jason Firch, 7. 2 2023. [Citace: 28. 10 2023.] https://purplesec.us/network-security-types/.
Trulove, James. 2009. *Sítě LAN: hardware, instalace a zapojení.* Praha : Grada, 2009.
Wilson, Ed. 2000. *Network monitoring and analysis : a protocol approach to troubleshooting.* New Jersey : Prentice Hall, 2000.

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

Obrázek 1: Vrstvy TCP/IP protokolu 16
Obrázek 2: Nagios Core 20
Obrázek 3: Zabbix 22
Obrázek 4: SolarWinds Network Performance Monitor 23
Obrázek 5: PRTG Network Monitor 25
Obrázek 6: VPN 36
Obrázek 7: Schéma původní struktury sítě 46
Obrázek 8: Schéma nové struktury sítě 47

8.2 Seznam tabulek

Tabulka 1: Srovnání relativních cen mezinárodních pevných okruhů v roce 1994 14

8.3 Seznam grafů

Graf 1: Porovnání počtu VLAN 45

8.4 Seznam použitých zkratek

LAN – Local area network

VLAN – Virtual local area network

VM – Virtual machine

FW – Firewall

IoT – Internet of things

DHCP – Dynamic Host Configuration Protocol

MAC adresa – Media Access Control adresa

FQDN – Fully Qualified Domain Name