Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Návrh zabezpečení počítačové sítě ve vybrané škole

Vojtěch Mňuk

Bakalářská práce
2024

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Vojtěch Mňuk**
Osobní číslo:	**E21587**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Návrh zabezpečení počítačové sítě ve vybrané škole.**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je navrhnout možnosti zabezpečení počítačové sítě ve vybrané škole. V práci bude provedena analýza současného stavu s cílem navrhnout případné změny pro bezpečné prostředí provozu používaných informačních systémů.

Osnova:
- Problematika bezpečnosti v této oblasti.
- Analýza současného stavu ve vybrané škole.
- Návrh na zlepšení zabezpečení počítačové sítě.

Rozsah pracovní zprávy: **cca 35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

BUREŠ, Miroslav, Miroslav RENDA, Michal DOLEŽEL, Peter SVOBODA, Zdeněk GRÖSSL, Martin KOMÁREK, Ondřej MACEK a Radoslav MLYNÁŘ. Efektivní testování softwaru: klíčové otázky pro efektivitu testovacího procesu. Praha: Grada, 2016. Profesionál. ISBN 978-80-247-5594-6.
KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80--88168-31-7.
PETROVIČ, Michal a Michal KOSTĚNEC. Bezpečnost počítačových sítí. Plzeň: Západočeská univerzita v Plzni, 2012. ISBN 978-80-261-0117-8.
STALLINGS, William. Network security essentials: applications and standards. Sixth edition. Hoboken: Pearson education, [2017]. ISBN 978-0134527338

Vedoucí bakalářské práce: **Ing. Hana Jonášová, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2023**
Termín odevzdání bakalářské práce: **30. dubna 2024**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

Ing. et Ing. Martin Lněnička, PhD. v.r.
garant studijního programu

V Pardubicích dne 1. září 2023

PROHLÁŠENÍ

Prohlašuji:

Práci s názvem Návrh zabezpečení počítačové sítě ve vybrané škole jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 29. 7. 2024

Vojtěch Mňuk v. r.

PODĚKOVÁNÍ:

Moc děkuji své vedoucí práce Ing. Haně Jonášová, Ph.D. za vedení mé bakalářské práce, cenné připomínky, rady a v neposlední řadě i za její ochotu.

Další poděkování patří správci sítě na vybrané škole za poskytnutí informací potřebných pro vypracování bakalářské práce.

Nesmím také opomenout poděkovat své rodině za jejich podporu.

ANOTACE

Tato bakalářská práce se zabývá návrhem zabezpečení počítačové sítě ve vybrané škole. Hlavním cílem práce je analyzovat aktuální stav počítačové sítě, identifikovat potenciální bezpečnostní rizika a navrhnout efektivní opatření k jejich minimalizaci. Práce se zaměřuje na teoretické základy počítačové sítě, typy útoků a hrozeb pro počítačovou síť a bezpečnost počítačové sítě. Dále práce zahrnuje analýzu současného stavu počítačové sítě ve vybrané škole a na základě tohoto popisu jsou identifikována hlavní bezpečnostní rizika, pro která jsou navržena konkrétní opatření k jejich odstranění.

KLÍČOVÁ SLOVA

počítačová síť, bezpečnost sítě, ochrana dat, firewall, škola, rizika

TITLE

Computer network security design for a selected school

ANNOTATION

This bachelor's thesis deals with the design of computer network security in the chosen school. The main objective of the work is to analyze the current state of the computer network, identify potential security risks and propose effective measures to minimize them. The work focuses on the theoretical foundations of computer network, types of attacks and threats to computer network and computer network security. Furthermore, the work involves analyzing the current state of the computer network in the chosen school and, on the basis of this description, identifying the main security risks for which specific measures are proposed to eliminate them.

KEYWORDS

computer network, network security, data protection, firewall, school, risks

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

AD DS	Active Directory Domain System
AES	Symetrický šifrovací algoritmus
AP	Přístupový bod
DoS	Denial of Service
Gbps	Gigabit za sekundu
GDPR	Obecné nařízení o ochraně osobních údajů
ICT	Informační a komunikační technologie
ISP	Internet service provider
LR	Longe-range
EMI	Elektromagnetické rušení
LAN	Lokální síť
Mbps	Megabit za sekundu
NAS	Datové úložiště na síti
PoE	Power over Ethernet
PSK	Předem sdílený klíč
RFI	Vysokofrekvenční rušení
SSID	Service Set Identifier
UPS	Záložní napájecí zdroj
VLAN	Virtuální lokální síť
VPN	Virtuální privátní síť
WLAN	Bezdrátová síť
WPA2	Wi-Fi Protected Access 2

Úvod

Školní počítačová síť je komplexní systém propojených počítačů a dalších zařízení, který umožňuje efektivní komunikaci a sdílení zdrojů mezi studenty, učiteli a administrativou. Tato síť je klíčovým nástrojem pro moderní vzdělávání, protože poskytuje přístup k digitálním výukovým materiálům, online kurzům a platformu pro spolupráci.

Hlavním cílem školní počítačové sítě je podpora vzdělávacího procesu prostřednictvím integrace technologií do výuky. To zahrnuje zajištění přístupu k internetu, sdílení vzdělávacích materiálů a umožnění komunikace a spolupráce v rámci školní komunity. Jejím přínosem pro školy je zlepšení efektivity výuky, podpora individuálního přístupu k učení a usnadnění administrativních procesů. Dále umožňuje přístup k informacím a zdrojům z celého světa a usnadňuje komunikaci mezi studenty, učiteli a administrativou, která zlepšuje spolupráci a koordinaci.

Hlavním úkolem bezpečnosti školní počítačové sítě je zajistit, aby citlivé informace, jako jsou osobní údaje studentů a zaměstnanců, zůstaly chráněny, a aby síť byla bezpečná a funkční pro všechny uživatele.

Cílem práce je navrhnout možnosti zabezpečení počítačové sítě ve vybrané škole. V práci bude provedena analýza současného stavu s cílem navrhnout případné změny pro bezpečné prostředí provozu používaných informačních systémů.

1 POČÍTAČOVÁ SÍŤ

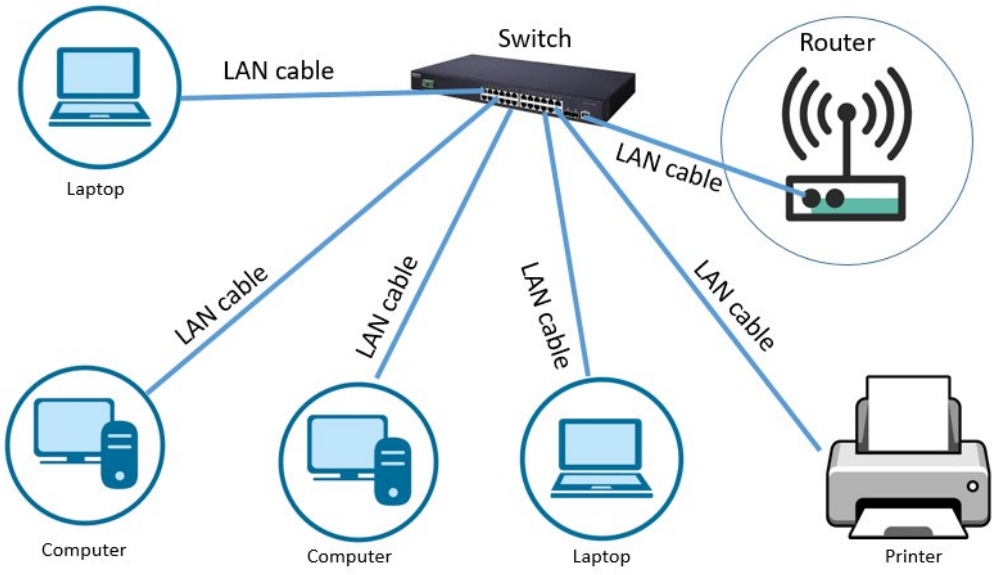
Počítačová síť je složitý systém propojující různé technologie, zařízení a protokoly, který umožňuje efektivní a rychlou komunikaci a sdílení zdrojů mezi uživateli a zařízeními v různých prostředích. Využívají se v mnoha různých prostředích, včetně domácností, kanceláří, škol, univerzit, nemocnic a dalších organizací. [11]

Podsíť (subnet) je částí větší počítačové sítě, která je logicky oddělena pomocí masky podsítě (subnet mask). Subnet je využíván ke snížení kolizní domény a ke správě adresního prostoru. Díky subnetování lze velkou síť rozdělit na menší a lépe ovladatelné části. To umožňuje efektivní správu IP adres, zlepšuje výkon, bezpečnost sítě a také ulehčuje implementaci různých síťových protokolů a technologií. [11][26]

Typy sítí

Počítačové sítě lze rozdělit do několika kategorií podle jejich rozsahu a způsobu propojení. Každý typ sítě má své specifické výhody a nevýhody a je vhodný pro různé typy prostředí. Nejčastěji používané typy sítě ve školách jsou lokální síť, bezdrátová síť a virtuální lokální síť. [12][13]

Lokální síť (Local Area Network) je počítačová síť, která pokrývá malé geografické území, například domácnost, kancelář nebo skupinu budov. Umožňuje zařízením, jako jsou počítače, tiskárny a servery, komunikaci a sdílení zdrojů. Tato zařízení jsou připojena pomocí LAN kabelu (ethernetového nebo optického kabelu) do jednoho switche (viz Obrázek 1). [12][13]



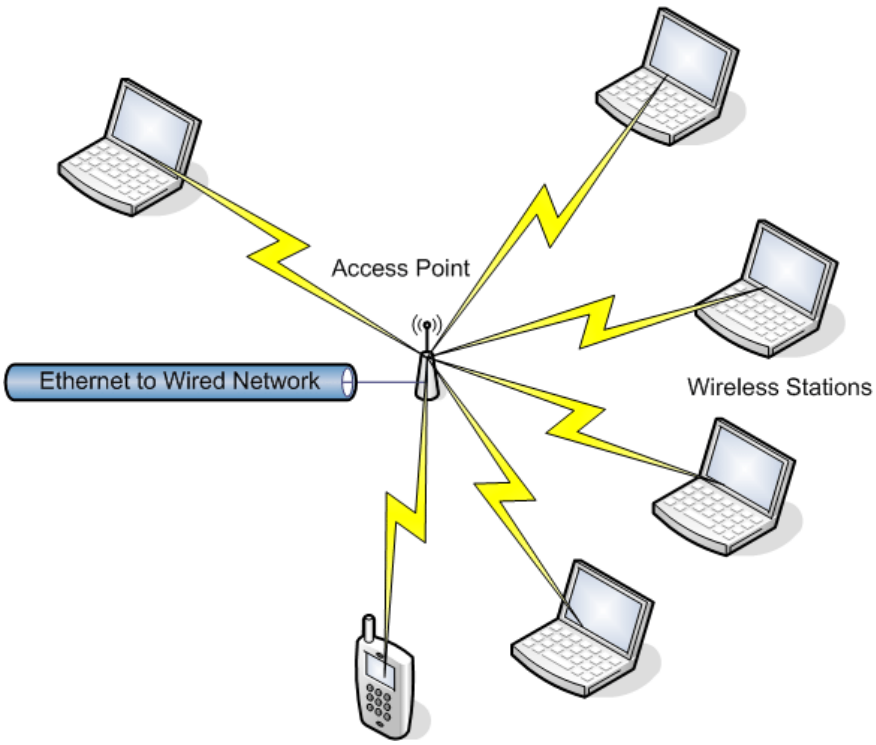
Obrázek 1: Lokální síť

Zdroj:[7]

Hlavní výhodou lokální sítě je přenosová rychlost, která se pohybuje od 100 Mbps do 1 Gbps a v některých případech i vyšší. To umožňuje rychlou a efektivní komunikaci mezi zařízeními. Další výhodou lokální sítě je jejich schopnost sdílet zdroje. Uživatelé mohou sdílet hardware, jako jsou tiskárny a skenery, a také software a data. To snižuje náklady na vybavení a zjednodušuje správu a údržbu. Také poskytuje vysokou úroveň zabezpečení, protože přístup k síti lze kontrolovat a monitorovat, což je obzvlášť důležité v podnikových prostředích. [12][13]

Nicméně, existují i nevýhody spojené s lokální sítí. Je navržena pro malé geografické oblasti a její dosah je omezen na několik stovek metrů. Pro větší vzdálenosti je nutné použít další zařízení, jako jsou switche a routery, které mohou zvyšovat složitost a náklady na instalaci a údržbu sítě. Další nevýhodou je potenciální přetížení sítě. Pokud je do LAN sítě připojeno příliš mnoho zařízení nebo pokud je přenášeno velké množství dat, může docházet k přetížení a zpomalení sítě. [12][13]

Bezdrátová síť (Wireless Local Area Network) je počítačová síť, která umožňuje zařízení připojit se k síti bez použití kabelů. Je založena na technologii rádiového přenosu a je využívána především v domácnostech, kancelářích, veřejných prostorech nebo na místech, kde je obtížné instalovat kabeláž, jako například historické budovy a dočasné instalace. Typickými zařízeními, která se připojují k WLAN, jsou notebooky, chytré telefony, tablety a další zařízení s podporou Wi-Fi. Hlavním prvkem této sítě je přístupový bod (Access Point), který zajišťuje spojení mezi bezdrátovými zařízeními a kabelovou sítí (viz Obrázek 2). [12][13]



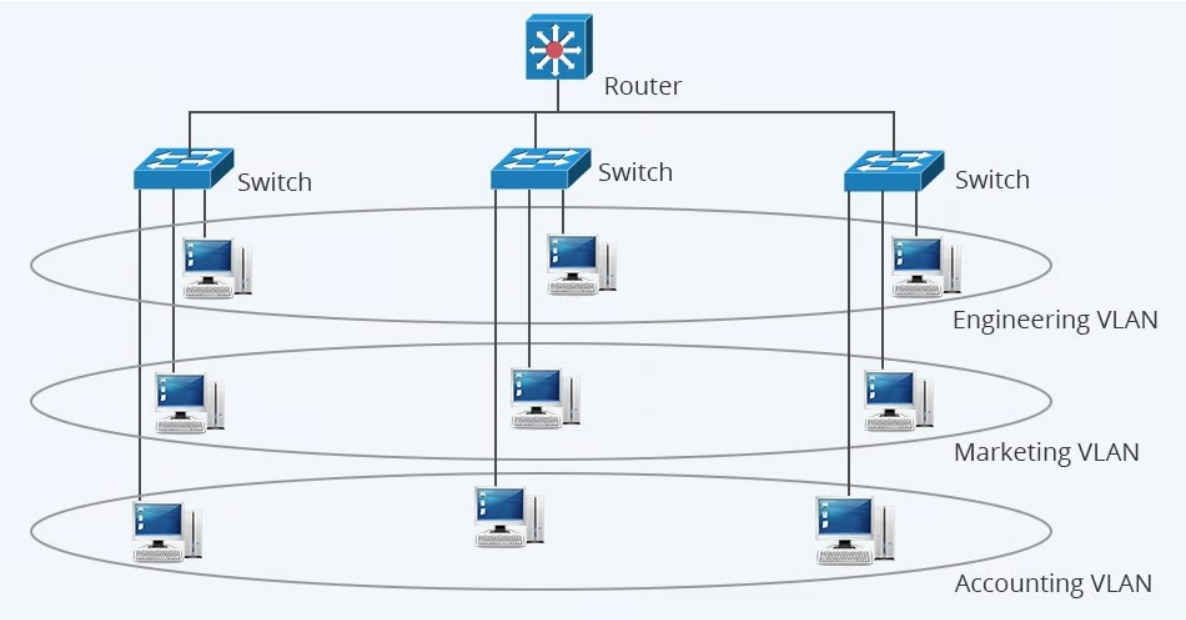
Obrázek 2: Bezdrátová síť

Zdroj:[14]

Jednou z hlavních výhod bezdrátových sítí je mobilita. Uživatelé se mohou volně pohybovat v rámci pokrytí sítě, aniž by byli omezeni kabely. Další výhodou je snadná instalace a rozšíření, protože instalace WLAN nevyžaduje komplikované kabelážní práce a to šetří čas a náklady. [12][13]

Na druhé straně má bezdrátová síť i své nevýhody. Jedním z hlavních problémů je bezpečnost. Bezdrátové přenosy mohou být snadno zachyceny neoprávněnými osobami, to zvyšuje riziko útoků na síť. Je proto nutné implementovat robustní bezpečnostní opatření, jako je šifrování a autentizace, aby byla zajištěna ochrana citlivých dat. Další nevýhodou je omezený dosah a rušení. Bezdrátový signál může být ovlivněn fyzickými překážkami, jako jsou stěny a nábytek, to vede k degradaci signálu a nižší kvalitě připojení. Jiná elektronická zařízení, která používají stejné frekvence, mohou způsobit rušení, které zhoršuje výkon sítě. [12][13]

Virtuální lokální síť (Virtual Local Area Network) je technologie používaná pro rozdělení jedné fyzické sítě na více logických sítí. VLAN je definován na základě switchů, které směrují data pouze mezi zařízeními v rámci stejné VLAN, ačkoli mohou být fyzicky rozmístěna v různých částech sítě (viz Obrázek 3). [12][13]



Obrázek 3: Virtuální lokální síť

Zdroj: [27]

Jednou z hlavních výhod VLAN je zvýšená bezpečnost. Vytvořením oddělených logických sítí lze kontrolovat přístup k citlivým datům a omezit možnosti neoprávněného přístupu. VLAN může izolovat různé skupiny uživatelů nebo aplikací, to minimalizuje riziko, že se škodlivý kód rozšíří po celé síti. Další výhodou je zlepšená správa sítě. VLAN umožňuje centralizovanou správu a konfiguraci sítě, která usnadňuje monitorování a řešení problémů. [12][13]

Nicméně, VLAN má i své nevýhody. Jedním z hlavních problémů je složitost konfigurace a správy. Vyžaduje správnou implementaci a technické znalosti. Nesprávně nakonfigurované VLAN mohou vést k problémům s komunikací mezi zařízeními a mohou zkomplikovat síťovou infrastrukturu. Při špatné konfiguraci může dojít k bezpečnostním mezerám, které mohou být zneužity. Další nevýhodou je závislost na switchích a dalších síťových zařízeních, která podporují VLAN. Ne všechna síťová zařízení jsou kompatibilní s VLAN, to může omezit možnosti jejich nasazení v některých prostředích. Navíc, pokud jsou použita starší nebo levnější síťová zařízení, je nutné investovat do modernějšího hardwaru a to zvyšuje náklady. [12][13]

2 HROZBY A ÚTOKY NA POČÍTAČOVOU SÍŤ

Počítačové sítě jsou vystaveny různým hrozbám, útokům a škodlivým softwarům, které mohou ohrozit jejich bezpečnost a integritu. V této kapitole budou takové hrozby, útoky a škodlivé softwary popsány.

2.1 Hrozby

Hrozba představuje možnost využití slabého bodu v informačním systému k útoku s úmyslem poškodit jeho aktiva. Tyto hrozby mohou být podle [10][11] klasifikovány jako:

Objektivní

- Přírodní a fyzické (například požáry, povodně, výpadky elektrické energie).
- Fyzikální (například elektromagnetické záření, vysokofrekvenční rušení).
- Technické nebo logické (poruchy paměti, softwarové backdoor vstupy).

Subjektivní

- Neúmyslné (například chyby nezkušených uživatelů).
- Úmyslné (vytvořené vnějšími nebo vnitřní útočníky).

Zranitelné místo představuje slabé místo v informačním systému, které může být využito k útokům nebo způsobení škod. Ta mohou mít podle [10][11] několik forem:

- Fyzické (umístění systému na místě snadno přístupném pro sabotáž).
- Přírodní (záplavy, požáry, zemětřesení, blesky).
- Fyzikální (vyzařování, útoky při komunikaci nebo výměně zpráv).
- Lidský faktor (který představuje nejzranitelnější prvek z všech).

Tato zranitelná místa vzniknou v důsledku chyb nebo opomenutí v různých fázích životního cyklu informačního systému, jako je návrh, specifikace, projektové řešení, konstrukce nebo provoz. [10][11]

2.2 Útoky

Útok, občas označovaný jako bezpečnostní incident, se skládá buď z cíleného využití zranitelného místa pro způsobení škody či ztrát v informačním systému, anebo z neúmyslné akce, která má za následek škodu na aktivních prvcích. [5][10]

Útočník je osoba nebo skupina osob, která se snaží získat neoprávněný přístup k síti nebo jejím zdrojům. Útočníci mohou být rozděleni podle [5][10] do několika kategorií podle jejich zdrojů a schopností:

- útočníky s omezenými zdroji;
- útočníky s průměrnými zdroji;
- útočníky s vysokými zdroji.

Mezi běžné a dobře známé metody podle [5][10] útoků patří:

- slovníkový útok;
- útok hrubou silou;
- útok na autentizační protokoly;
- útok na šifrovací algoritmy;
- DoS útoky (Denial of Service);
- spoofing;
- sniffing;
- spamming;
- cracking.

Slovníkový útok je metoda získávání přístupových hesel, při které útočník zkouší všechna možná hesla z předem připraveného seznamu, tzv. slovníku. Tento útok cílí na systémy s autentizací, kde se spoléhá na slabá nebo často používaná hesla. Dopad slovníkového útoku je významný, protože pokud útočník získá přístup k systému, může provádět nepovolené operace a získat citlivé informace. Slovníkové útoky mohou být rychlé a efektivní, pokud uživatelé používají jednoduchá hesla. [34]

Útok hrubou silou je technika, při které útočník zkouší všechny možné kombinace hesel, dokud nenalezne to správné. Tento útok je časově velmi náročný, ale je nevyhnutelný, pokud nejsou použity dostatečně silné hesla (viz kapitola 3.4). Dopad útoku hrubou silou je vážný, protože může vést ke kompromitaci systému a odcizení dat. Útoky hrubou silou často míří na systémy s nedostatečnou ochranou a slabými hesly. [34]

Útok na autentizační protokoly je zaměřen na zranitelnosti v procesech ověřování uživatelů. Útočníci se snaží obejít nebo prolomit autentizační mechanismy, jako jsou hesla, tokeny nebo biometrická data. Tyto útoky mohou vést k neautorizovanému přístupu k citlivým informacím a systémům. Dopad je rozsáhlý, protože kompromitace autentizačního protokolu může vést k úplnému převzetí kontroly nad systémem. [33]

Útok na šifrovací algoritmy se pokouší nalézt slabiny v šifrovacích mechanismech, které chrání data během přenosu nebo uložení. Úspěšné útoky mohou dešifrovat citlivé informace, což vede k narušení důvěrnosti a integrity dat. Dopad těchto útoků je velmi vážný, protože mohou odhalit chráněné informace, jako jsou finanční údaje nebo osobní informace. [32]

DoS (Denial of Service) útok je zaměřen na znepřístupnění služeb legálním uživatelům tím, že přetíží systém nadměrným množstvím požadavků. Tento útok může způsobit výpadky služeb, ztrátu příjmů a reputační škody. Dopad DoS útoku je značný, protože mohou paralizovat klíčové služby a infrastrukturu. [14]

Spoofing je technika, při které útočník vydává svůj komunikující systém za jiný, legitimní systém, aby získal důvěrné informace nebo způsobil škody. Spoofing útoky cílí na různé vrstvy síťové komunikace a mohou vést k odcizení dat nebo narušení systémů. Dopad spoofingu je závažný, protože může vést k neautorizovanému přístupu a podvodným aktivitám. [16]

Sniffing je metoda, při které útočník odposlouchává síťový provoz a získává citlivé informace, jako jsou hesla nebo osobní údaje. Sniffing útoky cílí na nešifrované nebo slabě zabezpečené komunikace. Dopad sniffingu je vysoký, protože umožňuje útočníkům získat přístup k důvěrným informacím bez vědomí uživatelů. [17]

Spamming je praktika odesílání velkého množství nevyžádaných zpráv, často s reklamním nebo podvodným obsahem. Spamování může způsobit zahlcení e-mailových schránek, snížení produktivity a zvýšení rizika phishingových útoků. Dopad spammingu je negativní jak pro jednotlivce, tak pro organizace, protože může vést k bezpečnostním incidentům a ztrátě času. [18]

Cracking je proces, při kterém útočník překonává ochranné mechanismy softwaru nebo hardwaru za účelem jeho nelegálního použití nebo zneužití. Útočí na integritu a ochranu duševního vlastnictví. Dopad může zahrnovat neoprávněné využití softwaru, ztrátu příjmů pro vývojáře a kompromitaci bezpečnosti systému. [19]

2.3 Malware

Škodlivý software, známý také jako malware, je jakýkoli softwarový program vytvořený s úmyslem poškodit, narušit nebo neoprávněně získat přístup k počítačovým systémům, sítím nebo datům. Malware může mít různé podoby a účely, od sběru citlivých informací po úplné zničení dat. Útoky pomocí malwaru mohou mít vážné důsledky pro jednotlivce i organizace, včetně finančních ztrát, narušení soukromí a ohrožení bezpečnosti. [30]

Mezi běžné a známé malware podle [30] patří:

- počítačový virus;
- trojský kůň;
- spyware;
- keylogger;

- adware.

Počítačový virus je škodlivý program, který se šíří tím, že infikuje další soubory a programy v počítačovém systému. Virus se obvykle spouští při spuštění infikovaného programu a následně se šíří na další programy nebo soubory. Útočí na integritu a funkčnost systému tím, že mění nebo ničí data, zpomaluje výkon počítače nebo dokonce způsobuje jeho úplné selhání. Dopad počítačových virů může být značný, zahrnující ztrátu důležitých dat, zvýšení nákladů na obnovu systému a snížení produktivity. [30]

Trojský kůň je škodlivý software, který se tváří jako legitimní program nebo soubor, ale ve skutečnosti skrývá škodlivý kód. Tento kód se aktivuje při spuštění trojského koně a může provádět různé škodlivé činnosti, jako je krádež dat, instalace dalšího škodlivého software nebo poskytování přístupu útočníkovi. Útočí na důvěru uživatelů a zabezpečení systémů. Dopad trojských koní může být katastrofální, zahrnující ztrátu citlivých informací, finanční ztráty a kompromitaci systémové bezpečnosti. [20]

Spyware je typ škodlivého software, který tajně sleduje a shromažďuje informace o aktivitách uživatele na počítači bez jeho vědomí. Může zaznamenávat stisknuté klávesy, sledovat navštívené webové stránky a shromažďovat osobní údaje. Útočí na soukromí a důvěrnost uživatelských dat. Dopad spyware zahrnuje narušení soukromí, krádež identity a finanční ztráty způsobené neoprávněným využitím shromážděných informací. [21]

Keylogger je typ spyware, který zaznamenává všechny stisky kláves na klávesnici a ukládá je pro pozdější analýzu. Tento typ útoku je obzvláště nebezpečný, protože může odhalit citlivé informace, jako jsou hesla, finanční údaje a osobní zprávy. Útočí na důvěrnost a bezpečnost dat. Dopad keyloggerů může být značný, zahrnující krádež identity, finanční ztráty a kompromitaci osobních a profesionálních účtů. [22]

Adware je software, který automaticky zobrazuje nebo stahuje reklamy do počítače uživatele. Často je distribuován jako součást jiných legitimních programů. Zatímco adware sám o sobě nemusí být škodlivý, může být obtěžující a zpomalovat výkon počítače. Útočí na uživatelskou zkušenost a výkon systému. Dopad adware zahrnuje snížení produktivity kvůli častým přerušením reklamami a možné riziko, že adware může otevřít dveře dalším, škodlivějším softwarem. [21][23]

3 BEZPEČNOST POČÍTAČOVÉ SÍTĚ

Bezpečnost počítačové sítě zahrnuje všechny opatření a strategie, které jsou navrženy k ochraně počítačové sítě, informačních systémů a dat před různými hrozbami a útoky. V této době představuje jedno z nejčastěji probíraných témat v oblasti informačních technologií a je vhodné mu věnovat zvýšenou pozornost při konstrukci školních, firemních a domácích sítí. Denně čelí mnohé sítě řadě pokusů o nedovolený přístup, využívajících různé metody hackerských útoků. [1][13]

Pro správce sítí je klíčové udržet plnou kontrolu nad sítí a chránit osobní data uživatelů. Základní postupy a rady od odborníků v oblasti bezpečnosti představují cenný nástroj pro dosažení alespoň minimální úrovně bezpečnosti sítě. Je však důležité si uvědomit, že kvůli chybám v technologiích a neustálému vývoji metod útočníků nelze dosáhnout stoprocentní ochrany před úspěšnými kybernetickými útoky. Je tedy vhodné zdůraznit, že každá dodatečná vrstva zabezpečení přispívá k odvrácení útoků nebo alespoň ztížení potenciálního neoprávněného přístupu. [1][13]

Hlavním cílem bezpečnosti počítačové je zajistit, aby citlivé informace, jako jsou osobní údaje zaměstnanců či zákazníků, zůstaly chráněny, a aby síť byla bezpečná a funkční pro všechny uživatele. Tento cíl je úzce propojen s nařízením GDPR, pravidelným školením zaměstnanců a implementací technických opatření. Do technických opatření se řadí zálohování dat, fyzické zabezpečení, politika hesel, šifrování, firewall, antivirový program překlad adres, zabezpečení bezdrátové sítě Wi-Fi a zabezpečení vzdáleného přístupu do sítě. [1][13]

3.1 GDPR

GDPR (General Data Protection Regulation), neboli Obecné nařízení o ochraně osobních údajů, je evropské nařízení, které bylo implementováno do české legislativy zákonem č. 110/2019 Sb. Zákon o zpracování osobních údajů. Toto nařízení klade přísné požadavky na ochranu osobních údajů, které se dotýkají všech organizací včetně škol. [23]

Podniky zpracovávají velké množství osobních údajů, které zahrnují informace o zaměstnancích, zákaznících či dalších osob. Tyto údaje mohou zahrnovat jména, adresy, rodná čísla, zdravotní záznamy a další citlivé informace. GDPR stanovuje, že všechny tyto údaje musí být zpracovávány zákonným, spravedlivým a transparentním způsobem. Podniky musí zajistit, aby osobní údaje byly shromažďovány pouze pro specifické, explicitní a legitimní účely a aby nebyly zpracovávány způsobem neslučitelným s těmito účely. [23][29]

Implementace GDPR má za cíl zvýšit úroveň ochrany osobních údajů a zamezit jejich neoprávněnému zpracování. Dodržování těchto předpisů přispívá k vyšší důvěře mezi firmami, zaměstnanci a třeba i dodavateli, které je nezbytné pro bezpečné a efektivní prostředí. [23][29]

Pro zajištění efektivního dodržování GDPR a také bezpečnosti sítě je nezbytné pravidelné školení zaměstnanců. Učitelé a administrativní pracovníci by měli být pravidelně školeni o zásadách ochrany osobních údajů, správném zpracování údajů a o tom, jak reagovat na bezpečnostní incidenty. Zvýšení povědomí o ochraně osobních údajů mezi zaměstnanci je klíčové pro předcházení porušení GDPR a zamezení úniku citlivých informací. [29]

3.2 Zálohování dat

Zálohování dat není způsob, jak zamezit útočníkům od získání dat ze sítě, ale je to jedno z opatření pro ochranu dat. Útočník nemusí mít za cíl pouze získat data, ale může se také snažit je zničit. Pokud uživatel neudělá zálohu dat nebo nemá zálohovací software, který by to udělal za něho, může přijít o tyto informace, pokud by došlo k jejich ztrátě. Pravidelné zálohování dat by mělo být jedním z klíčových ochranných opatření pro každého uživatele počítače. Jde o prevenci pro případ, že by se něco nepředvídatelného stalo. K zálohování důležitých dat, která by neměla chybět, existuje celá řada spolehlivých a známých zálohovacích systémů, jako je například Cobian Backup, Google Drive Backup and Sync, Microsoft OneDrive nebo Veeam Backup & Replication. [9]

3.3 Fyzické zabezpečení

Fyzická bezpečnost představuje jednu z nejzákladnějších forem zabezpečení sítě, která cíleně reguluje přístup k síťovým zařízením pouze pro autorizované osoby. Tento druh ochrany je úzce spojen s umístěním síťových prvků, na které je nutné myslet již při jejich instalaci. Nejvhodnější přístup se odvíjí od vytvoření samostatné technické místnosti pro umístění všech síťových prvků a serverů. Vyjma přístupových bodů pro bezdrátové sítě, u kterých je nezbytné omezit přístup standardním uživatelům. [1]

Vstupní dveře do těchto prostor, zvláště těch obsahujících servery, by měly být zabezpečeny alespoň zámkem. Klíče by měli mít přístup pouze administrátoři nebo odpovědná osoba za správu budovy. Moderní doba však přináší další možnosti ochrany před neoprávněným vniknutím, například vstup do místnosti pomocí autentifikace. [1]

Autentifikace se soustředí na metody, které slouží k ověření totožnosti uživatele nebo zařízení, které požaduje přístup k určitému zdroji. Provedení ověření zahrnuje poskytnutí potřebné sady informací ze strany klienta. Nejčastěji používanou metodou autentifikace je využití

uživatelského jména a hesla. Existuje mnoho dalších způsobů, jako je využití biometrických údajů, hlasové identifikace, otisků prstů nebo také čipových karet. [2]

Autentizace je proces potvrzování identity uživatele nebo zařízení, to je často považováno za synonymum pro autentifikaci. V praxi se oba termíny často zaměňují, ačkoliv autentizace může být specifikována jako krok, který následuje po úspěšné autentifikaci, kdy je ještě ověřováno, zda daná identita má skutečně platné a aktuální přístupové oprávnění. Tento krok je zásadní pro zajištění bezpečnosti v počítačových sítích a na internetu, protože zamezuje neoprávněnému přístupu a chrání citlivá data před zneužitím.

Autorizace je proces, který určuje, zda má identifikovaná a ověřená osoba vhodný přístup k určitému zdroji. To znamená, že autorizace definuje, jakým způsobem může uživatel využívat sítě a k jakým informacím a službám má oprávnění. Účtování slouží k monitorování událostí, které se v systému odehrávají během uživatelské interakce se síťovými službami. Účel účtování spočívá zejména v auditování, to znamená, že uchovává záznamy o událostech v systému. Auditování pomáhá správcům systému sledovat a kontrolovat chování uživatelů a identifikovat potenciální bezpečnostní problémy. [2]

3.4 Politika hesel

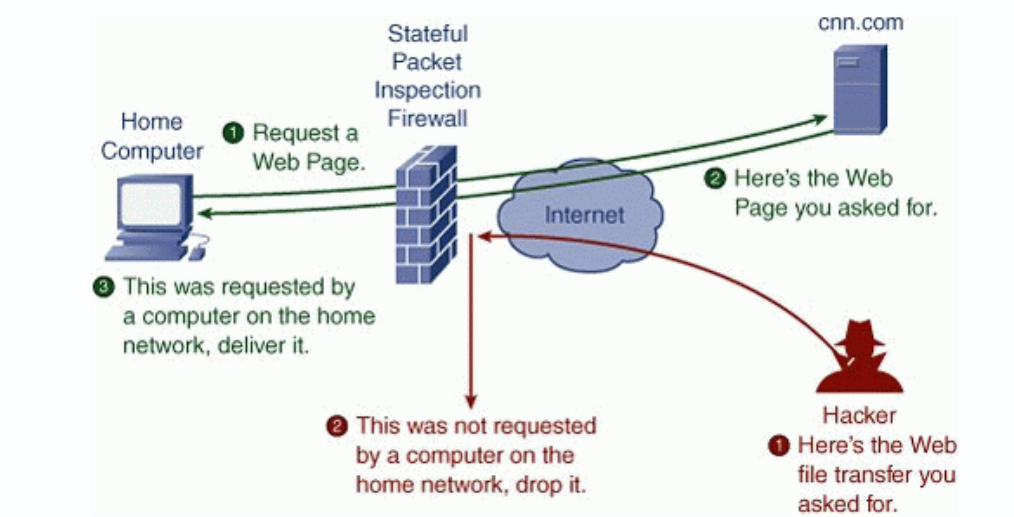
Pokud se provádí ověřování pomocí uživatelského jména a hesla, heslo se stává klíčovým prvkem pro ochranu uživatele. Vzhledem k relativně jednoduché povaze tohoto typu zabezpečení je důležité, aby správce nastavil optimální pravidla pro heslo. Správná politika stanovuje minimální délku hesla, jeho složitost, dobu jeho platnosti a zabránění opakování stejných znaků či řetězců. K posílení celkového zabezpečení přístupu lze kombinovat více různých ověřovacích faktorů. Zvláště pro citlivé aplikace je vhodné využít více faktorové autentizace, kde kromě uživatelského jména a hesla může být požadován PIN kód odeslaný na mobilní telefon nebo e-mail. [2]

3.5 Šifrování

Šifrování je součást kryptologie, to je věda zaměřující se na vývoj šifrovacích metod a kryptoanalýzu, která se snaží prolomit či rozluštit tyto šifrovací techniky. Princip šifrování spočívá v transformaci srozumitelného textu do nečitelné podoby, známé jako šifrovaný text. Jeho hlavním cílem je zajistit utajení informací tak, aby je nemohl dešifrovat neoprávněný člověk. I když data přijdou do cizích rukou, zůstávají nečitelná. Tato technika se využívá pro ochranu dat na počítačích, které mohou být přístupné jiným osobám, ať už přímo nebo přes síť a internet, a také pro bezpečný přenos dat. [3]

3.6 Firewall

Firewall je zařízení nebo software, které řídí tok dat mezi různými síťovými segmenty, ať už jsou to oddělené počítačové sítě nebo konkrétní oblasti v privátní síti. Slouží jako bariéra mezi důvěryhodnou interní sítí a nedůvěryhodnými externími sítěmi, jako je internet (viz Obrázek 4). Toto síťové zařízení reaguje na příchozí a odchozí datové pakety na základě definovaných pravidel komunikace, které obsahují informace jako zdrojové a cílové IP adresy, komunikační porty, síťové protokoly a další. [5]



Obrázek 4: Firewall

Zdroj: [6]

3.7 Antivirový program

Antivirový program je jednoduché označení pro bezpečnostní software, který identifikuje, detekuje, blokuje a odstraňuje kybernetické hrozby. Původně šlo o jednoduchý software, který detekoval a případně odstranil počítačové viry z infikovaného zařízení. Většina antivirových programů při hledání virů a malwaru spoléhala na detekci charakteristických řetězců, známých jako virové signatury. Každý virus měl jedinečný "otisk", který umožňoval jeho snadné rozpoznání a zabránění dalšímu šíření. [28]

Současný antivirový program obsahuje moderní technologie a různé bezpečnostní vrstvy, které chrání proti různým druhům hrozeb, čímž uživateli zajišťují vysokou úroveň bezpečnosti. Díky vícevrstvé ochraně dokáže antivirový program bojovat proti krádeži hesel a účtů, odcizení citlivých osobních údajů a dalším formám kybernetických útoků. Mezi nejznámější antivirové programy patří Avast Antivirus, ESET, nebo AVG Antivirus. [28]

3.8 Network address translation

Network Address Translation (NAT) je technologie, která umožňuje překládání IP adres uvnitř privátní sítě na veřejné IP adresy používané na internetu a naopak. Tuto technologii využívají routery k tomu, aby umožnily zařízení v lokální síti přístup na internet, aniž by každé zařízení muselo mít svou vlastní jedinečnou veřejnou IP adresu. NAT tak zajišťuje efektivní využití omezeného množství veřejných IP adres.[7]

NAT nabízí několik výhod. První a nejdůležitější je úspora IP adres. Díky NAT mohou organizace použít jednu veřejnou IP adresu pro mnoho zařízení v jejich vnitřní síti, čímž se snižuje potřeba velkého počtu veřejných IP adres. Další výhodou je zvýšená bezpečnost, protože NAT skryje vnitřní topologii sítě před vnějším světem, což může ztížit pokusy o útok. NAT také umožňuje snadnější změnu poskytovatele internetových služeb (ISP), protože změna veřejné IP adresy neovlivní vnitřní síť.[7]

Navzdory svým výhodám má NAT také několik nevýhod. Jednou z hlavních nevýhod je komplikace při navazování spojení zvenčí do vnitřní sítě, to může ovlivnit fungování IP telefonů, protože vyžadují přímé spojení mezi zařízeními. NAT může také zvýšit latenci a zpomalit výkon sítě, jelikož každá příchozí a odchozí IP adresa musí být přeložena. Další nevýhodou je komplikovanější konfigurace a údržba sítě, protože NAT vyžaduje pečlivé nastavení pravidel a mapování portů, aby bylo zajištěno správné směrování provozu. [7]

3.9 Zabezpečení bezdrátové sítě Wi-Fi

Zabezpečení bezdrátové sítě Wi-Fi je klíčové pro ochranu bezdrátových sítí před neoprávněným přístupem a zajištění bezpečné komunikace. Jedním ze základních pojmů v oblasti bezdrátových sítí je Service Set Identifier (SSID), který identifikuje konkrétní bezdrátovou síť. Každé zařízení připojené k Wi-Fi síti musí znát SSID, aby se mohlo správně připojit. Správná konfigurace SSID je prvním krokem k zajištění bezpečnosti Wi-Fi sítě. Skrytí SSID může poskytnout základní úroveň zabezpečení tím, že síť nebude viditelná při skenování bezdrátových sítí. Pro zajištění vyšší bezpečnosti Wi-Fi sítí se používají různé zabezpečovací protokoly, mezi nejběžnějšími jsou WPA2 Personal a WPA2 Enterprise. [25]

3.9.1 Wi-Fi Protected Access 2 Personal

Wi-Fi Protected Access 2 Personal (WPA2 Personal) je bezpečnostní protokol, který využívá předem sdílený klíč (PSK) k autentizaci uživatelů a šifrování dat přenášených v síti. Tento protokol je určen pro domácí a malé kancelářské sítě, kde je správa uživatelských účtů jednodušší. WPA2 Personal využívá šifrovací standard AES (Advanced Encryption Standard),

který poskytuje vysokou úroveň zabezpečení proti odposlechu a dalším typům útoků. Klíčovým prvkem WPA2 Personal je silný a komplexní PSK, který ztěžuje prolomení ochrany sítě pomocí brute-force útoků. [25]

3.9.2 Wi-Fi Protected Access 2 Enterprise

Wi-Fi Protected Access 2 Enterprise (WPA2 Enterprise) je pokročilejší forma zabezpečení Wi-Fi, která je určena pro rozsáhlejší sítě, jako jsou ty ve firmách nebo vzdělávacích institucích. Na rozdíl od WPA2 Personal nepoužívá předem sdílený klíč, ale místo toho využívá centralizovaný autentizační server (např. RADIUS server). Tento server ověřuje identitu každého uživatele zvlášť, což umožňuje lepší správu přístupových práv a zvyšuje celkovou bezpečnost sítě. WPA2 Enterprise také využívá AES pro šifrování dat, ale poskytuje vyšší úroveň zabezpečení díky individualizovaným přihlašovacím údajům pro každého uživatele. Tento přístup ztěžuje neoprávněným uživatelům přístup k síti, i když by získali přihlašovací údaje jednoho z uživatelů. [25]

3.10 Zabezpečení vzdáleného přístupu do sítě

Zabezpečení vzdáleného přístupu do sítě je dalším aspektem moderního IT prostředí, který umožňuje uživatelům bezpečně přistupovat k firemním zdrojům a aplikacím z jakéhokoli místa. Vzdálený přístup je důležitý pro organizace s mobilními zaměstnanci nebo pro situace, kdy zaměstnanci pracují na dálku. [1][4]

Virtual private network (VPN) je oblíbenou metodou pro bezpečný vzdálený přístup do sítě přes internet. Tato technologie vytváří zabezpečený šifrovaný tunel mezi dvěma komunikačními body, to umožňuje vzdálený přístup k lokálním sítím. Princip VPN spočívá v tom, že šifrovaná data jsou zabalená do jiného datagramu, který obsahuje směrovací informace pro doručení dat skrze tento tunel. Vzdálený přístup může být realizován buď pomocí metody Remote Access pro připojení klientů do firemní sítě z libovolného místa na internetu, nebo pomocí metody Site-to-Site, která spojuje dvě vzdálené lokální sítě, často využívaná pro propojení firemních poboček. Klíčovým prvkem VPN jsou protokoly, které spravují tunel a zajišťují bezpečnost datového toku. Každý z těchto protokolů se odlišuje svými parametry, jako je typ tunelu nebo způsob šifrování. Mezi nejčastěji využívané protokoly dnes patří L2TP, IPSec, SSTP a OpenVPN. [1][4]

4 ANALÝZA RIZIK

Analýze rizik je nástroj systému řízení informační bezpečnosti, poskytující organizaci efektivní způsob pro určení priorit v oblasti informační bezpečnosti na strategické i operativní úrovni. Rozhodnutí, zda dané riziko bude odstraněno, eliminováno nebo akceptováno, závisí na jeho závažnosti a nákladech na jeho řešení. Cílem analýzy rizik je zjistit, co je pro organizaci důležité a hodnotné, co je tolerovatelné a co ne, a připravit podklady pro strategické, řídící a kontrolní procesy v oblasti informační bezpečnosti. [10][30]

Podle [5][10] existuje několik metod, které se používají k provedení analýzy rizik:

- kvalitativní analýza rizik;
- kvantitativní analýza rizik;
- CBA (Cost-Benefit Analysis)
- HAZOP (Hazard and Operability Study);
- FMEA (Failure Mode and Effects Analysis).

Cost-Benefit Analysis (CBA), neboli analýza nákladů a přínosů, je metodou ekonomického hodnocení, která se používá k porovnání celkových nákladů a přínosů projektu nebo rozhodnutí. Cílem této analýzy je zjistit, zda jsou přínosy větší než náklady a zda je tedy projekt nebo rozhodnutí ekonomicky výhodné. CBA zahrnuje identifikaci a kvantifikaci všech nákladů a přínosů spojených s projektem. Náklady a přínosy jsou vyjádřeny v peněžních jednotkách, které umožňuje jejich srovnání. [5]

5 ANALÝZA SOUČASNÉHO STAVU VE ŠKOLE

Tato kapitola se zabývá analýzou a zhodnocením řešení počítačové sítě a jejího zabezpečení pro vybranou školu, která z důvodu bezpečnosti nebude jmenována. Na základě nalezených problémů bude vypracován návrh na zvýšení bezpečnosti sítě. Analýza bude zkoumat především kritické části sítě, které představují největší hrozbu. Určí aktiva školy, které by mohli být lehce napadnutelné a zneužitelné, popisuje současné vybavení školní sítě, fyzickou a logickou strukturu sítě.

5.1 Fyzické prostředí školy

Vybraná škola je čtyřpodlažní budova, která dříve byla rozdělena na dvě samostatné budovy. Po stavebních úpravách v minulých letech došlo ke spojení obou budov spojovacím tunelem a vznikl současný stav budovy. Současná počítačová síť je rozvedená téměř po celé budově. V 1. podzemním patře se nachází místnost s centrálním serverem této školy a zálohovacími zařízeními. Místnost je klimatizovaná, zabezpečená elektronickou zabezpečovací signalizací a přístupná pouze správci sítě školy. V 1. nadzemním patře se nachází učebny, které jsou vybaveny pracovními stanicemi pro učitele a zároveň jsou připojeny k interaktivním tabulím nebo projektorům a také je v tomto patře umístěna učebna výpočetní techniky. Zde je umístěn datový rozvaděč s páteřním rozvodem datové sítě školy. V 2. nadzemním patře se nachází sborovna a ředitelna. Ve 3. nadzemním patře se nachází školní dílna. Celá škola je pokryta signálem Wi-Fi.

5.2 Využití školní sítě

Školní datová síť je primárně využívaná pro výukové účely a administrativní úkony. Aktuálně jsou všechny lokálně poskytované služby dostupné jak přes Wi-Fi, tak po kabelovém vedení (není filtrován provoz). Školní síť je stavěna na horizontálním a vertikálním metalickém vedení. Učebny, které jsou vybavené stolním (desktopovým) počítačem jsou do školní sítě připojené právě pomocí těchto metalických vodičů. Administrativa školy využívá školní síť pro práci s databázovými softwary, které jsou uložené na centrálním serveru v serverovně, v 1. podzemním patře školy.

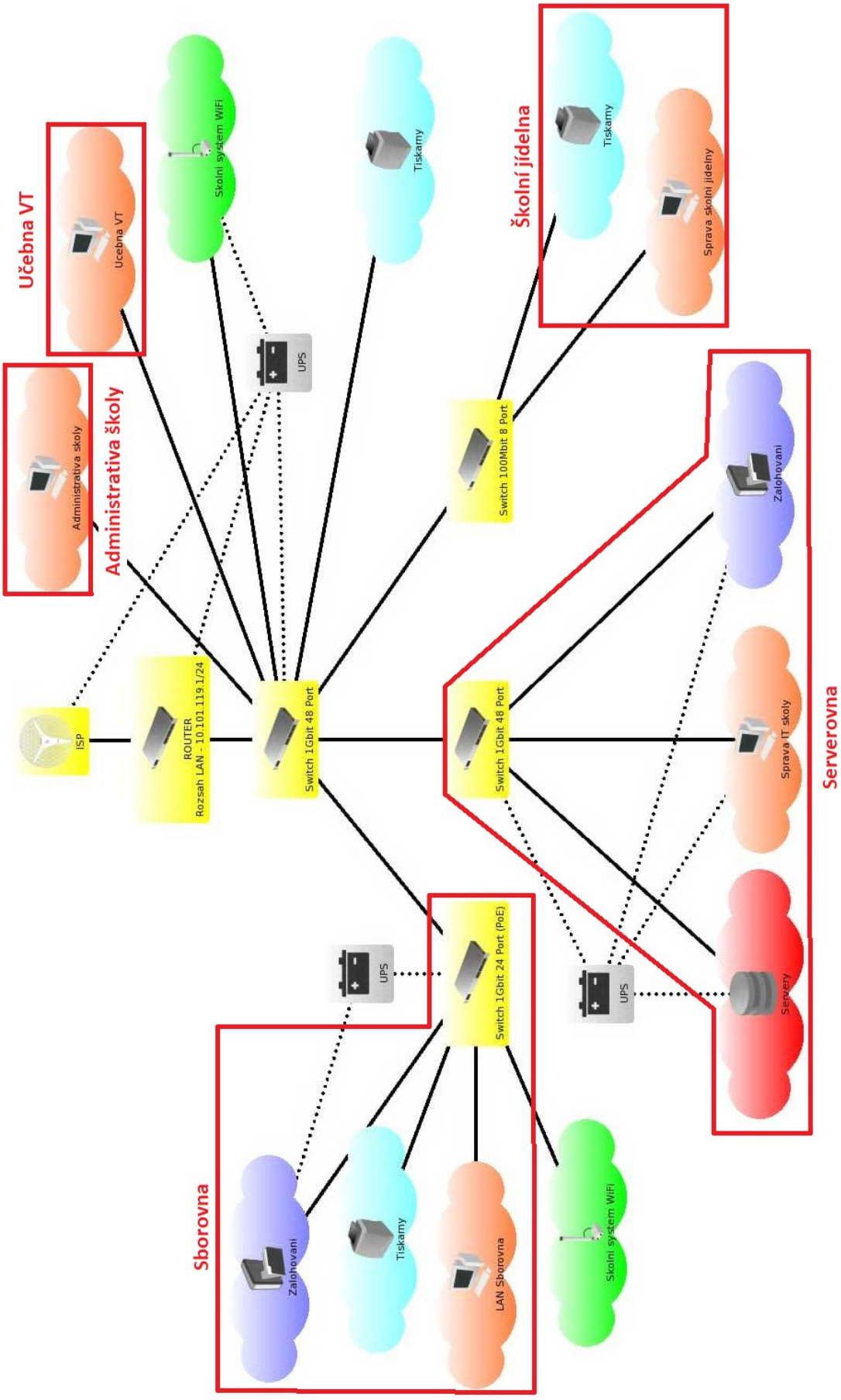
5.3 Současný hardware sítě

Celý síťový provoz školní sítě momentálně zprostředkuje router značky Mikrotik s čtyř-jádrovým procesorem na frekvenci 800MHz. Pomocí metalického vedení UTP kabelem kategorie cat 5e jsou data z routeru distribuována do hlavního switche této školy, 48-portového

switche značky Mikrotik. Pomocí vertikálního a horizontálního vedení v plastových lištách jsou metalické kabely, také konfigurace cat 5e rozvedeny do podružného datového rozvaděče ve sborovně, do 1. podzemním patře pro potřeby školního serveru a zálohovacích zařízení a do všech aktivních prvků rozmístěných po škole.

V ostatních prostorách školy jsou rovnoměrně rozmístěné přístupové body AP značky Ubiquiti ve verzi LR pro zajištění bezproblémového šíření signálu po celé budově školy. Na třech místech je nepřerušitelný zdroj napájení (UPS) značky APC a na chodbě v 1. a 2. nadzemním patře je síťová tiskárna.

Obrázek 5 (na další straně) zobrazuje logické schéma sítě ve vybrané škole. Jsou zde znázorněny všechny spoje mezi zařízeními a každý typ zařízení je barevně rozlišen. Plná černá čára znázorňuje ethernetový spoj mezi zařízeními, čárkovaná černá čára znázorňuje přívod záložního napájení z UPS. Žlutě jsou označeny síťové prvky (router, switche, ISP), oranžově jsou označeny počítačové stanice, červeně jsou označeny servery, zelenou barvou jsou označeny vysílače Wi-Fi signálu, světle modře jsou označeny tiskárny a tmavě modře jsou zálohovací zařízení. Pokud se propojená zařízení nacházejí v jedné místnosti, jsou červeně ohraničena s popisem, jaká místnost to je.



Obrázek 5: Logické schéma sítě

Zdroj: Vlastní zpracování

5.3.1 Administrativa školy

Zde se nachází 1 počítačová stanice pro ředitele školy, 2 počítačové stanice pro administrativní zaměstnance školy a podružný datový rozvaděč pro již zrekonstruovanou část školy.

5.3.2 Učebna výpočetní techniky

V učebně výpočetní techniky (VT) je umístěn datový rozvaděč s páteřním rozvodem datové sítě školy, 17 počítačových stanic (včetně toho pro vyučujícího).

5.3.3 Školní jídelna

Ve školní jídelně je jedna počítačová stanice pro zaměstnance jídelny a jedna síťová tiskárna.

5.3.4 Serverovna

V serverovně je umístěn volně ložený switch, 48-portový pro připojení síťových interfaců serveru, zálohovacích zařízení, počítače pro správce a přídavných dočasných zařízení. Hlavním školním serverem je server HP ProLiant G10 ve verzi Tower. Čítá diskové pole o velikosti 4 TB, 32 GB RAM a jeden 16 jádrový CPU Intel Xeon s 2,5 GHz frekvencí jader. Na fyzickém serveru umístěném v serverovně běží tři virtuální stroje pro zajištění bezproblémového chodu školní sítě. Doménový controller, SQL server a server pro zabezpečovací a antivirové řešení.

Dále je zde umístěno centrální síťové datové úložiště pro účely zálohování všech důležitých souboru či dokumentů školy a zároveň pro kompletní zálohu obrazu operačních systémů počítačů, stěžejních pro bezproblémové fungování školy (počítač účetní školy, ředitele, zástupce ředitele, vedoucí jídelny).

5.3.5 Sborovna

Ve sborovně je 1 počítačová stanice pro vyučující a 1 síťová tiskárna Dále je zde v datovém rozvaděči umístěn PoE switch, opět výrobce Mikrotik ve 24-portové variantě a také síťové datové uložiště pro data ze serveru, aby nebyla záloha zničena spolu se zdrojem dat pro zálohování.

5.4 Současný software sítě

Současný software v této škole zahrnuje různé operační systémy, antivirovou ochranu a specializované informační systémy, které společně zajišťují efektivní a bezpečný provoz školních počítačových zařízení a aplikací. Školní síť využívá několik různorodých operačních systémů, přizpůsobených specifickým potřebám jednotlivých zařízení a také míst, kde se daná zařízení nachází.

Na routerech a switchích Mikrotik běží operační systém RouterOS, který slouží k řízení a správě síťového provozu, a poskytuje široké možnosti konfigurace a zabezpečení síťových připojení. Na všech školních počítačích, které používají žáci a zaměstnanci školy, je nasazen operační systém Windows 10 Home s nainstalovaným balíčkem Microsoft 365 pro práce v aplikacích, jako je například Microsoft Word, Excel, PowerPoint a Outlook.

5.4.1 Administrativa školy

Počítače, které slouží pro administrativní činnost školy, mají nainstalován informační systém Gordic, který je používán pro správu majetku a finančních okruhů školy a informační systém VEMA, který je využíván pro správu mezd zaměstnanců školy a také zajišťuje přesné a efektivní zpracování mzdové agendy.

5.4.2 Učebna VT

Na počítačích pro žáky a učitele jsou naistalovány výukové softwary Terasoft a Didakta, které podporují výukové procesy.

5.4.3 Školní jídelna

Na počítači ve školní jídelně je naistalován informační systém VIS pro administraci stravování ve školní jídelně.

5.4.4 Serverovna

Na serverech školy je využíván Windows Server 2019 Standard, který slouží jako základní platforma pro správu síťových služeb a aplikací. Linux je využíván na serverech spravujících antivirovou ochranu pomocí ESET Protect. Pro síťové datové uložiště (NAS) Synology je operační systém DSM (DiskStation Manager). Zálohování jako takové probíhá v několika etapách a je z části automatické a z části manuální.

Automatické zálohování mají na starosti zálohovací softwary Cobian Backup a Veeam Backup & Replication. Konkrétně Veeam Backup & Replication vytváří denní obrazy operačních systému serverů včetně dat. Prováděna je tzv. rozdílová úloha – jsou denně pomocí jednotlivých bodů obnovy zálohovány pouze ten provedené změny. Jednou za měsíc je nastaveno provedení plné zálohy, pro možnost odmazání předchozích plných záloh, ke kterým by již bylo složité napasovat body obnovy z rozdílových záloh. Jednou týdně v sobotu v nočních hodinách je prováděna záloha dat mimo budovu do centrálního datového úložiště pro zachování minimálně týden starých dat v případě kybernetického útoku.

Druhým typem zálohování je záloha pomocí programu Cobian Backup, který provádí kopie souborů přímo na klientských počítačích. Data jsou ukládána pomocí plných záloh, bez rozdílové složky. Posledním typem prováděného zálohování je plnohodnotná kopie na externí disk, který je po provedení zálohy kompletně odpojen od školní sítě.

5.4.5 Sborovna

Na počítači ve sborovně je naistalován informační systém Bakaláři, který je určen pro správu školní administrativy, zahrnující evidenci žáků, rozvrhy, hodnocení a komunikaci s rodiči.

Pro síťové datové uložiště (NAS) Synology je operační systém DSM (DiskStation Manager). Zálohování dat ze serveru zde probíhá stejně jako zálohování dat celé školy na zálohovacím zařízení v serverovně.

5.5 Současný stav bezpečnosti sítě

V současné chvíli se školní počítačová síť skládá pouze z jedné lokální podsítě, do které spadají servery, počítače, přístupové body, tiskárny a jiné. V současné konfiguraci routeru ani není možné přemýšlet o nějakém rozdělení dané sítě, až třeba jen na podsítě VLAN – router nemá dostatek výkonu na tyto úkony. Dále také ani centrální switch nemá dostatek výkonu pro možnost spuštění dělení provozu sítě na jiné subnety.

Do lokální sítě je zařazena i síť Wi-Fi a i přes více konfigurovaných SSDISD se jedná o jednu podsíť. Přístup do sítě Wi-Fi je realizován pomocí protokolu WPA2 Personal, pouze pomocí hesla.

Momentálně není nastavena ochrana jednotlivých portů switchů pro připojení cizích zařízení, to znamená, že každé připojení zařízení se do sítě dostane, pokud je tedy port switche ve stavu Enabled.

Školní síť je chráněna komplexní antivirovou ochranou poskytovanou společností ESET. Tato ochrana je naprosto vyhovující pro udržení bezpečného a stabilního prostředí pro všechny uživatele školní sítě.

Veškeré datové vedení je kryto lištami na omítku, případně vedení přímo pod omítkou v umělohmotných chráničkách, aby nemohlo dojít k jeho fyzickému poškození. Vedení je také vždy vymezené dilatační mezerou od silnoproudé instalace z důvodu vnějších rušících vlivů EMI a RFI. Veškeré datové vedení je dimenzované na přenosovou rychlost minimálně 1 Gbps. Zakončení datového vedení je řešeno zásuvkami typu daného vodičem, který do zásuvky datový signál přivádí. Začátek datového vedení je zakončený v patch panelu a je pečlivě vyvázaný a přichycený na příslušné pozice U v rackové skříni. Rozměry patch panelů i jiných

aktivních či pasivních prvků jsou ve velikosti 1U. Datové skříně jsou umístěné v bezpečných místech ať už elektronické zabezpečovací signalizace, či přístupu pouze určených osob. Datové skříně jsou uzamčené a přístup do nich má pouze lokální správce sítě.

5.6 Přístupy a uživatelé školní sítě

Přístup do školní sítě je navržen tak, aby zajišťoval bezpečnost a efektivitu využívání všech informačních systémů. Uživatelé sítě jsou rozděleni do tří hlavních skupin: správce sítě, zaměstnanci školy a žáci, přičemž každá skupina má specifická přístupová práva a omezení.

Správce sítě má nejvyšší úroveň přístupu k síti, který je zajištěn pomocí dvoufázové autentifikace (2FA). Tento uživatel má přímý přístup do sítě, a to jak lokálně, tak vzdáleně prostřednictvím VPN. Díky tomuto přístupu může správce monitorovat, spravovat a konfigurovat veškeré síťové zařízení a služby. Správce má plná práva ke všem sekcím sítě, to mu umožňuje provádět potřebné úpravy a údržbu systému.

Zaměstnanci školy mají pro přístup do školních zařízení a školní sítě vytvořené uživatelské jméno, které vychází z jejich jména a příjmení, a heslo, které se jim každý půl rok generuje nové. Pomocí jejich přihlašovacích údajů mají také možnost připojit se k síti vzdáleně přes VPN. Tento přístup jim umožňuje bezpečně pracovat i mimo školní areál. Na rozdíl od správce sítě jsou však jejich práva omezená. Zaměstnanci mají přístup pouze k těm sekcím sítě, které jsou nezbytné pro jejich pracovní úkoly. Například učitelé mají přístup k výukovým materiálům a online vzdělávacím platformám, zatímco účetní má přístup k finančním systémům, ale nikoli k jiným částem sítě, které nesouvisejí s její prací. Tato omezení zajišťují, že citlivé části sítě zůstanou chráněny před neoprávněným zásahem.

Žáci mají pro přístup do školních zařízení a školní sítě vytvořené uživatelské jméno, které vychází z jejich jména a příjmení, a heslo, které se jim každý půl rok generuje nové. Obecně mají omezený přístup k síti, který je navržen tak, aby podporoval jejich vzdělávání, ale zároveň minimalizoval rizika spojená s bezpečností. Přístup žáků je omezen pouze na lokální síť, to znamená, že nemohou využívat VPN pro vzdálené připojení. V rámci lokálního přístupu mají žáci přístup pouze k výukovým materiálům a internetu. Tento přístup je pečlivě kontrolován a filtrován, aby se zajistilo, že žáci nebudou vystaveni nevhodnému obsahu a nebudou mít přístup k citlivým datům nebo administrativním sekcím sítě. Omezení přístupu žáků přispívá k bezpečnému a efektivnímu vzdělávacímu prostředí.

5.7 Školení zaměstnanců

V rámci dodržování GDPR a také kybernetické bezpečnosti se na škole provádí školení zaměstnanců 1x ročně. Tato školení provádí externí pracovník z místního obecního úřadu a správce ICT školy. V rámci těchto školení probíhá i test vědomostí, kdy školitelé si chtějí ověřit, zda zaměstnanci školy doopravdy vnímají vše, co jim říkají. Z hlediska bezpečnosti je takové školení dostačující, pokud se bude předpokládat, že školitel kybernetické bezpečnosti podrobně sleduje trendy v oblasti bezpečnosti počítačových sítí a aktualizuje bezpečnostní politiku školy.

5.8 Bezpečnostní rizika

Ze získaných informací při analyzování současného stavu školy a řízených rozhovorech se správcem školní sítě vyplynula následující bezpečnostní rizika.

5.8.1 Výskyt pouze jednoho subnetu

V této škole je historicky nasazen pouze jeden segment sítě, konkrétně 10.101.119.1/24. Tento segment je ve školní síti využíván od počátku digitalizace školy, tedy od nasazení prvním počítačových stanic. Součástí segmentu jsou tedy jak klientské koncové stanice, tak síťové servery, datová úložiště, IP telefony, Wi-Fi AP i tiskárny.

Bezpečnostní riziko výskytu pouze jednoho subnetu spočívá v tom, že když je v síti přítomný jenom jeden subnet a jsou do něho připojena všechna zařízení, tak každé zařízení vidí komunikace ostatních. Ta se dá odchytit pomocí různých aplikací pro odchyt komunikace a tím útočník může získat přístupové údaje a podobná citlivá data.

5.8.2 Absence ochrany fyzických portů

Spravovatelné aktivní prvky, které jsou ve škole nasazeny, nemají na svých fyzických portech aktivovanou fyzickou ochranu portů. To přináší riziko, že jakékoli zařízení, které třeba ani nemusí spadat pod správu školy, se může k danému portu pomocí datového kabelu připojit a zařadit se tím do datového provozu školní sítě. Může dojít k odchytu posílaných dat a odcizení těchto dat útočníkem, či k jiným bezpečnostním hrozbám, jako je například pokus o prolomení zabezpečení školních serverů, popřípadě jejich zahlcení. Volný přístup k síti tedy útočníkovi značně zjednodušuje narušení bezpečnosti sítě.

5.8.3 Absence hardwarového firewallu

Firewall je obsažen ve školní síť pouze na centrálním routeru, kde běží jako standartní služba kontroly provozu dovnitř a ven. Je ale definován pouze ručně nastavenými pravidly, která musí být konfigurována správcem sítě. Není zde tedy žádná proaktivní ochrana v podobě blokování přístupu na podezřelé webové stránky nebo spouštění nebezpečných síťových aplikací. Absence hardwarového firewallu přináší riziko softwarového poškození počítače, ztráty a odcizení dat, nebo narušení celkové bezpečnosti školní sítě.

5.8.4 Nestabilita sítě při výpadku napájení

Na páteřních prvcích sítě jsou instalovány zdroje nepřerušitelného napájení (UPS), které mají za úkol udržet trvalý pracovní stav síťových prvků při výpadku elektrické energie. Jejich počet a kapacita zálohování je však nedostatečná, a ne všechna zařízení jsou tedy po výpadku elektrického napájení schopná fungovat. Nestabilita sítě při výpadku napájení může poškození a ztráta neuložených dat. V krajních situacích může dojít k poškození zařízení, které není připojeno k UPS.

6 ANALÝZA RIZIK

Na základě zjištěných skutečností byla identifikována bezpečnostní rizika, která ohrožují chod a bezpečnost školní počítačové sítě. Pro analýzu rizik využiji Cost-Benefit Analysis (CBA), abych vyhodnotil, zda je ekonomicky výhodné investovat do řešení bezpečnostních rizik. Veškeré hodnoty jsou odhadované na základě rozhovoru se správcem sítě.

6.1 Výskyt pouze jednoho subnetu

Pravděpodobnost ztráty citlivých dat a údajů v důsledku výskytu pouze jednoho subnetu sítě je 0,005 za rok.

Očekávaná ztráta (přístupové údaje) je 250 000 Kč.

Očekávaná roční ztráta je tedy 250 000 x 0,05 = 1 250 Kč.

Cena práce za vytvoření více subnetů sítě je 20 000 Kč a její životnost je 20 let (tzn. ročně 1 000 Kč).

Jelikož roční náklady za vytvoření více subnetů sítě jsou nižší, než očekávané roční ztráty (1 000 Kč < 1 250 Kč), investice do vytvoření více subnetů sítě je v tomto případě efektivní.

6.2 Absence ochrany fyzických portů

Pravděpodobnost odchytu posílaných dat a odcizení těchto dat je 0,001 za rok.

Očekávaná ztráta (hodnota odcizených dat) je 200 000 Kč a za narušení bezpečnosti sítě 500 000 Kč.

Očekávaná roční ztráta je tedy (200 000 + 500 000) x 0,001 = 700 Kč.

Cena práce za nastavení ochrany fyzických portů je 5 000 Kč a její životnost je 10 let (tzn. ročně 500 Kč).

Jelikož roční náklady za nastavení ochrany fyzických portů jsou nižší, než očekávané roční ztráty (500 Kč < 700 Kč), investice do nastavení ochrany fyzických portů je v tomto případě efektivní.

6.3 Absence hardwarového firewallu

Pravděpodobnost softwarového poškození počítače, ztráty a odcizení dat, nebo narušení celkové bezpečnosti školní sítě v důsledku absence hardwarového firewallu je 0,1 za rok.

Očekávaná ztráta (poškození počítače) je 20 000 Kč a 80 000 Kč hodnota dat.

Očekávaná roční ztráta je tedy (20 000 + 80 000) x 0,1 = 10 000 Kč.

Cena hardwarového firewallu je 47 000 Kč a jejich životnost je 7 let (tzn. ročně 7 000 Kč).

Jelikož roční náklady na hardwarový firewall jsou nižší, než očekávané roční ztráty (7 000 Kč < 10 000 Kč), investice do hardwarového firewallu je v tomto případě efektivní.

6.4 Nestabilita sítě při výpadku napájení

Pravděpodobnost výpadku proudu ve škole na dobu delší než 10 sekund je 0,02 za rok.

Očekávaná ztráta (zaměstnanci nemohou pracovat z důvodu resetování systému) je 20 000 Kč, ztráta dat 20 000 Kč a 10 000 Kč ztráta času.

Očekávaná roční ztráta je tedy (20 000 + 20 000 + 10 000) x 0,02 = 1 000 Kč.

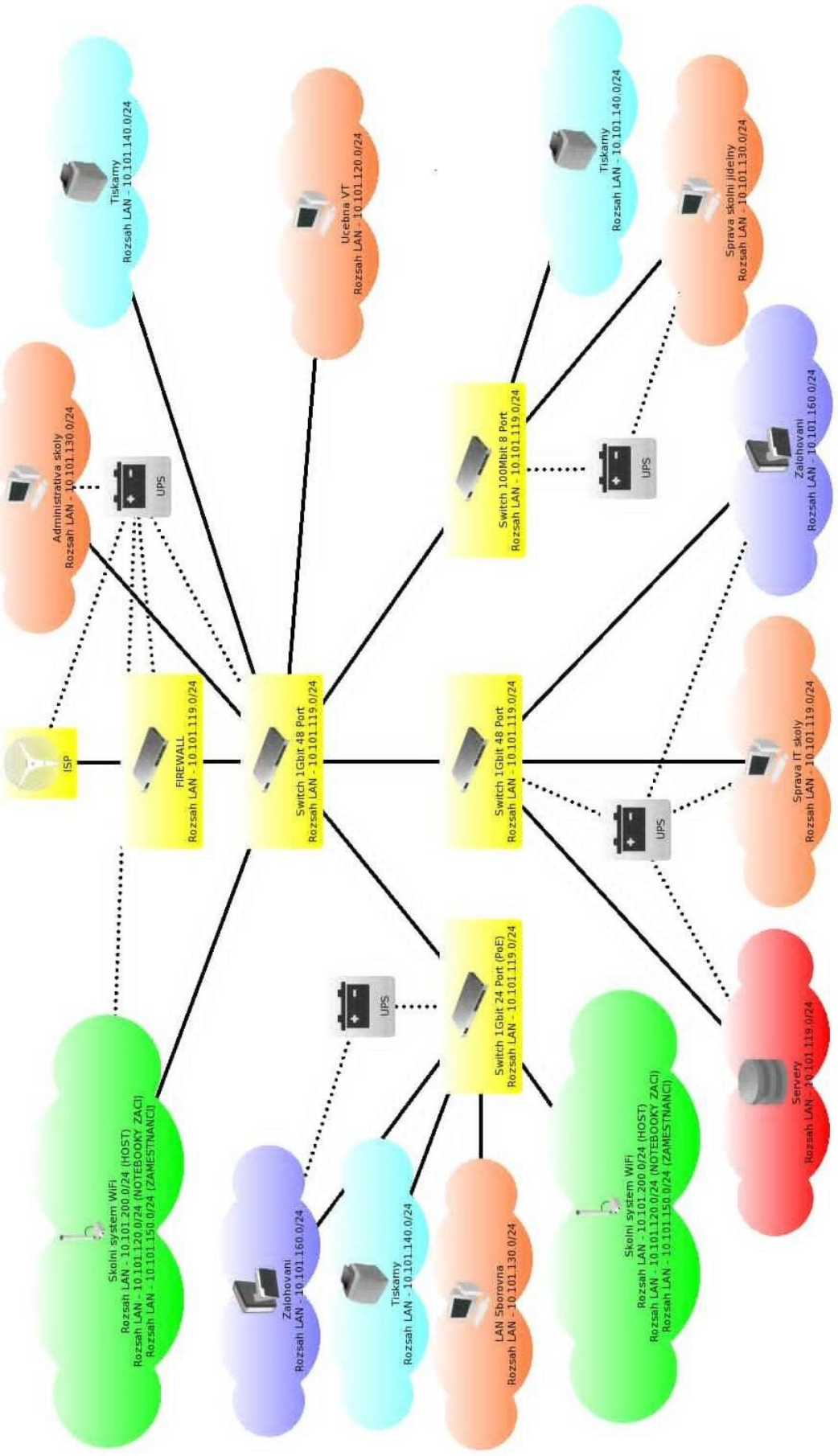
Cena UPS (záložní zdroj energie) je 9840 Kč a jejich životnost je 10 let (tzn. ročně 984 Kč).

Jelikož roční náklady na UPS jsou mírně nižší, než očekávané roční ztráty (984 Kč < 1 000 Kč), investice do UPS je v tomto případě efektivní.

7 NÁVRH ZMĚN ZABEZPEČENÍ

Z analýzy počítačové sítě školy a analýzy rizik vyplynula bezpečnostní rizika, které je potřeba vyřešit, protože zabezpečení školní sítě činí nedostatečným. V této kapitole jsem vytvořil návrh, jak se jednotlivých rizik zbavit. Své návrhy změn jsem také konzultoval se správcem sítě.

Obrázek 6 (na další straně) zobrazuje logické schéma návrhu sítě ve vybrané škole, na němž jsou zaznamenány technické změny, jako je vytvoření více subnetů sítě, implementace fyzického firewallu a přidání dalšího nepřerušitelné napájecí zdroje, v celkovém nákresu sítě. Jsou zde znázorněny všechny spoje mezi zařízeními a každý typ zařízení je barevně rozlišen (popis barevného rozlišení a čar mezi zařízeními je stejný jako u Obrázku 5 v předchozí kapitole). Podrobněji jsou všechny změny a doporučení popsány v kapitolách 7.1 – 7.5.



Obrázek 6: Výsledné schéma návrhu sítě

Zdroj: Vlastní zpracování

7.1 Nasazení více segmentů sítě IP

Ve škole je nasazen pouze jeden subnet počítačové sítě, ve znění 10.101.119.0/24. Do tohoto segmentu spadají všechna připojovaná zařízení. Není tedy možné efektivně nastavovat firewallová pravidla na základě filtrování IP adres. Po nasazení více subnetů je možné restrikovat přístupy jednotlivých zařízení k ostatním zařízením, právě na základě již zmíněného pravidla. Rozdělení sítě navrhuji následujícím způsobem.

7.1.1 Původní subnet

Původní subnet ve znění 10.101.119/24 navrhuji tak, aby obsahoval pouze servery a zařízení se servery spojena, jako je fyzický management pro správu serveru HP integrated Lights-OUT (HP iLO), SQL server, správa doménových služeb (DC), nástroj pro virtualizaci operačních systémů (HYPER-V) a aktivní síťové prvky (Router, Switche, AP). Tabulka 1 zobrazuje všechna zařízení a jejich IP adresy v původním subnetu sítě. Tento subnet může pohlížet na síť jako komplet, má přístup do všech ostatních subnetů, včetně internetu. Přístup ostatních subnetů do tohoto je řešen v následujících bodech.

Tabulka 1: Adresní seznam zařízení v původním subnetu

Zařízení	IP adresa
Router	10.101.119.1
HP iLO	10.101.119.5
SQL SERVER	10.101.119.8
DC	10.101.119.10
HYPERV	10.101.119.19
HYPERV	10.101.119.20
Switch	10.101.119.101
Switch	10.101.119.102
Switch	10.101.119.103
Switch	10.101.119.104
AP	10.101.119.151
AP	10.101.119.152
AP	10.101.119.153
AP	10.101.119.154
AP	10.101.119.155
AP	10.101.119.156
AP	10.101.119.157
AP	10.101.119.158
AP	10.101.119.159

Zdroj: Vlastní zpracování

7.1.2 Subnet Učebna VT

Do tohoto segmentu sítě ve znění 10.101.120.0/24 patří počítačové stanice v učebně výpočetní techniky. Navrhuji nastavenit segment pro komunikaci pouze se servery v subnetu 10.101.119.0/24 a samozřejmě do internetu. Díky oddělení počítačových stanic učebny výpočetní techniky od ostatních stanic mohou být nastaveny více restrikcí pomocí firewallu pro práci žáků, kteří na těchto stanicích pracují. Například omezení webového obsahu. Do tohoto subnetu také spadá samostatně vytvořená Wi-Fi síť, se samostatně vytvořeným SSID pro přístup do sítě žákovských notebooků. Aplikovaná pravidla jsou stejná jako u stanic počítačové učebny. Tabulka 2 zobrazuje počítačové stanice v učebně VT (které jsou označeny vnitřní zkratkou ve tvaru VT-PC-xx) a jejich IP adresy v novém subnetu učebny výpočetní techniky.

Tabulka 2: Adresní seznam zařízení v novém subnetu Učebna VT

Zařízení	IP adresa
VT-PC-01	10.101.120.101
VT-PC-02	10.101.120.102
VT-PC-03	10.101.120.103
VT-PC-04	10.101.120.104
VT-PC-05	10.101.120.105
VT-PC-06	10.101.120.106
VT-PC-07	10.101.120.107
VT-PC-08	10.101.120.108
VT-PC-09	10.101.120.109
VT-PC-10	10.101.120.110
VT-PC-11	10.101.120.111
VT-PC-12	10.101.120.112
VT-PC-13	10.101.120.113
VT-PC-14	10.101.120.114
VT-PC-15	10.101.120.115
VT-PC-16	10.101.120.116
VT-PC-17	10.101.120.117

Zdroj: Vlastní zpracování

7.1.3 Subnet Administrace školy

V tomto segmentu ve znění 10.101.130.0/24 navrhuji umístit veškeré administrativní stanice, které škola užívá. Patří sem tři stolní počítače v ředitelně školy, jeden v sborovně a jeden stolní počítač v kanceláři vedoucí jídelny. Subnet má přístup do segmentu 10.101.119.0/24 pro přístup k datům uloženým na centrálním serveru a samozřejmě pro přístup do AD DS pro přístup k přihlašovacím službám systému Windows. Tento subnet má také přístup do sítě tiskáren, předchozí subnet (10.101.120.0/24) tento přístup nemá. Tabulka 3 zobrazuje zařízení a jejich IP adresy v novém subnetu pro zařízení administrativy školy.

Tabulka 3: Adresní seznam zařízení v novém subnetu Administrace školy

Zařízení	IP adresa
REDITELNA-PC-01	10.101.130.101
REDITELNA-PC-02	10.101.130.102
REDITELNA-PC-03	10.101.130.103
JIDELNA-PC-01	10.101.130.104
SBOROVNA-PC-01	10.101.130.105

Zdroj: Vlastní zpracování

7.1.4 Subnet Tiskárny

Do segmentu subnetu 10.101.140.0/24 navrhuji přesunout veškeré síťové tiskárny v síti užívané. Tento subnet nemá stálý přístup do internetu, pouze na základě nutnosti (například online upgradu firmwaru), kdy je na základě pravidla firewallu vytvořeno pravidlo s povolením určitého portu pro komunikace do internetu. Do tohoto subnetu nemá přístup subnet 10.101.119.120/24 (Učebna VT), až na výjimku počítače učitele VT-PC-01. Tato výjimka je určena pravidly firewallu pomocí IP adresy učitelského počítače a je vytvořeno tzv. inverzní pravidlo – „zahoď vše, kromě požadavku z této adresy“. Tabulka 4 zobrazuje zařízení a jejich IP adresy v novém subnetu pro tiskárny.

Tabulka 4: Adresní seznam zařízení v novém subnetu Tiskárny

Zařízení	IP adresa
Tiskárna sborovna	10.101.140.101
Tiskárna ředitelna	10.101.140.102
Tiskárna ředitelna 2	10.101.140.103
Tiskárna jídelna	10.101.140.104

Zdroj: Vlastní zpracování

7.1.5 Subnet WLAN zaměstnanci

Subnet 10.101.150.0/24 navrhuji pro bezdrátovou síť LAN pro zaměstnance školy. Pravidla firewallu jsou nastavena tak, že subnet může přistupovat k serverům školy, k internetu a k tiskárnám. Je vytvořeno samostatné SSID pro vysílání sítě na tomto subnetu.

7.1.6 Subnet Zálohování

V subnetu 10.101.160.0/24 navrhuji umístit pouze servery NAS, ke kterým je přidělen přístup pouze na základě povoleného pravidla ze stanice, která má zálohování provádět. Tento segment má přístup do internetu z důvodu zasílání notifikací do e-mailového klienta. Tabulka 5 zobrazuje zařízení a jejich IP adresy v novém subnetu pro zálohovací servery.

Tabulka 5: Adresní seznam zařízení v novém subnetu Zálohování

Zařízení	IP adresa
NAS1	10.101.160.10
NAS2	10.101.160.11

Zdroj: Vlastní zpracování

7.1.7 Subnet WLAN žáci a veřejnost

Jako součást tohoto posledního subnetu 10.101.200.0/24 navrhuji vytvořit dvě bezdrátové sítě LAN se dvěma rozdílnými SSID pro žáky a veřejnost (například návštěvy školy). Tento segment nemá přístup k žádným vnitřním segmentům školní sítě, má přístup pouze do internetu. V případě, že je vytvořena přihlašovací instance žáků pomocí serveru RADIUS, je tomuto segmentu umožněn přístup do segmentu serverů, ale pouze pro port právě zmiňovaného serveru RADIUS.

7.2 Řešení ochrany portů na aktivních prvcích sítě

Spravovatelné prvky, které jsou ve škole užity, mají možnost nastavit na svých fyzických portech tzv. ochranu fyzického přístupu. Laicky řečeno, „pokud se na portu objeví jiné zařízení, než předem definované, provoz na portu bude zakázán“. Tento princip zabezpečení se hodí například pro blokování zařízení připojených k datovým zásuvkám rozmístěných po škole. Například žák, který si do školy přinese vlastní zařízení, které i přes zákaz bude chtít do školní sítě připojit pomocí datového kabelu, nalezne ve třídě datovou zásuvku, do které bude připojena dokovací stanice. Po připojení do stanice se mu zařízení do školní sítě nepřipojí, právě díky nastavené ochraně portů. Tato varianta také zamezuje umístění odposlechu sítě, například při připojení prvku pro sběr dat mezi koncová zařízení.

7.3 Hardwarový firewall

Ve školní síti současně veškerý provoz řídí klasický router značky Mikrotik. Pro zvýšení zabezpečení sítě, ale také pro zajištění snazší spravovatelnosti navrhuji nasadit hardwarový firewall značky Fortinet. Firewall má stejné funkce, jako klasický router, ale navíc má možnost do sebe nainstalovat určité utility, které obsahují definice bezpečné sítě. Pomocí definic firewall dokáže aktivně chránit zařízení připojena do vnitřní sítě před možnými hrozbami přicházejícími z internetu.

7.4 Zvýšení stability sítě při výpadcích elektrické energie

Ve školní síti sice už jsou nasazeny tři nepřerušitelné napájecí zdroje typu UPS. Veškeré UPS jsou typu L-I (line interaktiv), jsou tedy připraveny zálohovat v řádu milisekund přerušení

dodávky elektrické energie. Navrhuji umístění dalšího zařízení UPS, čímž se docílí funkčního stavu všech síťových prvků, včetně serverů a důležitých stanic po výpadku elektrické energie a také se docílí tak nižšího rizika poškození a ztráty dat při náhled „tvrdém“ ukončení operačního systému zařízení. Síťové prvky tím pádem dokáží pracovat ještě poměrně dlouhou dobu po výpadku elektrické energie a zařídí tím bezpečné douložení veškerých dat.

7.5 Organizační opatření

Co se týče organizačních opatření, škole doporučuji pravidelně aktualizovat bezpečnostní politiku školní sítě a také udržet kvalitu a pravidelnost školení pro zaměstnance. Tím si školní síť udrží dlouhodobou bezpečnost a efektivitu.

8 SHRNUTÍ DOPORUČENÝCH ZMĚN

V navržených změnách byla doporučena implementace několika opatření k posílení bezpečnosti a efektivity školní sítě.

Bylo doporučeno rozdělit tuto síť do několika subnetů, aby mohla být nastavena firewallová pravidla pro řízení přístupu jednotlivých subnetů, čímž se zvýší přehlednost a bezpečnost připojených zařízení.

Bylo zjištěno, že spravovatelné aktivní prvky nemají aktivovanou fyzickou ochranu portů. To znamená, že jakékoli zařízení se může připojit k portu a získat přístup do datového provozu školní sítě. Bylo doporučeno aktivovat fyzickou ochranu portů, aby se zamezilo neoprávněnému přístupu a potenciálním bezpečnostním hrozbám, jako je odposlouchávání dat nebo pokusy o prolomení zabezpečení.

Ve školní síti je přítomen pouze sotfwarový firewall na centrálním routeru, kde byla nastavena pouze ruční pravidla bez proaktivní ochrany. Bylo navrženo nasazení moderního hardwarového firewallu značky Fortinet, který díky aktualizacím definic zabezpečení dokáže rychle reagovat na hrozby a aktivně kontrolovat síťový provoz i uvnitř sítě.

Zdroje nepřerušitelného napájení (UPS) jsou instalovány pouze u některých klíčových síťových prvků a to je nedostatečné. Bylo navrženo navýšení počtu UPS, aby byla zajištěna stabilita sítě při výpadku elektrické energie a zamezilo se ztrátě dat.

Také je doporučeno pravidelně aktualizovat bezpečnostní politiku školní sítě a udržovat kvalitu a pravidelnost školení pro zaměstnance.

Implementace těchto opatření se škole vyplatí v porovnání s možnými ztrátami, které by mohly nastat při zneužití bezpečnostních hrozeb útočníkem (viz kapitola 6). Navrhovaná opatření zahrnují jak technické, tak organizační změny, které společně výrazně posílí bezpečnost a efektivitu školní sítě.

9 ZÁVĚR

Cílem této bakalářské práce bylo navrhnout možnosti zabezpečení počítačové sítě ve vybrané škole. Práce zahrnovala detailní analýzu současného stavu školní sítě s cílem identifikovat slabá místa a navrhnout změny, které by vedly k bezpečnějšímu prostředí pro provoz používaných informačních systémů.

Nejprve byla představena struktura počítačové sítě. Dále byly vymezeny možné hrozby a útoky, kterým může být síť vystavena, a popsány základní principy a technologie pro zabezpečení počítačové sítě. Tato část poskytla důkladný teoretický základ pro následnou praktickou analýzu a návrh opatření.

Poté se práce zaměřila na konkrétní analýzu současného stavu počítačové sítě ve vybrané škole. Byly identifikovány klíčové slabiny, které by mohly ohrozit bezpečnost sítě. Na základě této analýzy a analýzy rizik byl navržen plán inovací, který zahrnuje technická a organizační opatření. Mezi navržená technická opatření patří nasazení více segmentů sítě, implementace fyzického firewallu, ochrana fyzických portů a přidání dalšího nepřerušitelné napájecí zdroje. Organizační opatření zahrnují pravidelnou aktualizaci bezpečnostních politik a školení zaměstnanců v oblasti bezpečnosti IT.

Tato práce přináší praktická doporučení, která mohou být okamžitě implementována za účelem zvýšení bezpečnosti školní sítě. Návrhy uvedené v této práci mohou sloužit jako vzor pro další školy, které se potýkají s podobnými bezpečnostními problémy. Implementace navržených opatření přispěje k ochraně citlivých dat, zvýší odolnost proti kybernetickým útokům a zajistí hladký provoz školních informačních systémů.

Závěrem lze konstatovat, že navržená opatření, pokud budou implementována a pravidelně aktualizována, mohou významně přispět k celkové bezpečnosti počítačové sítě ve vybrané škole a vytvořit tak bezpečné a spolehlivé prostředí pro vzdělávání a administrativní činnosti.

POUŽITÁ LITERATURA

[1] BARRETT, Diane, Kalani K. HAUSMAN a Martin WEISS. CompTIA Security+ SY0-301 Exam Cram. 3rd ed. Pearson Education, 2011. ISBN 0-7897-4829-0.

[2] VAVREČKOVÁ, Šárka. Počítačová síť a internet [online]. Slezská univerzita v Opavě: Filozoficko-přírodovědecká fakulta v Opavě, 2017 [cit. 2023-12-21]. ISBN 978-80-7510-245-4. Dostupné z: http://vavreckova.zam.slu.cz/pocsit.html

[3] DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

[4] HORÁK, Jaroslav. Bezpečnost malých počítačových sítí: (praktické rady a návody) : podrobný průvodce začínajícího uživatele. Praha: Grada, 2003. ISBN 80-247-0663-6.

[5] DANICS, Štefan a STRNAD, Štěpán. Aspekty bezpečnosti. Vydání: první. Praha: Policejní akademie České republiky v Praze, 2016. ISBN 978-80-7251-455-7.

[6] PCPoradenství. Ze zabezpečení počítače: co je firewall? [online]. [cit. 2023-12-27]. Dostupné na: http://www.pcporadenstvi.cz/ze-zabezpeceni-pocitace-co-je-firewall

[7] What is Local Area Network? Online. Heavy.ai. Dostupné z: https://www.heavy.ai/technical-glossary/local-area-network. [cit. 2024-07-20].

[8] MMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Brno: Computer Press, 2010. ISBN 978-80-251-2359-1.

[9] VICNE, Jan. Zálohování dat: věnujte mu pár desítek minut a budete mít klid na X let dopředu. Digitální pevnost [online]. 2019-01-21 [cit. 2023-12-30]. Dostupné z: https://www.digitalnipevnost.cz/zpravodaj/detail/zalohovani-dat

[10] HUB, Miloslav. Bezpečnost a ochrana informací v prostředí internetu. Pardubice: Univerzita Pardubice, 2013. ISBN 978-80-7395-701-8.

[11] TANENBAUM, Andrew S., WETHERALL, David J. Computer Networks. 5th edition. Boston: Pearson, 2011. ISBN 978-0-13-212695-3.

[12] SMITH, John. Network Fundamentals. 2nd edition. New York: McGraw-Hill, 2018. ISBN 978-0-07-337617-4.

[13] STALLINGS, William. Data and Computer Communications. 10th edition. Upper Saddle River: Pearson, 2014. ISBN 978-0-13-350648-8.

[14] A typical wireless local area network configuration. Online. ResearchGate. Dostupné z: https://www.researchgate.net/figure/A-typical-wireless-local-area-network-configuration_fig1_224091293. [cit. 2024-07-20].

[15] GARMS, Jess a Daniel SOMERFIELD. Professional Java Security. Birmingham: Wrox Press, 2001. ISBN 978-1-861004-64-2.

[16] GOODRICH, Michael T. a Roberto TAMASSIA. Introduction to Computer Security. Boston: Pearson, 2011. ISBN 978-0-321-51294-9.

[17] KAUFMAN, Charlie, Radia PERLMAN a Mike SPECINER. Network Security: Private Communication in a Public World. 2nd ed. Upper Saddle River: Prentice Hall, 2002. ISBN 978-0-13-046019-6.

[18] GROSSMAN, Lev. Spam: A Shadow History of the Internet. New York: Bloomsbury Publishing, 2014. ISBN 978-1-62040-803-5.

[19] YAN, Song. Cybercrime and Cybercriminals: An Overview of Emerging Threats and Cyber Defense Strategies. London: Routledge, 2018. ISBN 978-1-138-04839-0.

[20] GORDON, Sarah a Richard FORD. Trojan Horses: Crafting and Exploring a Threat. Computer Fraud & Security, 2002, roč. 2002, č. 10, s. 8-12. ISSN 1361-3723.

[21] ERBSCHLOE, Michael. Spyware and Adware. Burlington: Elsevier, 2005. ISBN 978-0-12-369422-5.

[22] KNUDSEN, Jerker. Keyloggers: Definition, Types and Techniques. Journal of Digital Forensics, Security and Law, 2012, roč. 7, č. 3, s. 1-14. ISSN 1558-7215.

[23] WHITMAN, Michael E. a Herbert J. MATTORD. Principles of Information Security. 6th ed. Boston: Cengage Learning, 2018. ISBN 978-1-337-56893-5.

[24] Zákon č. 110/2019 Sb. Zákon o zpracování osobních údajů. Online. Zákon pro lidi. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110. [cit. 2024-06-16].

[25] SÉJOURNÉ, Damien. Wireless Security: Understanding and Protecting Wi-Fi Networks. 2nd ed. New York: Apress, 2016. ISBN 978-1-4842-1827-2.

[26] HALLBERG, Bruce. Networking: A Beginner's Guide. 8th ed. New York: McGraw-Hill Education, 2019. ISBN 978-1-26-045817-1.

[27] Network Segmentation Explained in Layman Term. Online. GeekFlare. Dostupné z: https://geekflare.com/network-segmentation/. [cit. 2024-07-20].

[28] Antivirus. Online. ESET. Dostupné z: https://www.eset.com/cz/antivirus-software/. [cit. 2024-06-16].

[29] Elnagdy, Moataz. "Understanding GDPR Compliance for Schools." International Journal of Computer Science and Information Security, vol. 17, no. 5, 2019, pp. 121-127.

[30] KALLMAN, Gregory J. a KEEN, Jack M. Managing Security Risks: The Onsite-Application Security Risk Management Guide. New York: McGraw-Hill Education, 2013. ISBN 978-0-07-179205-3.

[31] SKOUDIS, Ed a Lenny ZELTSER. Malware: Fighting Malicious Code. Upper Saddle River: Prentice Hall, 2003. ISBN 978-0-13-101405-3.

[32] SCHNEIER, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed. New York: Wiley, 1996. ISBN 978-0-471-12845-8.

[33] MENEZES, Alfred, Paul van OORSCHOT a Scott VANSTONE. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1996. ISBN 978-0-8493-8523-0.

[34] HILL, Richard. Dictionary Attack. In: Encyclopedia of Cryptography and Security. 2nd ed. Berlin: Springer, 2011, s. 317. ISBN 978-1-4419-5905-8.