Česká zemědělská univerzita v Praze

Technická fakulta

Katedra technologických zařízení staveb

Diplomová práce

Optimalizace a zabezpečení propojení lokálních sítí středních škol

Petr Firman

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Petr Firman

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Optimalizace a zabezpečení propojení lokálních sítí středních škol

Název anglicky

Optimization and security of interconnections of local networks of secondary schools

---

Cíle práce

Cílem práce je provézt kompletní technickou i bezpečnostní analýzu IS a počítačové sítě vybraných středních škol, navrhnout jejich propojení v rámci bezpečné integrace IS a navržené řešení prakticky ověřit.

Metodika

1. Úvod
2. Cíl práce
3. Metodika
4. Analýza vybraných škol
5. Shrnutí stávajícího stavu
6. Definovaní integračních požadavků
7. Analýza technických možností, volba řešení
8. Technické ověření a diskuse výsledku
9. Finanční náročnost
10. Závěr a vyhodnocení

Doporučený rozsah práce

50 – 60 stánek včetně obrázků a grafů

Klíčová slova

WAN, LAN, bezpečnost, VPN, VLAN

Doporučené zdroje informací

Barry L Williams: Information Security Policy Development for Compliance, ISBN: 1466580585, Taylor & Francis Ltd, 2013

COMER, D E. Computer networks and Internets : with Internet applications. Upper Saddle River: Prentice Hall, 2009. ISBN 0-13-091449-5.

ISO 27001 Systém managementu bezpečnosti informací

James F. Kurose: Počítačové sítě, Computer Press, 2014, EAN: 9788025138250

Zeegers Ruben: Information Security Management Professional based on ISO/IEC 27001 Courseware revised Edition- English, ISBN13 (EAN): 9789401803656, 2017

Předběžný termín obhajoby

2021/2022 LS – TF

Vedoucí práce

Ing. Zdeněk Votruba, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 3. 2. 2021

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 10. 2. 2021

doc. Ing. Jiří Mašek, Ph.D.

Děkan

V Praze dne 07. 02. 2022

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci na téma: Optimalizace a zabezpečení propojení lokálních sítí středních škol vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů.

Jsem si vědom, že odevzdáním diplomové práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Jsem si vědom, že moje diplomová práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí. Jsem si vědom/a že, na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.

V Praze dne .....

Poděkování

Rád bych touto cestou poděkoval vedoucímu práce Ing. Zdeňkovi Votrubovi, Ph.D. za konzultace, vstřícný přístup a cenné rady při vedení práce.

Zároveň bych chtěl poděkovat vedení školy Vyšší odborné školy ekonomické, sociální a zdravotnické, Obchodní akademii, Střední pedagogické škole a Střední zdravotnické škole, Most, za spolupráci a cenná poskytnutá data.

Optimalizace a zabezpečení propojení lokálních sítí středních škol

Abstrakt:

Cílem práce je provedení technické a bezpečnostní analýzy školního informačního systému a počítačové sítě ve vybrané škole, navržení jejich propojení v rámci optimalizace a zabezpečení. Návrh inovace vychází ze závěrů provedeného testování a analýzy stávající školní sítě a informačního systému a reálných možností vybudování modernější školní sítě a informačního systému.

Klíčová slova: WAN, LAN, VPN, VLAN, bezpečnost, analýza

Optimization and Security of interconnection od local networks of secondary schools

Abstract:

The aim of the work is to perform a technical and security analysis of the school information system and computer network in the selected school, to design their interconnection within the optimization and security. The innovation proposal is based on the conclusions of the performed testing and analysis of the existing school network and information system and the real possibilities of building a more modern school network and information system.

Keywords: WAN, LAN, VPN, VLAN, security, analysis

Obsah

1 Úvod **1**

2 Cíl práce **3**

3 Metodika **4**

4 Počítačová síť **5**

4.1 Rozdělení počítačových sítí 5

4.2 Rozdělení počítačových sítí podle velikosti 6

4.3 Speciální druhy sítí 8

4.4 Topologie počítačových sítí 8

4.5 Referenční model ISO/OSI 10

4.6 Model TCP/IP 11

4.7 Hardware sítě 13

4.7.1 Aktivní prvky 13

4.7.2 Pasivní prvky 15

4.8 Server 17

4.9 Internet a zabezpečení sítě 18

5 Informační systém **21**

5.1 Bezpečnost a kvalita IS 21

5.1.1 Bezpečnost IS 21

5.1.2 Kvalita IS 22

5.1.3 Autentizace 22

5.2 Penetrační testy 23

5.2.1 Metodika penetračního testování 25

5.2.2 Fáze penetračního testování 26

5.2.3 Typy penetračních testů 27

5.2.4 Dělení penetračních testů 27

5.2.5 Další způsoby testování 29

6 Normy a legislativy **30**

6.1 GDPR 30

6.2 Technická opatření školy pro dosažení souladu s nařízení GDPR 30

6.3 Vyhláška č. 523/2005 Sb.,..... 31

6.4 ISMS – Systémy řízení bezpečnosti informací 31

7 Bezpečnost počítačových sítí **33**

7.1 Ochrana síťové komunikace 34

7.2 Kontrola přístupu 35

7.3 Autentizace v síti ... 37
7.4 Aktivní útočník ... 37
7.5 Řízení zátěže ... 38
7.6 Integrita dat ... 39
7.7 Lokální sítě ... 39
7.8 Víceúrovňová bezpečnost ... 39
7.9 Bezpečnost komunikace ... 40
8 Škola a počítačová síť ... 41
8.1 Základní charakteristika školy ... 41
8.2 Charakteristika školní sítě ... 44
8.3 Testování a analýza ... 47
8.3.1 Penetrační testování ... 47
8.3.2 Testování propustnosti sítě ... 49
8.3.3 SWOT analýza ... 54
9 Návrh na zlepšení ... 57
9.1.1 Modernizace webových stránek ... 57
9.1.2 Modernizace školní sítě ... 59
9.1.3 Modernizace propojeni budov A, B ... 61
10 Závěr ... 62
11 Seznam použitých zdrojů ... 64
12 Přílohy ... 67

Seznam použitých obrázků

OBR. 1 BANDWIDTH TEST 1 (A NA B) 50
OBR. 2 BANDWIDTH TEST 2 (B NA A) 50
OBR. 3 TAMOSOFT TEST 1 52
OBR. 4 TAMOSOFT TEST 2 52
OBR. 5 NETIO-GUI TEST 1 54

Seznam použitých tabulek

TAB. 1 PŘEHLED A FUNKCE VRSTEV ISO/OSI 11
TAB. 2 ZRANITELNOSTI DLE RIZIKA A DŮVĚRY 48
TAB. 3 FINANČNÍ ROZVAHA KABELÁŽE 59
TAB. 4 FINANČNÍ ROZVAHA SÍŤOVÝCH PRVKŮ 60

Seznam zkratek:

IS – informační systém

PC – počítač

USB – univerzální sériová sběrnice (moderní způsob připojení periferií k počítači)

ICT – informační a komunikační technologie

GDPR – obecné nařízení o ochraně osobních údajů

EU – Evropská unie

ISO/OSI – standardizace počítačových sítí

CCITT – Mezinárodní telekomunikační unie

ISMS – systém řízení bezpečnosti informaci

Irda – komunikační infračervený port

GAN – globální síť

WAN – rozlehlé síť

MAN – metropolitní síť

CAN – univerzitní síť

LAN – lokální síť

PAN – osobní síť

VLAN – virtuální LAN

VPN – virtuální privátní síť

TCP – Transmission Control Protocol

IP – Internet Protocol

UDP – User Datagram Protocol

UPS – Zdroj nepřerušovaného napájení

AP – Přístupový bod

NAS – Datové úložiště připojené k místní síti LAN

NAT – Překlad síťových adres

PoE – Napájení po datovém síťovém kabelu, bez nutnosti přivést napájecí napětí k přístroji dalším samostatným kabelem

HTML – Textový značkovací jazyk

HTTP – Internetový protokol

HTTPS – Šifrovaný internetový protokol

XML – Rozšiřitelný značkovací jazyk

UTF-7 – Unicode Transformation Format (způsob kódování znaků)

UTF-8 – Unicode Transformation Format (způsob kódování znaků)

EoIP (Ethernet over IP) - protokol MikroTik RouterOS (vytváří ethernetový tunel mezi dvěma routery nad IP připojením)

DHCP – Dynamic Host Configuration Protocol (dynamické přidělování IP adres, masky sítě, implicitní brány a adresy DNS serveru)

DNS – Domain Name Systém

MAC – Media Access Control

SSID – Service Set Identiflier

WEP – Wired Equivalent Privacy

WPA – Wi-Fi procted access, zabezpečení sítě Wi-F

1 Úvod

21. století je považováno za období spojené s evolucí informačních a síťových technologií. Žijeme ve světě, ve kterém nás obklopují digitální technologie, bez kterých si již nedokážeme představit naše životy, jelikož nám ho v mnoha směrech velice usnadňují. V průběhu uplynulých několika desítek let začaly informační systémy a technologie hrát důležitou, někdy i rozhodující roli ve většině oblastech společnosti. Téměř každá organizace je v dnešní době na digitálních technologiích závislá a školy zdaleka nejsou výjimkou.

V souvislosti s rozvojem školského systému a snahou zefektivnit veškeré procesy, spojené s řízením, komunikací i samotnou výukou, stává se mimo jiné stále aktuálnější i problematika budování odpovídajícího bezpečnostního systému ve školách. Nárůst množství dat a informací, které je třeba zpracovávat, přenášet i archivovat, přináší s sebou zvyšující se riziko útoků, zneužití či krádeže a následné zneužití jak hackery, tak i samotnými zaměstnanci nebo studenty. Nedostatečná ochrana dat a zabezpečení systému může ve výsledku způsobit rozsáhlé škody, jelikož ve školních systémech je uchováváno velké množství dat souvisejících jak s osobními údaji zaměstnanců a studentů, tak i například se způsobem výuky a testování na škole. Proto je třeba klást tak velký důraz na bezpečnost školního informačního systému a školních počítačových sítí.

Ke zpracování této diplomové práce byla vybrána škola Vyšší odborná škola ekonomická, sociální a zdravotnická, Obchodní akademie, Střední pedagogická škola a Střední zdravotnická škola, Most, příspěvková organizace v Mostě. Důvodem volby této školy je skutečnost, že tato škola představuje takový školní komplex, který se skládá z jednotlivých budov rozmístěných po celém městě Most. Proto vybraná škola bude vhodným zdrojem informací pro zkoumání optimalizace a zabezpečení propojení lokálních sítí středních škol.

Diplomová práce se zabývá problematikou optimalizace a zabezpečení propojení lokálních sítí středních škol. Práce je rozdělena do pěti hlavních kapitol. V první kapitole bude čtenář seznámen se základními pojmy, termíny a definicemi, které souvisí s počítačovou sítí, jejím rozdělením, topologií a modely. Druhá kapitola se věnuje popisu bezpečnosti a kvalitě informačního systému a charakteristice penetračního testování. V další kapitole jsou

představeny základní normy a legislativy spolu s technickými opatřeními pro školy. Následující kapitola se zabývá bezpečností počítačových sítí, konkrétně ochranou síťové komunikace a kontrolou přístupu.

V praktické části diplomové práce pak bude představena vybraná škola a charakterizována její počítačová síť a informační systémy. Následně pomocí penetračního testování a SWOT analýzy se bude zjišťovat, jaké jsou přednosti a nedostatky stávající počítačové sítě a informačního systému a na základě zjištěných výsledků budou v závěru práce navržena určitá opatření, která povedou ke zlepšení a propojení stávající počítačové sítě a informačního systému ve škole.

Hlavní přínos této diplomové práce spočívá v návrhu opatření ke zlepšení propojení a zabezpečení počítačové sítě a informačního systému a jeho bezpečnostních režimů. Zjištěné závěry budou předloženy managementu školy tak, aby jich bylo možno efektivně využít.

2 Cíl práce

Cílem mé diplomové práce je technická a bezpečnostní analýza informačního systému a počítačové sítě vybrané školy. Jak jsem již v úvodu zmínil, vybraný školní subjekt je komplexem tří budov, které mají objekty s rozdílnou historií, stavebně technickou základnou a jejich správa stojí primárně na podpoře a možnostech zřizovatele. Cílem diplomové práce je zmapování stávajícího stavu funkčnosti a bezpečnosti počítačového prostředí a informačních toků ve škole. Vedení školy aktivně jedná se zřizovatelem o možnostech zdrojů pro investiční záměr pro komplexní modernizaci informačního a bezpečnostního prostředí školy.

Na základě provedené analýzy zpracuji návrh efektivnější formy propojení budov školy v rámci bezpečné integrace informačního systému.

V teoretické části práce je cílem práce seznámit čtenáře s odbornými tématy v oblasti počítačových sítí, informačního systému a zabezpečení a způsoby testování.

Cílem praktické části je aplikovat vstupní informace k dané problematice a z tohoto základu provést analýzu informačního prostředí a vhodně zvolenou formou testování počítačové sítě. V závěru diplomové práce bude z výsledků analýzy a testování navrhnuto vhodné řešení na inovaci počítačové sítě, propojení lokálních sítí odpovídajícím požadavkům dnešních standardů v prostředí bezpečné integrace informačních systémů.

3 Metodika

V diplomové práci byly používány tyto metody:

- testování (test na propustnost sítě a bezpečnostní audit webových stránek)
- analýza (zkoumání jednotlivých složek dané problematiky)
- kompilace (shromažďování souvisejících informací o dané problematice)
- komparace (srovnání)
- řízený rozhovor (tazatel pokládá otázky za účelem sběru dat).

Teoretická část přibližuje základní pojmy z oblasti počítačových sítí a jejich bezpečnosti, z oblasti informačních systémů a způsoby testování informačních systémů. Dále osvětluje problematiku norem a legislativy v informačních systémech, to vše pro nezbytné, k pochopení funkčnosti informačních systémů a fungování počítačových sítí. V této části diplomové práce budu pracovat s metodou komplice.

V praktické části diplomové práce budu realizovat vlastní analýzu informačního systému a testování webových stránek a propojení lokálních sítí. Dále využiji metody popisování, komparace a řízeného rozhovoru s určeným členem vedení školy. Podstatnou metodou této diplomové práce je metoda testování. Jde o tzv. penetrační testování, bandwitch testování, testováním pomocí aplikací TamoSoft a NetIO-GUI a SWOT analýzu. Všechny metodiky použité v diplomové práci povedou k naplnění cíle diplomové práce a stanovení doporučení k návrhu opatření na zlepšení informačního systému zvoleného subjektu.

4 Počítačová síť

Počítačová síť může být definována jako skupina vzájemně propojených výpočetních zařízení (zpravidla počítačů, tiskáren, faxů, scannerů apod.), která slouží ke vzájemné komunikaci, výměně informací a prostředků. [1], [3], [7], [10], [15]

Při pohledu do historie, prvotním nástrojem pro sdílení dat byly off-line přenosové systémy, například disky nebo děrné pásky. S rozvojem technologií přišla i potřeba zvyšování přenosové rychlosti a vzdálenosti, na které se data přenášejí, proto se začaly uvádět systémy on-line. Nejprve byly vybudovány centralizované sítě, které fungovaly na principu propojení přes jeden, centrální počítač. V dnešní době většina sítí, včetně internetu, jsou sítě decentralizované neboli nezávislé na jednom počítači. [1], [3], [7], [10], [15]

Základními prvky počítačových sítí jsou:

- počítače – pracovní stanice nebo servery
- síťový adaptér – zařízení (nejčastěji karta), umožňující připojení počítače do počítačové sítě
- komponenty umožňující propojení – přenosová média (optický kabel, kroucená dvoulinka, koaxiální kabel apod.), pasivní prvky (konektory, zásuvky) a aktivní prvky sítě (přepínač, směrovač, most atd.)
- software – operační systém, který umožňuje sdílení a přístup počítačů do sítě
- komunikační protokoly – společná sada pravidel, která definuje způsob komunikace v síti

4.1 Rozdělení počítačových sítí

Tato část práce se věnuje rozdělení počítačových sítí podle různých kritérií, která jsou podrobněji popsána v následujících kapitolách. [1], [3], [7], [10], [15]

Rozdělení pomocí použitého hardware

- homogenní – počítače mají stejný operační systém a používají stejný komunikační protokol, v dnešní době jsou málo používané.
- nehomogenní – zařízení, která využívají rozdílné operační systémy a používají různé přenosové protokoly. Většina sítí včetně internetu dnešní doby jsou nehomogenní.

Podle druhu připojení:

- client-to-server jsou sítě, které mají přesně definovanou funkci jednotlivých zařízení, v těchto sítích probíhá většina komunikace přímo mezi serverem a klientem. Tento typ je bezpečnější, ale náročnější na přenosové kapacity a rychlosti.
- peer-to-peer sítě umožňují klientům působit nejen jako klient, ale i jako server, a proto funkce jednotlivých počítačů není přesně vyhraněná. Výhodou je odlehčení zatížení serverů tím, že je zátěž rozložena mezi jednotlivé klienty.

Rozdělení podle způsobu připojení

- metalické připojení pomocí drátových kabelů, patří k těm levnějším a nejběžnějším a je využíváno pro připojení koncových zařízení v pevných rozvodech sítí, zejména v budovách. Nevýhodou jsou nižší přenosové rychlosti a omezení maximální délky kabelu pro spolehlivý přenos.
- optické připojení je spojení pomocí optických kabelů a řeší nevýhody metalického připojení, vyžaduje však zpravidla vyšší náklady.
- Bezdrátové připojení je využíváno zejména při mobilním připojení, příkladem je Wi-Fi, bluetooth, radiové vlny, IrDA apod.

4.2 Rozdělení počítačových sítí podle velikosti

Tato kapitola se věnuje rozdělení počítačových sítí podle velikosti, jelikož toto rozdělení patří k těm nejpodstatnějším.

GAN – Global Area Networks

Jedná se o globální a nejrozsáhlejší počítačovou síť, která využívá satelitů a bezdrátových technologií. Klasickým příkladem sítě GAN je internet. [1], [3], [7], [10], [15]

WAN – Wide Area Networks

Rozlehlé počítačové sítě často vznikají spojením několika lokálních (LAN) sítí do jednoho celku a jedná se o komunikační síť, která je tvořena počítači. [1], [3], [7], [10], [15]

MAN – Metropolitan Area Networks

Metropolitní sítě jsou mezistupeň mezi sítěmi LAN a WAN. Představují sítě o rozsahu města. Příkladem může být pražská akademická síť PASNET propojující jednotlivé vysoké školy v Praze. [1], [3], [7], [10], [15]

CAN – Campus Area Network

Univerzitní sítě jsou speciálním typem MAN sítí, které jsou omezené na prostory v rámci školy nebo korporace. Zahrnují propojení jednotlivých fakult, knihovny, administrativních budov, kolejí, jídelny. Síť bývá nejčastěji ve vlastnictví určité univerzity nebo organizace. Příkladem může být Googleplex nebo kampus Microsoftu. [1], [3], [7], [10], [15]

LAN – Local Area Networks

Lokální počítačové sítě jsou určeny pro místní použití v rozsahu několika desítek či stovek metrů, například ve firmách, institucích nebo v domácnostech. Uživatelé si je často budují sami na své náklady a využívají se pro sdílení internetového připojení, prostoru na disku, tiskáren, scannerů apod. [1], [3], [7], [10], [15]

PAN – Personal Area Network

Osobní sítě jsou rozsahově nejmenší a v praxi znamenají propojení počítače, chytrého mobilního telefonu nebo notebooku do sítě v blízkosti jedné osoby, tedy jen do několika metrů. Tyto spojení mohou být buď drátové pomocí USB popř. FireWire nebo bezdrátové prostřednictvím Wi-Fi, Bluetooth nebo IrDA připojení. [1], [3], [7], [10], [15]

4.3 Speciální druhy sítí

Mezi speciální druhy sítí patří sítě VLAN a VPN, které jsou charakterizovány kapitole následovně:

Virtuální lokální síť – VLAN

Virtuální lokální síť slouží k logickému rozdělení sítě nezávisle na tom, jak je poskládána fyzicky. Umožňuje například rozdělení LAN sítě na několik menších podsítí, aniž by bylo potřeba přemisťovat kabely nebo fyzicky měnit topologii. Účelem implementace této sítě je zvýšení výkonu a bezpečnosti sítě a také lepší správa zařízení, kdy je možné jednu síť ještě rozdělit podle různých oddělení ve firmě na účetní, ekonomické, marketing apod. [[1], [3], [7], [10], [15]

Virtuální privátní síť – VPN

Virtuální privátní sítě umožňují propojení více počítačů připojených v rozdílných sítích do jedné privátní sítě prostřednictvím počítačové sítě jako je např. internet. Zařízení v takových sítích spolu mohou komunikovat tak, jako by byly v jedné uzavřené (privátní) síti. Komunikace je šifrována a identita všech zařízení je ověřována pomocí digitálních certifikátů a autentizace, proto lze síť VPN považovat za bezpečnou. Typickým příkladem z praxe je připojení zaměstnanců firmy do firemního intranetu z domova. [1], [3], [7], [10], [15]

4.4 Topologie počítačových sítí

Topologie počítačové sítě se zabývá rozmístěním počítačové sítě a jejích komponent a zachycením její fyzické nebo virtuální podoby. Topologii je možné si představit jako určitý tvar či strukturu dané sítě. Existují tři základní druhy topologií – fyzická, logická a signálová. Podrobněji se tato kapitola věnuje fyzické topologii.

Fyzická topologie se zabývá zejména fyzickým rozmístěním sítě, to znamená kabeláží a propojením jednotlivých stanic. Do této kategorie spadá sběrnice, kruh, hvězda, strom a mesh topologie. [1], [3], [7], [10], [13], [15], [20]

Sběrnicová topologie (BUS)

Sběrnicová topologie je realizována pomocí jednoho souvislého úseku kabelu (backbone) na který se připojují ostatní zařízení pomocí spojek nebo odboček. Zakončení této sítě je realizováno pomocí terminátorů, které zabraňují zpětnému odražení signálu. Informace vyslaná z jednoho zařízení je vyslána ke všem zařízením současně, ale pouze adresát může tuto informaci zpracovat. [1], [3], [7], [10], [13], [15], [20]

Kruhová topologie (Ring)

Kruhová topologie je uspořádána tak, že jednotlivé stanice jsou navzájem propojeny a tvoří uzavřený kruh. Data v této síti obíhají od vysílajícího zařízení přes všechny ostatní zařízení v síti a mohou si je přečíst jen ty stanice, kterým jsou určena. Výhodou je jednoduchá rozšiřitelnost a snadné vysílání zpráv. Nevýhodou je, že při porušení některého zařízení nebo kabelu vypadne celá sít. [1], [3], [7], [10], [13], [15], [20]

Hvězdicová topologie (Star)

Hvězdicová topologie se skládá ze samostatných kabelů, které vedou od jednoho zařízení k rozbočovači (HUB) nebo přepínači (SWITCH). V přepínači (SWITCH) se pak data nasměrují ke správnému adresátovi. V rozbočovači (HUB) se data posílají k dispozici i ostatním stanicím, pro které nejsou určeny, ale přečíst si je může jen adresát. Výhodou je nezávislost na výpadku jednotlivých prvků, naopak jedinou slabinou může být centrální prvek, na kterém závisí funkčnost celé sítě. [1], [3], [7], [10], [13], [15], [20]

Stromová topologie

Stromová topologie je složená z několika hvězdicových topologií, které jsou vzájemně propojeny rozbočovači (HUB) nebo přepínači (SWITCH). [1], [3], [7], [10], [13], [15], [20]

Mesh topologie

Mesh topologie nebo také sítová, smyčková, pletivová nebo úplná topologie. Jedná se o topologii, v které je každé zařízení propojené s každým (full mesh) nebo může být použita alternativa, kdy se některé spoje vynechají (částečný mesh). [1], [3], [7], [10], [13], [15], [20]

4.5 Referenční model ISO/OSI

V dnešní době je nejpoužívanějším standardem v počítačových sítích referenční model ISO/OSI (často také označován RM ISO/OSI). Zkratky ISO patří standardizační organizaci, která normu vydala, tedy International Organization for Standardization a OSI je zkratka z anglického Open System Interconnection neboli propojování otevřených systémů. Tento model byl přijat v roce 1979 jako norma standardizační organizace ISO a posléze i jako doporučení X. 200 společnost CCITT. Tento model se skládá ze sedmi vrstev. [3], [7], [10], [13], [15], [20]

RM ISO/OSI zahrnuje základní pojmy, mezi které patří vrstva, entita, protokol a služba. Vrstva je přesně definována určitou funkcí a vždy sousedí s vrstvou nižší a vyšší. Výjimkami jsou vrstva nejvyšší (aplikační), která sousedí přímo s aplikačním procesem a vrstva nejnižší (fyzická), která sdílí rozhraní přímo s fyzickým médiem. Entita je objektem, který v dané vrstvě vykonává konkrétní činnost. Ve vrstvách vyšších se jedná o software, ve vrstvách nižších jde o hardware. Komunikace mezi entitami v odpovídajících vrstvách je realizována pomocí pravidel, které se nazývají protokoly a pro činnosti uvnitř entity využívají služby nižší vrstvy a poskytují služby vrstvě vyšší. Přehled všech sedmi vrstev RM ISO/OSI spolu s jejich funkcí je uveden v tabulce 1. [3], [7], [10], [13], [15], [20]

Tab. 1 Přehled a funkce vrstev ISO/OSI

Název vrstvy	**Funkce vrstvy**
Aplikační	Vytvoření zprávy v aplikaci.
Prezentační	Převedení zprávy do srozumitelného formátu pro příjemce.
Relační	Vytvoření spojení s příjemcem a jeho údržba.
Transportní	Dohled nad spolehlivým přenosem zpráv, opravy chyb, vytvoření packetů.
Síťová	Vytvoření trasy a opatření packetů adresami a dalšími náležitostmi.
Linková	Vytvoření rámců a jejich vysílání.
Fyzická	Přenos bitů elektrickými nebo optickými signály.

4.6 **Model TCP/IP**

Dalším velmi známým modelem, který se užívá v počítačových sítí, je model TCP/IP. Zkratka TCP znamená Transport Control Protocol a IP je zkratkou pro Internet protocol. Rodina protokolů TCP/IP se skládá ze čtyř vrstev a pro formát přenosu a dat známe tři různé protokoly. Jsou to protokoly TCP a IP, zmiňované výše, a třetím protokolem je protokol UDP, který popisuje nespojovanou komunikaci. Protokoly TCP a UDP fungují v transportní vrstvě, protokol IP je pak hlavním protokolem síťové vrstvy. [3], [7], [10], [13], [15], [20]

TCP/IP rozeznává ve svém komunikačním modelu celkem čtyři vrstvy:

- aplikační vrstva
- transportní vrstva
- internetová vrstva
- vrstva síťového rozhraní.

Na aplikační vrstvě najdeme software, s nímž je v přímém spojení koncový uživatel. Mezi programy aplikační vrstvy patří webové prohlížeče, e-mailoví klienti, příkazové řádky, kancelářské balíky. [3], [7], [10], [13], [15], [20]

Transportní vrstva slouží k provedení spolehlivého a spojovaného přenosu. Protokol UDP je zodpovědný za rozdělení odeslaných a přijímaných dat v rámci jednoho uzlu. TCP protokol funguje jako spolehlivá a spojovaná služba, která zajišťuje správné doručení dat. [3], [7], [10], [13], [15], [20]

Hlavním protokolem internetové vrstvy je IP protokol, který má na starosti přenos dat ve formě IP-packetů a je pro něj charakteristické, že pracuje nespojovaně a nespolehlivě, což v důsledku může znamenat doručení dat příjemci v různém pořadí a v poškozené formě. [3], [7], [10], [13], [15], [20]

Vrstva síťového rozhraní zajišťuje fyzickou komunikaci uzlů sítě. Cílem této vrstvy je zakrýt odlišnosti různých přenosových technologií a topologií sítě a nabídnout jednotné prostředí, služby, způsob zpracování.[3], [7], [10], [13], [15], [20]

Protokol TCP

TCP protokol (Transmition Control Protocol) je jedním ze základní sady protokolů internetu a typicky představuje transportní vrstvu komunikace. Je určen k vytvoření spojení pro přenos dat mezi aplikacemi na počítačích zapojených do počítačové sítě. Další funkcí TCP protokolu je rozlišování dat pro vícenásobné, současně běžící aplikace (například webový server a e-mailový server) běžící na stejném počítači. TCP podporuje na internetu mnoho aplikačních

protokolů a aplikací, včetně WWW, elektronické pošty a SSH (Secure Shell). [3], [7], [10], [13], [15], [20]

Protokol IP

IP protokol (Internet Protocol) je datový protokol, který je určen k přenosu dat přes paketové sítě. Data se pomocí IP posílají sítí po blocích nazývaných datagramy, což je datový paket pro prostředí protokolu IP. IP protokol v doručování datagramů poskytuje nespolehlivou službu, všechny stroje na trase se datagram snaží podle svých možností poslat blíže k cíli, ale nezaručuje praktické doručení do cíle. [3], [7], [10], [13], [15], [20]

4.7 Hardware sítě

Z hlediska aktivity můžeme prvky sítě rozdělit na aktivní a pasivní. Aktivní prvky se aktivně podílí na komunikaci v síti a vykonávají určitou aktivní činnost s datovým signálem. Do této skupiny prvků patří směrovač, přepínač, síťová karta apod. Pasivní prvky se na komunikaci podílejí pouze pasivně a většinou na svůj provoz nepotřebují ani napájení. Typickým příkladem jsou propojovací kabely, konektory, pasivní rozbočovač (hub) v síti Token Ring. [10], [13], [15], [24]

4.7.1 Aktivní prvky

Aktivní prvky vykonávají takové činnosti, jako je regenerace, zesílení, oprava či modifikace přenášeného signálu. Z hlediska funkcí můžeme aktivní prvky rozdělit na prvky základní, která nedokážou vysvětlit význam dat, například opakovač. Druhou skupinou jsou prvky „chytřejší“, která dokážou interpretovat přenášená data a následně tomu také přizpůsobit své chování. Příkladem může být směřovač, který směruje data, nebo přepínač, který má na starosti posílání dat do určité podsítě. [10], [13], [15], [24]

Rozbočovač (hub)

Rozbočovač je nezbytnou součástí počítačové sítě s hvězdicovou topologií. Pracuje na první vrstvě RM ISO/OSI a je zodpovědný za regeneraci přijatého signálu a jeho následné rozesílání

na všechny porty, na které je někdo připojen. Lze říci, že je to v podstatě opakovač s více porty a právě počet těchto portů bývá jedním z parametrů rozbočovače. Minimálně jsou čtyři, ale zpravidla jich bývá více, 8, 16, 24, 32 atd. Jelikož existují různé typy portů pro různé konektory, lze kombinovat různé druhy přenosových médií v jediné počítačové síti. Nevýhodou je přetížení jednotlivých segmentů přenášenými daty. To je důvod, proč jsou rozbočovače stále méně používány a nahrazují je zařízení typu přepínač. [10], [13], [15], [24]

Přepínač (SWITCH)

Přepínače pracují na druhé, linkové vrstvě RM ISO/OSI a mají obdobnou funkci jako rozbočovače s tím rozdílem, že přepínač zpravidla propojí jen dvojici portů (výjimkou jsou pouze vícesměrové a všesměrové vysílání a tzv. učení). Tyto dvojice portů tak mají k dispozici plnou přenosovou rychlost a data se zbytečně neposílají jiným uzlům. [10], [13], [15], [24]

Učební proces přepínačů je automatický, typicky z procházejícího provozu a fyzických (MAC) adres koncových zařízení. K tomuto učení používají tzv. zpětný učící algoritmus (Backward Learning Algorithm), díky němuž vychází ze své vnitřní tabulky, kde jsou uloženy MAC adresy připojených zařízení a pokud přijdou data pro nějaké zařízení, které tam ještě nemá, chová se jako rozbočovač (pošle je do všech segmentů) a předpokládá, že přijímací zařízení se ozve. Poté si jeho adresu uloží a příště už ví, kam mají být data poslána. [10], [13], [15], [24]

Směrovač (ROUTER)

Směrovač neboli router, je považován za nejinteligentnější zařízení z dosud jmenovaných. Je učen ke spojování sítě na třetí, síťové, vrstvě modelu ISO/OSI a musí znát skutečnou topologii sítě. Směrovač propojuje jakékoliv dvě sítě, na rozdíl od přepínače, který propojuje počítače pouze v místní síti. Je často používán v sítích WAN a také pro připojení lokální sítě k internetu. V malých sítích bývá často jako směrovač používán počítač (zpravidla server) se softwarovou podporou síťování. Ve vysokorychlostních sítích se používají speciální počítače se specifickým hardwarem nebo speciální směrovače podporující specializované funkce, které jsou používány při směrování. [10], [13], [15], [24]

4.7.2 Pasivní prvky

Jak již bylo uvedeno výše, pasivní síťové prvky jsou takové, které se aktivně nepodílí na síťové komunikaci. Nejčastěji se jedná o konektory, zásuvky a přenosová média. [7], [10], [13], [15], [24], [26]

Kroucená dvoulinka

Kroucená dvojlinka představuje svazek vodičů, typicky osmi, které jsou vždy spleteny v páru. Oba vodiče jsou v rovnocenné pozici a signál přenášení po vedení je dán rozdílem potenciálů obou vodičů, proto je toto vedení také označováno jako symetrické. Vodiče jsou zkrouceny v párech z toho důvodu, že jsou zlepšeny elektrické vlastnosti kabelu, což znamená že jsou minimalizovány přeslechy mezi jednotlivými páry a snižuje se vliv vodičů na okolí a z okolí. [7], [10], [13], [15], [24], [26]

Kroucená dvojlinka se dělí do tzv. kategorií:

- Kategorie 1 – není určena k datovým přenosům, používá se hlavně k telefonním rozvodům ať už analogovým, tak i ISDN apod. Přenosové rychlosti jsou do 1 Mb/s.
- Kategorie 2 – je již určena pro přenos dat s maximální šířkou pásma 1,5 MHz. Používá se pro digitální přenos zvuku a přenosové rychlosti jsou kolem 4 Mb/s.
- Kategorie 3 – asi nejpoužívanější rozvody určené pro přenos dat a hlasu s šířkou pásma 16 MHz a přenosovou rychlostí do 10 Mb/s.
- Kategorie 4 – určena pro přenos dat v síti Token ring, má šířku pásma 20 MHz a přenosovou rychlost do 16 Mb/s.
- Kategorie 5 – tato kategorie pracuje se šířkou pásma 100 MHz a je určena pro rozvody počítačových sítí s rychlostí do 100 Mb/s nebo 1 Gb/s při využití všech 8 vláken.
- Kategorie 5E – nahrazuje předchozí kategorii, pracuje taktéž s šířkou pásma 100 MHz, ale jsou na ni kladeny přísnější parametry s cílem využití v 1Gb/s sítích.
- Kategorie 6 – tato kategorie pracuje s šířkou pásma 250 MHz a využívá se pro ultrarychlé páteřní rozvody v lokálních sítích. V dnešní době je to nejpoužívanější rozvod v nových budovách.
- Kategorie 6E – pracuje se s šířkou pásma 500 MHz a využívá se pro superrychlé rozvody s rychlostí do 10 Gb/s

- Kategorie 7 – využívá šířku pásma 600 MHz s rychlostí do 10 Gb/s a každý pár je samostatně stíněn a používá se pro přenosy plné šířky videa. Zatím se na této technologii pouze provádí pokusy a běžně se nepoužívá
- Kategorie 7A – využívá šířku pásma 600 MHz s rychlostí do 10 Gb/s a každý pár je dvojité stínění. Zatím se na této technologii pouze provádí pokusy a běžně se nepoužívá
- Kategorie 8 – pracuje se s šířkou pásma až 2000 MHz a s rychlostí od 25 Gb/s do 40 Gb/s. Je omezen na 30 metrů. Zatím se na této technologii běžně se nepoužívá, protože by aktivní prvky museli splňovat certifikaci.

Další dělení kroucené dvojlinky ve výše uvedených kategoriích je podle stínění na:

- nestíněné (angl. Unshielded Twisted Pair – UTP), kde není žádné dodatečné stínění, pouze zapletení kabelů po dvojicích
- stíněné, kde stínění je prováděno buď tím, že každá zkroucená dvojice je zapletena do folie (angl. Shielded Twisted Pair – STP), nebo celý kabel je stíněn vodivou folií (angl. Foiled Twisted Pair – FTP), popř. kombinací stínění páru i celé dvojice (angl. Screened Shielded Twisted Pair – S/STP). [7], [10], [13], [15], [24], [26]

Výhodou kroucené dvojlinky je snadné připojení jednotlivých zařízení, možnost využití například i pro telefonní rozvody, snadná instalace a nízká cena. Mezi nedostatky patří to, že stíněný kabel je silnější a náročněji se s ním pracuje, u nestíněného je horší EMS než např. u koaxiálního kabelu. [7], [10], [13], [15], [24], [26]

Optický kabel

Optické kabely jsou v praxi často označovány jako Fiber-Optic (FO). Vysílač (označován Tx), zpravidla LED nebo laserová dioda, má na starosti přenos elektrických signálů na světelné impulsy a přijímač (Rx) je složen z fotodetektoru, který převádí optický signál do elektrického tvaru, zesilovače, který signál zesiluje a převádí do tvaru připraveného ke zpracování a procesoru, je převádí původní signál na signál elektrický, přičemž dochází ke změně kódování. Optické vedení je tvořeno svazkem optických vláken, které mají rozdílné rozměry, složení a vlnové délky, které mohou přenášet. [7], [10], [13], [15], [24], [26]

Optická vlákna lze rozdělit na jednovidová a mnohavidová. Jednovidová (angl. singlemode) vlákna jsou charakteristická tím, že mají velmi tenké jádro (méně než 10 μm) a světlo může v jádru postupovat jen jednou cestou, má velký útlum, při instalaci vyžaduje větší přesnost a přenosové rychlosti jsou až 50 Gb/s. Umožňují přenos až na 100 km bez opakovače, ale jsou dražší než mnohavidová. Mnohavidová (angl. Multimode) vlákna jsou širší než jednovidová, světelný paprsek tak má více prostoru a má možnost probíhat v jádru více cestami, což ale může vést k rušení signálu na straně přijímače. Je pro ně typické, že se snáze spojují, jsou levnější než jednovidová, ale nejvyšších rychlostí dosahují do vzdálenosti 1 km od vysílače. [7], [10], [13], [15], [24], [26]

Konektory a zásuvky

Do skupiny pasivních prvků spadají i konektory a zásuvky. Konektor je zařízení na konci síťového média, které je připojené na straně síťového uzlu do síťové karty a na straně druhé buď do aktivního síťového prvku nebo do zásuvky, v případě strukturovaného kabelového rozvodu v budovách. [9], [10], [26]

Kroucená dvojlinka používá konektor RJ-45, který je také označován jako 8P8C (8 Position 8 Contact). Existuje velké množství typů konektorů pro optické kabely, nejčastěji používanými jsou konektory SC, ST s bajonetovým závitem a LC. [9], [10], [26]

4.8 Server

Server představuje instanci počítačového programu, který přijímá a reaguje na požadavky jiného programu, známého jako klient. Lze říct, že každé zařízení, které spouští serverový software, může být považováno za server. Servery se používají ke správě síťových zdrojů. [13], [15], [24]

Servery mohou být označovány jako vyhrazené nebo sdílené. Za vyhrazené servery jsou považovány tiskové servery, souborové servery, síťové servery a databázové servery. Pro sdílené servery je typické, že mohou v případě webového serveru převzít zodpovědnost s emailem, DNS, FTP, a dokonce s několika webovými stránkami. [13], [15], [24]

Servery jsou běžně využívány k poskytování nepřetržitě požadovaných služeb, proto se nikdy nevypínají. To je důvod, proč selhání serverů může způsobit mnoho problémů pro uživatelé sítě a společnosti. Servery jsou typicky prvotřídní počítače, které jsou nastavené jako tolerantní k určitým chybám. [13], [15], [24]

NAS server

Network Attached Storage (NAS) fungují jako datová úložiště, která jsou připojená k síti LAN. Úložiště NAS jsou přístupné přes zmapované síťové ovladače, kde probíhá komunikace se serverem a klientem přes síťový souborový systém nebo běžný internetový souborový systém prostřednictvím IP protokolu. Technologie serveru je spolehlivá a jednoduchá pro webovou administraci. Do NAS lze pořídit externí disky, které je možné zapojit do diskového RAID pole a následkem takového zapojení je nižší spotřeba a kompaktní velikost, která ovšem záleží na počtu disků. Síťové úložiště NAS poskytuje služby jako HTTP server, FTP server nebo Print server. [5], [11]

RAID pole

RAID (Redundant Array of Independent Disks) je označení metody, která se využívá pro zabezpečení dat proti selhání pevného disku. Zabezpečení je realizováno na principu ukládání dat na více disků, které jsou na sobě nezávislé, proto jsou data zachována i v případě selhání některého z nich. Skupina pevných disků se nazývá diskové pole. Disky, které pracují společně v konfiguraci RAID, jsou označovány jako jednotka RAID nebo pole RAID. V systému se více disků v jednotce RAID zobrazí jako jedna logická jednotka. Mezi výhody tohoto pole patří zvýšená kapacita úložiště a potenciální sdílení více fyzických nebo logických pevných disků, aby se zajistila celistvost a dostupnost dat. [5], [11]

4.9 Internet a zabezpečení sítě

Internet je komplexní globální síť, která se skládá z propojených počítačových sítí umožňující komunikaci mezi počítači pomocí rodiny protokolů TCP/IP. S rozšířeným používáním internetu

úzce souvisí zabezpečení počítačových sítí, aby se zabránilo útokům, neoprávněnému přístupu, zneužití nebo zamítnutí počítačové sítě v síti přístupových zařízení.

Existuje řada možností zabezpečení a mezi ty nejběžnější patří SSD, Filtr MAC adres, WEP a WPA protokol. [6] [13], [24]

SSID

SSID je jménem sítě WLAN a stanice ho musí znát pro přístup do této sítě. AP neboli přístupový bod (access point) pravidelně vysílá rámec (beacon frame) obsahující toto SSID, a tak je snadné běžnými přístroji toto SSID zjistit. Principem této formy zabezpečení je skrytí SSID, které v důsledku zabrání AP vysílat identifikátor SSIS. Metoda SSID je považována za velmi slabou formu zabezpečení, jelikož je možné identifikátor SSIS lehce odposlechnout.

U některých AP lze vypnout broadcast vysílání SSID. [6] [13], [24]

Filtr MAC adres

Administrátor WLAN může pro AP vytvořit seznam MAC adres, které s ním mohou komunikovat. Přístup je následně povolen pouze předem schváleným MAC adresám. Tato metoda je velice jednoduchá, ovšem nepraktická pro sítě větších rozměrů a je neúčinná, jelikož MAC adresu adaptéru lze snadno změnit. Navíc MAC adresu může útočník snadno odposlechnout a následně se přihlásit do sítě. [6] [13], [24]

Protokol WEP

Protokol WEP (Wired Equivalent Privacy neboli soukromí ekvivalentní s kabelovým přenosem) poskytuje šifrování dat v rámcích 802.11 s pomocí symetrické šifry RC4. Pracuje se 40bitovými nebo 104bitovými klíči a jedná se o algoritmus proudového šifrování dat v bezdrátovém spojení. Přítomnost šifry je indikována bitem WEP v poli FS (Field Control) záhlaví rámce 802.11. WEP se považuje za relativně slabou úroveň ochrany, protože jeho šifrovací mechanismus je možné úspěšně napadnout. [13], [15], [24]

Protokol WPA

Protokoly WPA (Wi-Fi Protected Access, chráněný přístup k Wi-Fi) a WPA2 jsou nejaktuálnější generací protokolů pro šifrování a autentizaci sítí 802.11x. Řeší některé

problémy protokolu WEP tím způsobem, že zavádějí generování klíčů mechanismem TKIP (Temporary Key Integrity Protocol, protokol dočasné integrity klíčů). V rámci TKIP se používá 48bitový inicializační vektor IV a 128bitový šifrovací klíč, s jejichž pomocí je vygenerován nový klíč pro každý přenášený paket. Naopak WEP používal stejný klíč pro všechny pakety.

Pokud je v akci WPA, oba koncové body spojení mají stejný sdílený klíč (PSK, Pre-Shared Key). Z toho důvodu tento klíč nelze odečíst z komunikace, a WPA je proto mnohem bezpečnější. [13], [15], [24]

WPA2 je úplným uskutečněním požadavků na bezpečnostní standard 802.11i. Všechna zařízení splňující normu pro WPA2 jsou povinně označena obchodní známkou s logem Wi-Fi. Protokol CCMP (Cipher Block Chaining Message Authentication Code Protocol) a jeho opačný režim (Counter Mode) jsou součástí WPA2. Je využíván šifrovací algoritmus AES (Advanced Encryption Standard, pokročilý šifrovací standard). [13], [15], [24]

5 Informační systém

Informační systémy jsou úzce spojeny s příchodem nových technologií a digitální transformací, která má za cíl nahradit tradiční metodiky metodikami novými a více efektivními. IS je systém pro sběr, přenos, uchování, zpracování a poskytování informací. Obecně lze IS chápat jako uspořádání vzájemné propojených informací a procesů. Jinými slovy je infomační systém softwarovým vybavením organizace, které řídí procesy na základě získaných informací. Nezbytnou součástí provozu každé organizace jsou informace, které jsou nejprve získávány z různých zdrojů a následně zpracovávány za konkrétním účelem. Informační systém je určen zejména k efektivnímu řízení na všech úrovních podniku, koordinaci a organizaci těchto informací a usnadnění procesů práce s nimi. [6], [25], [27]

Pojem informační systém v sobě zahrnuje jak programové vybavení společnosti, tak i hardware, firemní politiku, normy a lidskou složku. Efektivita IS proto závisí nejen na správném výběru a implementaci vhodného systému, ale i na zaměstnancích, kteří s těmito systémy pracují. Mezi aspekty, které mohou ovlivnit vývoz a provoz IS, patří například aspekty organizační, ekonomické, právní nebo sociální. [6], [25], [27]

5.1 Bezpečnost a kvalita IS

5.1.1 Bezpečnost IS

Informace jsou v dnešní době velice cenné a neexistuje organizace, která by nějakými důležitými informacemi nedisponovala. Pojem informace je definován jako aktivum, které obsahuje data důležitá pro danou organizaci. Může se jednat o osobní údaje zaměstnanců, informace o zákaznících nebo know-how. Společné mají však to, že je potřeba je chránit, proto jednou z priorit informačních systému je zajištění jejich ochrany a bezpečnosti před kybernetickými útoky. [6], [22], [23]

Pojem bezpečnost představuje ochranu informačních systémů a informací, které jsou v nich uchovávány a zpracovávány. Bezpečnost informací je určena třemi hlavními faktory: důvěrností, dostupností a integritou informací. Ochrana důvěrnosti znamená ochranu před

neoprávněným vniknutím do IS, tedy zajištění přístupu k informacím pouze oprávněným osobám. Zajištění dostupnosti je zajištění včasného přístupu do IS a že autorizovaným osobám nebude přístup odmítnut. Ochrana integrity je zabezpečení přesnosti a kompletnosti informace a metod jejího zpracování. [6], [22], [23]

5.1.2 **Kvalita IS**

Pro zhodnocení kvality zabezpečení počítačových zařízení nebo systému se používají různé testovací metody za pomocí bezpečnostních testů. Bezpečnostní testy fungují na principu simulace reálného pokusu o kompromitaci IS s cílem zjistit, jaké škody by mohly nastat nebo jaké informace by mohli uniknout. [6], [25], [27]

Jedním ze základních typů bezpečnostních testů jsou penetrační testy. Cílem penetračního testu je prověřit a zhodnotit úroveň zabezpečení. Využívají se například pro určení zneužitelnosti, odhalení bezpečnostních nedostatků, testování schopnosti odhalovat a reagovat na útoky. Mezi další typy testů patří unit testy, integrační testy, funkční testy nebo zátěžové testy. [6], [25], [27]

5.1.3 **Autentizace**

Autentizace je hlavním prvkem v ochraně informací před útoky. Představuje proces ověřování pravosti identity, který je nezbytný pro přidělení určitých práv pro výkon dané činnosti. Tento proces zahrnuje porovnávání jednoho nebo více faktorů s databází platných identit. Procesu autentizace předchází proces identifikace, ve kterém se potvrdí, zda je uživatel skutečně tím, za koho se vydává. Identifikace a autentizace představují dva nezbytné kroky, které musí být provedeny společně a jeden bez druhého by ztratily význam. [6], [25], [27]

Autentizační metody lze rozdělit do tří základních kategorií. Volba konkrétní metody pak závisí na mnoha faktorech, například na ceně a jednoduchosti nasazení, náročnosti pro uživatele, míře bezpečnosti, spolehlivosti. V případech, kdy je potřeba vysoká míra zabezpečení, lze využít kombinace dvou a více přístupu a jedná se o vícefaktorovou autentizaci. [6], [25], [27]

Důkaz znalostí

Tento způsob spočívá v tom, že uživatel musí být vybaven určitou znalostí, například heslem, PIN kódem, frází a předpokládá se, že nikdo jiný tuto znalost nemá. Mezi nedostatky tohoto způsobu patří riziko zapomenutí či odcizení hesla. Výhodou jsou minimální náklady na implementaci této metody. [6], [22], [23], [25], [27]

Důkaz vlastnictvím

Tento způsob je založen na tom, že uživatel vlastní fyzický předmět, který přiloží nebo vloží do čtecího zařízení. Fyzický předmět může mít podobu čipové karty, flash disku, osobního dokladu. Ve spojení s tímto přístupem se často využívá dvoufaktorové autentizace, kombinace znalosti a vlastnictví předmětu. Mezi přednosti této metody patří vysoká míra bezpečnosti. Nevýhodou je riziko porouchání čtecího zařízení nebo ztráty daného fyzického předmětu. [6], [22], [23], [25], [27]

Důkaz vlastností

Tento způsob představuje důkaz lidskou vlastností a souvisí s biometrií, která je založena na předpokladu, že každý člověk má jedinečné tělesné charakteristiky. Do této kategorie spadají otisky prstů, hlas, sken oční duhovky nebo sítnice, geometrie ruky. Výhodou je nemožnost ztráty, zapomenutí či odcizení těchto biometrických charakteristik a jedná se o nejbezpečnější metodu autentizace. Nedostatkem je to, že je třeba počítat s určitou chybovostí, například hlasová identifikace může být ovlivněna hlukem z okolí nebo otisk prstu může být ovlivněn vlhkostí prstu. Zároveň tato metoda je spojená s rizikem oklamání biometrického snímače nahrávkou hlasu či fotografií oka někoho jiného a náklady spojené s nasazením této metody jsou vyšší než u předchozích dvou. [6], [22], [23], [25], [27]

5.2 Penetrační testy

Penetrační test představuje metodu, která slouží ke zhodnocení zabezpečení počítačových zařízení, systémů a aplikací. Provedení samotného testu je založeno na simulaci možných útoků mířících na určitý systém, které mohou být jak zvenčí, tak i zevnitř. Proto penetrační testy zahrnují následující dvě hlediska:

- analýza zabezpečení systému z hlediska jeho vnějšího narušení z prostředí internetu nebo jiných sítí, ke kterým je organizace připojena
- analýza bezpečnosti systému proti potencionálnímu narušiteli, který se nachází v prostředí organizace, například zaměstnanec organizace.

Cílem penetračních testů je prověření a zhodnocení úrovně zabezpečení, odhalení zranitelnosti cílového informačního systému a následné podání zprávy (reportu) na úrovni technických i organizačních opatření, která bude obsahovat doporučení vedoucí k nápravě. Tyto výsledky by měly zahrnovat také informace ohledně reálných dopadech jednotlivých chyb jak na samotný systém, tak i na jeho vlastníky. Zároveň by měla být poskytnuta doporučení možných protiopatření, která by měla ve výsledku zmírnit rizika týkající se prolomení systému. [6], [23], [25], [27]

Mezi další cíle penetračních testů se řadí také poskytnutí uceleného přehledu o stavu zabezpečení infrastruktury a aplikačního prostředí, který může být využit jako vstup pro analýzu rizik. [6], [23], [25], [27]

Celkové výsledné využití penetračních testů je následující:

- určují zneužitelnost systému
- odhalují velké bezpečnostní nedostatky, které mohou být výsledkem nahromaděním menších nedostatku dosažených v určité sekvenci
- odhalují nedostatky, které mohou být nezjistitelné pomocí automatické detekce systémových chyb
- posuzují možné dopady na organizaci
- testují schopnost obranných prvků systému odhalovat aktuální útoky a následně na ně reagovat
- poskytují podklady podporující zvýšené náklady na vývoj zabezpečení systému.

V současné době existuje velké množství způsobů, jak mnohou být informační systémy napadeny. Z důvodu stále se zvyšující se komplexnosti operačních systémů a aplikačního programového vybavení dochází k častějším objevům bezpečnostních děr. Útočníci těchto děr

využívají a vytváří programy, pomocí kterých mohou prolomit informační systém. [6], [23], [25], [27]

Útoky se mohou lišit použitými prostředky nebo cíli a mohou způsobit následující škody:

- nedostupnost služby – DoS (Denial of Service) útoky způsobí, že služba, na kterou byl proveden útok, přestane fungovat
- neoprávněný přístup – daným útokem útočník neoprávněně získá plný nebo částečný přístup k zařízení, což mu následně umožní provádět neautorizované změny v konfiguraci, mazání nebo modifikaci souborů
- získání důvěrných informací – výsledkem útoku je získání důvěrných informací, například seznam uživatelských jmen a hesel.

Mezi nejčastější příčiny zranitelnosti systémů se řadí:

- nedodržování platných standardů (RFC, W3C, ISO)
- nedůsledná konfigurace zařízení (povoleny zbytečné/nevyužité síťové služby, slabé šifrování)
- nevyhovující topologie systému
- neznalost managementu/odborné obsluhy
- nepořádek.

Celý proces penetračního testování zahrnuje řadu kroků, mezi které se řadí podrobná analýza systému se zaměřením na případné bezpečnostní nedostatky, které vycházejí z chybného nastavení systému, známých či neznámých hardwarových a softwarových nedostatků nebo také nedostatečných funkčních protiopatření. Proces je založen na simulaci útoků skutečného útočníka, který by se snažil daný systém napadnout. [6], [23], [25], [27]

5.2.1 **Metodika penetračního testování**

Penetrační testování může být provedeno na základě následujících metodik:

- OWASP – Open Web Application Security Project
- ISO/IEC 27001 / Zákon o kybernetické bezpečnosti

5.2.2 Fáze penetračního testování

Penetrační testování lze rozdělit z pravidla do tří fází.

První fáze

První fází je průzkum neboli detailní naplánování penetračního testu. Tato fáze zahrnuje shromažďování a přípravu podkladů a informací, které následně poslouží k provedení samotného testování. V této fázi je také provedena pasivní analýza datových toků v segmentu sítě, ve kterém bude test proveden. Na základě shromážděných informací se formulují cíle. Jsou vybrány nástroje, pro maximální efektivnost testování. [6], [23], [25], [27]

Druhá fáze

Druhou fází je samotné testování neboli řízení, koordinace a provedení vlastního testování. Pokud je identifikováno chování, které by mohlo prokázat zranitelnost, je provedeno další podrobné testování, které mají za cíl ověřit možnosti zneužití. Při ověřování zranitelnosti je třeba předejít ohrožení stability, integrity či důvěrnosti dat. Během procesu testování mohou být objeveny dodatečné cíle, které nebyly stanoveny v první průzkumné fázi. Po vyčerpání a zdokumentování veškerých cílů je test ukončen. [6], [23], [25], [27]

Třetí fáze

Třetí fáze představuje reportování výsledků. V reportu penetračního testu jsou zahrnuty následující informace:

- manažerské shrnutí – poskytuje základní přehled o průběhu testu, jeho vyhodnocení úrovně zabezpečení testovaného systému, obecná doporučení pro zvýšení úrovně zabezpečení a zmapované rizikové oblasti
- technický popis nálezů – obsahuje detailní popis zranitelností a potenciálních nebezpečných konfigurací, dále informace o zranitelných místech, jak mohou být zneužitá a co může útočník zneužitím získat
- navrhovaná opatření – obsahuje kroky vedoucí k odstranění nalezených zranitelných míst [6], [23], [25], [27]

5.2.3 Typy penetračních testů

Mezi základní typy penetračních testů se řadí:

1. Test infrastruktury – je zaměřen na použitou platformu (OS, webový server, databázi), zahrnuje vyhledávání a ověřování zranitelností operačních systémů a aplikací, které představují riziko (kompromitace systému, neautorizovaný přístup k datům, DoS), chybné konfigurace a využití nedoporučovaných protokolů a revizi architektury.
2. Test aplikačního prostředí – je zaměřen na logiku webové aplikace, cílem je nalezení a ověření takových zranitelností na zvolené webové aplikaci
3. Testy mobilních zařízení – jsou zaměřeny na provedení bezpečnostních testů mobilních zařízení s následnými návrhy efektivních ochranných opatření. [6], [23], [25], [27]

5.2.4 Dělení penetračních testů

V praxi existuje několik základních kritérií, dle kterých lze dělit penetrační testy.

Interní a externí test

V tomto typu testování záleží na pozici útočníka neboli testera vůči systému. Při interním testování je útočníkovi umožněn přístup do vnitřní sítě a zároveň mu mohou být přidělena určitá oprávnění. Externí testování simuluje útok z prostředí internetu a je založeno na překonání ochranných opatření, například firewall, intrusion detection/prevention systém a další. [6], [23], [25], [27]

Black-box a white-box test

Tento typ testování závisí na množství informací, které jsou útočníkovi poskytnuty.

V případě black–box testování nejsou poskytnuty žádné informace, proto testování představuje simulaci útočníka bez znalosti systému a záleží na jeho schopnostech, kolik informací si dokáže získat sám. V tomto případě je nutné dát si pozor na to, aby se tester omylem nezaměřil i na aktiva, příslušící jiné organizaci, jelikož to může mít právní důsledky. [6], [23], [25], [27]

Ve případě white–box testování je poskytnuto dostatečné množství podkladů a informací k provedení testování dle připraveného scénáře. Rozsah poskytnutých informací závisí na podobě testování, při testu infrastruktury může být poskytnuta síťová topologie či popis používaných technologií a při testu webových aplikací se pak jedná o poskytnutí zdrojového kódu. Vhodné je zde také zmínit blacklist, což je seznam pracovníků, IP adres či doménových jmen, kterým se má test vyhnout. [6], [23], [25], [27]

V praxi se často vyskytuje grey-box testování, které vzniká kombinací dvou výše uvedených testů. Znamená to, že testerovi jsou poskytnuty pouze částečné informace, které doplní vlastním výzkumem. Výhodou tohoto postupu je, že je bližší postupu reálného útočníka a zároveň umožňuje identifikaci maximálního počtu zranitelností. [6], [23], [25], [27]

Skrytý a otevřený test

Tento způsob dělení je na základě rozsahu informací, které jsou poskytnuty správcům testované infrastruktury.

Při skrytém testování nejsou správci informováni s předstihem a součástí testování je zkoumána i jejich schopnost detekce a reakce na pokus o útok. [6], [23], [25], [27]

V případě otevřeného testování jsou správci informováni o naplánovaném testování. Výhodou tohoto způsobu je spolupráce se správci systému a jejich aktivní účast na testování. Zároveň se předejde nepřiměřené reakce na pokus o útok, například odpojení organizace od internetu. [6], [23], [25], [27]

Komplexní a omezený test

Komplexní testy jsou zaměřeny na celý informační systém a záleží na samotném testerovi, jaký si zvolí rozsah a cestu. V případě omezeného testování je jasně zadán cíl, který pokrývá jen část systému, například webovou aplikaci či multifukční tiskárny. [6], [23], [25], [27]

5.2.5 Další způsoby testování

- Unit testy – slouží k ověření, zda individuální funkčnost je nastavena nebo vyvinuta dle požadavků stanovených v definici požadavků, testují se individuální konfigurační elementy a procesní kroky většinou asociované s transakcí nebo reportem, což odpovídá testovaným případům.
- Procesní testy – slouží k určení posloupnosti kroků, které na sebe navazují, tvoří provázaný řetězec procesních kroků a jsou provázány daty.
- Integrační testy – slouží k testování integrace celého řešení, a to jak vnitřní, tak vnější, testují se takzvané end-to-end scénáře v plné délce
- Akceptační testy – slouží k akceptaci řešení zástupci odborných útvarů klienta formou testů na prostředí, které funkčně i datově co nejvíce odpovídá budoucímu produktivnímu.
- Objemové testy – ověřují schopnost systému zpracovat požadované velké množství dat v požadovaném čase.
- Zátěžové testy – ověřují schopnost systému zvládnout velké množství současně pracujících uživatelů a spouštěných programů.

6 Normy a legislativy

6.1 GDPR

GDPR představuje právní rámec ochrany osobních údajů s cílem hájit práva občanů EU proti neoprávněnému zacházení s jejich osobními údaji. Týká se to jednotlivců, organizací, firem, online služeb jako jsou e-shop a všech institucí. GDPR je zkratka pro General Data Protection Regulation, v překladu do českého jazyka je to Obecné nařízení o ochraně osobních údajů. [6], [17]

6.2 Technická opatření školy pro dosažení souladu s nařízení GDPR

Opatření jsou navrhována na základě provedené analýzy rizik, ve které byla shledána následující významná rizika:

- v případě využití emailu pro předávání osobních údajů musí být tyto údaje šifrovány (nejméně metodou ZIP s heslem)
- nedoporučuje se využití freemailových účtů a pokud, tak pouze s kompletně šifrovaným obsahem
- namísto elektronické pošty lze bezplatně využít informační systém datových schránek
- limitovat přístupy na webové stránky pro sdílení dat (uloz.to, uschovna.cz aj.)
- zajistit omezení připojení flash, vypalování CD/DVD z jednotlivých stanic na úrovni politiky, jejich zpřístupnění pouze na jednotlivé pracovníky, kteří nezbytně potřebují flash disky nebo externí disky využívat
- v případě využití flash disku nebo externího disku k uložení osobních údajů je nezbytné tato data šifrovat, pokud jsou datové média vynášena mimo prostory organizace
- zajistit opakované technické testování znalostí uživatelů v rámci sociálního inženýrství (testování podvrženým emailem aj.)
- notebooky, které obsahují osobní údaje a jsou vynášeny mimo prostory organizace, musí být šifrovány
- chytré telefony, které obsahují osobní údaje a jsou vynášeny mimo prostory organizace, musí být zabezpečeny přihlašovacím heslem (vynuceno politikou) a dále vzdáleně ovladatelné v nejlepším případě (výmaz).

6.3 Vyhláška č. 523/2005 Sb.,

Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor stanovuje požadavky na informační systém nakládající s utajovanými informacemi. Informační systém nakládající s utajovanými informacemi má různé stupně utajení. Důvěrné nebo vyšší utajení musí zajišťovat různé bezpečnostní funkce, k jejichž zajištění se v informačním systému realizují identifikovatelné a programově technické mechanismy. Ty musí být v celém životním cyklu informačního systému chráněny před narušením nebo neautorizovanými změnami. [6], [29]

6.4 ISMS – Systémy řízení bezpečnosti informací

Systém řízení bezpečnosti informací se skládá z postupů, směrnic a příslušných zdrojů a činností, kterými se organizace řídí, s cílem zaručení ochrany informačních aktiv, řízení rizik bezpečnosti informací a kontrole zavedených opatření. Představuje systematický přístup k nařízení, implementaci a provozování, monitorování, přezkoumávání, udržování a zlepšování informací organizace tak, aby byly zajištěny její cíle. Princip ISMS je založen na posuzování rizik a úrovni přijetí rizik organizace, které byly navrženy pro minimalizaci rizik a jejich zvládnutí. K úspěšnosti ISMS přispívá analýza požadavků na ochranu informačních aktiv a aplikace opatření s cílem zajistit ochranu aktiv v souladu s požadavky. Pro úspěšnou implementaci ISMS jsou zásadní tyto základní principy: [4], [6]

- povědomí o potřebné bezpečnosti informací
- určení odpovědnosti za bezpečnost informací
- začlenění závazku managementu a zájmů zúčastněných stran
- zvýšení společenských hodnot
- posouzení rizik, díky kterému se stanový patřičná opatření, aby byla splněna přijatelná úroveň rizika
- bezpečnosti začleněná jako základní prvek do informačních sítí a systémů
- aktivní prevence a detekce incidentů bezpečnosti informací

- zajištění komplexního přístupu k řízení bezpečnosti informací
- neustálé posuzování bezpečnosti informací a provádění modifikací dle potřeby.

Zavedení ISMS je pro organizaci strategickým rozhodnutím a je třeba jej začlenit, odstupňovat a aktualizovat s potřebami organizace. Návrh a implementace jsou rovněž ovlivněny potřebami a cíli organizací. Dále jsou zohledňovány požadavky na bezpečnost a procesy organizace. ISMS je pro činnost organizace jak veřejného, tak privátního sektoru velmi důležitý. Díky této normě mohou organizace demonstrovat obchodním partnerům a dalším zainteresovaným stranám svoji schopnost používat konzistentní a vzájemné principy bezpečnosti informací. [6], [17]

ČSN ISO/IEC 27000 Systémy řízení bezpečnosti informací – Přehled a slovník

Norma ČSN ISO/IEC 27000 poskytuje přehled systému řízení bezpečnosti informací, termíny a definice obecně používané v několika normách ISMS neboli Information Security Management System. Tato norma je využívána různými typy organizací a umožňuje vytvoření a používání bezpečnostního řízení aktiv obsahující informace, které byly organizacemi získány nebo jim byly poskytnuty zákazníky či třetími stranami.

Dnešní zákony, týkající se informační bezpečnosti jsou vytvořené z norem ISO/IEC 27000. Normy ISO/IEC 27001 a ISO/IEC 27002 jsou základním podkladem pro vytvoření bezpečných informačních systému a jejich užívání je zásadní pro spolupráci s institucemi a obchodními partnery. V nich jsou určeny zásadní postupy a hodnocení pro budování bezpečnosti IS a umožnují snadné ověření stavu bezpečnosti, výměnu informací. [6], [17]

ČSN ISO/IEC 27001 Systémy řízení bezpečnosti informací – Požadavky

Zmíněná norma zavádí požadavky na ustanovení, implementaci, udržování a zlepšování systému řízení bezpečnosti informaci pro organizaci. Norma se skládá z následujících oblastí: [6], [17]

- požadavky na ISMS
- odpovědnost vedení organizace
- vnitřní audit ISMS
- ISMS zkontroluje vedení organizace
- vylepšování ISMS.

7 Bezpečnost počítačových sítí

Zabezpečení sítí představuje ustanovení, pravidla a politiky, které slouží k prevenci a kontrole neoprávněného přístupu úpravě, zneužití, zamítnutí počítačové sítě a jsou zavedený správcem sítě. Mezi zranitelná místa, která je potřeba chránit patří informace a data, služby, zařízení a uživatelé (z hlediska identity). Bezpečnostní politika sítě představuje rozpoznání autorizovaného a neautorizovaného chování. Cílem síťového zabezpečení je zajištění důvěrnosti dat, zajištění autentizace uživatelů sítě, zajištění integrity dat, zajištění neodmítnutelnosti zpráv, zabezpečení dostupnosti síťových služeb a přiřazování přístupových práv. Zabezpečení sítě také zahrnuje přístup k datům v síti, který je řízen správcem sítě. Každý uživatel má svoje ID (identifikační číslo) a heslo nebo jiný ověřovací prostředek, který jim umožní přístup k informacím a programům. Do síťového zabezpečení spadají veřejné i soukromé počítačové sítě, které jsou každodenně používány k přenosu informací a komunikaci. Bezpečným a jednoduchým způsobem ochrany sítě zaheslovaní síťového spojení, což znamená, že každý, kdo se bude chtít připojit k této síti, se musí prokázat unikátním názvem (přihlašovacím jménem, ID) a k němu platným a odpovídajícím heslem. [6], [23], [25], [27]

Mezi zdroje bezpečnostních obtíží patří:

- sdílení – potenciální přístup má velmi velké množství lidí, různé stroje mohou být řízeny různými ne nutně bezpečnými systémy
- složitost – v síti se vyskytují nejrůznější operační systémy komunikující spolu přes spojovací mechanismus, který by měl zajišťovat ochranu, tento mechanismus však musí být dostatečně obecný, navíc síť jako celek nelze podrobit testování či dokonce certifikaci
- neznámý perimeter – nikdy nevíme, kdo všechno je připojen, není jasné, jak se ostatní stroje chovají
- množství zranitelných míst – je nutné uvěřit bezpečnostním mechanismům na všech strojích, mnohé části sítě leží mimo jakýkoliv dohled provozovatelů
- neznámá cesta – většinou nelze ovlivnit, kudy budou data přenášena, tedy není k dispozici žádná informace, kdo s nimi může přijít do styku.

Útoky mohou být rozděleny na pasivní a aktivní. Mezi pasivní útoky patří wiretapping, port scanner a idle scan. Aktivní útoky zahrnují denial of service attack, spoofing, man in the middle, ARP poisoning, smurf attack, buffer overflow, heap overflow, format string attack, SQL injection a cyber attack. [6], [23], [25], [27]

7.1 Ochrana síťové komunikace

Komunikaci je možné chránit jako:

- proud dat neboli „stream enciphering“, což představuje šifrování proudu dat a spolehlivost komunikačního kanálu z hlediska možného útoku, tento způsob je možné provádět mezi dvěma uzly sítě nebo mezi dvěma aplikacemi běžícími na těchto uzlech
- jednotlivé zprávy, což představuje šifrování aplikačních zpráv pomocí „messagingu. [6], [23], [25], [27]

Šifrování na úrovni linky (Link Encryption)

Šifrování je počítačovým nástrojem pro zajištění bezpečnosti sítě. Šifrování dat probíhá těsně před vstupem do komunikačního media a dešifrování ihned po příchodu na druhý počítač. Toto šifrování se provádí na úrovni fyzické případně linkové vrstvy referenčního modelu. Výhodou tohoto konceptu je transparentnost a rychlost pro uživatele. [6], [23], [25], [27]

End-to-End šifrování

End-to-End neboli koncové šifrování poskytuje kryptografickou ochranu po celou dobu přenosu a je prováděno na úrovni aplikační nebo prezentační vrstvy referenčního modelu. Mechanismus je takový, že odesílaná zpráva se prostřednictvím aplikace zašifruje pomocí klíče, který je uložený v zařízení příjemce, putuje zašifrovaná internetem a dešifruje se na svém konci. Nevýhodou tohoto šifrování je, že už nebývá transparentní, a aby bylo účinné, musí být vhodně zakomponováno do celého systému. Mezi výhody patří to, že nemusí být šifrována veškerá komunikace, ale pouze citlivá data a je schopno zajistit autentizaci a integritu na rozdíl od šifrování linky. [6], [23], [25], [27]

V některých případech jsou implementovány obě výše uvedené metody šifrování, šifrování linky za účelem běžné preventivní ochrany dat a End-to End šifrování pro docílení skutečně kvalitní ochrany senzitivních dat.

Aby bylo zavedeno šifrování, je potřeba zavedení mechanismu distribuce a správy nezbytných šifrovacích klíčů a existence potřebných centrálních autorit pro zajištění provozu systému kryptografické ochrany a nutnost vhodných kryptografických zařízení, které zajistí základní funkce kryptografické ochrany. [6], [23], [25], [27]

7.2 Kontrola přístupu

Problematika kontroly přístup zahrnuje následující okruhy.

Ochrana komunikačních portů (Port protection)

Procesu autentizace uživatele předchází mechanismus ochrany vlastního komunikačního portu, který zahrnuje automatické zpětné volání, odstupňovaná přístupová práva, tichý modem, řízení přístupu z vnějšího prostředí, parcelizaci vnitřní sítě a autentizaci uzlů. [6], [23], [25], [27]

Automatické zpětné volání

Tato metoda funguje na principu toho, že poté, co je navázáno spojení a uživatel se identifikuje, systém ukončí spojení, v interních tabulkách zjistí adresu daného uživatele a pokusí se o navázání spojení s touto adresou. Automatické zpětné volání zajišťuje přístup pouze z omezeného množství uzlů (adres) a proto je zásadně omezena možnost průniku ‘zvenčí’. [6], [23], [25], [27]

Odstupňovaná přístupová práva

Tato metoda zajišťuje, že přístup k citlivým datům je omezen pouze na některé uzly. To znamená, že pokud i autorizovaný uživatel žádá o přístup z jiného uzlu, díky této metodě mohou jeho přístupová práva být výrazně omezena, nebo přístup k datům může být zcela odepřen. [6], [23], [25], [27]

Tichý modem (Silent Modem)

Tichý modem je metodou, kdy po přijetí volání modem nezačne bezprostředně generovat nosnou, ale vyčká na pokus o vyjednávání druhé strany, což zajišťuje omezení přístupu do určité míry pouze na uživatele, kteří vědí, že jde o linku vedoucí k počítači. Tento mechanismus omezuje možnost náhodného nalezení daného portu. [6], [23], [25], [27]

Řízení přístupu z vnějšího prostředí

Mezi řízení přístupu z vnějšího prostředí patří:

- firewally – filtry, aplikační brány
- policy gateway
- překlad adres
- kontrola přenášených dat – antiviry, java, scripty,
- omezení přístupu ke zdrojům / obsahu dat
- prioritizace, qos
- IDS, IPS (intrussion detection/prevention system) – síťové, aplikační
- demilitarizované zóny
- content filtry.

Parcelizace vnitřní sítě

Parcelizace vnitřní sítě zahrnuje oddělení kritických zdrojů, zónování, vydělení zvláštní sítě pro senzitivní informace a traffic shaping. [6], [23], [25], [27]

Autentizace uzlů

Autentizace uzlů představuje nutnost mechanismů, které umožňují vzájemnou autentizaci nejen uživatelů, ale i jednotlivých uzlů. [6], [23], [25], [27]

7.3 Autentizace v síti

Zde nastíním autentizační mechanismy v síťovém prostředí, které jsou odolné vůči odposlechu neboli aktivním útokům. V této kategorii je třeba řešit jednotné přihlášení (single sign on):

- cookies
- tickety
- certifikáty, PKI
- čipové karty
- tokeny / jednorázová hesla.

Proces integrace autentizačních mechanismů souvisí se zavedením centrální správy uživatelů a synchronizací záznamů o uživatelích. [6], [23], [25], [27]

7.4 Aktivní útočník

Nejprve je třeba vysvětlit, co se skrývá pod pojmem aktivní útočník. Aktivní útočník se pokouší proniknout do bezpečnostních systémů prostřednictvím agresivního útoku. Tyto útoky zahrnují pokusy obejít či prolomit bezpečnostní software a poškodit systém ochrany dat. [6], [23], [25], [27]

Playback starších zpráv

Prostřednictvím tohoto útoku se útočník pokouší o znovu používání starších zachycených zpráv. Metodou ochrany mohou být časová razítka v kombinaci s šifrováním, různé tokeny s omezenou časovou platností, notarizace, nebo ofsetování zpráv. [6], [23], [25], [27]

Narušení služeb

Dalším způsobem útoku je přetěžování sítě nesmyslnými zprávami. Účinnou metodou obrany je změna routovací informace nebo zachycování či poškozování zpráv, které jsou zasílané určitému uživateli. Zároveň je možné se bránit vytvořením duplicitních linek, prostřednictvím kterých mohou být zprávy posílány a omezit se pouze na důvěryhodné uzly. [6], [23], [25], [27]

Vkládání poškozených zpráv

Tímto útokem se útočník pokouší vkládat poškozené zprávy, při jejichž zpracování může dojít ke zhroucení nebo nesprávné funkci služby konajícího stroje. [6], [23], [25], [27]

7.5 Řízení zátěže

Řízení zátěže představuje útok, kdy útočník zachycuje veškerou komunikaci a provádí rozbor, kdo s kým a jak často komunikuje. Jedná se o analýzu zátěže a z náhlých změn zátěže lze usoudit nadcházející události.

Vhodná metoda obrany zahrnuje generování vycpávací zátěže v době, kdy nedochází ke skutečné komunikaci. [6], [23], [25], [27]

Vycpávací zátěž

Generovaná vycpávací zátěž je prostředkem pro vytvoření skrytého kanálu. Je třeba, aby administrátor zajistil generování dalších vycpávacích zpráv, které doplňují komunikaci mezi dvěma libovolnými uzly sítě. [6], [23], [25], [27]

Kontrola routování

Touto metodou může administrátor aktivně zasahovat do procesu routování a náhodně měnit způsob routování určitých zpráv, což ve výsledku znamená dosažení větší náhodnosti do procesu přenosu zpráv a omezení možnosti předchozích útoků. [6], [23], [25], [27]

Další metody ochrany

Dalšími metodami ochrany, které jsou prováděny administrátorem, mohou být například aktivní zásahy prostřednictvím náhodného zachycování a mazání zpráv, náhodné změny adresáta zprávy na nejnižší úrovni nebo pozdržování doručení náhodně vybraných zpráv. [6], [23], [25], [27]

7.6 Integrita dat

Integrita dat znamená zachování kompletnosti a představuje stav, kdy přečtená data jsou totožná s uloženými daty, což znamená, že během přenosu nedošlo k jejich poškození nebo změně. Přenos zpráv je proto řízen přenosovými protokoly, které zajišťují tuto datovou integritu a pořadí doručených částí. Pro zajištění integrity dat je vhodné použití kryptografických kontrolních součtů, které představují proces, kdy do každého šifrovaného bloku zprávy je přidáno jeho pořadové číslo, za účelem, aby útočník nemohl provádět záměny pořadí notarizace zpráv. [6], [23], [25], [27]

7.7 Lokální sítě

Charakteristickým prvkem lokálních sítí je to, že jejich uživatelé jsou lidé, kteří často pracují ve společném oboru, jsou laici v oblasti počítačů a do značné míry si mezi sebou důvěřují, což vede ke snížení obranyschopnosti v případě náhlého útoku. Problémy nastávají při vzájemném propojování těchto sítí. Typologie lokálních sítí, dle které lze modifikovat ochranné mechanismy, je převážně jednotná, bývá umístěna uvnitř jedné budovy. Typická je také přítomnost administrátora, který může efektivně vynucovat dodržování stanovené bezpečnostní politiky ve všech uzlech. [6], [23], [25], [27]

7.8 Víceúrovňová bezpečnost

V počítačových sítích mohou pracovat uživatelé s různým stupněm prověření a síť obsahuje data různých stupňů utajení Prostředkem ochrany je často modifikace military security modelu. Operační systémy, které jsou navrhovány pro vysokou bezpečnost, jsou rozděleny na moduly, které přistupují k chráněným objektům prostřednictvím spolehlivých modulů, jež tvoří spolehlivou výpočetní bázi (TCB) [6], [23], [25], [27]

Spolehlivé síťové rozhraní (trusted network interface)

Spolehlivé síťové rozhraní je model, který zajišťuje, že každý uzel sítě naváže spojení pouze s takovým uzlem, který má spolehlivé síťové rozhraní funkce. K implementaci spolehlivého síťového rozhraní vedou následující kroky:

- zajištění bezpečnosti vlastního uzlu před útoky zvenčí
- veškerá výstupní data musí být označena příslušnou bezpečnostní klasifikací
- před uvolněním dat je provedena verifikace oprávněnosti žadatele a jeho autentizace
- ověření konzistence došlých dat
- zamezení míchání dat různého stupně utajení, nebo samovolnému předávání informací ostatním uzlům
- bezpečnost dat nesmí záviset na bezpečnosti linky.

7.9 Bezpečnost komunikace

Bezpečnost komunikace je závislá na použitém přenosovém mediu. Útoky proti komunikačním linkám se dělí na pasivní, například odposlech, nebo aktivní, které zahrnují vkládání dalších informací do komunikace. [6], [23], [25], [27]

Bezpečná komunikace

Bezpečná komunikace je zajišťována samotnými komunikačními procesy a ve spolupráci s operačními systémy jsou dodržována určitá pravidla Bell-LaPadula bezpečnostního modelu.

Jedním z prvků bezpečné komunikace je zavedení potvrzování zpráv, což je zajištěno komunikačním serverem na každém uzlu. [6], [23], [25], [27]

Kabely

Jedním ze způsobů útoků je tzv. napíchnutí (wiretaping). Metody obrany zahrnují bezbranné metalické vodiče nebo monitoring optických kabelů. Za nejbezpečnější metalické kabely jsou považovány koaxiální kabely, které mohou být s omezeným vyzařováním nebo s detekcí napíchnutí. Pevné linky jsou obecně náchylnějšími k napíchnutí a vyšší pravděpodobnost útoku je u některého z konců linky. [6], [23], [25], [27]

8 Škola a počítačová síť

Pro diplomovou práci byla vybrána Vyšší odborná škola ekonomická, sociální a zdravotnická, Obchodní akademie, Střední pedagogická škola a Střední zdravotnická škola, Most, příspěvková organizace v Mostě, protože problematika počítačových sítí ve školním prostředí je aktuální a je potřeba stále sledovat a implementovat inovace v tomto odvětví. Jelikož ve školních systémech je shromažďováno a uchováváno velké množství citlivých informaci, jak o samotné škole, tak i o jejích žácích a zaměstnancích, je nezbytné umět s těmito informacemi správně nakládat a zajistit jejich bezpečnost. To jsou hlavní důvody, které mne vedly k výběru tohoto tématu.

8.1 Základní charakteristika školy

Škola vznikla na základě usnesení Zastupitelstva Ústeckého kraje k 1. 9. 2009 sloučením Vyšší odborné školy, Střední pedagogické školy a Obchodní akademie v Mostě a Vyšší odborné školy zdravotnické a Střední školy zdravotnické J. E. Purkyně v Mostě. Jako páteřní škola je důležitá pro upevnění vzdělávací nabídky kraje ve vzdělávacích oborech humanitního, ekonomického a zdravotnického zaměření.

Škola má kapacitu 2 150 žáků a studentů, z toho 860 studentů vyššího odborného vzdělávání a 1290 žáků středního vzdělávání a skládá se ze tří budov, v budově A jsou realizovány ekonomické, sociální a pedagogické obory, v budově B je sekce zdravotnického vzdělávání. V budově C je domov mládeže s kapacitou 135 lůžek, jehož ubytování využívají žáci maturitního vzdělávání i studenti vyšší odborné školy. Docházková vzdálenost mezi budovami je 15 minut.

Budova A

Budova disponuje 22 kmenovými učebnami (všechny jsou vybaveny notebookem a dataprojektorem) a 21 odbornými učebnami s následujícím vybavením a zaměřením – 6 jazykových učeben s notebookem a projekční technikou, 1 učebna fiktivních firem, 2 učebny výtvarné výchovy, 4 učebny hudební výchovy, 2 učebny komunikativních dovedností, 2 učebny písemné a elektronické komunikace s 43 počítači řady Intel Core i3 a i5, 3 učebny

informačních technologií, které jsou vybaveny PC řady Intel Core i3 a i5 v celkovém počtu 52 kusů (všechny učebny jsou zapojeny do počítačové sítě a na internet).

Odborné učebny jsou dále doplněny 2 tělocvičnami a studovnou pro studenty VOŠ a dvěma jednacími místnostmi pro projektovou činnost. Velmi významnou z hlediska výukových možností je multimediální učebna, kde lektorské pracoviště disponuje lektorským počítačem, dataprojektorem, vizualizérem a další audiovizuální technikou. Dále jsou v budově další dvě učebny, které jsou vybavené speciálními stolky s 34 notebooky pro žáky a studenty školy, které byly v roce 2019 modernizovány (Intel Core i3). Část notebooků byla pořízena v rámci projektu OPVVV Šablony II. V každé z uvedených učeben je jedno lektorské pracoviště, které disponuje lektorským počítačem, dataprojektorem a další audiovizuální technikou. Všechny pracovní pozice jsou připojeny na internet a 5 učeben je vybaveno interaktivní tabulí. Pro výuku byla pořízena mobilní tabletová učebna s tablety pro 15 žáků a 1 učitele.

Vybavenost budovy A doplňuje knihovna se studijním atypickým koutkem. Svým pojetím umožňuje žákům, studentům i učitelům získávat informace z různých typů médií. Studovna byla vybavená v rámci projektu OP VK – serverem, 15 terminály, 3 tiskárnami a internetem. Na všech terminálech je studentům k dispozici právní informační systém CODEXIS. Provoz studovny je zajišťován pracovníkem školy v rozsahu 8 hodin denně, po dohodě i během víkendové výuky.

Bezproblémově funguje elektronický zabezpečovací systém budovy školy, který v současnosti obsahuje otvírání všech vchodů do budovy pomocí čipového zařízení nebo ISIC karty pro studenty a učitele školy. ISIC karta se všemi výhodami studentského mezinárodního průkazu byla přijata školou jako průkaz školy, průkazka do školní knihovny a průkazka na stravování. Vstup do budovy ostatních zaměstnanců umožňují osobní čipy, cizím osobám je vstup povolován pomocí video snímače u hlavního vchodu školy. Tímto způsobem je zajištěna bezpečnost provozu školy v denním i nočním režimu. Systém čipů byl doplněn kamerovým systémem u všech třech vchodů, které používají žáci, studenti, zaměstnanci a veřejnost.

Budova B

V budově je 27 učeben z toho 22 učeben slouží jako odborné učebny s následujícím vybavení a zaměřením – 2 jazykové učebny, 4 učebny pro ošetřovatelství, 2 učebny informačních technologií s celkem 42 PC, 2 učebny masérství, dále po jedné učebna první pomoci, chemie, fyziky, biologie, somatologie. Praktická cvičení probíhají v laboratoři chemie a v laboratoři fyziky. Přednášková místnost s kapacitou 70 míst může fungovat díky mobilní stěně učebny, která umožňuje variabilní rozdělení do dvou samostatných učeben. Ve 3 učebnách je interaktivní tabule.

Budova C

Budova domova mládeže slouží k ubytování žáků a studentů vlastní školy, ale i ostatních škol Mostecka. Domov mládeže je vybaven jídelnou, která zajišťuje celodenní stravování pro ubytované v domově mládeže, pro zaměstnance, žáky a studenty. V domově mládeže je 65 dvoulůžkových pokojů pro ubytování žáků a studentů a 2 dvojlůžkové pokoje a jeden jednolůžkový pokoj pro komerční ubytování. Dále je v domově mládeže jeden kondiční sálek a studovna vybavená několika počítači připojenými k internetu, v každém patře je pro volnočasové aktivity ubytovaných jedna klubovna.

Popis dalšího vybavení školy

Všechny budovy školy jsou připojeny k internetu optickým kabelem o rychlosti 750 Mbps. Každý učitel disponuje pracovním notebookem, který je ve škole připojen ke školnímu intranetu. Pro studijní administrativu středních škol se využívá elektronický informační systém školy Bakalář. Tento systém je doplněn systémem IS VOŠ pro studijní administraci vyšší odborné školy. Studijní materiály jsou žákům a studentům zprostředkovány formou e-learningu v systému Moodle. Na jaře 2020 začala škola využívat pro online výuku systém MS Teams. Telefonické spojení funguje na základě IP Telefonie, která umožňuje bezplatnou komunikaci mezi všemi místy všech tří budov.

Škola má zřízenu svojí vlastní doménu vos-sosmost.cz. Areál všech tří budov je pokryt technologií Wifi, která umožňuje studentům připojení vlastních notebooků a dalších mobilních zařízení k internetu.

Všichni učitelé mají zřízeny e-mailové školní adresy, pomocí nichž žáci komunikují s učiteli. Studijní materiály a sylaby pro jednotlivé moduly jsou studentům k dispozici prostřednictvím systému Moodle, který je studentům přístupný pomocí internetu. Systém Moodle je provozován na školním webovém serveru.

K administrativní komunikaci se studenty vyšší školy odborné v minulosti využívali informační systém Noisy, který zajišťoval evidenci průběžného hodnocení studentů a přihlašování na zkoušky.

8.2 Charakteristika školní sítě

Současná Wi-Fi infrastruktura plně pokrývá všechny budovy školy, čehož je dosaženo díky vhodnému rozmístění přístupových bodů. Na každém patře se vyskytuje od dvou do sedmi přístupových bodů. Počet uživatelů, kteří se mohou připojit k síti prostřednictvím bezdrátové sítě nebo LAN, je 2500. Jako hlavní router škola používá zařízení od značky Mikrotik RB4011iGS+RM, který je vybaven čtyřmi jádry s frekvencí 1400 MHz a hardwarovou akcelerací. Zároveň tento router podporuje pasivní PoE vstup i výstup a je schopný routovat s rychlostí 2,5 Gbps. Optický modul lze rozšířit o 10 Gbps. Další podrobnosti týkající se parametrů popisovaného routeru lze nalézt v příloze 1.

Další router, který je využíván školou, je Mikrotik RG750Gr3. Vzhledem k velkému výkonu může splňovat funkci firemního firewallu a být vhodný pro centrální zprávu AP, jak v režimu CAPsMAN, tak i v režimu hotspot. Router je možné napájet nejen pomocí klasického konektoru jack, ale také přes PoE. Podrobnější parametry jsou uvedeny v příloze 2.

Switche, vyskytující se v budovách školy, jsou od značky TP-Link, SMC a Mikrotik. Switche od značky TP-Link mají ve škole největší zastoupení. Gigabitově řízený L2 switch TP-LINK JetStream T2600G-28TS je vybaven 24 porty a 4 gigabitovými SFP sloty. Mezi jeho přednosti patří poskytování velkého výkonu a výkonných funkcí, jako jsou například statické směrování, řízení síťového provozu QoS na podnikové úrovni a jiné pokročilé strategie zabezpečení. Podrobnější parametry jsou obsaženy příloze 3. Dalšími typy jsou TL-SG3424, TL-SG1428PE, TL-SG1024. Switche od značky SMC jsou typu SMC8024L2, a od značky Mikrotik typu CRS125-24G-1S-RM.

Přístupových bodů neboli access points, má škola dva druhy. První druh přístupových bodů je od značky TP-Link EAP245. Tyto přístupové body jsou dvoupásmové a nabízí podporu Wi-Fi 5, bezdrátovou rychlost 450 Mb/s na frekvenci 2,4 GHz a 1300 Mb/s na frekvenci 5GHz. Více parametrů je uvedeno v příloze 4. Druhou značkou přístupových bodů, která se na škole vyskytuje, je Unifi.

Další zařízení, která se vyskytují ve vybrané školní síti, jsou NAS servery typu Synology DS1621+, Synology DS412+ a Fujitsu CELVIN Q800. Synology DS1621+ je robustní NAS s výkonem serverové třídy v šesti šachtovém stolním provedení. Je vybavený vestavěnými 2 sloty pro mezipaměť SSD M. 2, rozšiřitelnou pamětí a škálovatelným úložištěm. O hardware a výkon se stará čtyřjádrový procesor AMD Ryzen V1500B s frekvencí 2,2 GHz a operační pamětí 4 GB typu DDR4 ECC SODIMM, která je rozšiřitelná až na 32 GB. Všechny parametry jsou k nalezení v příloze 5.

NAS server Fujitsu CELVIN Q800 je poháněn procesorem Intel Atom D525 pracujícím na frekvenci 1.8 GHz, který je doplněn o 1 GB operační paměti DDR3. Server je osazen dvojicí pevných disků s kapacitou 2x 2 TB. Všechny parametry jsou uvedeny v příloze 6.

Na hlavním routeru jsou nastaveny tři veřejné IP adresy, jedna pro provoz školy a další dvě pro servery. Na vybrané škole je nastavena metoda modifikace zdrojové a cílové adresy v záhlaví paketu typu DSTNAT na daných portech serverů. Tento typ NAT se realizuje na paketech, které jsou určeny do natované sítě. Proces probíhá tak, že směrovač NAT provádějící DSTNAT, nahradí cílovou IP adresu paketu IP, který prochází směrovačem do privátní sítě. Následným nastavením je VPN server pro ekonomické oddělení a vybrané provozní zaměstnance školy. Dále je zřízený EOIP tunel na druhý router v budově B. V neposlední řadě je zde také přítomný základní firewall, na kterém jsou zakázány share servery a pornografické stránky. Další filtrování nežádoucího obsahu je nastaveno u providera, ten má vlastní pravidla nastavená u sebe, která jsou z 90 % dostačující. Provider školy je WMS s.r.o. Na routeru bylo vytvořeno několik VLAN. DHCP bylo rozděleno pro určité VLANy a zároveň přiděluje adresy z poolu, brány a DNS. Rozdělení VLAN v síti je následující:

1. VLAN pro servery
2. VLAN Wifi učitel
3. VLAN WIFI žák
4. VLAN PC učebny budova A
5. VLAN Učitelé + provoz
6. VLAN Kmenová učebny
7. VLAN PC + kmenové budova B
8. VLAN technologie (EZS, switche, řízení bazénu atd.).

Strukturovaná kabeláž vyskytující se v budově A patří z 90 % do kategorie CAT6 a ze zbylých 10 % do kategorie CAT5E. Kabeláž, která se nachází v budově B spadá z poloviny do kategorie CAT6 a z poloviny do kategorie CAT5E. Kabeláž v kancelářích v budově C, která je mimo jiné nejstarší, spadá z 20 % do kategorie CAT6 a zbylá část budovy, tedy 80 %, je tažená kategorií CAT5E. Schéma rozmístění rozvaděčů a strukturované kabeláže je k nalezení v příloze 7. Uspořádání rozvaděčů v budovách je následující:

- budova A 1x hlavní, 1x podružný, 6x v PC učebnách
- budova B 1x hlavní, 3x v PC učebnách
- budova C 1x hlavní

Rozvaděče jsou umístěny v serverovně, kde se zároveň nachází i optický přívod internetu a NAS servery s elektronickou zabezpečovací signalizací včetně elektronické požární signalizace. Jedním z bezpečnostních prvků jsou mříže na oknech serverovny a povolený přístup mají pouze pověření zaměstnanci. Na NAS jsou disky v RAID 1, které jsou nastavené jako sdílený disk SMB V3. Propojení mezi budovami A a B je řešeno pomocí optického kabelu, který vede z budovy A na budovu providera, a z něhož je část řešena bezdrátovým přenosem o rychlosti 500 Mbit/s na budovu B. Toto propojení nese název EOIP tunelu. Řešení propojení budovy B a C je opět pomocí optického kabelu. Propojení budov a schéma sítě naleznete v příloze č. 8.

Na všech PC je nastavená pravidelná aktualizace, která probíhá prostřednictvím internetu. Aktualizace serverů, routerů, switchů a Wi-Fi provádí správce sítě ručně. V síti je vytvořený společný adresář pro čtení a oprávnění uživatelé jej mohou využít i pro zápis. Pro každého

uživatele byl vytvořen účet s vyhrazenými pravidly. Prostřednictvím daného účtu se uživatelé mohou připojit do informačního systému a ke sdíleným adresářům.

8.3 Testování a analýza

Tato část diplomové práce se věnuje rozboru provedeného testování a analýze školní sítě a webových stránek.

8.3.1 Penetrační testování

Jako první bylo zvoleno penetrační testování webových aplikací metodou OWASP. Testování bylo provedeno na škole na základě povolení od vedení školy. Prostřednictvím komunity vedených open source softwarových projektů, stovek místních poboček po celém světě, desítek tisíc členů a předních vzdělávacích a školících konferencí je OWASP Foundation pro vývojáře a technology zdrojem pro zabezpečení webu.

Pro penetrační testování byl vybrán program OWASP ZED attack proxy (ZAP). Je to světově nejrozšířenější skener webových aplikací, je zdarma a open source. Zároveň je aktivně udržován specializovaným mezinárodním týmem dobrovolníků. Proces testování je manuální i automatizovaný. Penetrační testování probíhá v následujících třech fázích:

1. **Fáze: Prozkoumat**

Tester se pokouší dozvědět se o testovaném systému. Tento proces zahrnuje snahu zjistit, jaký software se používá, jaké koncové body existují, jaké záplaty jsou nainstalovány. Dále je v této fázi zahrnuto také hledání skrytého obsahu, známých zranitelností a dalších náznaků slabosti na webu.

2. **Fáze: Útok**

Tester se pokouší zneužít známé nebo předpokládané zranitelnosti k prokázání jejich existence.

3. **Fáze: Zpráva**

Tester hlásí výsledky svého testování, včetně zranitelností, způsobu jejich zneužití a obtížnosti zneužití a závažnosti zneužití.

Ve výsledcích mého testování bylo prokázáno několik zranitelností, které jsou podrobněji rozebrány v následujících odstavcích.

Tab. 2 Zranitelnosti dle rizika a důvěry

		Důvěra			
		Vysoký	Střední	Nízký	Celkový
Riziko	Vysoký	0 %	0 %	0 %	0 %
	Střední	0 %	11,1 %	11,1 %	22,2 %
	Nízký	0 %	33,3 %	11,1 %	44,4 %
	Informační	0 %	11,1 %	22,2 %	33,3 %
	Celkový	0 %	55,6 %	44,4 %	100 %

První zranitelností střední úrovně je absence tokenů Anti-CSRF. Webová aplikace dostatečně neověřuje nebo nemůže dostatečně ověřit, zda uživatel, který požadavek odeslal, úmyslně poskytl správně vytvořený, platný a konzistentní požadavek. Znamená to, že webový server je navržen tak, aby přijímal požadavek od klienta bez jakéhokoli mechanismu pro ověření a je možné, že útočník oklame klienta, aby odeslal neúmyslný požadavek na webový server, který bude považován za autentickou žádost. To lze provést prostřednictvím adresy URL, načtením obrázku, XMLHttpRequest atd., a může to vést k odhalení dat nebo nechtěnému spuštění kódu. Viz příloha č. 9.

Druhou vyhodnocenou zranitelností střední úrovně je nepřítomnost záhlaví Anti-clickjacking. To znamená, že odpověď nezahrnuje ani Content-Security-Policy s direktivou 'frame-ancestors' ani X-Frame-Options na ochranu proti útokům 'ClickJacking'. Bylo nalezeno záhlaví X-Frame-Options (XFO), odpověď s více položkami záhlaví XFO nemusí být předvídatelně ošetřena všemi uživatelskými agenty. V odpovědi bylo přítomno záhlaví X-Frame-Options, ale hodnota nebyla správně nastavena. Viz příloha č. 10.

Zranitelností nižší úrovně je stránka obsahující jeden nebo více souborů skriptů z domény třetí strany. Další zranitelnost nižší úrovně spočívá v tom, že chybí záhlaví X-Content-Type-Options. Záhlaví Anti-MIME-Sniffing X-Content-Type-Options nebylo nastaveno na 'nosniff'. To umožňuje starším verzím Internet Exploreru a Chrome provádět MIME sniffing v těle odpovědi, což může způsobit, že tělo odpovědi bude interpretováno a zobrazeno jako jiný typ obsahu, než je deklarovaný typ obsahu. Současné (od počátku roku 2014) a starší verze Firefoxu budou používat deklarovaný typ obsahu (pokud je nastaven), spíše než provádění MIME-sniffování. Viz příloha č. 11.

Poslední zranitelnost spadá do úrovně informativní s názvem nesoulad znaků. Webový prohlížeč provádí kontrolu a identifikuje odpovědi, kde hlavička HTTP Content-Type deklaruje znakovou sadu, která se liší od znakové sady definované tělem HTML nebo XML. Pokud dojde k nesouladu znakové sady mezi hlavičkou HTTP a tělem obsahu, webové prohlížeče mohou být nuceny přejít do nežádoucího režimu sniffování obsahu, aby určily správnou znakovou sadu obsahu.

Útočník by mohl manipulovat s obsahem na stránce, aby byl interpretován v kódování podle vlastního výběru. Pokud například útočník může ovládat obsah na začátku stránky, mohl by vložit skript pomocí textu kódovaného UTF-7 a zmanipulovat některé prohlížeče, aby tento text interpretovaly. Viz příloha č. 12.

8.3.2 Testování propustnosti sítě

Testování se provádělo několika způsoby:

- Mikrotik Bandwidth test
- TamoSoft Throughput test
- NetlO-GUI

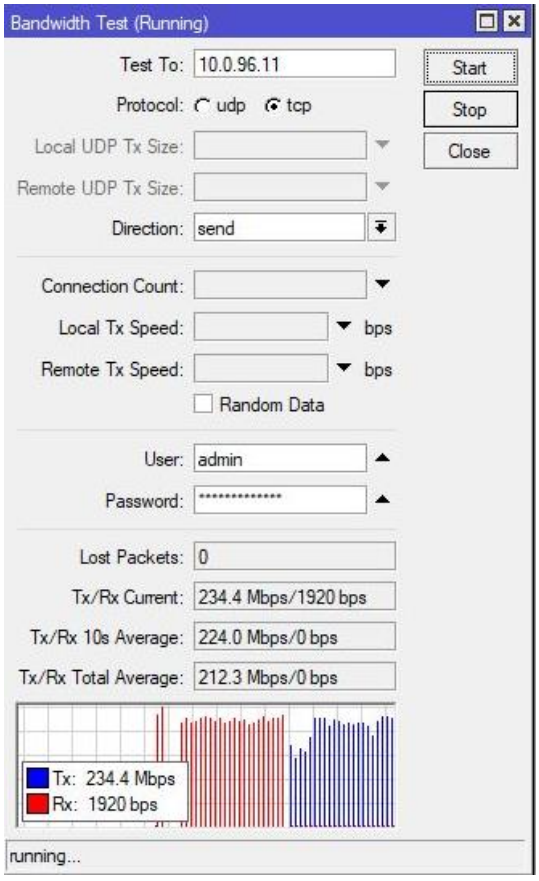
Mikrotik Bandwidth test

MikroTik RouterOS je operační systém hardwaru MikroTik RouterBoard. Lze jej také nainstalovat na PC a promění jej v router se všemi nezbytnými funkcemi – směrování, firewall,

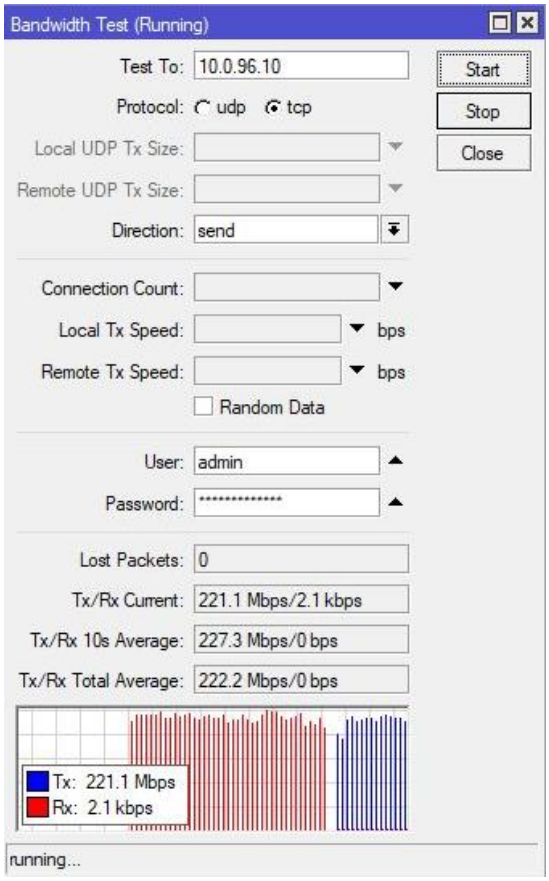
správa šířky pásma, bezdrátový přístupový bod, backhaul link, hotspot brána, VPN server a další. V zařízeních MikroTik můžete otestovat šířku pásma k místu, kde jste připojeni. Test používá standardní protokol TCP. Něž se spustí samotný test je potřeba provedení několika kroků:

- **Test To:** Cílová IP adresa, se kterou chcete vidět šířku pásma
- **Protokol:** vyberte testovací protokol, jako je UDP a TCP
- **Směr:** vyberte test šířky pásma odeslání nebo příjmu
- **Uživatel a heslo:** pokud má cílový uzel uživatelské jméno a heslo, zadejte pole.

Obr. 1 Bandwidth test 1 (A na B)



Obr. 2 Bandwidth test 2 (B na A)



Zdroj: Autor

Shnutí testu

Test byl proveden z budovy A na budovy B a naopak za podmínek běžného provozu školy v době odpoledních hodinách, kdy je považováno, že síť je podprůměrně vytěžována.

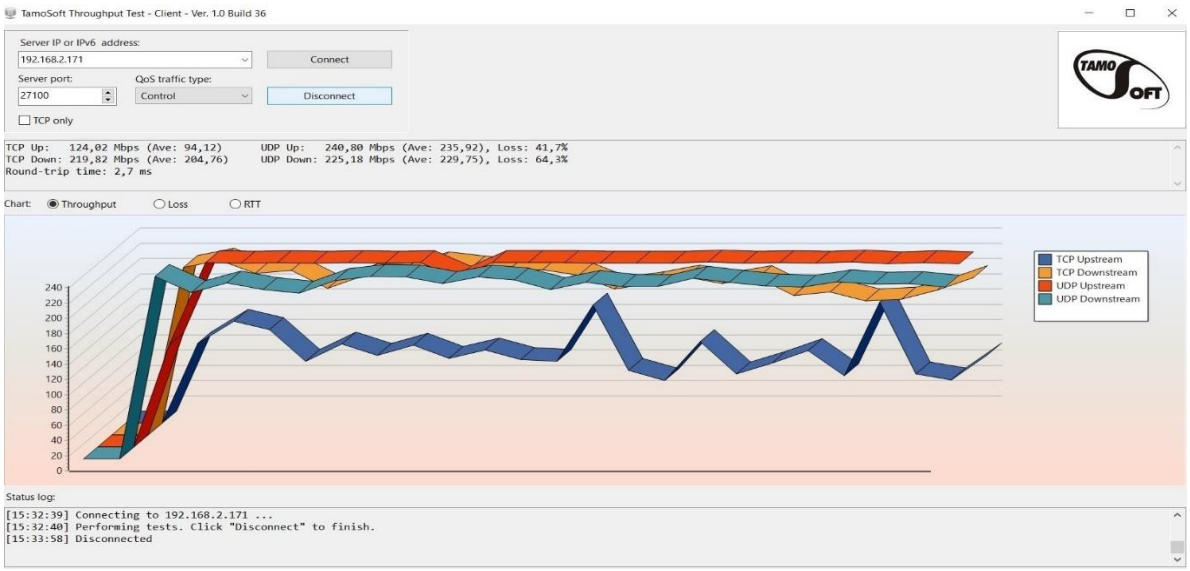
Teoretická hodnota propustnosti je 500 Mbps. Naměřené hodnoty jsou ve směru routeru na budově A, router na budově B 234,4 Mbps, a naopak je to 221,1 Mbps. V testu byl použit TCP protokol a test je továrně nastavený tak, že počítá pouze TCP data (TCP hlavička a IP hlavička nejsou zahrnuty). Výsledky měření se neshodují ani nepřibližují k hodnotě, kterou se provider zaručil poskytovat. Hodnoty ukazují výrazné zpomalení rychlosti sítě a propustnosti dat. Důsledkem těchto naměřených hodnot jsou povětrnostní podmínky, které nastali před měsícem. Silný vítr pootočil jednou z antén, tudíž antény nemají plnou viditelnosti mezi sebou, což má negativní vliv na kvalitu a stabilitu bezdrátového spojení.

TamoSoft Throughput test

První aplikace pro testování výkonu bezdrátové nebo kabelové sítě je TamoSoft Throughput test. Tento nástroj nepřetržitě odesílá datové toky TCP a UDP po vaší síti a vypočítává důležité metriky, jako jsou hodnoty propustnosti směrem nahoru a dolů, ztráta paketů a doba oběhu, a zobrazuje výsledky v číselném i grafickém formátu. Test průchodnosti TamoSoft podporuje připojení IPv4 i IPv6 a umožňuje uživateli vyhodnotit výkon sítě v závislosti na nastavení kvality služby (QoS).

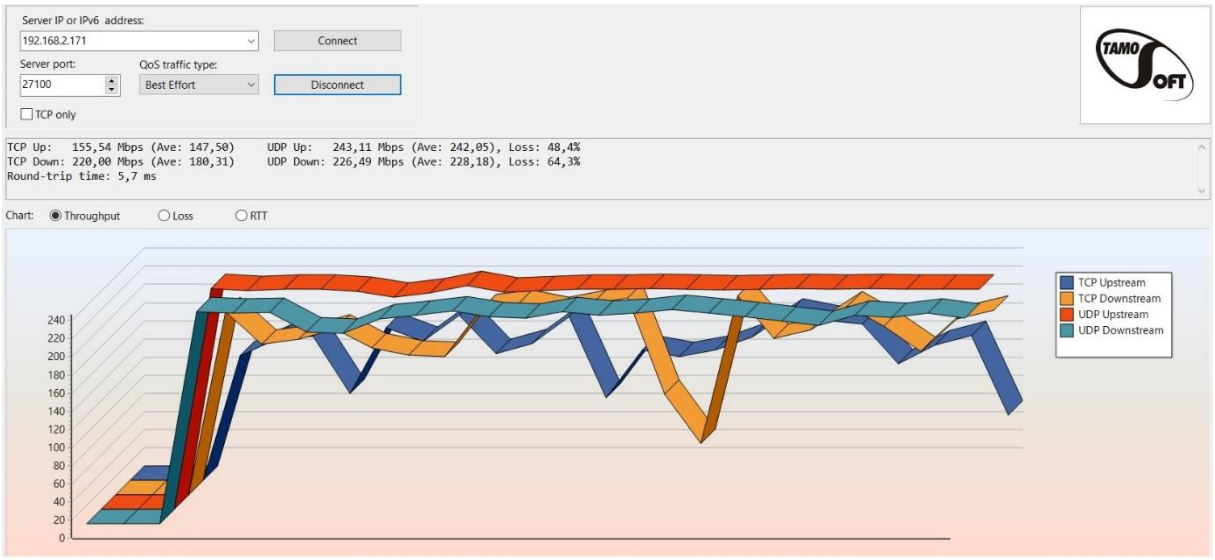
K provedení testu propustnosti je zapotřebí dvou počítačů s používá aplikace: Na prvním PC režim server a na druhém PC režim klienta. Na straně klienta je potřeba zadat IP adresu serverové části druhého počítače. IP adresu lze zjisti v nastavení síťového adaptéru nebo pomocí příkazu „ipconfig“, který zapíšeme do příkazového řádku cmd.exe na operačním systému Windows. Serverová část aplikace naslouchá připojení od klienta a klient se připojí k serveru. Jakmile je spojení navázáno, klient a server odesílají data oběma směry a klientská část aplikace vypočítá a zobrazí síťové metriky.

Obr. 3 TamoSoft test 1



Zdroj: Autor

Obr. 4 TamoSoft test 2



Zdroj: Autor

Shrnutí testování

Testování pomocí této aplikace probíhalo za podmínek běžného neboli středního vytížení sítě, kde bylo naměřeno TCP Up 124 Mbps a TCP Down 219 Mbps viz obrázek č. 3. Zde je názorně vidět, že propustnost sítě je snížena v důsledků většího množství lidí připojených do sítě. Další

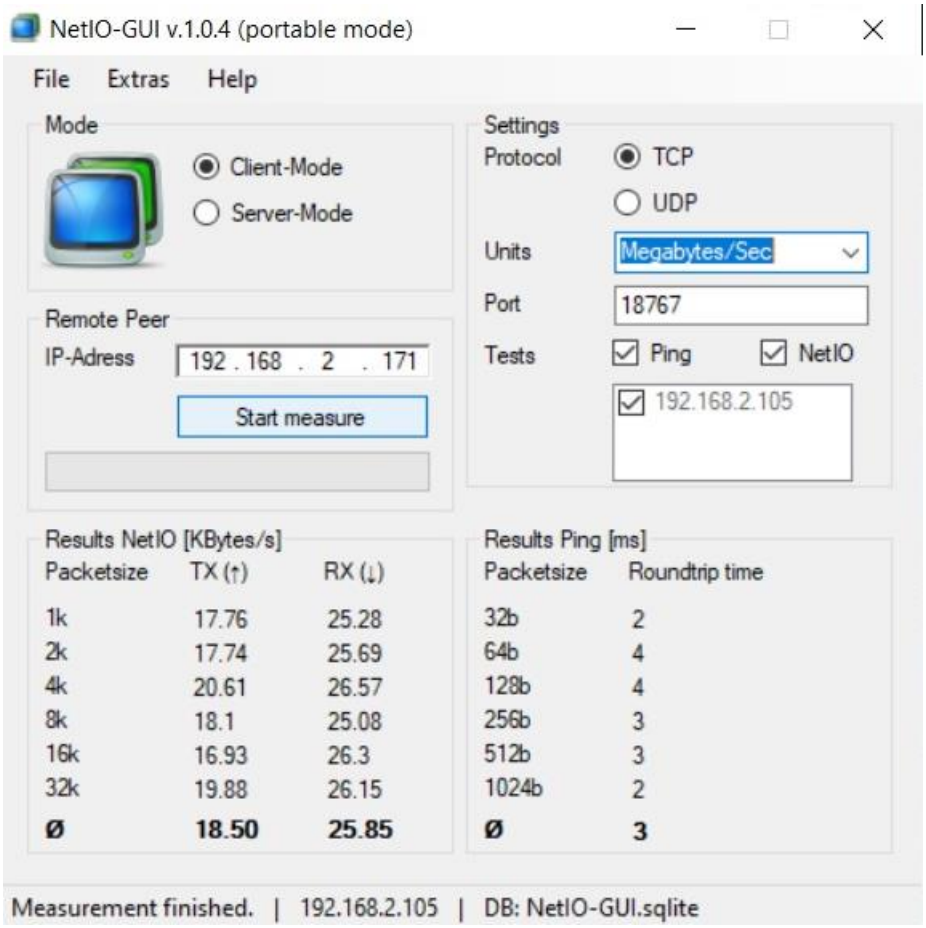
měření bylo za podmínek, kdy ve škole bylo minimální počet lidi tudíž i menší vytížení sítě viz obrázek č. 4. V tomto případě byli výsledky oproti předchozí podmínce lepší. Bylo naměřeno TCP Up 155 Mbps a TCP Down 220 Mbps. Měření bylo provedeno 10krát, aby bylo dosaženo potlačení chyb vzniklé při měření. Všechna měření jsou v příloze č. 13. Naměřené výsledky ukazují rozdíl mezi sítí za běžného provozu v době plné probíhající výuky a v doby sníženého zatížení sítě v době odpoledních, kdy ve škole probíhá méně výuky. Hodnoty od předešlého testu jsou více výrazně nižší, než od hodnoty zaručené poskytovatelem což je důsledkem špatné viditelnosti antén mezi sebou.

NetIO-GUI

Druhou aplikací, která byla při měření použita, byla NetIO-GUI. Aplikace je open source a je podporována pouze na operačním systému Microsoft Windows. Aplikace je továrně nastavena tak, že směrem k serveru se pokusí odeslat packety o velikosti 1k až 32k a následně rychlosti zaslaných packetů zprůměruje. Neopomenutelnou součástí aplikace je také odezva (PING), kdy se aplikace pokusí odeslat packety o velikosti 32b až 1024b a následně opět zprůměruje naměřené výsledky.

Vlastní měření probíhá tak, že se aplikace spustí na dvou počítačích, kdy na jednom se spustí v Client-Mode a na druhém v Server-Mode. Na počítači s klientskou částí je poté nutné specifikovat IP adresu serverové části – druhého počítače. IP adresu lze na počítači zjistit například pomocí příkazu „ipconfig“, který zadáme do příkazové řádky (cmd.exe na systému Microsoft Windows). Na závěr je nutné vybrat, zdali chceme k měření využít protokol TCP nebo UDP.

Obr. 5 NetIO-GUI test



Zdroj: Autor

Testování aplikací NetIO-GUI probíhalo za běžného provozu školy. Měření bylo provedeno 20krát, aby bylo dosaženo potlačení chyb vzniklé při měření. Průběh testu byl takový, že se nastavila aplikace na dvou počítačích a směrem na počítač kde byl nastaven Server-Mode se začali posílat pakety o různých velikostí. Teoretická rychlost sítě je 500 Mbps a průměrná hodnota měření je 145 Mbps. Všechna měření jsou v příloze č.14. Jak bylo zmíněno v předchozích testování je to důsledkem špatné viditelnosti antén v bezdrátovém spoji.

8.3.3 SWOT analýza

Dalším krokem praktické části této diplomové práce bylo provedení analýzy, pro kterou byla vybrána metoda SWOT analýza, jelikož tato metoda umožňuje jednoduché a vhodné zpracování získaných informací. Byla provedena pouze jednou osobou se závěrem zmapovat

školní informační systém. SWOT analýza je nástrojem, který slouží ke zjištění situace v organizaci. Zkratka SWOT se skládá z prvních písmen čtyř anglických slov, kterými jsou Strenghts, Weaknesses, Opportunities a Threats. V překladu se SWOT analýza zabývá zkoumáním silných a slabých stránek, dále příležitostí a hrozeb. Tato analýza je využívána především v marketingu a je součástí dlouhodobého, tedy strategického plánování organizace. Z tohoto důvodu není SWOT analýza pouhým vyjádřením silných a slabých stránek, možností a hrozeb, ale také nalezením možných strategií při řešení problémů, které se v organizaci vyskytují.

Na základě poskytnutých materiálů a rozhovorů se správcem školní sítě byla zpracována analýza celé školní sítě.

Silné stránky:

- ve všech učebnách a kabinetech je možný přístup do školní sítě a na internet
- plné pokrytí Wi-Fi na budově A, B, C
- optický přívod internetu (rychlost 750Mbit/s)
- sjednocená síť na všech budovách
- segmentace sítě pomocí VLAN
- centrální správa Wi-Fi.

Slabé stránky:

- Wi-Fi na budově C je nestabilní (zastaralá technologie)
- stáří switchů na budově C
- zastaralý a z části nefunkční kamerový systém budovy B
- pomalý bezdrátový spoj mezi budovou A a B (250Mbit/s)
- nedostatečná dokumentace sítě
- nestabilní elektrická síť v budově B
- nedostatek povědomí o bezpečnosti u zaměstnanců.

Příležitosti:

- získání finančních prostředků od zřizovatele školy na modernizaci celé školní sítě

- využití projektů EU na modernizaci školní sítě
- možnost zajištění potenciálních dárců pro modernizaci školní sítě
- zvýšení přenosové rychlosti a stability školní sítě
- posílení monitoringu datové sítě
- možnost rozšíření nástrojů Microsoft Office 365
- možnost zavedení moderního a funkčního přístupového systému (monitorování vstupů žáků, čipování zaměstnanců pro přehled pracovní doby, odesílání SMS rodičům a jiné)
- zvýšení bezpečnosti a možnost dohledávat bezpečnostní incidenty.

Hrozby:

- výpadek školní sítě 42
- fyzické poškození optického kabelu
- napadení vnitřním uživatelem sítě
- odcizení technického vybavení
- morální zastaralost systému školní sítě
- porušení nebo selhání technického vybavení
- zneužití identity
- nedostatek zaměstnanců s odbornou úrovní
- chybné používání techniky
- porušení bezpečnostní politiky
- škodlivý kód (viry, spyware, trojské koně)
- pochybení ze strany zaměstnanců.

Shrnutím zjištěných informací jsem dospěl k závěru, že je potřeba nahradit zastaralé datové rozvody a rozšířit optickou síť. Tato výměna by měla být provedena v prvním kroku. Z analýzy dále vyplynulo, že na budově B jsou současné přístupové body a Wi-Fi zastaralé, měly by být vyměněny ve druhém kroku. Protože kamerový systém je zastaralý, z části nefunkční, a elektrická síť je nestabilní, bude toto další oblastí na vylepšení.

9 Návrh na zlepšení

Z předchozí kapitoly, kde je popsáno penetrační testování a provedena analýza školní sítě školy, bylo zjištěno, že její stav v budovách B a C je zastaralý a neodpovídající dnešním moderním standardům a požadavkům pro maximální využití ICT techniky ve škole. Pro modernizaci sítě bylo proto navrženo řešení, které se týká dvou oblastí.

9.1.1 Modernizace webových stránek

Prvním krokem pro webových stránek by mělo být odstranění absence tokenů Anti-CSRF, které probíhá v několika fázích.

Fáze: Architektura a návrh

Použití prověřené knihovny nebo rámce, který nedovolí, aby se tato slabina vyskytla, nebo poskytuje konstrukce, díky nimž se této slabosti lze snadněji vyhnout. Použití například balíčků anti-CSRF, jako je OWASP CSRFGuard.

Fáze: Implementace

Ve fázi implementace by mělo proběhnout zajištění toho, aby aplikace neobsahovala problémy se skriptováním mezi weby, protože většinu obran CSRF lze obejít pomocí skriptu řízeného útočníkem.

Fáze: Architektura a design

V této fázi se pak pro každý formulář vygeneruje unikátní nonce. Následuje vložení nonce do formuláře a ověření nonce po obdržení formuláře. Dále by mělo proběhnout ujištění, že nonce není předvídatelné (CWE-330), což lze ovšem obejít pomocí XSS. Dalším krokem je identifikace zvláště nebezpečné operace. Když uživatel provede nebezpečnou operaci, odešle samostatnou žádost o potvrzení za účelem ujištění, že uživatel zamýšlel tuto operaci provést.

Popis postupu použití metody „double-submitted cookie“, která byla popsána Feltenem a Zellerem: „*Když uživatel navštíví web, web by měl vygenerovat pseudonáhodnou hodnotu a nastavit ji jako soubor cookie na počítači uživatele. Web by měl vyžadovat, aby každé odeslání formuláře obsahovalo tuto hodnotu jako hodnotu formuláře a také jako hodnotu souboru cookie. Když je na web odeslán požadavek POST, měl by být požadavek považován za platný pouze v případě, že hodnota formuláře a hodnota souboru cookie jsou stejné.*“

Kvůli zásadám stejného původu nemůže útočník číst nebo upravovat hodnotu uloženou v souboru cookie. Pro úspěšné odeslání formuláře jménem uživatele by útočník musel správně uhodnout pseudonáhodnou hodnotu, ovšem pokud je pseudonáhodná hodnota kryptograficky silná, bude to neúměrně obtížné. Jelikož technika vyžaduje Javascript, nemusí fungovat pro prohlížeče, které mají JavaScript vypnutý.

Použití ovládacího prvku ESAPI Session Management, který obsahuje komponentu pro CSRF. Nedoporučuje se použití metody GET pro žádný požadavek, který spouští změnu stavu.

Fáze: Implementace

Ve fázi implementace probíhá kontrola hlavičky HTTP Referer, za účelem zjištění, zda požadavek pochází z očekávané stránky. Tím by se mohly narušit legitimní funkce, protože uživatelé nebo proxy by mohli zakázat odesílání Referera z důvodu ochrany osobních údajů.

Druhým doporučením na zlepšení je odstranění chybějícího záhlaví Anti-clickjacking. Moderní webové prohlížeče podporují HTTP hlavičky Content-Security-Policy a X-Frame-Options. Mělo by se provést ujištění, že jeden z nich je nastaven na všech webových stránkách vrácených vaším webem. Pokud se očekává, že stránka bude orámována pouze stránkami na vašem serveru (např. je součástí FRAMESET), pak by se měl použít SAMEORIGIN, jinak pokud se nikdy neočekává, že stránka bude orámována, mělo by se použít DENY. Případné také připadá v úvahu zvážení implementace direktivy „frame-ancestors“ zásad zabezpečení obsahu. Další tip na zlepšení chybějícího záhlaví Anti-clickjacking je ujištění, že v odpovědi je přítomno pouze jediné záhlaví X-Frame-Options.

Třetím doporučením pro zlepšení stránek je zajištění načtení zdrojových souborů JavaScriptu pouze z důvěryhodných zdrojů, tak aby zdroje nemohly být ovládány koncovými uživateli aplikace.

Posledním návrhem na inovaci je vynucení UTF-8 pro veškerý textový obsah v hlavičce HTTP i v Meta značkách v HTML nebo v deklaracích kódování v XML.

9.1.2 Modernizace školní sítě

Pří návrhu inovace je doporučeno mít v celé síti sjednocenou kategorii kabeláže. Po provedení analýzy bylo zjištěno, že na budově C je větší zastoupení kategorie CAT5E. Proto jsem zvolil sjednotit strukturovanou kabeláž na všech budovách na UTP kategorie CAT6A zajištující 1Gb/s přenos po celé jeho délce a rychlosti 10 Gb/s na vzdálenost 55 metrů. Po prozkoumání nabídek na trhu byl vybrán instalační kabel PremiumCord CAT6A FTP v krabicovém balení (305 m). Tyto kabely by se měly uložit do vhodných elektroinstalačních lišt, aby se zamezilo jejich poškození. Pro rychlejší datový přenos mezi rozvaděči a zlepšení propustnosti celé datové sítě by se měla vybudovat optická síť. Z tohoto důvodu byl vybrán typ kabelu Masterlan optický patch cord, LCupc/LCupc, Simplex. Pro připojení k zařízení je ale nutné zakoupit dále moduly SFP shodující se s výrobcem aktivních prvků.

Tab. 3 Finanční rozvaha kabeláže

Položka	Počet kusů	Cena vč. DPH
PremiumCord FTP kabel CAT6A Box (305 m)	7	37 240,00 Kč
Masterlan optický patch cord, LCupc/LCupc, Simplex	30	2 670,00 Kč
Konektor Solarix RJ-45 CAT6 UTP (100 ks)	2	476,00 Kč
Mikrotik SFP optický modul	60	18 000,00 Kč
Celkem s DPH		**58 386,00 Kč**

Škola má tři budovy, a proto je nutné zavést rychlé a stabilní propojení mezi budovami A, B a C. Následující modernizací je nový a výkonnější záložní zdroj UPS, jelikož stávající záložní zdroj je slabý a v případě poruchy napájení dokáže nabíjet pouze třicet minut. Na základě těchto požadavků byl zvolen záložní zdroj APC Smart-UPS SRT 5000VA, který disponuje napájecí jednotkou s výstupním výkonem na úrovni 4,5 kW/ 5 kW.

Dalším krokem by mělo být navrhnutí modernizace serveru za výkonnější s možností virtualizace. S tím se současně navazuje zavedení výkonnějšího firewallu. První vrstvu ochrany lokální sítě od poskytovatele internetu zastoupí firewall nové generace od společnosti Fortinet, konkrétně typ FortiGate 100F. Zařízení disponuje dostatečným výkonem i pro případné rozšíření sítě. Ochranu sítě lze podpořit rozšiřujícími moduly, které jsou poskytovány formou ročních licencí. Kalkulace obsahuje základní verzi bez přidaných modulů. Zástupce pro server byl zvolen Fujitsu Primergy TX2550 M4. Tento výkonný server je vybaven nejnovější rodinou škálovatelných procesorů Intel Xeon s až 26 jádry. Spolu s až 768 GB paměti DDR4 je ideální pro většinu aplikací spoléhajících na procesor a paměť. Dále na budově C byla navrhnuta nová instalace aktivních prvků s dostatečnou kapacitou a rychlostí. Pro inovaci přístupových bodů jsem vybral TP-LINK EAP265 HD. Přístupový bod disponuje dlouhým dosahem přes všesměrové antény, možnosti připojení až 120 klientů a mnoha dalšími užitečným funkcemi. Dále byl zvolen směrovač MikroTik Cloud Core CCR1016-12S-1S+ se 16-ti jádry a nabídkou až 12 portů SFP a mnoha dalšími technologiemi. V posledním aktivním prvkem je přepínač od stejné značky jako směrovač kvůli lepší správě prvků. MikroTik CRS354-48G-4S+2Q+RM je vhodný díky vysoké datové propustnosti a že obsahuje operační prostředí RouterOS.

Tab. 4 Finanční rozvaha síťových prvků

Položky	Počet kusů	Cena vč. DPH
APC Smart-UPS SRT 5000VA	1	118 225,00 Kč
Fortinet FortiGate 100F	1	54 942,00 Kč
Fujitsu Primergy TX2550 M4	1	52 490,00 Kč
TP-LINK EAP265 HD	8	24 472,00 Kč
MikroTik Cloud Core CCR1016-12S-1S+	1	14 790,00 Kč
MikroTik CRS354-48G-4S+2Q+RM	1	9 000,00 Kč
Celkem s DPH		**273 919,00 Kč**

Budova B disponuje zastaralým a z části nefunkčním kamerovým systémem, a proto je potřeba instalovat nový kamerový systém včetně zavedení čipů na vstupy do budovy. Na této budově byla dále navrhnuta nová elektrická síť, protože současná elektrická sít je nestabilní a vyskytují se zde časté výpadky proudu, což je pro výuku a praktické vyučování ve zdravotnictví velice problematické. V neposlední řadě bylo doporučeno proškolení zaměstnanců o chování na

internetu a ve školní síti v rámci bezpečnosti a ochrany dat. A v rámci poslední modernizace by bylo vytvoření kompletní dokumentace sítě.

9.1.3 **Modernizace propojeni budov A, B**

Při testování propojení LAN sítí školy, byli zjištěné negativní vlivy, které mají za důsledek snížení propustnosti sítě. Prvním návrhem na zlepšení je konzultace od daném problémem s providerem, který zajištuje internet a správu propojení. O provedení nové kalibraci bezdrátového spoje, aby bylo dosaženo hodnot, kterýma se provider zaručil poskytovat.

Druhým návrhem je nový bezdrátový spoj od firmy ALCOMA a.s. která je přední česká společnosti zabývající se vývojem a výrobou mikrovlnných radioreléových spojů bod-bod. Nový spoj by byl bezdrátový v 60GHz pásmu s 1 Gb/s rychlostí. V tomto návrhu je zapotřebí placení licencovaného pásma Českému telekomunikačnímu úřadu za využívání pásma. Cena této modernizace se pohybuje kolem 250 000 Kč za antény, práci a roční poplatky za využívání pásma.

Třetím návrhem, je efektivně propojit sítě pomocí vybudováním optického spoje z budovy A do budovy B. Toto řešení je ale výrazně ve vyšší finanční náročnosti, protože samotná škola a zřejmě ani zřizovatel školy by neměl takové finanční prostředky. Proto by se škola musela zapojit do Evropského projektu pro vývoj vzdělávání a odborné přípravy. Finanční odhad řešení je v řádech milionu vzhledem ke vzdálenosti a umístění budov.

10 Závěr

Tato diplomová práce se věnovala popisu problematiky počítačových sítí v rámci optimalizace a zabezpečení lokálních sítí na příkladu vybrané školy. Pro účely této diplomové práce byla provedena technická a bezpečnostní analýza IS a počítačové sítě na škole Vyšší odborná škola ekonomická, sociální a zdravotnická, Obchodní akademie, Střední pedagogická škola a Střední zdravotnická škola, Most, příspěvková organizace a byla navržena efektivnější opatření, která zrychlí veškeré procesy spojené s prací s daty, umožní bezpečnější uchování a přenos dat a také zabrání výpadkům. Jinými slovy byla navržena taková konkrétní opatření, která by mohla zajistit školu odpovídajícím technickým zázemím a vytvořit vhodné prostředí pro efektivní užívání počítačové sítě ve vzdělávání.

Ze základní charakteristiky školy vyplynulo, že rozměry školy jsou nadprůměrné, a v rámci školy nebyla v posledních letech provedena žádná technologická modernizace. Sice na základě požadavků doby se vždy technicky přizpůsobila potřebám ICT, ale současné nároky, které jsou kladeny na využívání ICT, jenž jsou mnohem vyšší a náročnější, jsou na hranici odpovídajícího technického provedení infrastruktury sítě školy.

Nejdříve byla zmapována stávající školní síť včetně jejích bezpečnostních prvků a poté byla zmapována webová stránka školy, na základě čehož bylo provedeno testování webové stránky metodou penetračního testování. Bylo nalezeno několik zranitelných míst včetně uvedení úrovně rizika ve zdrojovém kódu a následně byla navržena vhodná opatření pro minimalizaci zranitelných míst a zefektivnění užívání a zabezpečení webových stránek. Poté mi vedení školy již další penetrační testování neumožnilo. Následně na to, bylo zmapováno propojení lokálních sítí a prověření propojení sítí pomocí testů. Výsledky testů ukázaly, že propojení není takové, jaké se poskytovatel internetu zaručil poskytovat. V návaznosti na to byla navrhnuta řešení vedoucí k eliminaci daného problému. První byl požadavkem na poskytovatele internetu o proměření a nastavení antén. Druhým byl návrh na vybudování nového bezdrátového spoje a vysoké přenosově rychlosti. Následujícím návrhem bylo možné budoucí zapojení školy do Evropského projektu pro vývoj vzdělávání a odborné přípravy pro vybudování nové optické propojení budov.

Na základě provedení SWOT analýzy byly vyhodnoceny kladné a záporné stránky sítě a navrženy příležitosti k zefektivnění jejich užívání, včetně uvedení možných ohrožení a rizik. Výsledkem diplomové práce je návrh modernizace stávající sítě a s tím související i modernizace informačního systému školy. Provedenou modernizací by měla být kompletní rekonstrukce kabelové infrastruktury včetně vybudování optické sítě, která by zlepšila propustnost celé datové sítě včetně instalace vhodných elektroinstalačních lišt pro jejich ochranu. Také vyměnění nových switchů a přístupových bodů za nové a modernější v budově C. Rovněž modernizace prvků v servrovně budovy, a to v podobě novějších a výkonnějších záložních zdrojů, serverů a firewallu. Dále obnovení staré elektrické sítě v budově B za takovou, která bude vyhovovat požadavkům školní sítě a dnešní doby a modernizace zabezpečení v budově B v podobě kamerového systému včetně zabezpečení přístupových bodů na vstupy do budovy. Z toho pohledu byl cíl diplomové práce naplněn.

Dále je navrženo proškolení zaměstnanců ohledně chování na internetu a ve školní síti v rámci bezpečnosti a ochrany dat. Velmi důležitým faktorem, který je potřeba brát v úvahu při rozboru a řešení problematiky bezpečnosti je komplexní pohled. Protože nevyváženost může být způsobena zaměřením se na oblast technického zabezpečení, která je zpravidla v popředí, ale neméně důležitá je i oblast „lidského“ zabezpečení. Celý systém řízení bezpečnosti IS ve škole by se měl zaměřit jak na povědomí všech pracovníků školy o bezpečnosti IS, tak i na výběr a implementaci vhodných technických opatření.

Pro správnou funkčnost bezpečnostních opatření v dané škole platí, a i nadále bude platit, dodržování základních pravidel při práci s informačními systémy jako jsou například nesdělovat si přístupová jména, hesla a kódy, nezapisovat si hesla na volně přístupná místa a v neposlední řadě pohybovat se rozvážně v prostředí internetu a nestahovat neznámé aplikace.

Výsledky analýzy a návrh opatření budou následně předloženy a projednány s vedením školy za účelem modernizace technického prostředí pro budoucí užívání informačních a digitálních technologií ve škole v 21. století.

11 Seznam použitých zdrojů

[1] BAGAD, V. S. a I. A. DHOTRE. *Computer Networks. India: Technical Publications Pune*, 2009. ISBN 9788184316179.

[2] BUCHALCEVOVÁ, Alena. *Metodiky vývoje a údržby informačních systémů: kategorizace, agilní metodiky, vzory pro návrh metodiky.* Praha: Grada, 2005. Management v informační společnosti. ISBN isbn80-247-1075-7.

[3] BURIAN, Pavel. *Internet inteligentních aktivit*. Praha: Grada, 2014. Průvodce (Grada). ISBN isbn978-80-247-5137-5.

[4] *ČSN EN ISO/IEC 27000 (369790): Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník*. 2017. Brusel: CEN-CENELEC, 2017.

[5] DEAN, Tamara. *CompTIA Network+ 2009 In Depth*. United States: Cengage Learning, 2009. ISBN 978-15-986-3878-3.

[6] FIRMAN, Petr. *Bezpečnostní analýza školního informačního systému*. Praha, 2020. Bakalářská práce. Česká zemědělská univerzita v Praze. Vedoucí práce Ing. Zdeňkovi Votrubovi, Ph.D.

[7] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 5., aktualiz. vyd. Brno: Computer Press, 2011. ISBN isbn978-80-251-3176-3.

[8] HUŽVÁR, Miroslav a Peter LACO. *Informačné technológie v ekonomickej praxi*. Bratislava: Wolters Kluwer, 2014. Ekonómia. ISBN 978-80-8168-085-4.

[9] CHROMÝ, Jan. *Informační a komunikační technologie pro hotelnictví a cestovní ruch*. Praha: Vysoká škola hotelová v Praze 8, 2008. ISBN isbn978-80-86578-76-7.

[10] *Internet a jeho služby* [online]. [cit. 2022-01-25]. Dostupné z: http://ijs.8u.cz/

[11] Jaký RAID nasadit v NAS? Digitální domácnost [online]. [cit. 2022-01-24]. Dostupné z: https://www.digitalnidomacnost.cz/clanek/jaky-raid-nasadit-v-nas

[12] KALUŽA, Jindřich a Ludmila KALUŽOVÁ. *Informatika*. Praha: Ekopress, 2012. ISBN 978-80-86929-83-5.

[13] KLEMENT, Milan. *Technologie bezdrátových sítí – základní principy a standardy*. Olomouc: Univerzita Palackého, 2017. ISBN 978-80-244-5156-5.

[14] KNOPOVÁ, Martina. *Bezpečnost dat v informačních systémech*. *Ikaros* [online]. 2011, 2011, 15(6), 1 [cit. 2020-02-19]. ISSN 1212-5075. Dostupné z: https://ikaros.cz/bezpecnost-dat-v-informacnich-systemech

[15] KUROSE, James F. a Keith W. ROSS. Počítačové sítě. Brno: Computer Press, 2014. ISBN ean:9788025138250.

[16] *Nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů*. In:. Praha: Evropský parlament, Evropská rad, 2018, ročník 1, 2016/679.

[17] *Nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů*. In:. Praha: Evropský parlament, Evropská rad, 2018, ročník 1, 2016/679.

[18] POKORNÝ, Miroslav a Jan LAVRINČÍK. *Teorie systémů I*. Olomouc: Moravská vysoká škola Olomouc, 2009. ISBN 978-80-87240-09-0.

[19] POUR, Jan. *Informační systémy a technologie*. Praha: Vysoká škola ekonomie a managementu, 2006. ISBN 80-86730-03-4.

[20] PROCHÁZKA, David. *První kroky s internetem*. 3., aktualiz. vyd. Praha: Grada, 2010. Snadno a rychle (Grada). ISBN isbn978-80-247-3255-8.

[21] ŘEPA, Václav. *Analýza a návrh informačních systémů*. Praha: Ekopress, 1999. ISBN isbn80-861-1913-0.

[22] SODOMKA, Petr a Hana KLČOVÁ. *Informační systémy v podnikové praxi*. 2., aktualiz. a rozš. vyd. Brno: Computer Press, 2010. ISBN isbn978-80-251-2878-7.

[23] SOMSEDÍK, Jan. *Zabezpečení informačního systému v podniku* [online]. Praha, 2014 [cit. 2020-02-19]. Dostupné z: https://is.ambis.cz/th/y7tmx/JAN_SOMSEDIK_.pdf. Diplomová práce. Bankovní institut vysoká škola Praha.

[24] SOSINSKY, Barrie A. *Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]*. Brno: Computer Press, 2010. ISBN isbn978-80-251-3363-7.

[25] SVATÁ, Vlasta. *Audit informačního systému*. Praha: Professional Publishing, 2011. ISBN isbn978-80-7431-034-8.

[26] ŠILHAVÝ, Radek, Petr ŠILHAVÝ, Zdenka PROKOPOVÁ, Pavel POKORNÝ, Martin SYSEL, Miroslav MATÝSEK, Karel VLČEK a Libuše SVOBDOVÁ. *Vybrané aspekty návrhu webových informačních systémů*. Vsetín: Scientific Press, 2013. ISBN 978-80-904741-3-0

[27] ŠULC, Vladimír. *Kybernetická bezpečnost*. 2018. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN isbn978-80-7380-737-5.

[28] VOŘÍŠEK, Jiří. *Informační systémy a jejich řízení*. 3. vyd. Praha: Bankovní institut vysoká škola, 2007. ISBN 978-80-7265-100-9.

[29] *Vyhláška o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor*. In: . Praha: Národní bezpečnostní úřad, 2005, ročník 2, 523/2005 Sb.

12 **Přílohy**

Příloha 1…… Parametry Mikrotik RB4011iGS+RM

Příloha 2…… Parametry Mikrotik RB750Gr3

Příloha 3…… Parametry TP-Link T2600G-28TS (TL-SG3424)

Příloha 4…… Parametry TP-Link EAP245

Příloha 5…… Parametry Synalogy DS1621+

Příloha 6…… Parametry Fujitsu CELVIN Q800

Příloha 7…… Schéma budov s rozmístěním aktivních prvků a rozvodů

Příloha 8…… Schéma topologie sítě školy

Příloha 9…… Zranitelnost úrovně střední: absence tokenů Anti-CSRF

Příloha 10…….. Zranitelnost úrovně střední: záhlaví Anti-clickjacking

Příloha 11…….. Zranitelnost úrovně nižší: chybí záhlaví X-Content-Type-Options

Příloha 12……... Zranitelnost úrovně informativní: nesoulad znaků

Příloha 13……Výsledky testování pomocí aplikace TamoSoft

Příloha 14…… Výsledky testování pomocí aplikace NetIO-GUI

Příloha 1 Parametry Mikrotik RB4011iGS+RM

Tabulka č. 1 Parametry Mikrotik RB4011iGS+RM

Značka	
Výrobce:	MIKROTIK
Upřesnění typu:	Routerboard
Technické detaily	
Použití v interiéru:	ano
Použití v exteriéru:	ne
Podpora IPv6:	ano, plná
DHCP:	ano
NAND (MB):	512
Provozní teplota max (°C):	60
Provozní teplota min (°C):	-20
Firewall:	ano
IPSec:	ano
PoE vstup:	pasivní
PoE výstup:	pasivní
PoE výstup (počet):	1
Procesor	
Počet jader procesoru:	4
Procesor:	Alpine AL21400, 1,4 GHz
Paměť	
Velikost paměti (MB):	1000
Displej a zobrazení	
Displej:	ne
Komunikace	
Podpora 3G:	ne
Podpora 4G/LTE:	ne
Síťová rozhraní	
LAN:	ano
Gigabit LAN:	ano
Wi-Fi:	ne
Rychlost portů:	1 Gb/s
Vstupy a výstupy	
RJ-45 (počet):	10
Rozhraní:	LAN, SFP

SFP (počet):	1
RS-232 port:	ne
Napájení	
Podpora POE:	ano
Napájení max (jack) (V):	230
Napájení max (PoE) (V):	57
Napájení min (PoE) (V):	12
Operační systém	
Operační systém:	MikroTik RouterOS
Licence:	L5
Záruka	
Délka záruky IČO (měsíce):	24
Délka záruky (měsíce):	24
Podpora	
Slot pro SIM:	ne
Zabezpečení	
Výchozí jméno:	admin
Fyzické vlastnosti	
Barva:	černá
Hmotnost (kg):	I.18
Rozměry:	228 x 120 x 30 mm
Výška (mm):	30
Šířka (mm):	228
Hloubka (mm):	120
Další výbava a vlastnosti	
LED indikace:	ano
LED indikace:	ano
Modelové číslo	
Modelové číslo:	RB4011iGS+RM

Příloha 2 Parametry Mikrotik RB750Gr3

Tabulka č. 2 Parametry Mikrotik RB750Gr3

Značka	
Výrobce:	MIKROTIK
Upřesnění typu:	Routerboard
Technické detaily	
Použití v interiéru:	ano
Použití v exteriéru:	ne
Podpora IPv6:	ano, plná
DHCP:	ano
NAND (MB):	16
Provozní teplota max (°C):	70
Provozní teplota min (°C):	-30
Firewall:	ano
IPSec:	ano
PoE vstup:	pasivní
Procesor	
Počet jader procesoru:	2
Procesor:	MediaTek MT7621A, 880 MHz
Paměť	
Velikost paměti (MB):	256
Displej a zobrazení	
Displej:	ne
Komunikace	
Podpora 3G:	ne
Podpora 4G/LTE:	ne
Síťová rozhraní	
LAN:	ano
Gigabit LAN:	ano
Wi-Fi:	ne
Rychlost portů:	1 Gb/s
Vstupy a výstupy	
USB 2.0 (počet):	1
RJ-45 (počet):	5
Rozhraní:	LAN
RS-232 port:	ne

Čtečka karet	
Podpora MicroSD karet:	ano
Napájení	
Podpora POE:	ano
Spotřeba (W):	5
Napájení max (jack) (V):	30
Napájení max (PoE) (V):	30
Napájení min (jack) (V):	8
Napájení min (PoE) (V):	8
Operační systém	
Operační systém:	MikroTik RouterOS
Licence:	L4
Podpora	
Slot pro SIM:	ne
Zabezpečení	
Výchozí IP:	192.168.88.1
Výchozí jméno:	admin
Fyzické vlastnosti	
Barva:	bílá
Hmotnost (kg):	0.142
Rozměry:	113 x 89 x 28 mm
Výška (mm):	28
Šířka (mm):	113
Hloubka (mm):	89
Další výbava a vlastnosti	
LED indikace:	ano
LED indikace:	ano
Shoda:	CE, FCC
Modelové číslo	
Modelové číslo:	RB750Gr3

Příloha 3 Parametry TP-Link T2600G-28TS (TL-SG3424)

Tabulka č. 3 Parametry TP-Link T2600G-28TS (TL-SG3424)

Značka	
Výrobce:	TP-Link
Typ	T2600G-28TS (TL-SG3424)
Hardwarové funkce	
Standardy a protokoly	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE802.3z, IEEE 802.3ad, IEEE 802.3x, IEEE 802.1d, IEEE 802.1s, IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3x, IEEE 802.1d, IEEE 802.1s, IEEE 802.1w, IEEE 802.1q, IEEE 802.1x, IEEE 802.1p
Rozhraní	24 10/100/1000 Mbps RJ45 portů (Auto Negotiation/Auto MDI/MDIX) 4 1000Mbps SFP sloty 1 port konzoly RJ45 1 Micro-USB konzolový port
Sítová média	10BASE-T: Kabel UTP kategorie 3, 4, 5 (maximálně 100 m) 100BASE-TX/1000Base-T: Kabel kategorie UTP 5, 5e nebo vyšší (maximálně 100 m) 1000BASE-X: MMF, SMF
Počet ventilátorů	Bez ventilátorů
Fyzický bezpečnostní zámek	Ano
Napájení	100~240VAC, 50/60Hz
Spotřeba energie	max. 19,15W (220V/50Hz)
Rozměry	(Š x H x V) 17,32 * 8,7 * 1,73 palce (440 * 220 * 44 mm)
Montáž	Montáž do racku
Maximální spotřeba	15,33W (220V/50Hz)
Maximální odvod tepla	52,30 BTU/h
Výkon	
Šířka pásma / propojovací rovina	56 Gbps
Rychlost předávání paketů	41,67 Mpps

MAC adress table	16k
Jumbo Frame	9216 bajtů
Softwarové funkce	
Quality of Service	Support 802.1p CoS/DSCP priority Support 8 priority queues Queue scheduling: SP, WRR, SP+WRR Port/Flow- based Rate Limiting Voice VLAN
L2 and L2+ Features	Static Routing、DHCP Relay* IGMP Snooping V1/V2/V3 802.3ad LACP (Up to 14 aggregation groups, containing 8 ports per group) Spanning Tree STP/RSTP/MSTP BPDU Filtering/Guard TC/Root Protect Loopback detection 802.3x Flow Control L2PT*
VLAN	Supports up to 4K VLANs simultaneously (out of 4K VLAN IDs) 802.1Q/ MAC/Protocol-based/Private VLAN GARP/GVRP
Access Control List	L2～L4 package filtering based on source and destination MAC address, IP address, TCP/UDP ports, 802.1p, DSCP, protocol and VLAN ID Time Range Based
Security	IP-MAC-Port Binding AAA* 802.1x and Radius Authentication DoS Defend Dynamic ARP Inspection (DAI) SSH v1/v2 SSL v3/TLSv1 Port Security Broadcast/Multicast/Unknown-unicast Storm Control

IPv6	Dual IPv4/IPv6 stack Multicast Listener Discovery (MLD) Snooping IPv6 neighbor discovery (ND) Path maximum transmission unit (MTU) discovery Internet Control Message Protocol (ICMP) version 6 TCPv6/UDPv6 IPv6 ACL* DHCPv6 Snooping* IPv6 Interface*
IPv6 Applications	DHCPv6 Client Ping6 Tracert6 Telnet(v6) IPv6 SNMP IPv6 SSH IPv6 SSL Http/Https IPv6 TFTP IPv6 ACL* IPv6 Interface* IPv6 Routing* DHCPv6 Relay* DHCPv6 Snooping*
Management	Web-based GUI and CLI management SNMP v1/v2c/v3,compatible with public MIBs and TP-LINK private MIBs RMON (1, 2, 3, 9 groups) sFlow* PPPoE Circuit ID* DHCP Relay* DHCP Server* DHCP/BOOTP Client, DHCP Snooping, DHCP Option82 Dual Image CPU Monitoring Port Mirroring Time Setting: SNTP Integrated NDP/NTDP feature Firmware Upgrade: TFTP & Web System Diagnose: VCT SYSLOG & Public MIBS Password Recovery*

Příloha 4 Parametry TP-Link EAP245

Tabulka č. 4 Parametry TP-Link EAP245

Značka	
Výrobce:	TP-Link
Typ:	Dual-Band Wall
Hardwarové funkce	
Standardy a frekvence	802.11a (5GHz), 802.11b (2,4GHz), 802.11g (2,4GHz), 802.11n, 802.11ac
Typ WiFi	WiFi 5
Bezdrátové funkce	
Bezdrátové standardy	IEEE 802.11ac/n/g/b/a
Frekvence	2,4 GHz , 5 GHz
Bezdrátové funkce	• Více SSID (až 16 SSID, 8 pro každé pásmo) • Povolit/zakázat bezdrátové rádio • Automatické přiřazení kanálů • Ovládání vysílacího výkonu (upravte vysílací výkon na dBm) • QoS (WMM) • MU-MIMO • Bezproblémový roaming* • Omada Mesh* • Pásmové řízení • Vyvážení zátěže • Spravedlnost vysílacího času • Beamforming • Sazba limit • Plán restartu • Plán bezdrátového připojení • Statistika bezdrátového připojení založená na SSID/AP/Client

Bezdrátové zabezpečení	• Autentizace portálu* • Řízení přístupu • Bezdrátové filtrování MAC adres • Bezdrátové izolace mezi klienty • Mapování SSID na VLAN • Rogue AP Detection • Podpora 802.1X • 64/128/152-bit WEP / WPA / WPA2-Enterprise, • WPA-PSK / WPA2-PSK
Přenosový výkon	• CE : ≤20 dBm (2.4GHz) ≤23 dBm (5GHz) • FCC: ≤24 dBm (2.4 GHz) ≤24 dBm (5 GHz)
Rychlost	
Rychlost WiFi přenosu	1 750 Mb/s
Přenosová rychlost LAN portů	1 Gbit
Zabezpečení	
Šifrování	WEP 64bit, WEP 128bit, WPA-Enterprise, WPA2-Enterprise
Konektory	
LAN	1 ×
Vlastnosti antény	
Počet interních antén	6 ks
Typ antény	2,4 GHz: 3× 3,5 dBi; 5 GHz: 3× 4 dBi
Pokročilé parametry	
Pokročilé funkce	Gigabit LAN, PoE (Power over Ethernet), QoS (Quality of Service)
Maximální počet SSID	16 ks
Rozměry a hmotnost	
Hloubka	180 mm
Šířka	180 mm
Výška	47,5 mm

Příloha 5 Parametry Synalogy DS1621+

Tabulka č. 5 Parametry Synalogy DS1621+

Značka	
Výrobce:	Synalogy
Upřesnění typu:	DS1621+
Procesor	
Model CPU	AMD Ryzen V1500B
Počet CPU	1
CPU architektura	64-bit
Frekvence CPU	4-core 2.2 GHz
Systém hardwarového šifrování (AES-NI)	ano
Paměť	
Systémová paměť	4 GB DDR4 ECC SODIMM
Předinstalovaný pamětový modul	4 GB DDR4 ECC SODIMM
Celkový počet pamětových slotů	2
Maximální kapacita paměti	32 GB (16 GB x 2)
Uložistě	
Šachty pevného disku	6
Maximální počet šachet pevného disku s rozšiřující jednotkou	16
Sloty disku M.2	2 (DX517 x 2)
Kompatibilní typ disku	3.5" SATA HDD 2.5" SATA HDD 2.5" SATA SSD M.2 2280 NVMe SSD
Extertní porty	
RJ-45 1GbE LAN port	4
Port USB 3.2 Gen 1	3

Port eSATA	2
PCIe	
Rozšíření PCIe	1 x Gen3 x8 slot (x4 link)
Správa úložště	
Maximální velikost jednoho svazku	108 TB
Max. počet interních svazků	64
Mezipamět SSD pro čtení/zápis	ano
SSD trim	ano
Podporovaný typ RAID	Synology Hybrid RAID Basic JBOD RAID 0 RAID 1 RAID 5 RAID 6 RAID 10
Migrace svazku RAID	Basic to RAID 1 Basic to RAID 5 RAID 1 to RAID 5 RAID 5 to RAID 6
Rozšíření svazku pomocí větších pevných disků	Synology Hybrid RAID RAID 1 RAID 5 RAID 6 RAID 10
Rozšíření přidáním pevného disku	Synology Hybrid RAID JBOD RAID 5 RAID 6
Global Hot Spare podporuje RAID typu	Synology Hybrid RAID RAID 1 RAID 5 RAID 6 RAID 10

Příloha 6 Parametry Fujitsu CELVIN Q800

Tabulka č. 6 Paramatry Fujitsu CELVIN Q800

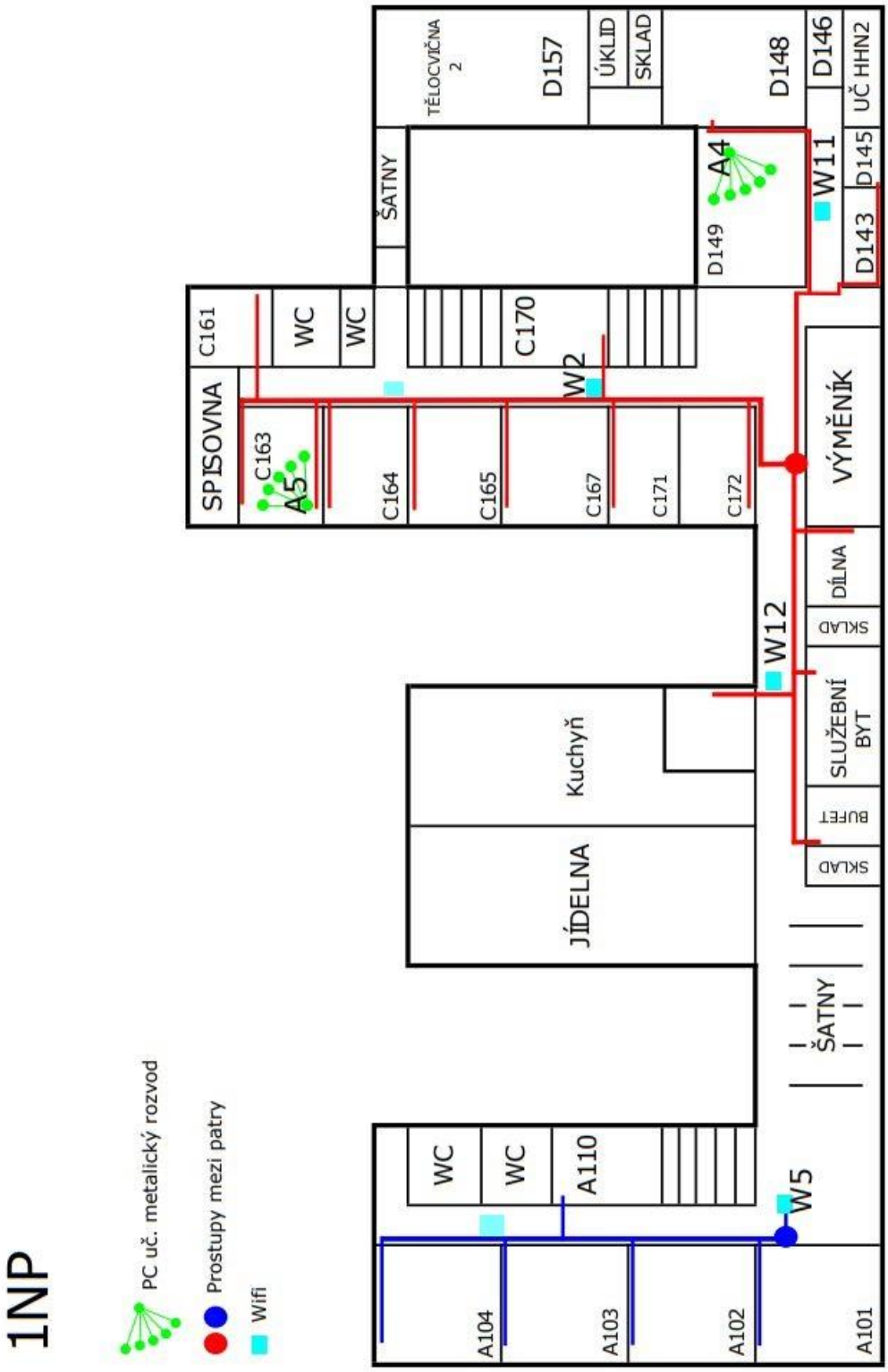
Značka	
Výrobce:	Fujitsu
Upřesnění typu:	CELVIN Q800
Technické specifikace	
Procesor	Intel Atom D525
Pamět	1 GB DDRIII RAM 3 GB DDRIII RAM v kombinaci s BC HDD 512 MB Flash na DOM
Kapacita pevného disku	4 x 2.5-inch or 3.5-inch SATA I/II HDD
Typ pevného disku	SATA
Požadované rozhraní	USB 2.0 / eSATA / Ethernet
LED	USB Status HDD 1 -4 LAN Power
USB	Rear side: 4x USB2.0 (Device class: Printer, mass storage, hub, UPS, pen-drive)
eSATA	2 x (rear / SATA)
Ovládací prvky systému	Tlačítko napájení, tlačítko kopírování jedním dotykem, bzučák (systémové varování), tlačítko reset, tlačítko režimu zobrazení
Softwarové specifikace	

Networking	TCP/IP (IPv4 /IPv6 dual stack), multi IP setting,LACP, Port trunking /NIC teaming: Balance-rr (Round-Robin), Active Backup, Balance XOR, Broadcast, IEEE 802.3ad, Balance-tlb (Adaptive, Transmit Load Balancing), Balance-alb (Adaptive Load Balancing) DHCP client, DHCP server, CIFS/SMB, AFP, NFS v3, HTTP, HTTPS, FTP,SFTP(admin), DDNS, NTP, Telnet, SSH, iSCSI, SNMP,WebDAV Dual Gigabit w/ Jumbo Frame, Bonjour iSCSI initiator for virtual disks (max 8 disks); stack chaining master Virtual disk support for EXT3/ EXT4/ NTFS/ FAT32/ HFS+ Support for VMware VSphere (ESX / ESXi 4.0 and above) via NFS and iSCSI Windows Server 2008 support (Hyper-V & failover clustering) iSCSI target (with multi-LUNs per target) iSCSI LUN online expansion LUN mapping / LUN masking SCSI Primary Commands -3 (SPC-3) support / persistent reservation MC/S (multiple TCP connections / session) support to reach iSCSI target MPIO (multipath input output) for load balancing and failover VLAN 802.1Q USB WiFi-Adapter support IEEE 802.11b/g/n WEP, WPA-personal (AES/TKIP), WPA2-personal (AES)
Správa systému souborů	Správa sdílení v síti “(max. 512 sdílení) Podpora ACL na úrovni sdílené složky Podpora Unicode Žurnálování souborového systému Web Správce souborů Podpora Dokumentů Google (pdf,tif/tiff,ppt,doc,xls,pptx,docx,xlsx,svg,odt)

Správa disků	Správa stavu využití disku; HDD S.M.A.R.T.; Skenování špatných bloků RAID 0/1/5/5+HS/10/6, JBOD, jeden disk Online rozšíření kapacity RAID; online migrace na úrovni RAID Obnova RAID, podpora bitmap
Správa uživatelů	Správa uživatelských kvót Podpora Windows Active Directory, max. 10 tisíc uživatelů Správa uživatelských účtů (max. 4096 uživatelů) Správa uživatelských skupin (max. 512 skupin) Sdílené složky (max. 512) Souběžná připojení (max. 256) Podpora dávkového vytváření uživatelů Uživatelský import/export pro více nasazení CELVIN NAS Oprávnění k podsložce (ACL k souboru/adresáři) Microsoft Networking (Samba) Řízení přístupu k hostiteli (doména/IP)

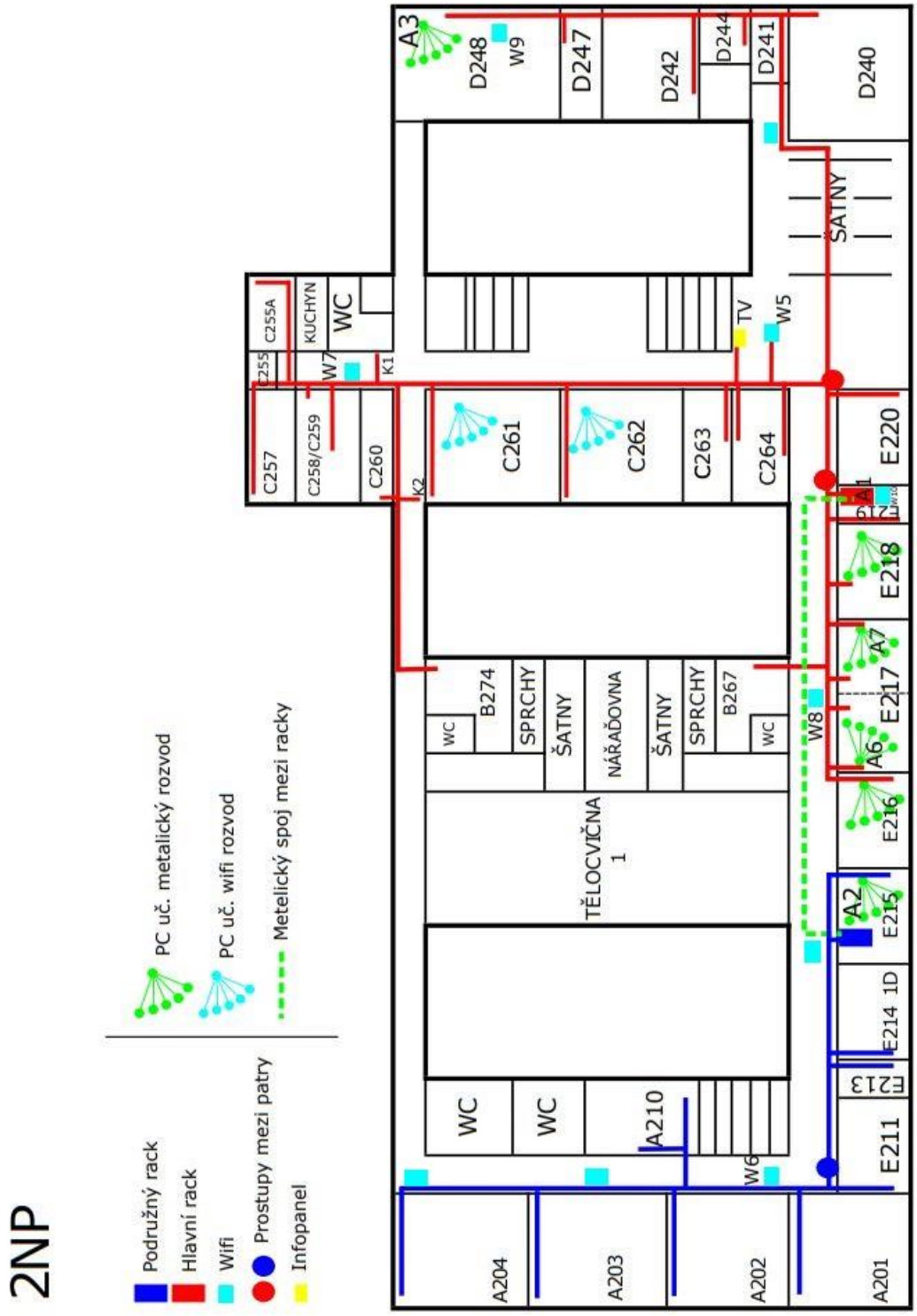
Příloha 7 Budova A 1NP

Schéma rozmístění rozvodů a aktivních prvků s popisem: 1NP



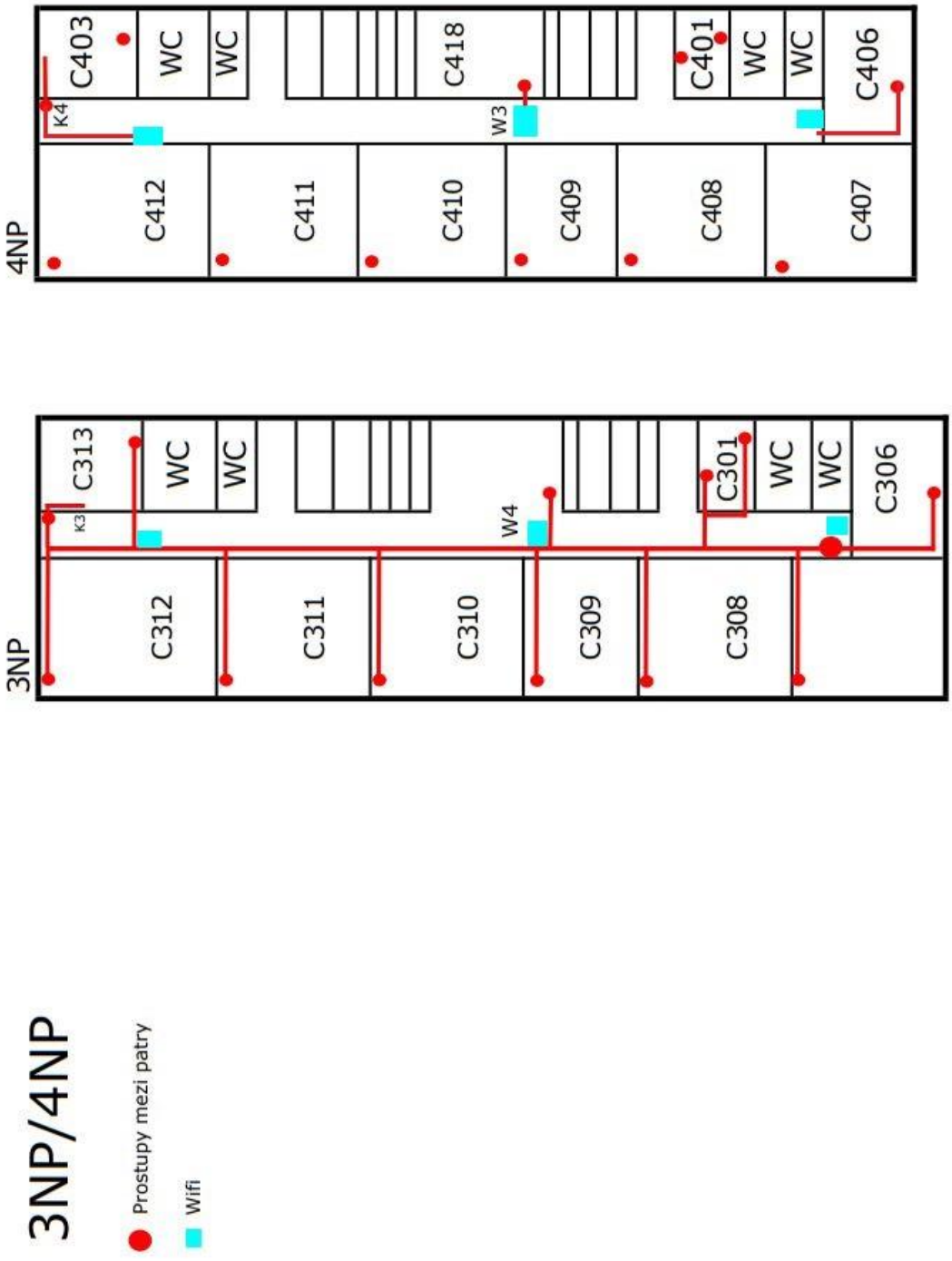
Budova A 2NP

Schéma rozmístění rozvodů a aktivních prvků s popisem: 2NP



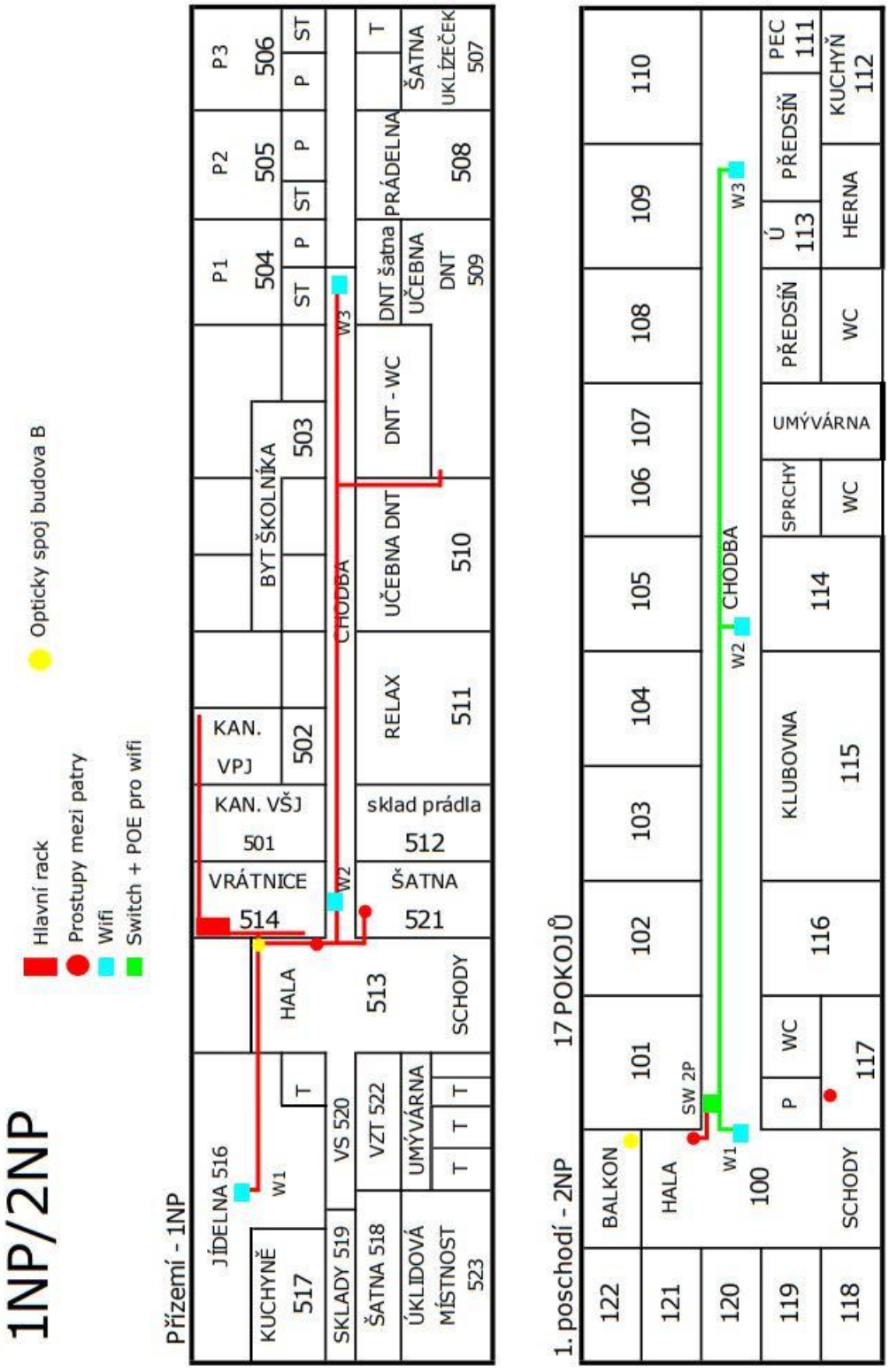
Budova A 3NP/4NP

Schéma rozmístění rozvodů a aktivních prvků s popisem: 3NP/4NP



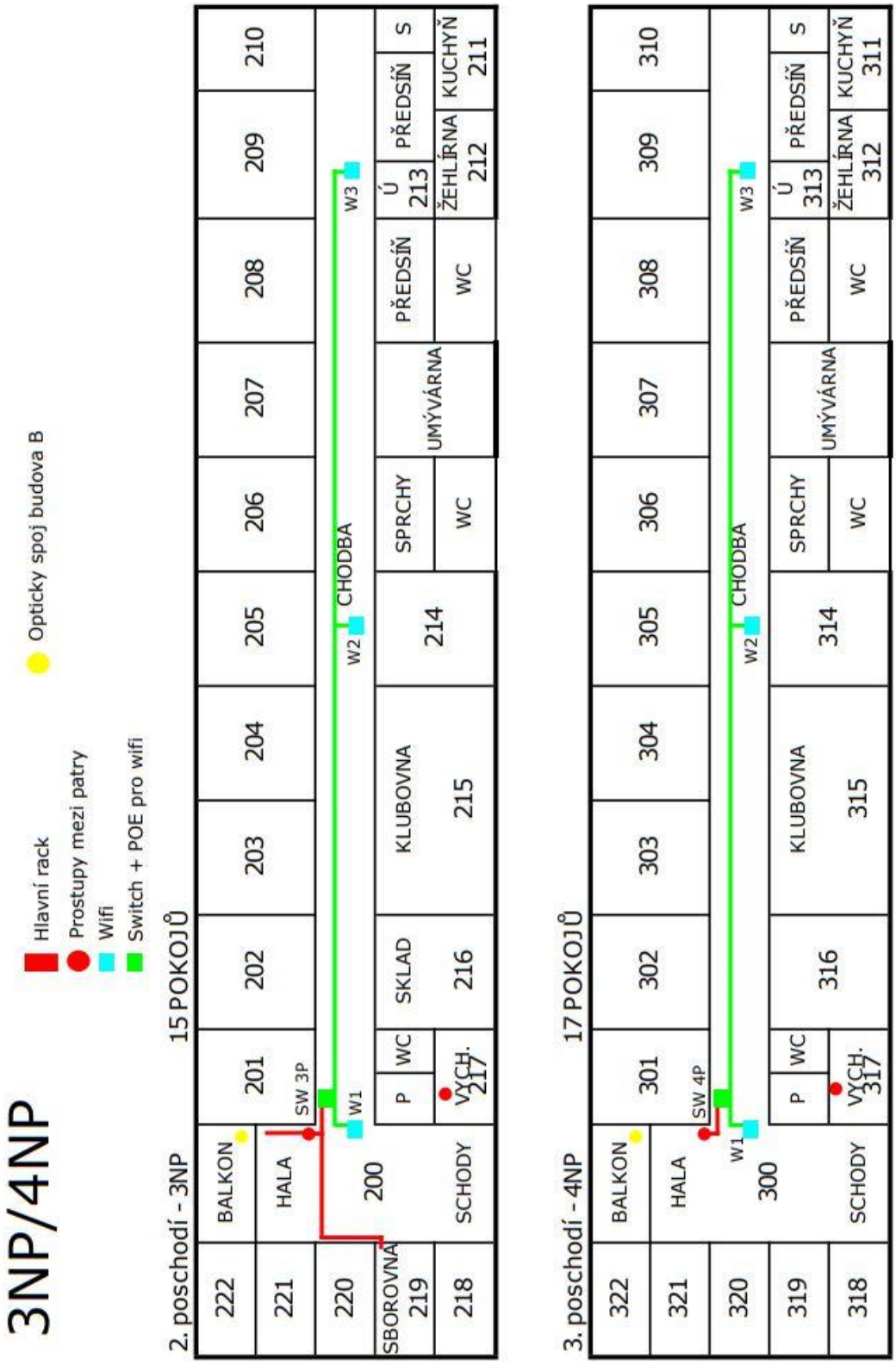
Budova B 1NP/2NP

Schéma rozmístění rozvodů a aktivních prvků s popisem: 1NP/2NP



Budova B 3NP/4NP

Schéma rozmístění rozvodů a aktivních prvků s popisem: 3NP/4NP

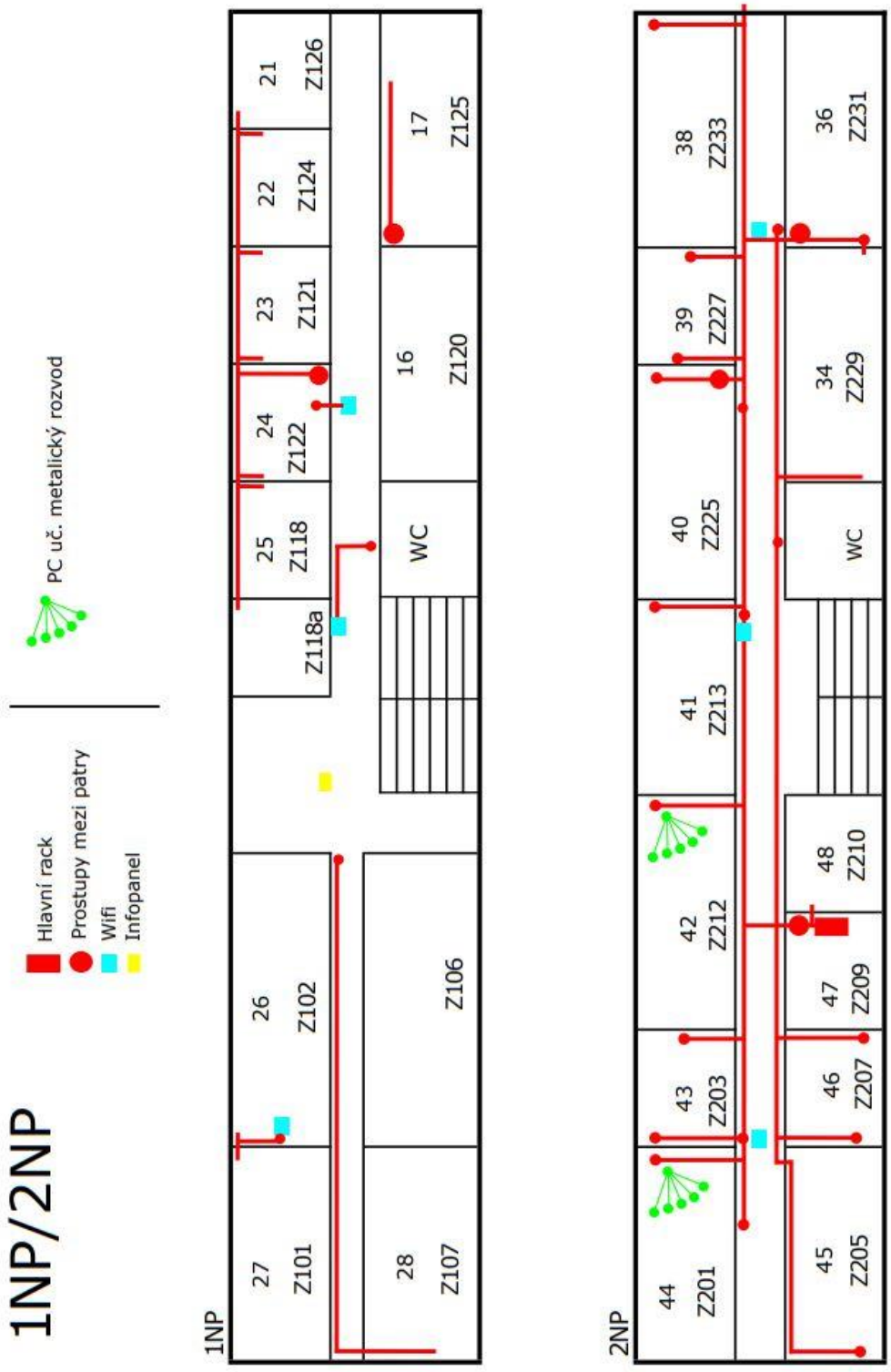


Budova B 5NP

Schéma rozmístění rozvodů a aktivních prvků s popisem: 5NP

Budova C 1NP/2NP

Schéma rozmístění rozvodů a aktivních prvků s popisem: 1NP/2NP



Příloha 8 Schéma topologie sítě školy

Schéma budovy A

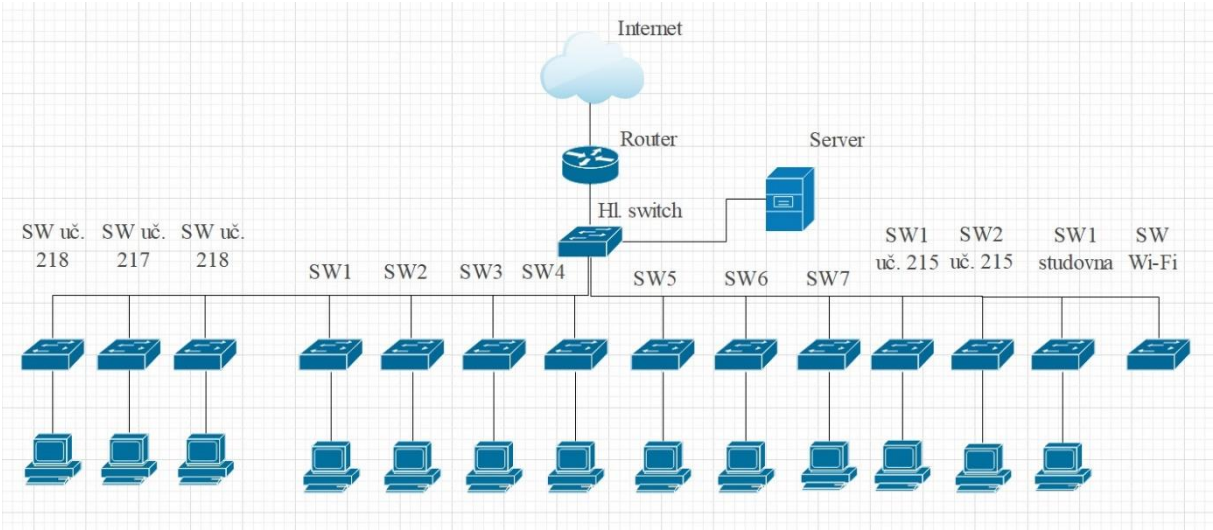


Schéma budovy B

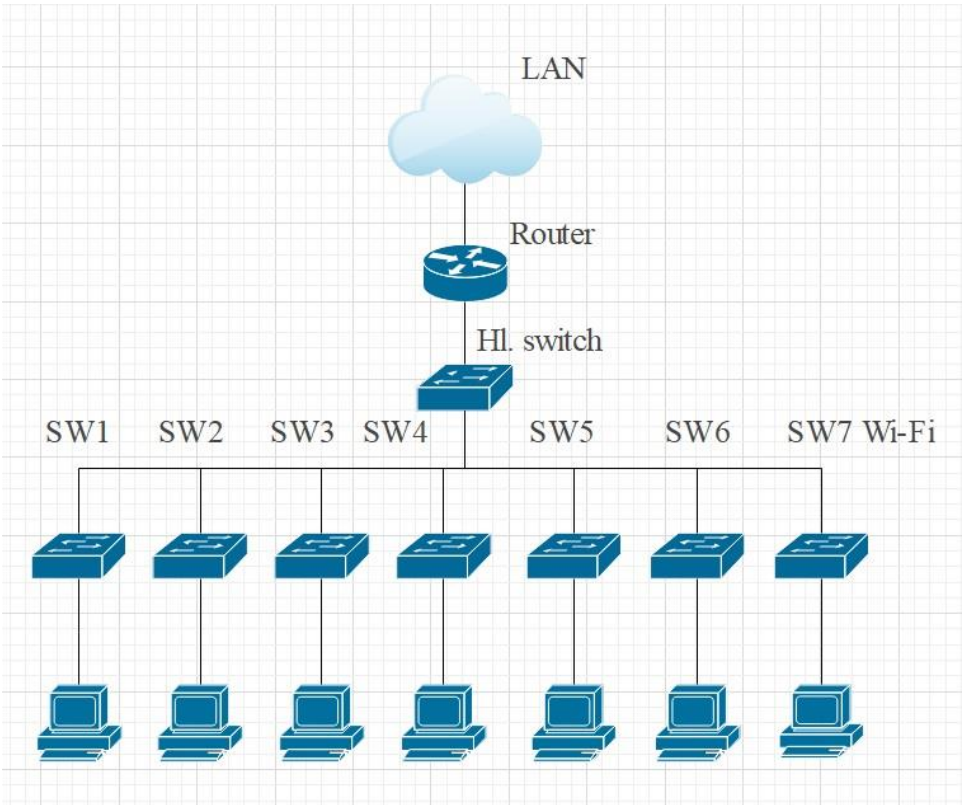


Schéma budovy C

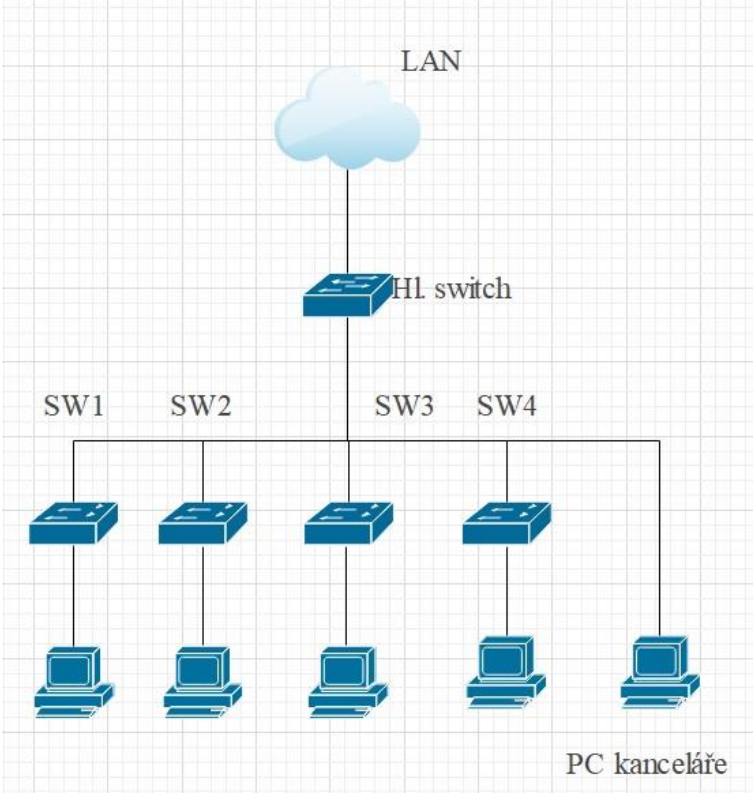


Schéma propojení

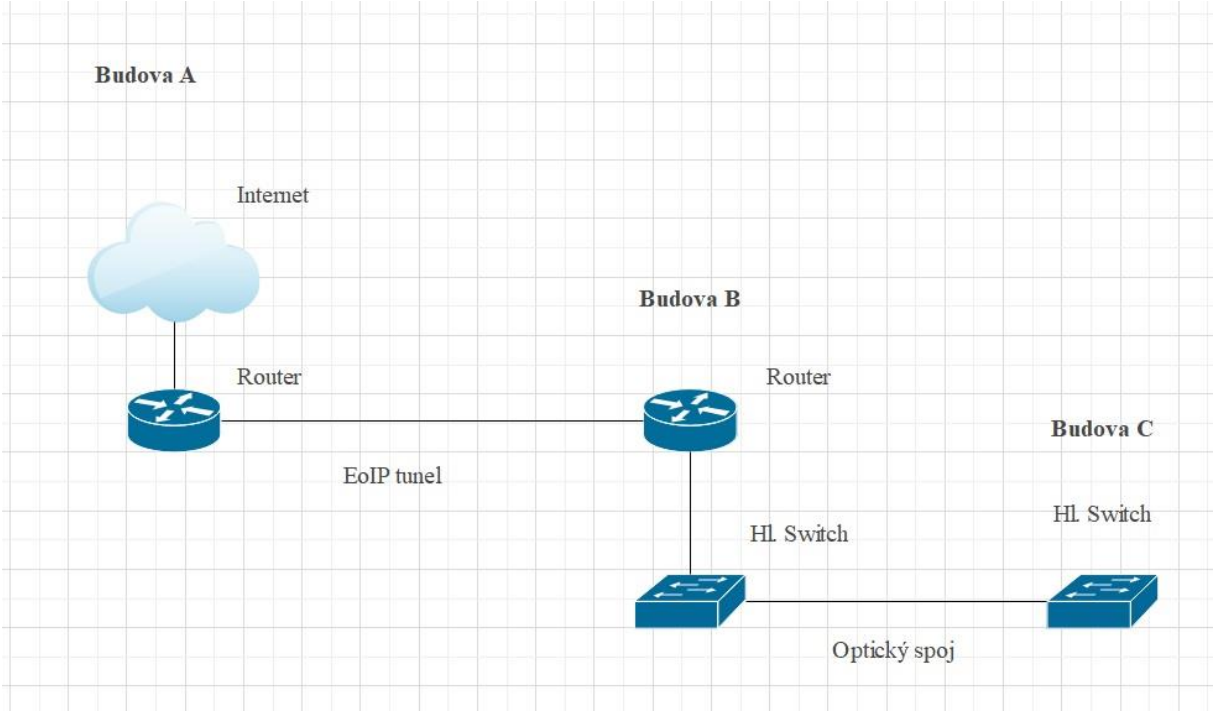
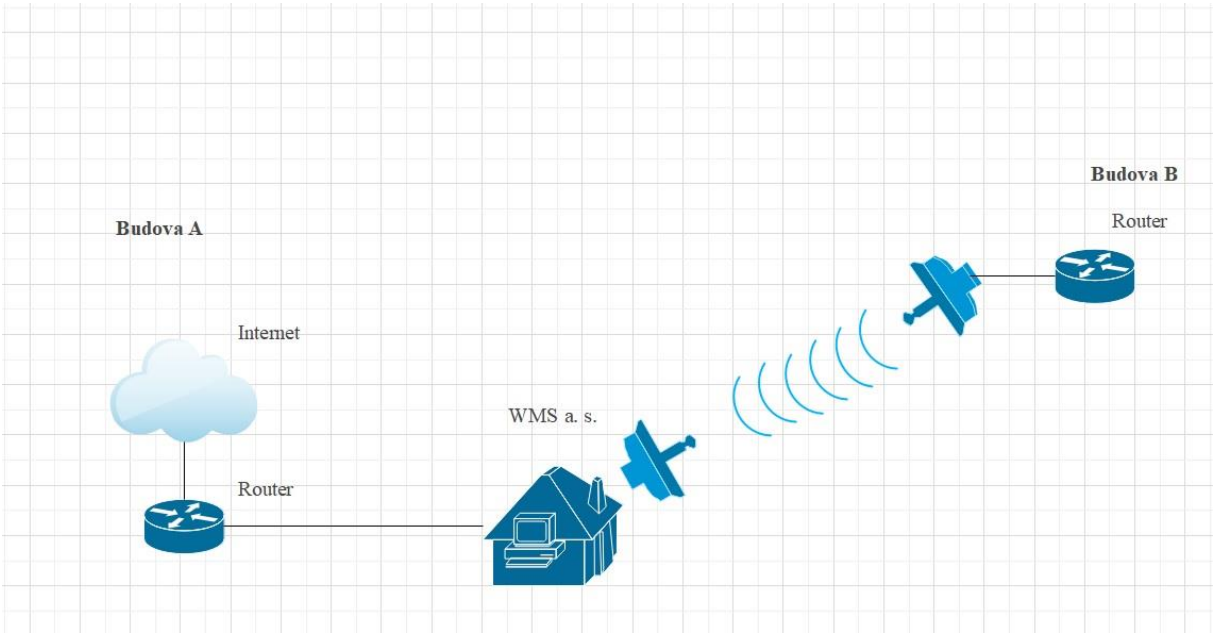


Schéma EoIP tunelu



Příloha 9 Zranitelnost úrovně střední: absence tokenů Anti-CSRF

Screen s ukázkou zranitelného místa s rizikem: střední

Příloha 10 Zranitelnost úrovně střední: záhlaví Anti-clickjacking

Screen s ukázkou zranitelného místa s rizikem: střední

Příloha 11 Zranitelnost úrovně nižší: chybí záhlaví X-Content-Type-Options

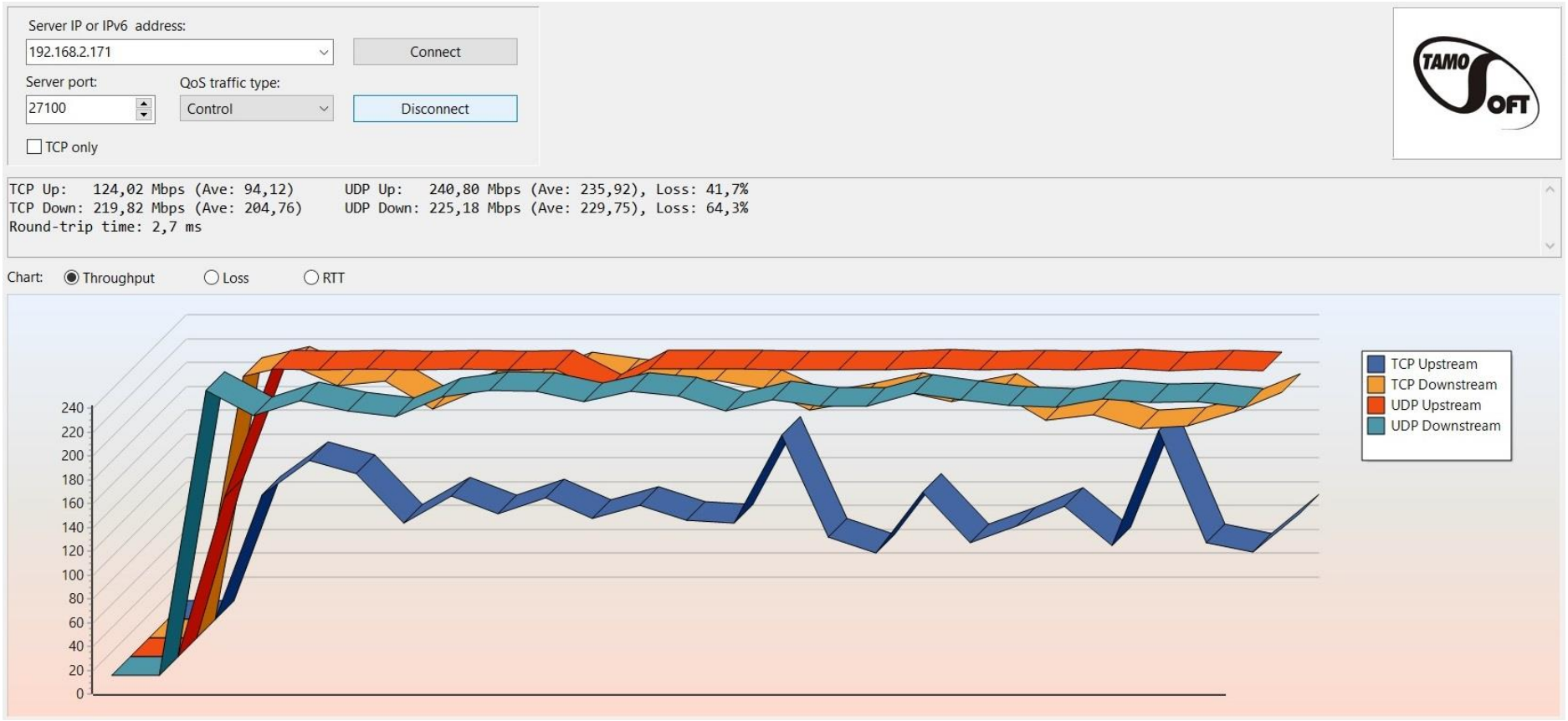
Screen s ukázkou zranitelného místa s rizikem: nižší

Příloha 12 Zranitelnost úrovně informativní: nesoulad znaků

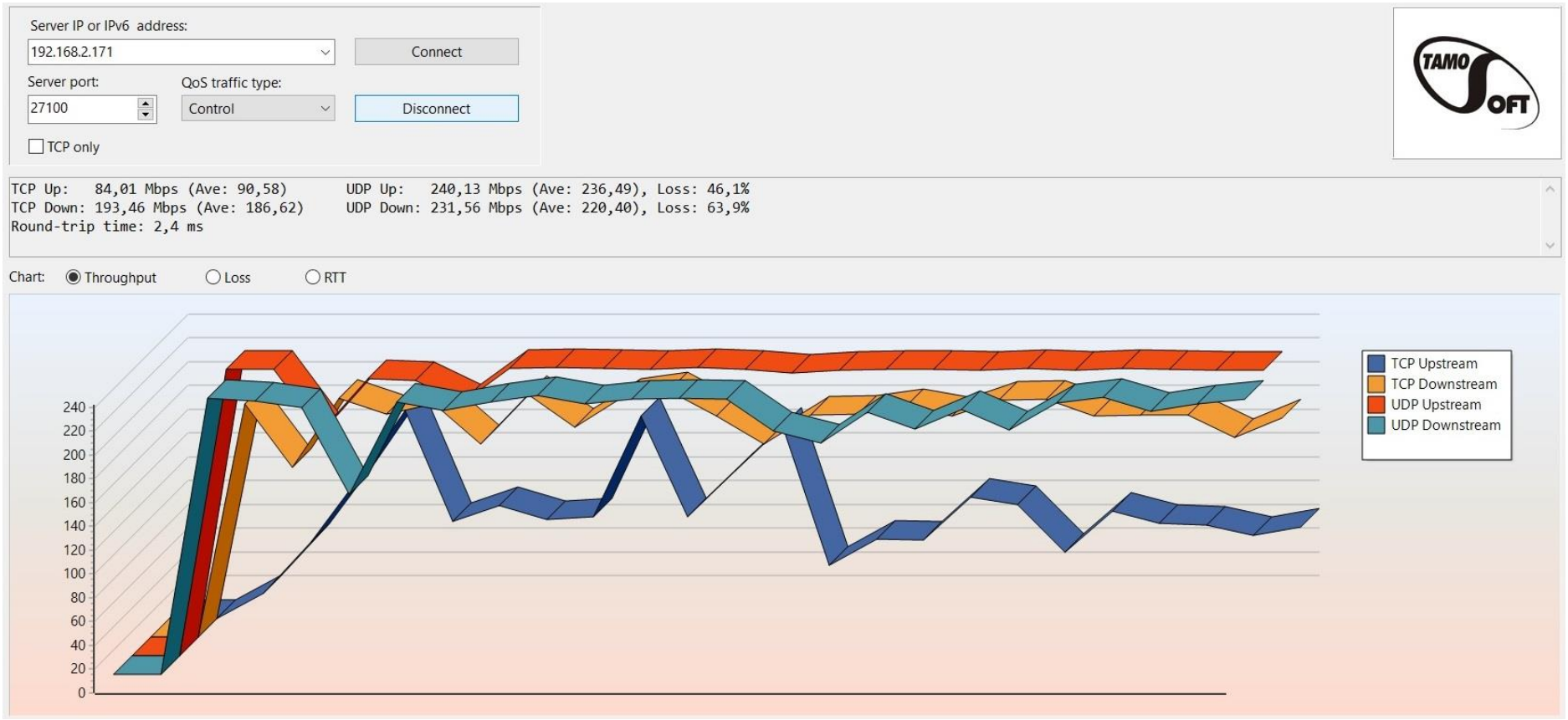
Screen s ukázkou zranitelného místa s rizikem: informativní

Příloha 13 Výsledky testování pomocí aplikace TamoSoft

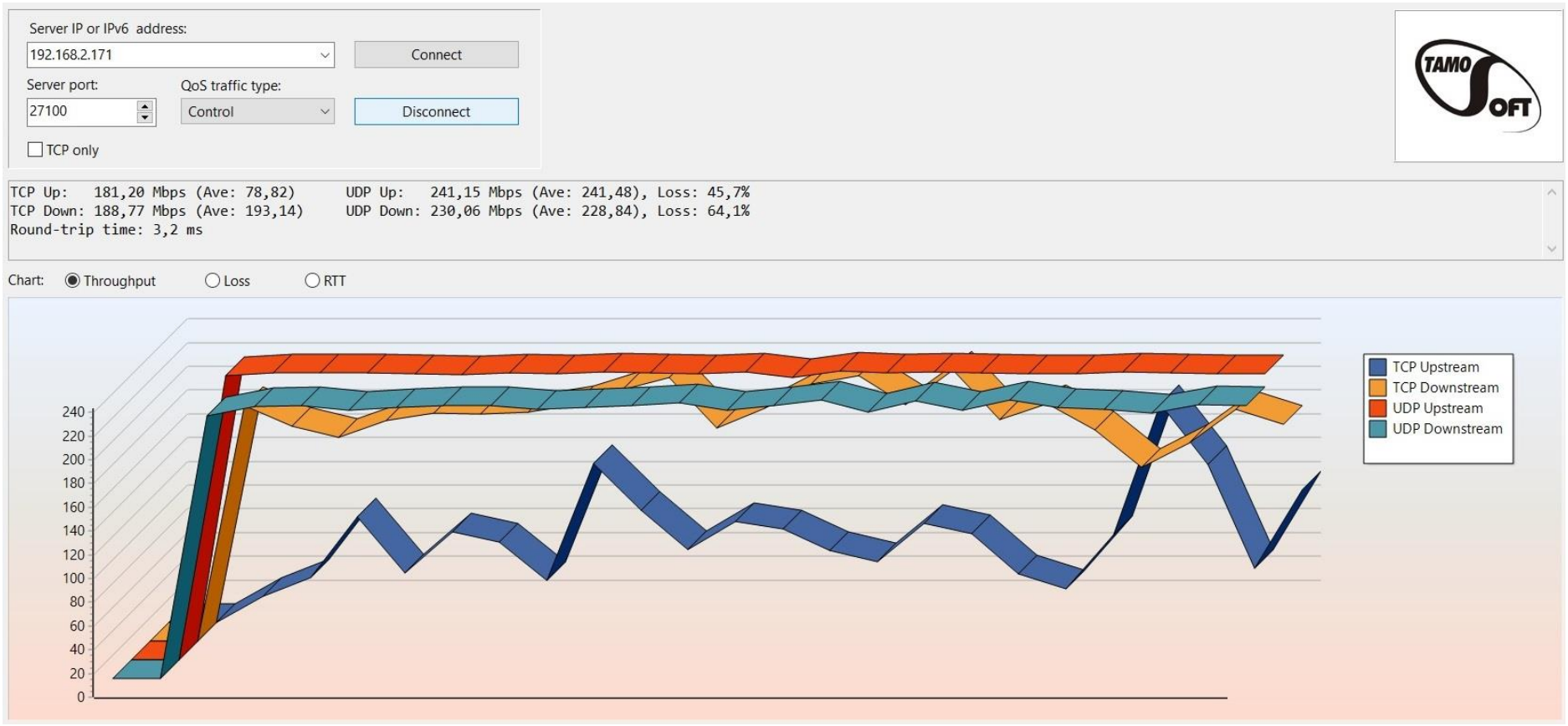
Graf naměřených hodnot test 1



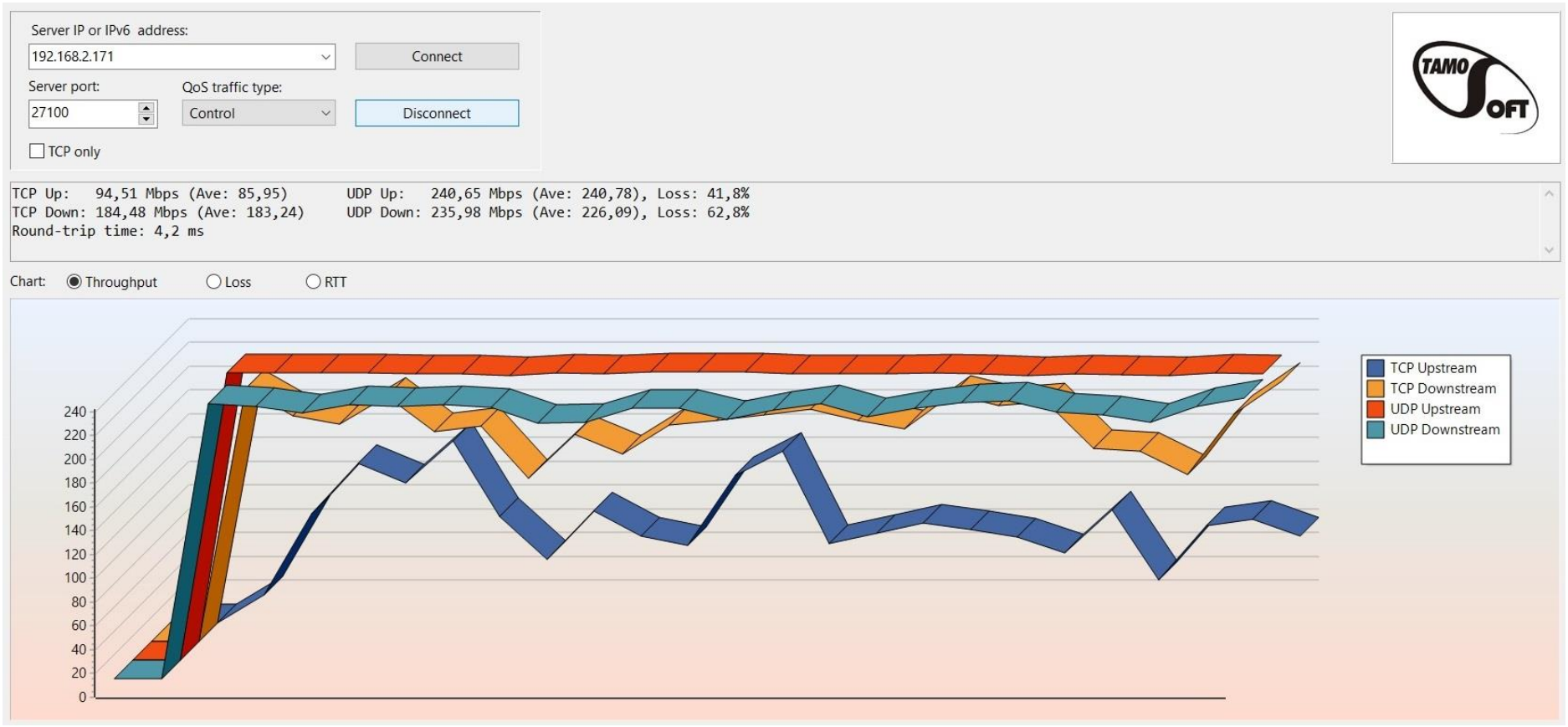
Graf naměřených hodnot test 2



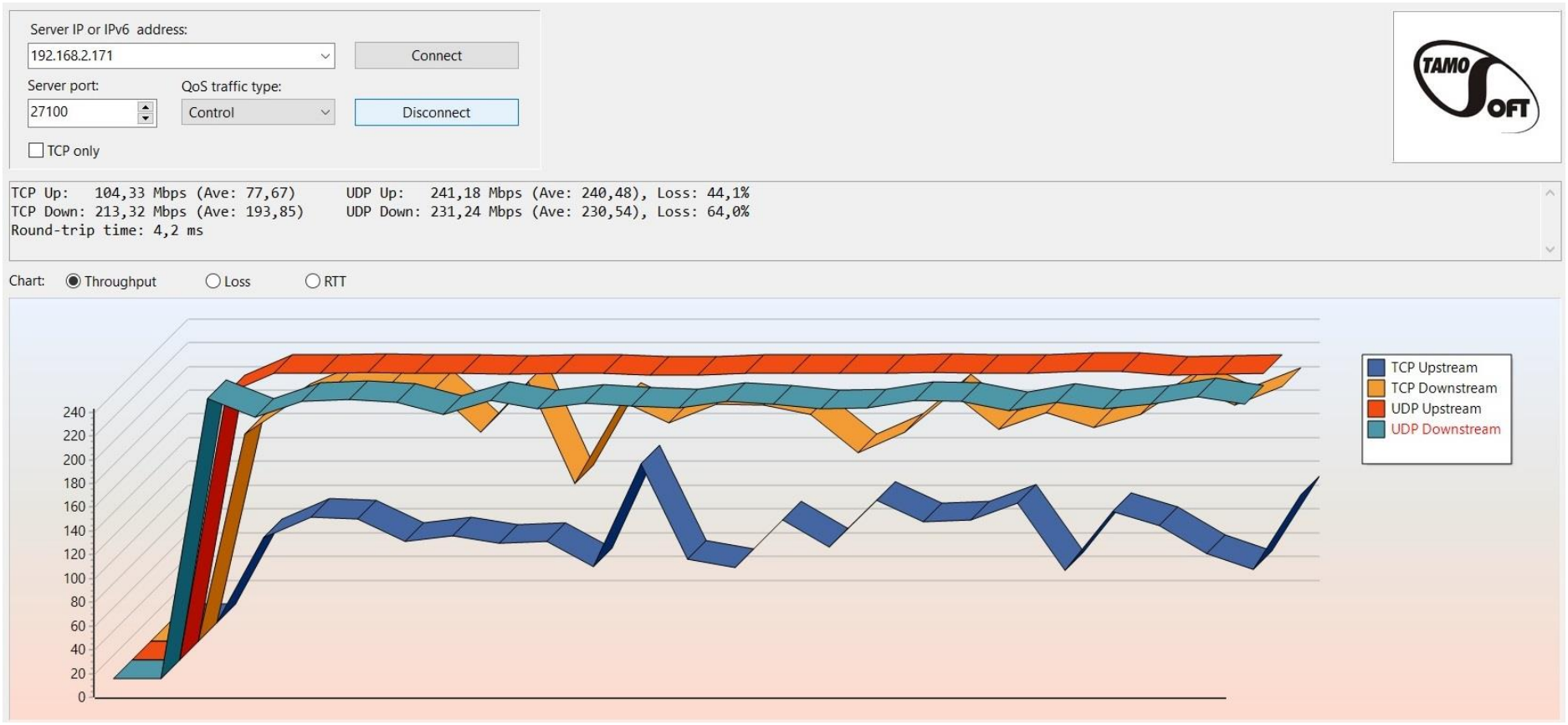
Graf naměřených hodnot test 3



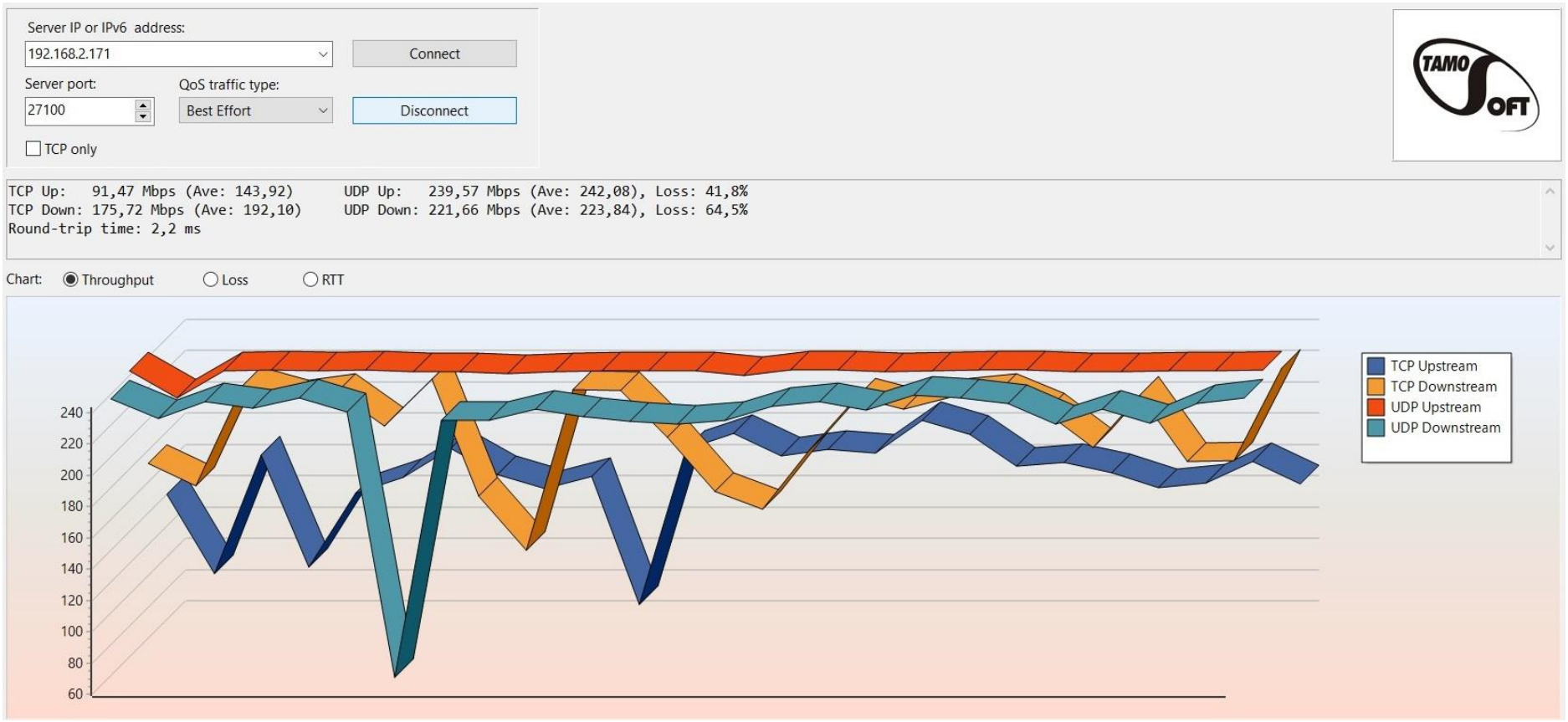
Graf naměřených hodnot test 4



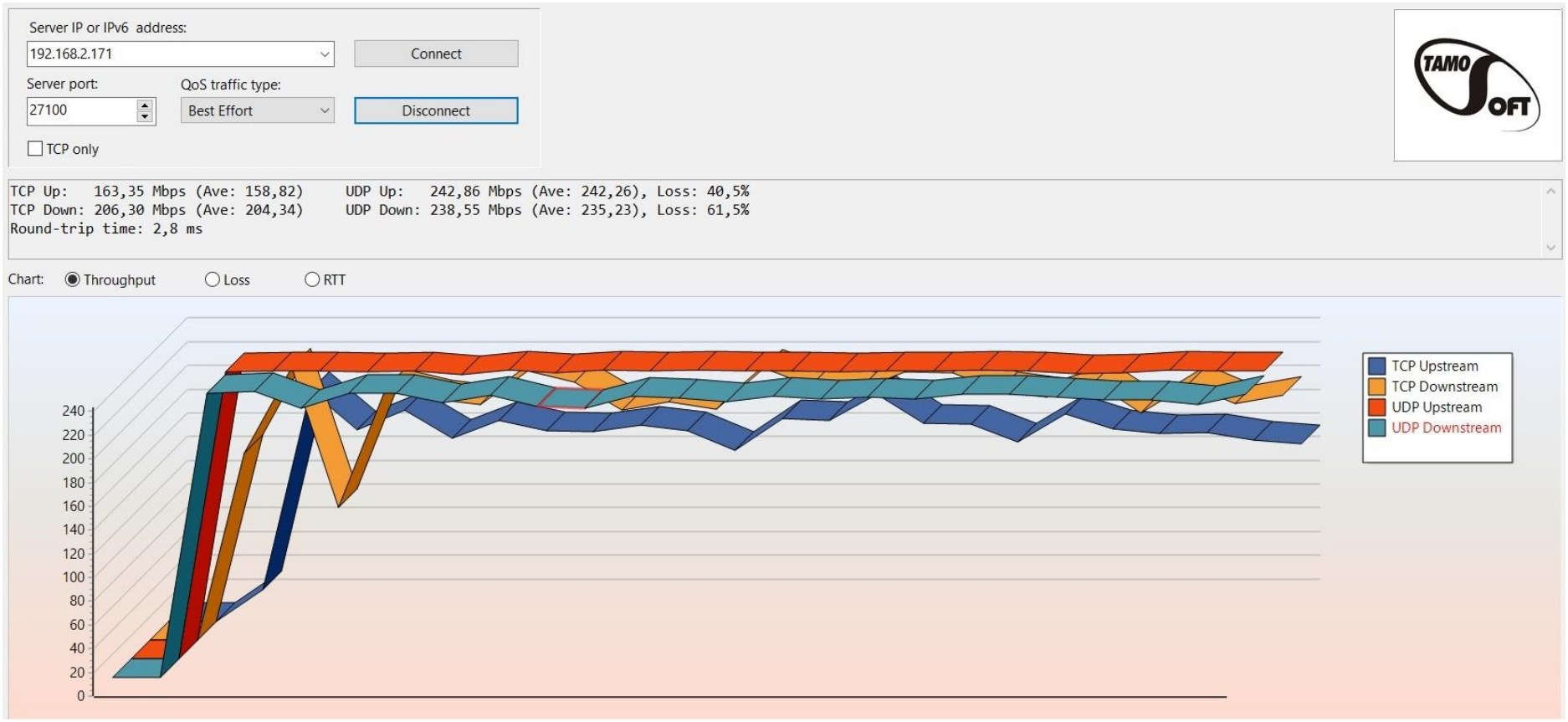
Graf naměřených hodnot test 5



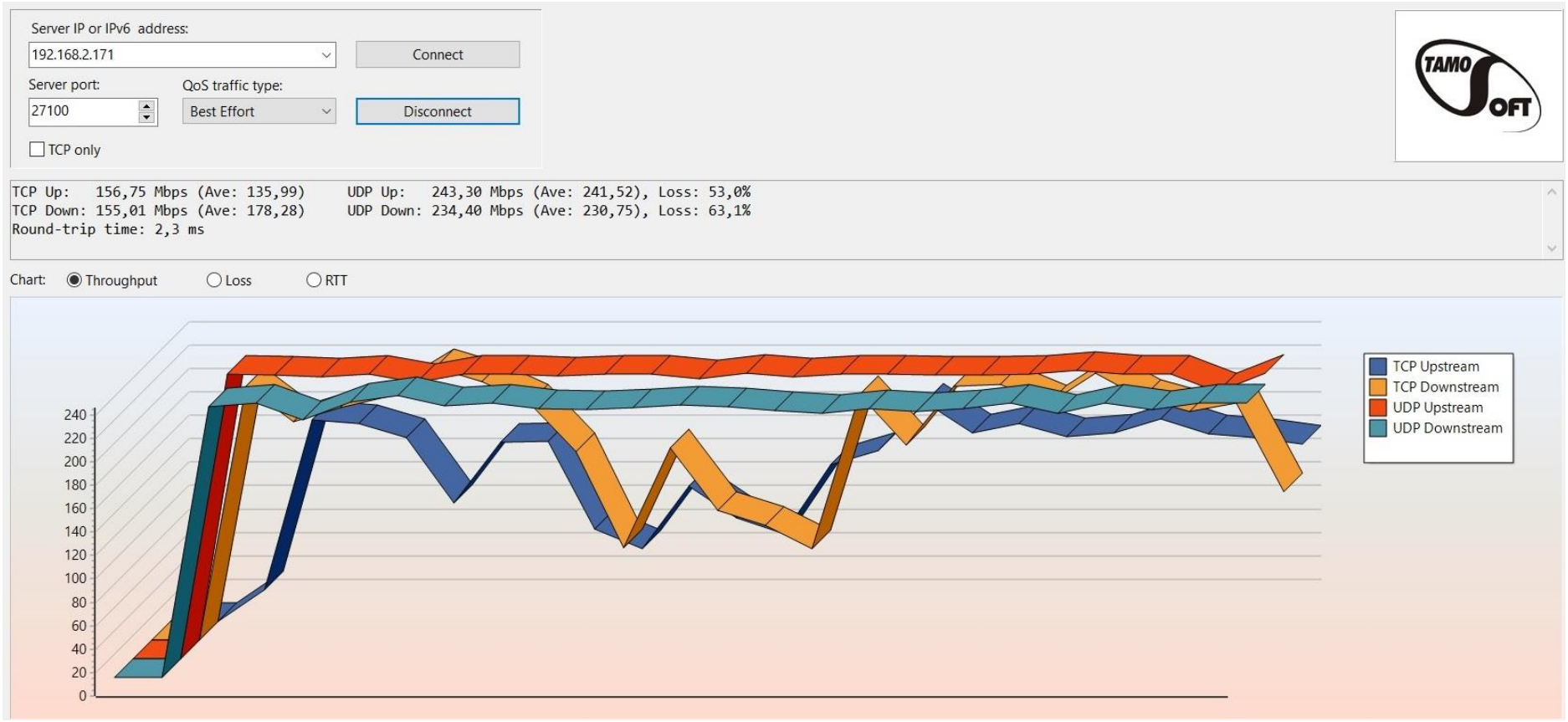
Graf naměřených hodnot test 6



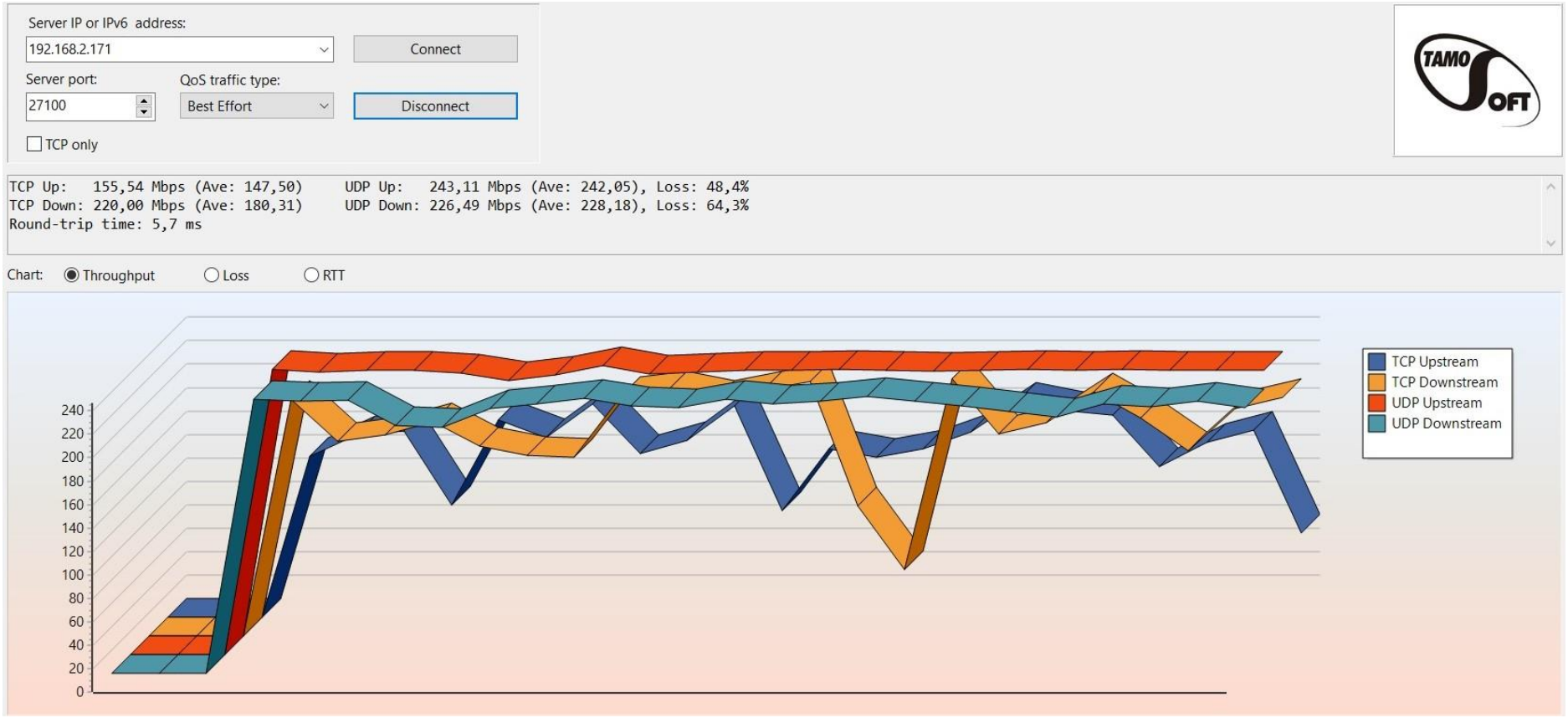
Graf naměřených hodnot test 7



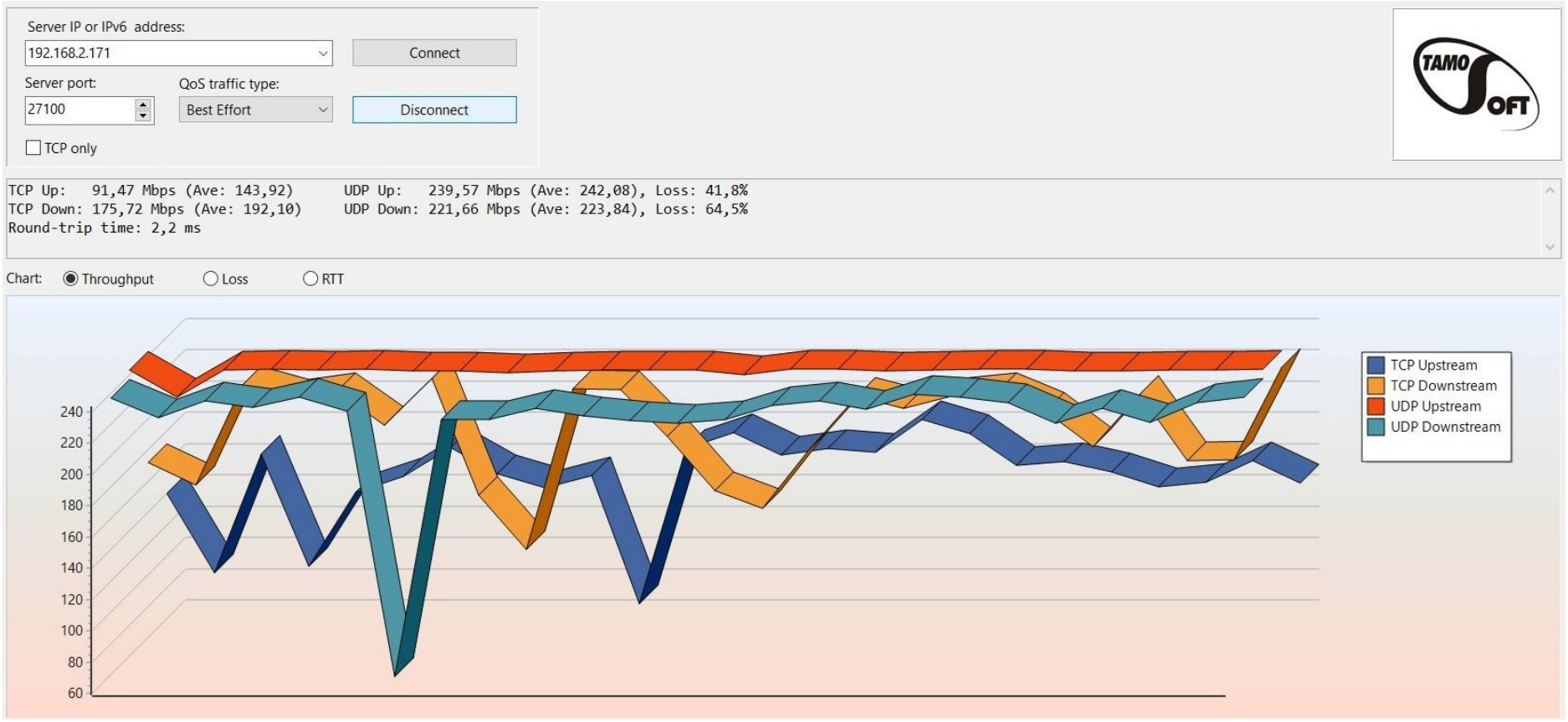
Graf naměřených hodnot test 8



Graf naměřených hodnot test 9



Graf naměřených hodnot test 10



Příloha 14 Výsledky testování pomocí aplikace NetIO-GUI

Tabulka naměřených hodnot

	Výsledky NetIO [Mbps]						Výsledky Ping [ms]								
	TX 1k	**TX 2k**	**TX 4k**	**TX 8k**	**TX 16k**	**TX 32k**	**RX 1K**	**RX 2K**	**RX 4K**	**RX 8K**	**RX 16K**	**RX 32K**	**TX Ø**	**RX Ø**	**Ping AVG**
Test 1	148,98	148,79	172,88	151,82	142,01	166,75	212,06	215,54	222,88	210,36	220,62	219,37	155,21	216,80	3
Test 2	156,06	111,49	176,22	146,13	152,69	152,14	150,55	149,06	208,02	216,55	218,29	181,50	149,12	187,33	4
Test 3	147,52	141,58	167,09	138,30	141,71	122,75	211,31	210,64	206,80	197,05	207,79	218,32	143,16	208,65	5
Test 4	163,45	155,77	94,12	139,35	145,25	135,44	210,82	203,23	189,90	178,00	187,74	193,52	138,89	193,87	4
Test 5	140,30	148,89	132,84	127,92	135,18	146,44	199,32	192,06	209,84	188,89	195,88	209,90	138,60	199,32	3
Test 6	130,33	127,66	137,51	119,19	147,30	139,45	207,81	209,74	209,37	213,06	188,91	208,20	133,57	206,18	4
Test 7	167,09	119,19	139,45	156,06	172,88	163,45	199,01	180,52	155,86	158,36	185,14	212,01	145,99	205,05	5
Test 8	148,89	135,18	135,18	147,52	146,13	155,77	172,39	189,28	146,35	170,53	201,70	214,76	142,61	180,39	3
Test 9	134,12	135,44	139,35	130,33	167,09	94,12	156,55	194,86	165,75	163,66	185,23	180,44	134,74	219,67	4
Test 10	138,30	152,14	141,58	166,75	141,58	139,35	164,46	207,75	161,08	181,57	216,98	193,17	143,54	198,82	4
Test 11	139,44	138,77	125,00	146,05	156,32	164,75	211,00	214,21	220,44	208,12	218,13	215,56	145,05	214,58	3
Test 12	147,97	138,99	141,96	136,55	157,61	150,04	164,48	198,94	138,07	156,42	188,64	194,95	145,52	173,58	4
Test 13	156,51	139,20	128,42	147,39	158,91	122,90	160,79	199,51	130,45	151,59	186,76	193,70	142,22	170,47	5
Test 14	135,04	143,85	124,33	136,23	160,21	133,33	157,11	200,07	122,83	146,76	184,89	192,44	138,83	167,35	4
Test 15	143,58	142,55	131,02	148,74	135,18	141,85	153,43	200,64	115,22	141,93	183,01	191,19	140,49	164,24	3
Test 16	132,11	139,83	135,42	129,45	162,80	134,45	149,74	201,20	107,60	137,10	181,14	189,93	139,01	161,12	4
Test 17	150,64	150,45	122,25	150,09	138,30	112,95	146,06	201,77	99,98	132,28	179,26	188,67	137,45	158,00	5

Test 18	139,22	139,75	139,45	150,77	165,40	152,25	142,37	202,33	92,36	127,45	180,11	187,42	147,81	155,34	3
Test 19	137,22	140,46	141,55	151,44	147,89	107,97	138,69	202,90	84,75	122,62	182,55	186,16	137,76	152,94	4
Test 20	135,26	144,12	133,96	162,12	167,99	140,01	135,00	203,46	77,13	117,79	173,64	184,91	147,24	148,65	4