UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO-SPRÁVNÍ

DIPLOMOVÁ PRÁCE

2025 Bc. Václav Krtek

Univerzita Pardubice
Fakulta ekonomicko-správní

Bezpečnost bezdrátových sítí

Diplomová práce

2025 Bc. Václav Krtek

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Václav Krtek**
Osobní číslo:	**E23162**
Studijní program:	**N0688A140007 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Bezpečnost bezdrátových sítí**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je identifikovat bezpečnostní rizika bezdrátových počítačových sítí z pohledu koncových uživatelů a navrhnout řešení zjištěných nedostatků.

Osnova:

- Aktuální hrozby bezdrátových počítačových sítí.
- Návrh způsobu hodnocení bezpečnosti bezdrátových počítačových sítí z pohledu koncových uživatelů.
- Zhodnocení bezpečnosti bezdrátových počítačových sítí z pohledu koncových uživatelů.
- Návrh řešení zjištěných nedostatků.

Rozsah pracovní zprávy: **Cca 55 stran.**
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

BARKEN, Lee a VESELSKÝ, Jiří. *Wi-Fi: jak zabezpečit bezdrátoovou síť*. Brno: Computer Press, 2004. ISBN 9788025103463.
CACHE, Johnny, WRIGHT, Joshua, LIU, Vincent. *Hacking exposed wireless.* New York: The McGraw-Hill companies, 2010. ISBN 978-0-07-166661-9.
GAST, Matthew. *802.11 wireless networks: the definitive guide*. Beijing: O'Reilly, 2002. ISBN 0-596--00183-5.
PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace: jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G*. Brno: CP Books, 2005. ISBN 80-251-0791-4.

Vedoucí diplomové práce: **doc. Ing. Miloslav Hub, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání diplomové práce: **1. září 2024**
Termín odevzdání diplomové práce: **30. dubna 2025**

L.S.

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

prof. Ing. Jitka Komárková, Ph.D. v.r.
garant studijního programu

V Pardubicích dne 1. září 2024

Prohlašuji:

Práci s názvem Bezpečnost bezdrátových sítí jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

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

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

V Pardubicích dne 19. 12. 2025

Bc. Václav Krtek v.r.

PODĚKOVÁNÍ

Na tomto místě bych rád poděkoval všem, kteří mi pomohli při zpracování mé diplomové práce. Především bych chtěl vyjádřit svůj velký dík vedoucímu práce, doc. Ing. Miloslavu Hubovi, Ph.D., za jeho odborné vedení, cenné rady a ochotu pomoci při řešení odborných problémů v průběhu celého zpracování diplomové práce.

Dále děkuji všem respondentům za čas, který věnovali vyplnění dotazníku. Bez jejich vstřícnosti a ochoty by realizace výzkumu nebyla možná.

V neposlední řadě patří mé upřímné poděkování mé rodině, která mě po celou dobu studia podporovala, poskytovala mi motivaci a zázemí a umožnila mi tak úspěšně se dopracovat až k vytvoření této závěrečné práce.

ANOTACE

Tato diplomová práce se zaměřuje na bezpečnost bezdrátových počítačových sítí, především Wi-Fi sítí podle standardu IEEE 802.11. Cílem práce je identifikovat bezpečnostní rizika z pohledu koncových uživatelů a navrhnout praktická opatření ke zlepšení jejich ochrany. Teoretická část stručně popisuje vývoj a principy šifrovacích standardů (WEP, WPA, WPA2, WPA3) a hodnotí jejich odolnost vůči běžným útokům. Praktická část analyzuje chování uživatelů při připojování k nezabezpečeným sítím a úroveň jejich povědomí o rizicích. Na základě získaných poznatků jsou formulována technická a vzdělávací doporučení pro zvýšení bezpečnosti uživatelů i samotných sítí.

KLÍČOVÁ SLOVA

bezdrátová síť; zabezpečení; šifrování; WEP; WPA; kybernetické útoky; VPN; autentizace; kybernetické hrozby; Wi-Fi; šifrovací protokoly

ANNOTATION

This thesis focuses on the security of wireless computer networks, particularly Wi-Fi networks based on the IEEE 802.11 standard. The main objective is to identify security risks from the perspective of end users and propose practical measures to improve their protection. The theoretical part outlines the development and principles of encryption standards (WEP, WPA, WPA2, WPA3) and evaluates their resistance to common attacks. The practical part analyzes user behavior when connecting to unsecured networks and assesses their awareness of related risks. Based on the findings, technical and educational recommendations are proposed to enhance both user and network security.

KEYWORDS

wireless network; cybersecurity, encryption; WEP; WPA; cyber attacks; VPN; authentication; cyber threats; Wi-Fi; encryption protocols

OBSAH

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK

Zkratka	Význam
2FA	Dvoufaktorové ověřování (*Two-Factor Authentication*)
802.11	Standard IEEE pro bezdrátové sítě
AES	Pokročilý šifrovací standard (*Advanced Encryption Standard*)
AP	Přístupový bod (*Access Point*)
ARP	Protokol pro přidělování IP adres (*Address Resolution Protocol*)
CCMP	Režim šifrování s autentizací založený na AES (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*)
CRC-32	32bitová kontrola integrity (*Cyclic Redundancy Check*)
DNS	Systém doménových jmen (*Domain Name System*)
DoS	Znepřístupnění služby (*Denial of Service*)
DSSS	Přímé rozprostřené spektrum (*Direct Sequence Spread Spectrum*)
EAP	Extensible Authentication Protocol
FHSS	Přeskakování frekvence (*Frequency Hopping Spread Spectrum*)
GCMP	Varianta AES šifrování (*Galois/Counter Mode Protocol*)
GDPR	Nařízení pro zpracování osobních údajů (*General Data Protection Regulation*)
IEEE	Institut inženýrů elektriky a elektroniky *(Institute of Electrical and Electronics Engineers)*
IoT	Internet věcí = zařízení připojená k internetu (*Internet of Things*)
IV	Inicializační vektor (*Initialization Vector*)
MAC	Řízení přístupu k médiu (*Media Access Control*) nebo MAC fyzická adresa

Zkratka	**Význam**
MIC	Kontrola integrity zprávy (*Message Integrity Code*)
MITM	Útok typu prostředník (*Man-in-the-Middle*)
OWE	*Opportunistic Wireless Encryption*
PSK	Předem sdílený klíč (*Pre-Shared Key*)
RC4	Šifra s proudovým tokem (*Rivest Cipher 4*)
SAE	Současné ověření rovného s rovným (*Simultaneous Authentication of Equals*)
SSID	Identifikátor sítě (*Service Set Identifier*)
TKIP	Dočasný protokol integrity klíče (*Temporal Key Integrity Protocol*)
VPN	Virtuální privátní síť (*Virtual Private Network*)
WEP	Ochrana na úrovni kabelového připojení (*Wired Equivalent Privacy*)
Wi-Fi	Bezdrátový přenos dat (*Wireless Fidelity*)
WLAN	Bezdrátová lokální síť (*Wireless Local Area Network*)
WPA	Zabezpečený bezdrátový přístup *(Wi-Fi Protected Access)*
WPA2	Zabezpečený bezdrátový přístup 2 *(Wi-Fi Protected Access II)*
WPA3	Zabezpečený bezdrátový přístup 3 *(Wi-Fi Protected Access III)*
WPS	Zjednodušené připojení k Wi-Fi (*Wi-Fi Protected Setup*)

ÚVOD

Bezdrátové sítě představují dnes jednu z nejrozšířenějších forem komunikace mezi zařízeními, ať už jde o domácnosti, podniková prostředí, nebo veřejná místa. Díky své flexibilitě a jednoduchosti použití umožňují bezdrátové technologie široké možnosti připojení bez nutnosti fyzického propojení kabely. Tento komfort je však vykoupen zvýšenými bezpečnostními riziky, která pramení z otevřeného přenosového média, tedy vzduchu. Právě z tohoto důvodu se bezpečnost bezdrátových sítí stala klíčovým tématem v oblasti informačních technologií a kybernetické bezpečnosti.

Na rozdíl od tradičních kabelových sítí, kde je přístup omezen fyzickým rozhraním, mohou být bezdrátové signály zachyceny kýmkoliv v dosahu. Tato zranitelnost otevírá prostor pro řadu potenciálních útoků, jako jsou odposlechy, neoprávněný přístup, manipulace s přenášenými daty nebo zahlcení sítě. Historie vývoje bezpečnostních protokolů Wi-Fi sítí ukazuje, že původní řešení nebyla na tato rizika dostatečně připravena. Postupem času se však objevily nové standardy, které reagují na aktuální hrozby a nabízejí vyšší úroveň ochrany.

Cílem této diplomové práce je zhodnotit bezpečnostní úroveň bezdrátových sítí s důrazem na Wi-Fi technologie založené na standardu IEEE 802.11. Práce sleduje vývoj jednotlivých šifrovacích protokolů, od původního WEP přes přechodné WPA až po moderní standardy WPA2 a WPA3, a porovnává jejich schopnosti chránit síť proti útokům v různých scénářích. Práce je zaměřena nejen na technické parametry těchto protokolů, jako jsou typy šifrování, ochrana integrity nebo rotace klíčů, ale i na odolnost vůči konkrétním typům útoků, které jsou v dnešní době stále aktuálnější.

Součástí práce je také praktická analýza chování uživatelů bezdrátových sítí. Bezpečnost totiž není jen otázkou technologie, ale i lidského faktoru. I ta nejbezpečnější síť může být ohrožena, pokud uživatelé nedodržují základní pravidla bezpečného připojení. Práce proto zahrnuje dotazníkové šetření a praktický experiment, jehož cílem je ověřit, jak uživatelé reagují na otevřené nebo nezabezpečené sítě a zda si uvědomují možná rizika spojená s jejich využíváním.

Na základě teoretických poznatků a praktických zjištění bude formulováno doporučení pro návrh osvědčených bezpečnostních opatření, která mohou být aplikována jak v domácím, tak i firemním prostředí. Práce zároveň upozorňuje na nutnost pravidelného přehodnocování bezpečnostních strategií, protože hrozby v kyberprostoru se neustále vyvíjejí a s nimi i způsoby útoků na bezdrátové infrastruktury.

1. BEZPEČNOST BEZDRÁTOVÝCH SÍTÍ

Bezdrátové technologie se staly nedílnou součástí moderní společnosti a významně ovlivnily způsob, jakým lidé přistupují k informacím, komunikaci a službám. S rostoucím počtem bezdrátových zařízení a jejich masivnímu rozšíření nejen v domácnostech, ale i ve veřejných a firemních prostředích, se však zvyšuje i potřeba jejich adekvátního zabezpečení. Bezpečnost bezdrátových sítí se stala klíčovou oblastí nejen pro organizace a podniky, ale také pro jednotlivce, kteří jsou vystaveni různým kybernetickým hrozbám. [1]

Kromě bezdrátových Wi-Fi počítačových sítí existují další komunikační zařízení a technologie používající vzduch jako médium pro šíření svých signálů, například všechny rádiové prostředky, a to jak pro přenos hlasu, tak i dat. Lze se v tomto případě bavit i o televizním a rádiovém signálu, který je třeba také zabezpečit, ne sice proti odposlechu ale spíše proti rušení. Dále lze potom zmínit například dotazovače a odpovídače používající se v letecké dopravě pro výměnu dat mezi řízením letového provozu a letadlem. Technologií využívajících rádiové vlny je tedy spousta, tato práce ovšem bude řešit pouze Wi-Fi sítě jako takové, tedy signály šířící se frekvencí 2,4 a 5 GHz.

Bezdrátové síťové technologie, jako jsou Wi-Fi a mobilní sítě, umožňují pohodlnou konektivitu bez potřeby fyzického propojení elektronického zařízení kabelem. Tato flexibilita však přináší řadu výzev v oblasti zabezpečení, protože bezdrátové signály mohou být snadno zachyceny a zneužity útočníky. V průběhu let se vyvíjely různé bezpečnostní standardy, avšak kybernetické hrozby se neustále vyvíjejí a vyžadují pravidelnou aktualizaci bezpečnostních opatření. [2]

Jednou z hlavních hrozeb pro bezdrátové sítě je neautorizovaný přístup. Slabá nebo žádná autentizace může vést k útokům typu "Man-in-the-Middle" (MitM), kde útočník zachytává komunikaci mezi dvěma zařízeními. Další riziko představují útoky na slabé šifrovací protokoly, jako byl historický WEP, který byl snadno prolomitelný, a proto byl nahrazen silnějšími protokoly WPA a WPA2. V posledních letech byla zavedena novější technologie WPA3, která poskytuje ještě lepší ochranu uživatelů. [3]

Další podstatný faktor při zabezpečení bezdrátových sítí je správné nastavení přístupových bodů (AP), správa hesel a pravidelná aktualizace firmware. Organizace a jednotlivci by měli dbát na zavedení bezpečnostních opatření, jako je filtrování MAC adres, vypnutí SSID broadcastu a používání VPN při připojování k neznámým Wi-Fi sítím. [4]

1.1 Počátky bezdrátových sítí a jejich zranitelnosti

Bezdrátové sítě se začaly vyvíjet v 80. letech 20. století, kdy standard IEEE 802.11 položil základ pro dnešní Wi-Fi technologie. IEEE 802.11 představuje klíčový standard v oblasti bezdrátových lokálních sítí (WLAN), jehož vznik a vývoj výrazně ovlivnil problematiku bezpečnosti bezdrátové komunikace. V roce 1985 uvolnila americká Federal Communications Commission (FCC) pásmo 2,4 GHz pro nelicencované využití, což otevřelo možnosti pro vývoj bezdrátových technologií, ale současně položilo základy pro vznik bezpečnostních rizik spojených s volně přístupným pásmem. [3]

Oficiální práce na standardu IEEE 802.11 započaly v roce 1987 založením pracovní skupiny Wireless LAN Working Group v rámci Institute of Electrical and Electronics Engineers (IEEE). Cílem této skupiny bylo nejen zajistit interoperabilitu zařízení, ale také řešit bezpečnostní otázky vyplývající z bezdrátové povahy komunikace, která je přirozeně náchylnější k odposlechům a rušení než tradiční kabelové spojení. Pracovní skupina musela řešit mnoho technických a bezpečnostních výzev, zejména v oblasti ochrany soukromí a integrity dat v prostředí sdíleného bezdrátového média. [4]

První verze standardu IEEE 802.11, vydaná v roce 1997, definovala základní bezpečnostní mechanismy, které však byly omezené a nedostatečné pro dlouhodobou ochranu komunikace. V této fázi se primárně řešila fyzická bezpečnost komunikace prostřednictvím různých technik modulace signálu jako Frequency Hopping Spread Spectrum (FHSS) a Direct Sequence Spread Spectrum (DSSS), které měly za cíl snížit pravděpodobnost zachycení či rušení komunikace. Přestože tyto techniky poskytovaly určitou úroveň zabezpečení proti jednoduchým formám odposlechů, rychle se ukázalo, že jsou nedostatečné vůči sofistikovanějším útokům. [1], [4]

S dalším vývojem standardu, zejména od verzí 802.11a a 802.11b z roku 1999, rostla potřeba robustnějších bezpečnostních řešení vzhledem k rychle se rozšiřujícímu počtu zařízení a uživatelů. Tyto verze přinesly vyšší přenosové rychlosti, což ale současně zvýšilo potenciální dopady narušení bezpečnosti. Zvýšená rychlost a dostupnost technologie přitáhly větší pozornost ze strany útočníků a bezpečnostní rizika se začala projevovat zřetelněji. Ochrana sítí se stala stále důležitější nejen pro podniková prostředí, ale také pro domácnosti, kde se bezdrátová síť stávala běžnou součástí každodenního života. [3]

Významným krokem vpřed byl standard IEEE 802.11g z roku 2003, který spojil vyšší rychlosti se zpětnou kompatibilitou v pásmu 2,4 GHz. Nárůst popularity standardu však dále prohloubil bezpečnostní výzvy, které musely být řešeny pokročilejšími metodami ochrany dat

a autentizace uživatelů. Standard 802.11g vyvolal potřebu intenzivnějšího zkoumání nových technik pro zajištění bezpečnosti, včetně pokročilých autentizačních metod a řízení přístupu k síti. [1]

Standard IEEE 802.11n, dokončený v roce 2009, zaváděl technologii Multiple-Input Multiple-Output (MIMO), která kromě zlepšení propustnosti a dosahu přinesla také nové bezpečnostní aspekty. Díky sofistikovanější modulaci a signálovým technologiím se částečně snížila pravděpodobnost odposlechu a útoků typu "Man-In-The-Middle". Nicméně složitější infrastruktura vyžadovala komplexnější přístup k bezpečnostní správě sítě. Technologický pokrok také zvýšil nároky na řízení spektra a koordinaci zařízení v síti, což otevřelo nové otázky v oblasti zabezpečení řízení přístupu a autentizace zařízení. [4]

Vývoj pokračoval vydáním standardu IEEE 802.11ac v roce 2013, který využívá širší kanály a pokročilé metody MIMO. Tato verze přinesla kromě vyšších přenosových rychlostí také vyšší bezpečnost přenosu díky pokročilé modulaci a možnosti přesnějšího řízení přístupu k síti. Vyšší propustnost a kapacita sítě vyžadovala robustnější ochranu datových toků, protože zvýšený objem přenášených dat představoval větší potenciální hodnotu pro případné útočníky. [3]

Nejnovější standard IEEE 802.11ax (Wi-Fi 6), ratifikovaný v roce 2021, se zaměřuje mimo jiné na efektivnější využití spektra a zlepšení odolnosti proti různým typům útoků a rušení. Díky technologii Orthogonal Frequency Division Multiple Access (OFDMA) je možné lépe kontrolovat komunikaci jednotlivých zařízení a efektivněji chránit před potenciálními bezpečnostními incidenty. Wi-Fi 6 přinesla také výrazné posílení ochrany komunikace v prostředí s vysokou hustotou uživatelů, což je klíčové například pro velké podnikové sítě, veřejné prostory či stadiony, kde bezpečnostní požadavky na bezdrátovou komunikaci neustále rostou. [5]

Historický vývoj IEEE 802.11 jasně ukazuje, že s rostoucími požadavky na kapacitu a výkon bezdrátových sítí stoupá také důležitost a komplexnost bezpečnostních opatření, která jsou klíčová pro bezpečný a spolehlivý provoz těchto sítí. [1]

1.2 Vývoj šifrovacích standardů

Kvůli nedostatkům protokolu WEP se odborníci na bezpečnost začali zabývat návrhem nových metod zabezpečení bezdrátových sítí. Tento proces vedl k vývoji standardů Wi-Fi Protected Access (WPA) a později WPA2 a WPA3, které postupně eliminovaly slabiny předchozích generací. [1]

1.2.1 WEP a jeho problémy

Wired Equivalent Privacy (WEP) byl prvním pokusem o zabezpečení bezdrátových sítí v rámci standardu IEEE 802.11. Jeho cílem bylo nabídnout úroveň ochrany srovnatelnou s běžnými drátovými sítěmi. WEP používal symetrickou šifru RC4, jejíž jednoduchost a rychlost byly zpočátku považovány za výhody. K šifrování se využíval 40bitový nebo 104bitový klíč, ke kterému byl připojen 24bitový inicializační vektor (IV), tvořící dohromady šifrovací klíč pro RC4 stream cipher. [6]

Zásadním problémem WEPu byl právě tento IV, který byl příliš krátký a generován pseudonáhodně, často s opakováním. Útočník mohl pasivně odposlouchávat provoz a sbírat šifrované rámce s různými, nebo opakovanými IV. Jakmile měl dostatek dat, mohl s využitím veřejně dostupných nástrojů (např. AirSnort) rekonstruovat šifrovací klíč během několika minut. WEP navíc neimplementoval žádnou ochranu integrity, čímž umožňoval podvržení rámců pomocí „bit flippingu“ bez nutnosti znát klíč. [6]

Tyto slabiny vedly ke značnému zneužívání veřejných a firemních Wi-Fi sítí, zejména v období masového rozšíření notebooků a hotspotů začátkem 21. století. Ačkoliv byl WEP technicky překonaný již brzy po svém zavedení, některá zařízení jej podporovala ještě řadu let, což z něj činilo dlouhodobý bezpečnostní problém. [6]

1.2.2 Přechod na WPA a WPA2

Vzhledem ke kritickým nedostatkům WEPu byla nutná rychlá náhrada. Wi-Fi Alliance proto představila v roce 2003 přechodný standard WPA, který měl poskytnout lepší zabezpečení a zároveň zůstat kompatibilní se starším hardwarem. Hlavní zlepšení představoval přechod na dynamické klíčování prostřednictvím protokolu Temporal Key Integrity Protocol (TKIP). TKIP pravidelně měnil šifrovací klíče pro každý paket, čímž se eliminovala slabina statického IV u WEP. [6]

WPA sice představoval významný krok vpřed, nicméně byl stále postaven na šifře RC4, a tudíž zůstával zranitelný vůči určitým typům útoků, především těm, které využívaly slabiny v implementaci TKIP. Navíc TKIP nebyl navržen s důrazem na budoucnost, byl spíše „dočasným záplatováním“ stávající situace, než komplexním a odolným řešením. [6]

Oproti tomu WPA2, představený v roce 2004 a postupně zavedený jako povinný od roku 2006, přinesl skutečnou technologickou změnu. Nahradil RC4 za blokovou šifru Advanced Encryption Standard (AES) a TKIP za Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), což zajistilo nejen vysokou kryptografickou

bezpečnost, ale i integritu přenášených dat. Díky těmto vlastnostem se WPA2 stal dlouholetým standardem pro zabezpečení bezdrátových sítí, a to jak v domácím, tak korporátním prostředí. [6]

1.2.3 WPA3 – současná generace šifrování

Nejnovějším vývojovým stupněm je WPA3, představený Wi-Fi Alliance v roce 2018. Tento standard reaguje na několik dlouhodobých bezpečnostních nedostatků, které přetrvávaly i u WPA2. Ačkoliv WPA2 poskytoval silnou ochranu, zůstával zranitelný vůči tzv. offline slovníkovým útokům, zejména v režimu Pre-Shared Key (PSK). WPA3 nahrazuje tento mechanismus novým protokolem Simultaneous Authentication of Equals (SAE), který využívá princip výměny klíčů na bázi Diffie-Hellman a zajišťuje robustní autentizaci i při použití slabších hesel. [7]

Další výhodou WPA3 je zavedení forward secrecy, která zajišťuje, že i při kompromitaci hesla nelze zpětně dešifrovat starší komunikaci. To posiluje ochranu dlouhodobých citlivých dat. WPA3 také zvyšuje ochranu proti aktivním útokům v otevřených sítích prostřednictvím šifrování rámců i bez nutnosti autentizace, tato funkce je známa jako Opportunistic Wireless Encryption (OWE). [7]

Implementace WPA3 je podporována ve většině nových zařízení, přičemž některé směrovače a klienti nabízí možnost přechodového režimu, který kombinuje podporu WPA2 a WPA3. Vzhledem ke zpětné nekompatibilitě je ale široké nasazení postupné, především kvůli nutnosti obměny starších zařízení. [7]

WPA3 představuje současný vrchol v oblasti zabezpečení Wi-Fi sítí, který reaguje na vývoj hrozeb i rostoucí nároky na ochranu dat v bezdrátovém prostředí. Jeho adopce je důležitým krokem k budoucnosti bezdrátové bezpečnosti, ačkoliv zůstává závislá na schopnosti trhu adaptovat se na nová technologická a bezpečnostní doporučení. [4]

1.2.4 Porovnání jednotlivých zabezpečení

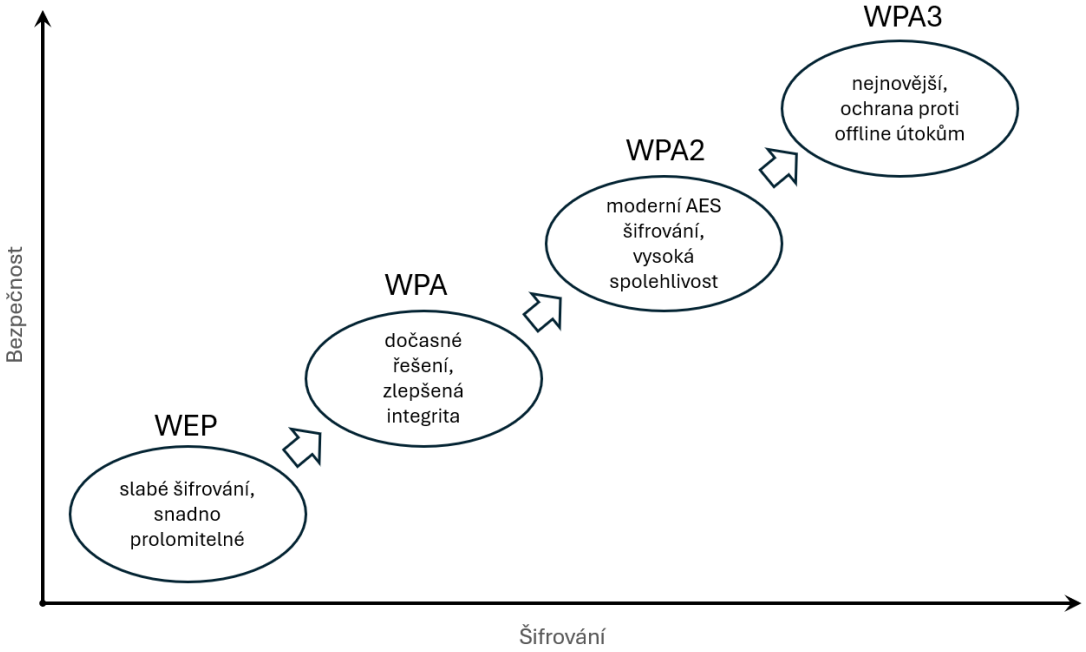
V Tabulka 1 jsou uvedeny rozdíly mezi jednotlivými standardy, přičemž šifra nám říká, jaký šifrovací algoritmus byl použit, to nám potom ovlivňuje sílu ochrany proti odposlechu. Integrita je ochrana proti tomu, aby nemohla být data během přenosu změněna. Ochrana proti offline útokům nás chrání proti slovníkovým útokům a forward secrecy zajišťuje, že pokud dojde k prolomení jednoho klíče, tak nelze dešifrovat předchozí konverzace, zvyšuje tedy soukromí. [1]

Tabulka 1: Rozdíly v šifrovacích standardech

Standard	Šifra	Integrita	Ochrana proti offline útokům	Forward secrecy	Rok zavedení
WEP	RC4	CRC-32	Ne	Ne	1997
WPA	RC4	MIC(TKIP)	Částečná	Ne	2003
WPA2	AES	CCMP	Ano	Ne	2004
WPA3	AES	GCMP-256/CCMP	Ano (SAE)	Ano	2018

Zdroj: vlastní zpracování

Obrázek 1 ukazuje vývoj síly zabezpečení jednotlivých Wi-Fi standardů graficky.



Obrázek 1: Graf vývoje bezpečnosti šifrování

Zdroj: vlastní zpracování

1.3 Současný stav zabezpečení bezdrátových sítí

Dnešní bezdrátové sítě prošly dlouhým vývojem v oblasti zabezpečení, přičemž moderní technologie neustále přinášejí inovace, které mají za cíl eliminovat historické i nově vznikající hrozby. Přestože WPA3 představuje nejpokročilejší standard zabezpečení Wi-Fi, stále existují výzvy a problémy spojené s implementací a adopcí nových bezpečnostních mechanismů. [8]

Většina zařízení dnes stále využívá WPA2, ačkoliv jeho bezpečnostní úroveň již není považována za zcela dostatečnou. Implementace nového standardu WPA3 je sice doporučovaná, ale jeho širší nasazení je omezeno kompatibilitou starších zařízení a nutností jejich modernizace. Některé podniky a organizace již začaly přecházet na WPA3, avšak mnoho domácností a malých podniků stále setrvává u starších metod autentizace a šifrování, což zvyšuje riziko kompromitace jejich bezdrátových sítí. [7]

Autentizační mechanismy v současných bezdrátových sítích prošly významným vývojem. Tradiční modely, jako je Pre-Shared Key (PSK), jsou sice stále běžné, ale ve větších organizacích dochází k častějšímu využívání robustnějších metod autentizace, například 802.1X/EAP, které umožňují centralizovanou správu přístupových oprávnění. Tento model autentizace se osvědčil zejména ve firemním prostředí, kde je nutné spravovat velké množství uživatelských účtů a zajistit jejich bezpečné připojení k síti. [3]

Dalším důležitým aspektem současného stavu zabezpečení bezdrátových sítí je zvýšený důraz na ochranu soukromí a prevenci sledování uživatelů. Tradiční metody identifikace zařízení v síti, například na základě MAC adres, jsou v dnešní době stále častěji nahrazovány dynamickými a náhodně generovanými MAC adresami, což ztěžuje pasivní sledování uživatelů a jejich online aktivity. Tento trend je součástí širšího posunu směrem k větší ochraně soukromí uživatelů a k eliminaci možností zneužití síťových identifikátorů ke sledování polohy nebo aktivity jednotlivců. [9]

Rovněž se rozšiřuje využití pokročilých bezpečnostních funkcí, jako je segmentace sítí a řízení přístupových oprávnění na základě kontextu. Současné firemní a podnikové Wi-Fi sítě často využívají oddělené VLAN segmenty pro různé kategorie uživatelů, což snižuje riziko horizontální eskalace útoků mezi zařízeními připojenými ke stejné síti. Tato segmentace umožňuje lepší kontrolu nad síťovým provozem a minimalizaci škod v případě kompromitace jednoho z připojených zařízení. [9]

Moderní bezpečnostní architektury bezdrátových sítí stále častěji implementují model zero-trust, který vychází z principu, že žádný uživatel ani zařízení by neměly být automaticky považovány za důvěryhodné. Tento přístup zahrnuje neustálé ověřování uživatelů a zařízení při každém přístupu k síti, bez ohledu na jejich fyzickou lokalitu. Tímto způsobem lze minimalizovat riziko kompromitace v důsledku neoprávněného přístupu nebo zneužití legitimních přístupových údajů. [8]

Zavedení nových technologií, jako je Wi-Fi 6 (802.11ax), přineslo vylepšení nejen v oblasti výkonu a efektivity přenosu dat, ale také v bezpečnosti. Wi-Fi 6 zahrnuje podporu pro WPA3, lepší správu přístupu k síti a pokročilé šifrovací algoritmy, které eliminují některé z dříve existujících slabin. Přestože Wi-Fi 6 stále není standardem u všech nových zařízení, jeho rozšíření se očekává v nadcházejících letech, což přispěje k celkovému posílení bezpečnostní infrastruktury bezdrátových sítí. [5]

Navzdory pokrokům v oblasti autentizace, šifrování a ochrany soukromí stále existují výzvy, kterým musí současné bezdrátové sítě čelit. Patří mezi ně například narůstající počet Internet Of Things (IoT) zařízení, která často nejsou vybavena dostatečně silnými bezpečnostními mechanismy, nebo rostoucí sofistikovanost útočníků, kteří hledají nové způsoby, jak obejít zavedené ochranné mechanismy. Z tohoto důvodu je nezbytné, aby organizace i jednotliví uživatelé pravidelně aktualizovali svá zařízení, používali moderní autentizační metody a implementovali vícevrstvá bezpečnostní opatření k minimalizaci potenciálních rizik a zajištění tzv. triády CIA, tedy Confidentiality (důvěrnost), Integrity (integrita) a Availability (dostupnost): [10]

- **Důvěrnost** – zajišťuje, že informace jsou přístupné pouze těm, kteří mají oprávnění. Cílem je zabránit neoprávněnému přístupu k citlivým datům.
- **Integrita** – zajišťuje, že data nejsou neoprávněně nebo neúmyslně změněna. Uživatelé musí mít jistotu, že informace jsou přesné a úplné.
- **Dostupnost** – zajišťuje, že informace a systémy jsou dostupné, když je uživatelé potřebují. Cílem je minimalizovat výpadky a zajišťovat provozuschopnost.

2. HROZBY A ZRANITELNOSTI BEZDRÁTOVÝCH SÍTÍ

Bezdrátové sítě se staly klíčovou součástí moderního propojení zařízení a přenosu dat. S rostoucí dostupností Wi-Fi sítí však roste i počet bezpečnostních hrozeb, kterým tyto sítě čelí. Na rozdíl od kabelových sítí, kde je fyzický přístup ke kabelu nutný pro zachycení provozu, bezdrátová komunikace umožňuje útočníkům snadnější přístup k síťovým paketům, což činí tyto sítě atraktivním cílem kybernetických útoků. [11]

Základní bezpečnostní problémy bezdrátových sítí zahrnují neautorizovaný přístup, zachytávání a manipulaci s přenášenými daty, prolomení autentizačních mechanismů a narušení dostupnosti sítě. Útoky mohou mít různé podoby, od pasivního odposlechu až po aktivní zásahy do síťové infrastruktury. Jedním z hlavních faktorů ohrožení je špatná konfigurace bezpečnostních mechanismů a použití zastaralých protokolů, jako je WEP, který lze snadno prolomit metodami popsanými v této kapitole. [11]

Bezdrátové sítě jsou vystaveny celé řadě hrozeb, které mohou ohrozit jejich bezpečnost a spolehlivost. Mezi nejčastější patří odposlech a zachytávání dat, kdy útočník pomocí nástrojů jako Wireshark sleduje nešifrovanou komunikaci a získává citlivé informace. Dalším rizikem jsou útoky typu Man-in-the-Middle, například prostřednictvím falešného přístupového bodu (Evil Twin), kdy útočník přesměruje komunikaci přes své zařízení a může ji měnit. Neautorizovaný přístup se často realizuje prolomením slabého hesla k Wi-Fi síti, například pomocí nástrojů jako Aircrack-ng. Útoky typu Denial of Service (DoS) mohou zahrnovat zahlcení sítě deautentizačními rámci, což způsobí odpojení legitimních uživatelů.

Důsledky těchto zranitelností mohou být závažné, od ztráty citlivých informací a narušení soukromí až po ztrátu kontroly nad síťovými zdroji či finanční škody. Firmy navíc čelí riziku přerušení provozu a poškození reputace v důsledku úniku zákaznických údajů. Efektivní ochrana vyžaduje pochopení těchto hrozeb a implementaci vhodných bezpečnostních opatření, jako je šifrování komunikace, silná autentizace a monitorování sítě.

2.1 Definice zdrojů hrozeb

Bezdrátové sítě čelí řadě bezpečnostních hrozeb, které lze rozdělit do několika kategorií. Mezi hlavní zdroje nebezpečí patří neautorizovaný přístup, prolomení šifrování, podvržené přístupové body a sofistikované metody zneužití síťových protokolů. [11]

Jedním z klíčových problémů bezdrátových sítí je jejich otevřená povaha, signály se šíří volným prostorem a mohou být zachyceny kýmkoliv v jejich dosahu. To umožňuje útočníkům provádět odposlech, manipulovat s daty nebo se dokonce neautorizovaně připojit k síti. [12]

Dalším zdrojem nebezpečí jsou zastaralé bezpečnostní protokoly, jako je WEP, který lze snadno prolomit. WPA a WPA2 přinesly vylepšené zabezpečení, avšak stále existují způsoby, jak je napadnout, například slovníkové útoky na hesla nebo zneužití chyb v implementaci protokolu. Moderní WPA3 eliminuje některé z těchto slabin, ale není vždy široce podporován. [3]

Mezi další rizikové faktory patří nedostatečná kontrola nad přístupem k síti, slabá hesla a absence vícefaktorové autentizace. Mnoho uživatelů používá výchozí přístupová hesla nebo jednoduché kombinace, což usnadňuje jejich prolomení pomocí brute-force útoků. [11]

2.2 Typy útoků na bezdrátové sítě

Útoky na bezdrátové sítě lze rozdělit do několika hlavních kategorií. Každý typ útoku cílí na konkrétní slabinu v síti a může mít různé důsledky, od odposlechu dat po kompletní převzetí kontroly nad sítí.

- **Odposlech a zachytávání dat** – pasivní útoky, při kterých útočník monitoruje síťový provoz bez aktivního zasahování do komunikace.
- **Útoky typu Man-in-the-Middle (MITM)** – umožňují útočníkovi manipulovat s přenášenými daty a získat přístup k citlivým informacím.
- **Neautorizovaný přístup a prolomení hesel** – zneužití slabých hesel nebo nešifrovaných sítí pro získání neautorizovaného přístupu.
- **Denial of Service (DoS) útoky** – útoky zaměřené na narušení dostupnosti služby, například deautentizační útoky nebo zahlcení sítě nevyžádaným provozem.

Každý z těchto útoků představuje vážné bezpečnostní riziko a organizace i jednotlivci by měli zavést opatření, která minimalizují jejich dopad. [13]

2.2.1 Odposlech a zachytávání dat

Odposlech je jedním z nejčastějších útoků na bezdrátové sítě. Útočník může zachytávat síťovou komunikaci pomocí specializovaných nástrojů, jako jsou Wireshark nebo Kismet. I když jsou moderní sítě často šifrovány, některé protokoly stále přenášejí metadata v nešifrované podobě, což může být zneužito ke sledování uživatelů nebo k rekonstrukci přenášených dat. [11]

Ve veřejných Wi-Fi sítích jsou uživatelé obzvláště zranitelní, protože často nejsou použita dodatečná bezpečnostní opatření, jako je VPN. Útočník může například analyzovat DNS požadavky a získat přehled o navštívených stránkách. [13]

2.2.2 Útoky typu „Man-in-the-Middle‘‘

MITM útoky umožňují útočníkovi vstoupit mezi dvě komunikující strany a manipulovat s datovým tokem. Existuje několik variant těchto útoků:

- **ARP Spoofing** – útočník zmanipuluje ARP tabulky v síti tak, že provoz oběti směřuje přes jeho zařízení.
- **Rogue Access Point (Evil Twin)** – útočník vytvoří falešný přístupový bod, ke kterému se oběť připojí, což mu umožní odposlouchávat a manipulovat s provozem.
- **SSL Stripping** – technika, která odstraní šifrování HTTPS a umožní odposlech nešifrovaných přenosů.

Úspěšné MITM útoky mohou vést k získání přihlašovacích údajů, finančních informací nebo k instalaci škodlivého softwaru do zařízení oběti. [11]

2.2.3 Neautorizovaný přístup a prolomení hesel

Útoky na autentizaci jsou běžným způsobem, jak se útočníci dostávají do bezdrátových sítí. Mezi nejčastější metody patří slovníkové a brute-force útoky, při kterých útočník testuje různé kombinace hesel, dokud nenalezne správnou. [11]

Slabá hesla jsou často první linií obrany, kterou útočníci zneužívají. Proti těmto útokům lze bojovat použitím silných hesel a vícefaktorové autentizace. WPA3 zavádí ochranu proti offline slovníkovým útokům, což ztěžuje prolomení hesla. [11]

2.2.4 Denial of service útoky

DoS útoky jsou zaměřeny na narušení dostupnosti bezdrátových sítí. Mezi běžné metody patří:

- **Deauthentication Attacks** – útočník posílá falešné deautentizační pakety, čímž odpojí uživatele od sítě.
- **Jamming** – rušení Wi-Fi signálu silným vysílačem, což znemožňuje komunikaci.
- **Beacon Flooding** – zahlcení sítě falešnými SSID, což může zpomalit síť nebo znemožnit připojení legitimních uživatelů. [13]

2.3 Dopady zranitelností na uživatele a organizace

Bezpečnostní hrozby v bezdrátových sítích mohou mít závažné důsledky nejen pro jednotlivé uživatele, ale i pro organizace a podniky. Zranitelnosti v síťové infrastruktuře mohou vést k úniku citlivých dat, narušení provozu služeb a vážným ekonomickým a právním dopadům.

2.3.1 Dopady na jednotlivé uživatele

Bezdrátové sítě jsou běžnou součástí každodenního života jednotlivců, ať už se jedná o domácí Wi-Fi, veřejné přístupové body nebo firemní sítě. Každý uživatel, který se připojuje k nezabezpečené síti nebo používá slabá bezpečnostní opatření, se vystavuje riziku:

1. **Úniku osobních údajů** – útočníci mohou zachytit citlivé informace, jako jsou přihlašovací údaje, e-maily, bankovní informace nebo soukromá komunikace. Takto získané údaje mohou být zneužity k podvodům, krádeži identity nebo dalším útokům.
2. **Ztráty finančních prostředků** – kyberzločinci mohou zneužít odcizené přihlašovací údaje k přístupu na bankovní účty, online platební služby nebo k provádění neautorizovaných transakcí. Útoky, jako je phishing nebo Man-in-the-Middle (MITM), mohou vést k velkým finančním ztrátám.
3. **Kompromitace zařízení** – prostřednictvím zranitelné bezdrátové sítě mohou útočníci získat přístup k samotnému zařízení uživatele, instalovat malware nebo vzdáleně ovládat jeho systém. To může vést ke ztrátě dat, jejich zašifrování ransomwarem nebo dokonce ke sledování uživatele prostřednictvím webkamery či mikrofonu.
4. **Sociální a psychologické dopady** – ztráta citlivých informací, například osobních fotografií nebo konverzací, může mít vážné sociální dopady, včetně narušení soukromí, šikany či vydírání. Lidé, kteří se stanou oběťmi kybernetického útoku, mohou zažívat stres, úzkost nebo ztrátu důvěry v digitální technologie. [11]

2.3.2 Dopady na organizace a firmy

Firmy a organizace, které provozují bezdrátové sítě, musí dbát na jejich dostatečné zabezpečení, protože případné zranitelnosti mohou mít dalekosáhlé následky:

1. **Únik důvěrných firemních dat** – kompromitace firemní sítě může vést k odcizení citlivých obchodních informací, smluv, zákaznických dat nebo výzkumných a vývojových materiálů. Takový únik může poškodit konkurenceschopnost firmy a vést k právním sporům.

2. **Narušení provozu a ztráta produktivity** – útoky typu Denial of Service (DoS) mohou ochromit síť a znemožnit zaměstnancům přístup k firemním zdrojům. To může vést k výraznému poklesu produktivity a finančním ztrátám.
3. **Finanční ztráty a sankce** – firmy mohou čelit nejen přímým finančním ztrátám v důsledku kybernetických útoků, ale také pokutám za nedodržení bezpečnostních předpisů (např. GDPR). Právní odpovědnost za únik zákaznických dat může vést k žalobám a vysokým kompenzacím.
4. **Poškození reputace** – ztráta důvěry zákazníků je jedním z nejzávažnějších důsledků kybernetických incidentů. Jakmile se veřejně provalí, že společnost nedokázala ochránit citlivé údaje, může dojít ke ztrátě zákazníků a dlouhodobému poškození značky.
5. **Zneužití firemní infrastruktury k dalším útokům** – kompromitovaná síť může být útočníky využita k dalším škodlivým aktivitám, například k šíření malwaru, botnet útokům nebo phishingovým kampaním. [11]

3. POSTUPY PROVÁDĚNÍ PRŮZKUMŮ

Průzkumy představují důležitý nástroj pro získání dat, která umožňují lépe porozumět chování uživatelů a identifikovat slabá místa v oblasti bezpečnosti bezdrátových sítí. Díky systematickému sběru informací lze odhalit nejen technické zranitelnosti, ale také lidské faktory, které často hrají klíčovou roli při vzniku bezpečnostních incidentů. Správně zvolený postup průzkumu je proto zásadní pro získání relevantních a objektivních výsledků.

3.1 Průzkum připojování uživatelů k nezabezpečeným bezdrátovým sítím

Jednou z praktických částí zkoumání bezpečnosti bezdrátových sítí bylo provedení terénního testu, který měl za cíl analyzovat chování uživatelů ve veřejném prostoru při výskytu otevřené Wi-Fi sítě. Experiment byl navržen jako jednoduchá simulace reálného bezpečnostního rizika s využitím běžného mobilního telefonu, jenž byl nakonfigurován jako přenosný přístupový bod (hotspot) bez zabezpečení.

Cílem bylo zjistit, kolik zařízení se samovolně nebo úmyslně připojí k síti, která nese název odkazující na konkrétní umístění, například název nákupního centra, kavárny, restauračního zařízení nebo dopravní společnosti. Většina uživatelů vnímá názvy Wi-Fi sítí jako indikátor legitimity, a pokud se v jejich okolí objeví síť s důvěryhodně znějícím jménem, neváhají se k ní připojit. Tento předpoklad tvořil základ celé simulace.

Mobilní telefon, respektive hotspot, byl umístěn v různých lokalitách, například na fotbalovém stadionu, v nákupním centru a v kasárna Armády České republiky. Místa byla volena náhodně ovšem s předpokladem, že se jedná o místa s vyšší koncentrací přítomných osob. Jednotlivé lokace budou blíže popsány ve vyhodnocovací části této práce. V rámci experimentu nebyl aktivně zachytáván žádný obsah přenášených dat, pouze identifikace zařízení v podobě jeho fyzické síťové adresy. Pozornost byla ale soustředěna hlavně na záznam počtu připojených zařízení, jejich síťovou adresu a zda mají nastavené automatické připojování.

Původní záměr celého tohoto výzkumu šel však ještě dále. Po připojení uživatele k síti mělo dojít k automatickému přesměrování na jednoduchou webovou stránku, která by vyžadovala zadání e-mailové adresy, údajně pro účely autorizace připojení. Tento prvek měl simulovat běžnou situaci z praxe, například hotelové nebo kavárenské sítě, které požadují přihlášení či registraci před poskytnutím internetového připojení.

Z pohledu bezpečnostního výzkumu by takové řešení mohlo poskytnout cenné údaje o důvěřivosti uživatelů a jejich ochotě sdílet osobní údaje v nezabezpečeném prostředí. Avšak

ještě před realizací této části byl celý návrh konzultován s právním poradcem. Ten upozornil na potenciální právní a etické problémy spojené s tímto přístupem.

Hlavní riziko spočívalo v tom, že by mohl být výzkum považován za cílený zásah do pověsti konkrétních lokalit, firem nebo institucí, kde by experiment probíhal, a to i v případě jiného názvu sítě, než jaký je název sítě provozované konkrétní společností. Přestože by e-mailové adresy nebyly uchovávány ani nijak dále zpracovávány, samotné vyvolání dojmu legitimního připojení k síti provozované daným subjektem by mohlo být vnímáno jako manipulativní nebo škodlivé jednání. Navíc jakékoliv získávání osobních údajů bez souhlasu by mohlo být v rozporu se zákony na ochranu osobních údajů (například GDPR v rámci EU).

Na základě těchto doporučení bylo rozhodnuto od původního návrhu ustoupit a test omezit výhradně na sledování počtu připojených zařízení bez interakce s uživateli nebo sběru jakýchkoliv citlivých údajů. Tento přístup sice neposkytuje tak hlubokou analýzu chování uživatelů, ale zachovává etické a právní limity výzkumu a zároveň ukazuje, že i samotná přítomnost otevřené Wi-Fi sítě může představovat výrazné bezpečnostní riziko.

Výsledek experimentu nám ukáže, jak snadno může útočník zneužít důvěryhodnosti názvu sítě a zneužít přirozené chování uživatelů. Mnoho zařízení je totiž konfigurováno tak, aby se automaticky připojovala k dříve známým nebo silným signálům bez ověření jejich legitimity. Tento fakt podtrhuje potřebu edukace uživatelů v oblasti digitální bezpečnosti a potřebu implementace bezpečnostních opatření i na straně koncových zařízení.

Z hlediska navrženého postupu je důležité dodat, že i v této omezené podobě přinese průzkum relevantní data a podpoří hypotézu, že uživatelé často nevědomky podstupují rizika spojená s používáním veřejných sítí.

3.2 Technické řešení průzkumu s nezabezpečenou Wi-Fi sítí

Tento průzkum byl prováděn pomocí mobilního telefonu Xiaomi Redmi Note 9, který, oproti telefonu od společnosti Apple, umožňoval nastavit a zapnout mobilní hotspot bez hesla. Použita byla pouze technologie 2,4 GHz a to z důvodu jejího většího dosahu.

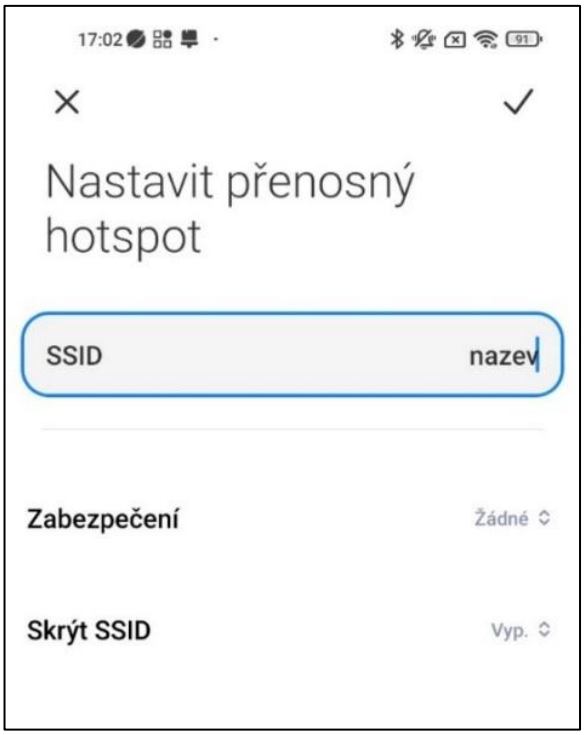
Rozdíl mezi technologiemi 2,4 a 5 GHz je hlavně ve větším dosahu a lepším průnikem signálu přes překážky u technologie 2,4 GHz, naproti tomu technologie 5 GHz zvládne vetší rychlosti přenosu, ale to nebylo předmětem zájmu tohoto průzkumu.

U nastavení hotspotu bylo důležité nastavit tyto parametry:

- Změnit název sítě SSID.
- Vypnout heslo.
- Zvolit technologii 2,4 GHz.
- Vypnout funkci automatického vypnutí hotspotu při nečinnosti.

V rámci průzkumu bylo dále vypnuto automatické zhasínání displeje, aby mohl být neustále sledován stav připojených zařízení a nemusel se telefon neustále odemykat.

Přiložený Obrázek 2: Nastavení Hotspotu na mobilním telefonu nám ukazuje snímek obrazovky s oknem nastavení hotspotu v telefonu.



Obrázek 2: Nastavení Hotspotu na mobilním telefonu
Zdroj: vlastní zpracování

Samotná část testování automatického připojování probíhala manuálně tak, že po připojení konkrétního zařízení bylo potom manuálně odpojeno od sítě a sledovalo se, jestli dojde ihned k jeho připojení. Výsledek může tedy být potencionálně zkreslen, a to konkrétně v případě, kdy by uživatel ihned po odpojení telefonu od sítě zkoušel manuálně jeho opětovné připojení. Při tomto testu byla tedy snaha o co nejmenší časovou dotaci a bylo spoléháno na to, že si během tohoto krátkého času uživatel neuvědomí jeho odpojení od W-Fi sítě. Identifikace byla velice snadná díky získaným síťovým adresám jednotlivých zařízení.

3.3 Dotazníkový průzkum o vzdělanosti uživatelů

Cílem tohoto průzkumu bylo získat data o povědomí uživatelů z oblasti bezpečnosti bezdrátových sítí.

Při volbě metody pro zjištění povědomí a znalostí uživatelů o bezpečnosti bezdrátových sítí bylo rozhodnuto pro dotazníkové šetření. Dotazník je efektivní nástroj pro sběr dat, který umožňuje analyzovat odpovědi od širokého vzorku respondentů v rámci relativně krátké doby. Tento nástroj je také vhodný pro kvantitativní analýzu a snadno se interpretuje. Dotazníkové šetření umožní zjistit nejen to, jaké mají lidé znalosti o zabezpečení bezdrátových sítí, ale také jak se v praxi chovají a zda si uvědomují možná rizika.

Další důvod pro volbu dotazníku je jeho flexibilita. Dotazník lze distribuovat online, čímž se zvýší dosah a zapojení respondentů z různých sociodemografických skupin. Oproti jiným metodám, jako jsou rozhovory nebo experimenty, poskytuje dotazníkové šetření standardizované odpovědi, které lze snadno analyzovat statistickými metodami. Online dotazníky navíc umožňují rychlé a efektivní zpracování dat, což je výhodné zejména při větším počtu respondentů.

Dotazník poskytuje také možnost anonymního vyplnění, což je klíčový faktor ovlivňující upřímnost odpovědí. Uživatelé jsou více ochotni sdílet své zkušenosti a názory bez obav z negativních důsledků. Tímto způsobem lze získat spolehlivější výsledky než například při osobních rozhovorech, kde může docházet k ovlivňování odpovědí přítomností tazatele.

Pro účely této diplomové práce bylo zvoleno umístění dotazníku online do prostoru poskytovaného na internetovém portálu www.vyplnto.cz. Umístění dotazníku online zvýší jeho dosah, což povede k rozsáhlejšímu souboru respondentů.

3.4 Odůvodnění volby jednotlivých otázek

Dotazník je sestaven tak, aby poskytl ucelený pohled na chování uživatelů a jejich povědomí o bezpečnosti bezdrátových sítí. Otázky byly pečlivě vybrány s ohledem na klíčové aspekty tématu.

Otázky na demografické údaje pomohou identifikovat, zda existuje rozdíl ve znalostech a chování uživatelů na základě věku a pohlaví. Například mladší generace může mít větší povědomí o bezpečnostních opatřeních, zatímco starší uživatelé mohou být zranitelnější kvůli

nižší technologické gramotnosti. Podobně mohou být rozdíly mezi pohlavími, například v přístupu k technologickým inovacím nebo úrovni zájmu o kybernetickou bezpečnost.

Otázky zaměřené na způsob připojování k veřejným Wi-Fi sítím jsou klíčové pro pochopení rizik, které uživatelé podstupují. Z odpovědí lze zjistit, zda si lidé uvědomují nebezpečí spojené s nezabezpečenými sítěmi a jak často se k nim připojují. Časté připojování k otevřeným sítím může znamenat vyšší pravděpodobnost vystavení kybernetickým útokům, jako je například odposlech dat či podvržené přístupové body.

Použití VPN je jednou z nejefektivnějších metod ochrany soukromí při připojení k veřejné bezdrátové síti. Odpovědi na tuto otázku ukážou, nakolik je tato technologie rozšířená mezi uživateli a zda je potřeba větší osvěta. Pokud se ukáže, že mnoho respondentů VPN nevyužívá, lze doporučit edukativní kampaně nebo zavádění uživatelsky přívětivějších řešení.

Otázky ze sady o bezpečnostních technologiích jsou zaměřené na znalost WEP, WPA a WPA2/WPA3 a jsou důležité pro zjištění, zda si uživatelé uvědomují rozdíly mezi těmito standardy a zda používají dostatečně silné zabezpečení ve svých vlastních sítích. Pokud většina respondentů odpoví, že tyto technologie nezná, může to znamenat, že je potřeba větší osvěta v oblasti síťové bezpečnosti.

Tato sada otázek ohledně opatření pro ochranu osobních údajů zjišťuje, jaké další bezpečnostní mechanismy uživatelé používají, například dvoufaktorové ověřování, kontrolu legitimity bezdrátových sítí nebo deaktivaci automatického připojování. Odpovědi mohou ukázat, jak moc jsou uživatelé opatrní při ochraně svých dat a zda jsou ochotni přijmout další bezpečnostní opatření.

Použití dotazníkové metody umožní nejen zjistit, jaké mají lidé znalosti o bezpečnosti bezdrátových sítí, ale také analyzovat jejich chování a identifikovat potenciálně rizikové skupiny. Díky kvantitativní povaze dotazníku lze data efektivně zpracovat a vyvodit z nich důležité závěry, které mohou být užitečné při navrhování opatření pro zvýšení bezpečnosti. Dotazník je tedy ideálním nástrojem pro dosažení cílů diplomové práce a poskytne hodnotná data pro další analýzu.

4. VÝSLEDKY PRŮZKUMŮ

Pro získání relevantních dat byla realizována dvě samostatná šetření zaměřená na zjištění chování uživatelů při připojování k nezabezpečeným bezdrátovým sítím a na získání informací ohledně vzdělanosti uživatelů z oblasti bezdrátových sítí. V následujících částech jsou prezentovány klíčové poznatky, které vyplynuly z analýzy získaných dat.

4.1 Výsledky průzkumu o chování uživatelů bezdrátových sítí

V rámci výzkumu byla vytvořena falešná nezabezpečená Wi-Fi síť ve veřejném prostoru, jejímž cílem bylo sledovat, kolik zařízení se k této síti automaticky nebo vědomě připojí. Tímto způsobem bylo možné ověřit, jak snadno se lidé připojují k neznámým sítím a jaké bezpečnostní riziko z toho může plynout. Výsledky experimentu poskytují cenný vhled do reálného chování uživatelů a jejich schopnosti rozpoznat potenciálně nebezpečné situace v bezdrátovém prostředí.

Výsledky experimentu ukázaly, že uživatelé mají tendenci se k otevřeným sítím připojovat spontánně. V některých lokalitách, jako například na fotbalovém stadionu AC Sparta Praha, se během několika minut připojilo i více zařízení. Připojení byla v některých případech aktivní, v jiných případech šlo o automatické pokusy zařízení o opětovné připojení k síti s dříve uloženým SSID. Získané screenshoty jsou přiloženy jako přílohy této práce.

Stadion AC Sparta Praha fotbal, a.s., zápas 8. 3. 2024

Stadion patří mezi moderní sportovní areály s vysokou koncentrací návštěvníků a disponuje vlastní oficiální Wi-Fi sítí pro fanoušky. Přestože je připojení přes oficiální síť běžně dostupné, cílem experimentu bylo zjistit, kolik zařízení se automaticky nebo vědomě připojí k nezabezpečené, falešně pojmenované Wi-Fi síti, která byla v rámci měření spuštěna přímo na jedné z tribun stadionu.

Testovací síť nesla důvěryhodně znějící název, který mohl u některých uživatelů vzbudit dojem legitimního připojení ke klubové infrastruktuře. Měření ukázalo, že i přes přítomnost oficiální Wi-Fi se během zápasu vyskytovalo několik zařízení, která se k falešné síti buď pokusila připojit automaticky, nebo byla aktivní při vyhledávání přístupových bodů. To naznačuje, že část návštěvníků má na svých zařízeních aktivované automatické připojování nebo nerozlišuje mezi důvěryhodnými a potenciálně nebezpečnými sítěmi. Podrobnější výsledky jsou zobrazeny v Tabulka 3: Výsledky měření stadion AC Sparta a parametry měření potom v Tabulka 2.

Tabulka 2: Parametry měření stadion AC Sparta

Parametr měření	Hodnota
Datum	8. 3. 2025
Čas měření	18:30 – 21:00 (150 minut)
Počet připojených zařízení za dobu měření	4
Průměrný interval připojení	každých 37 minut a 30 sekund

Zdroj: vlastní zpracování

Tabulka 3: Výsledky měření stadion AC Sparta

Síťová adresa zařízení	Automatické připojování
a6:eb:29:f7:41:99	ano
ea:70:56:67:2e:c5	ne
86:72:80:a8:31:6e	ne
10:32:7e:89:85:b0	ne

Zdroj: vlastní zpracování

Vlak společnosti České dráhy, a.s.

Během jízdy vlaku Českých drah na trase Praha hlavní nádraží – Tišice bylo zaznamenáno pouze jedno zařízení, které detekovalo testovací falešnou Wi-Fi síť. Toto zařízení mělo síťovou adresu 62:56:68:e0:2a:82 a z dostupných údajů vyplývá, že automatické připojování nebylo aktivní. To znamená, že uživatel se sice připojil, ale po jeho odpojení již ne.

Vzhledem k velmi nízkému počtu cestujících ve voze, pouze několik jednotlivců, byl očekávaný počet zachycených zařízení omezený. I přesto výsledek ukazuje, že alespoň část uživatelů má své zařízení správně nastavené, a to buď s vypnutým automatickým připojováním, nebo s vyšší mírou ostražitosti vůči neznámým sítím. Měření tak poskytlo doplňující pohled na rozdílné chování uživatelů v prostředí s nízkou hustotou osob a podtrhuje důležitost správného nastavení mobilních zařízení jako základního bezpečnostního prvku. Parametry měření jsou v Tabulka 4 a výsledky v Tabulka 5.

Tabulka 4: Parametry měření ve vlaku Českých drah

Parametr měření	Hodnota
Datum	8. 3. 2025
Čas měření	21:45 – 22:30 (45 minut)
Počet připojených zařízení za dobu měření	1
Průměrný interval připojení	každých 45 minut

Zdroj: vlastní zpracování

Tabulka 5: Výsledky měření ve vlaku Českých drah

Síťová adresa zařízení	Automatické připojování
62:56:68:e0:2a:82	ne

Zdroj: vlastní zpracování

Vojenská základna Armády České republiky

V době měření nebyla na místě provozována žádná oficiální Wi-Fi síť, což umožnilo pozorovat reakce zařízení v prostředí s minimální síťovou infrastrukturou. Po celou dobu nebyl zaznamenán žádný pokus o připojení k falešné nezabezpečené síti, ani automatický, ani vědomý ze strany uživatelů.

Tento výsledek vnímám jako důkaz, že cílená edukace a osvěta v oblasti bezpečnosti bezdrátových sítí mají smysl a přinášejí reálné výsledky. Uživatelé v daném prostředí zřejmě dobře rozumějí rizikům spojeným s připojováním k neznámým sítím, což může být důsledkem systematického školení, bezpečnostních směrnic a důrazu na kybernetickou disciplínu. Absenci připojení tedy chápu jako pozitivní zpětnou vazbu na moje vlastní působení v oblasti zvyšování bezpečnostního povědomí u těchto uživatelů, které považuji za klíčový prvek obrany před hrozbami v bezdrátovém prostředí. Parametry tohoto měření ukazuje Tabulka 6.

Tabulka 6: Parametry měření Vojenská základna

Parametr měření	Hodnota
Datum	10. 3. 2025
Čas měření	14:00 – 15:00 (60 minut)
Počet připojených zařízení za dobu měření	0
Průměrný interval připojení	X

Zdroj: vlastní zpracování

Obchodní dům Baumax společnosti BM Česko s.r.o.

Cílem bylo ověřit, zda se v běžném komerčním prostředí připojují zařízení návštěvníků k neznámé nezabezpečené Wi-Fi síti, případně zda dojde k automatickým pokusům o připojení ze strany mobilních zařízení. Po dobu měření bylo zařízení vysílající falešnou Wi-Fi síť přítomno přímo v interiéru prodejny, a to i s aktivním pohybem v rámci prostoru, kdy se hotspot pohyboval mezi regály i hlavními uličkami, aby signál pokryl co největší plochu. Přesto nebyl zaznamenán žádný pokus o připojení, ať už automatický, nebo ruční.

Výsledek může být částečně ovlivněn tím, že se v obchodě v době měření pohybovalo relativně malé množství zákazníků, což snižovalo pravděpodobnost výskytu aktivních zařízení v dosahu.

Svou roli mohl sehrát i fakt, že se hotspot v době měření pohyboval po prodejní ploše, čímž mohl být signál vnímaný zařízeními jako méně stabilní nebo méně důvěryhodný. I přesto nulový výskyt připojených zařízení naznačuje, že v tomto typu prostředí je riziko připojení k podvržené síti nižší než v jiných veřejných prostorech, zejména tam, kde lidé setrvávají delší dobu a intenzivněji využívají svá zařízení. Výsledek měření zde přispívá k celkovému obrazu o chování uživatelů a ukazuje, že kontext prostředí i hustota pohybu osob mohou významně ovlivnit úroveň rizika. Tabulka 7 nám ukazuje parametry tohoto měření.

Tabulka 7: Parametry měření Baumax

Parametr měření	Hodnota
Datum	29. 3. 2025
Čas měření	14:00 – 14:30 (30 minut)
Počet připojených zařízení za dobu měření	0
Průměrný interval připojení	X

Zdroj: vlastní zpracování

Obchodní centrum Letňany, odpočinková zóna

Testovací zařízení bylo umístěno v tzv. chill zóně, tedy odpočinkové části centra vybavené sedacími vaky a pohodlným prostorem pro relaxaci. Tento typ prostředí přirozeně láká návštěvníky k delšímu setrvání a používání mobilních zařízení, a to se potvrdilo i při samotném měření. V okolí se vyskytovali převážně mladší lidé, kteří zde trávili čas se svými telefony nebo tablety. Přestože se nejednalo o prostor s výrazným pohybem davů, byly zaznamenány celkem 4 připojení k falešné Wi-Fi síti, což představuje reálné bezpečnostní riziko.

Pozitivním zjištěním však je, že žádné z těchto zařízení nemělo aktivní automatické připojování. Všechna připojení byla provedena vědomě uživateli, kteří se nechali zmást názvem sítě, ten byl záměrně zvolen tak, aby odpovídal názvu skutečné Wi-Fi poskytované obchodním centrem. Tento fakt ukazuje, že uživatelé sice nejsou zcela pasivní, ale zároveň mohou být snadno oklamáni podobností názvu s důvěryhodnou sítí, bez ověření její legitimity. Zjištění tak potvrzuje, že i v prostředí, kde nejsou aktivní automatické připojovací funkce, zůstává útok prostřednictvím podvržené sítě velmi účinný, zvláště pokud je cílen na běžné návštěvníky s nižší mírou technické ostražitosti. Výsledky z tohoto měření tak poukazují na potřebu větší opatrnosti při výběru veřejných Wi-Fi sítí a na důležitost edukace i u mladší generace, která je často technologicky aktivní, ale ne vždy dostatečně informovaná. Parametry a výsledky měření jsou zobrazeny v Tabulka 8 a Tabulka 9.

Tabulka 8: Parametry měření z obchodního centra Letňany

Parametr měření	Hodnota
Datum	29. 3. 2025
Čas měření	14:40 – 15:30 (50 minut)
Počet připojených zařízení za dobu měření	4
Průměrný interval připojení	Každých 12 minut a 30 sekund

Zdroj: vlastní zpracování

Tabulka 9: Výsledky měření z obchodního centra Letňany

Síťová adresa zařízení	Automatické připojování
66:12:f9:70:72:fc	ne
32:c9:db:51:50:91	ne
2e:70:d5:0b:b7:89	ne
c2:20:18:00:7d:0a	ne

Zdroj: vlastní zpracování

Restaurace společnosti McDonald´s ČR spol. s.r.o. v OC Letňany

Restaurace v době měření provozovala svou vlastní oficiální Wi-Fi síť, která byla veřejně přístupná a pravděpodobně známá většině pravidelných návštěvníků. V prostoru se nacházelo přibližně 20 hostů, z nichž někteří aktivně používali svá mobilní zařízení. Testovací zařízení vysílalo falešnou Wi-Fi síť s názvem imitujícím oficiální připojení restaurace.

Během měření byly zachyceny 2 zařízení, která se k falešné síti připojila. V obou případech se nejednalo o automatické připojení, jak vyplývá z údajů, uživatelé provedli připojení vědomě, patrně na základě známého názvu sítě, bez ověření její legitimity. Tento výsledek opět potvrzuje, že název sítě hraje klíčovou roli při rozhodování uživatele o připojení a že přítomnost skutečné Wi-Fi v dané lokalitě nevylučuje úspěšné zneužití její identity. I přes relativně malý počet zachycených zařízení lze považovat tento výsledek za varovný signál, že uživatelé často nepřikládají dostatečný význam kontrole zdroje připojení, zvláště v prostředí, které působí důvěryhodně a známě. Tabulka 10 a Tabulka 11 prezentují parametry a výsledky tohoto měření.

Tabulka 10: Parametry měření v restauraci McDonald

Parametr měření	Hodnota
Datum	29. 3. 2025
Čas měření	15:30 – 15:45 (15 minut)
Počet připojených zařízení za dobu měření	2
Průměrný interval připojení	Každých 7 minut a 30 sekund

Zdroj: vlastní zpracování

Tabulka 11: Výsledky měření v restauraci McDonald

Síťová adresa zařízení	Automatické připojování
16:d6:30:90:89:8b	ne
06:24:13:0e:d1:af	ne

Zdroj: vlastní zpracování

Čínská restaurace Štěstí

Restaurace nabízela vlastní zabezpečenou Wi-Fi síť, kterou mohli hosté využívat. V průběhu měření se v podniku nacházelo přibližně 30 hostů, přičemž falešná nezabezpečená Wi-Fi síť, vysílaná testovacím zařízením, byla po celou dobu aktivní. Výsledkem bylo, že nedošlo k žádnému připojení k této falešné síti. Tento výsledek lze vnímat pozitivně, naznačuje buď vyšší míru důvěry k zabezpečené oficiální síti, nebo opatrnější přístup ze strany návštěvníků, kteří se k neznámé síti nepřipojili, i přesto že byla v dosahu. Parametry měření jsou zobrazeny v Tabulka 12.

Tabulka 12: Parametry měření restaurace Štěstí

Parametr měření	Hodnota
Datum	4. 4. 2025
Čas měření	12:15 – 13:00 (45 minut)
Počet připojených zařízení za dobu měření	0
Průměrný interval připojení	X

Zdroj: vlastní zpracování

Stadion AC Sparta Praha fotbal, a.s., zápas 9. 4. 2024

Měření probíhalo v jednom z méně obsazených sektorů stadionu, což mohlo mít vliv na počet zaznamenaných zařízení. Tabulka 13 ukazuje parametry samotného měření. Přestože byla fanouškovská účast nižší než obvykle, právě delší doba měření umožnila zachytit větší objem provozu a zvýšit pravděpodobnost výskytu pokusů o připojení k falešné Wi-Fi síti.

Během této doby bylo detekováno celkem 10 zařízení, která navázala spojení s testovací sítí. Z toho 4 zařízení se připojila automaticky, což poukazuje na rizikové nastavení mobilních zařízení, které se mohou bez vědomí uživatele připojit ke známým nebo podvrženým sítím. Zbylých 6 zařízení se připojilo ručně, což naznačuje, že si uživatelé s největší pravděpodobností spletli testovací síť s oficiálním Wi-Fi připojením stadionu, případně se snažili připojit pouze na základě názvu bez ověření legitimity. Tyto výsledky, zobrazené v Tabulka 14, potvrzují, že i v prostředí s nižší hustotou osob je útok prostřednictvím podvržené sítě reálný a účinný, a zároveň poukazují na nedostatečné zabezpečení některých zařízení i na důvěřivost části

uživatelů. Měření tak dále rozšiřuje poznatky o chování návštěvníků stadionu a podtrhuje důležitost technické i uživatelské prevence v prostředí hromadných akcí.

Tabulka 13: Parametry Výsledky druhého měření stadion AC Sparta

Parametr měření	Hodnota
Datum	9. 4. 2025
Čas měření	19:00 – 21:30 (150 minut)
Počet připojených zařízení za dobu měření	10
Průměrný interval připojení	Každých 15 minut

Zdroj: vlastní zpracování

Tabulka 14: Výsledky druhého měření stadion AC Sparta

Síťová adresa zařízení	Automatické připojování
aa:af:89:de:19:31	ano
3a:36:29:8d:f4:79	ne
4a:45:cc:ea:f1:01	ano
fc:02:96:f3:b0:ce	ano
7e:36:6b:70:2f:af	ne
c0:b5:cd:cc:44:a2	ne
6e:b4:40:cb:3a:36	ano
e6:02:bc:88:64:9d	ne
76:3a:b3:fe:b5:b4	ne
ba:d2:74:21:4e:60	ano

Zdroj: vlastní zpracování

Restaurace společnosti McDonald´s ČR spol. s.r.o. Kralupy nad Vltavou

Restaurace byla v době měření středně zaplněná, nacházelo se v ní přibližně 30 hostů, převážně staršího věku. Parametry měření jsou zobrazeny v Tabulka 15. Během měření bylo aktivováno testovací zařízení vysílající nezabezpečenou Wi-Fi síť, která imitovala název běžně provozované sítě této franšízy. I přes poměrně rušné prostředí se k této falešné síti nikdo nepřipojil.

Tento výsledek lze interpretovat jako poměrně příznivý z pohledu kybernetické bezpečnosti. Naznačuje, že buď většina přítomných hostů žádnou síť aktivně nevyhledávala, nebo měli zařízení správně nakonfigurovaná, případně, že starší uživatelé využívají veřejné Wi-Fi méně často.

Tabulka 15: Parametry měření McDonald Kralupy nad Vltavou

Parametr měření	Hodnota
Datum	26. 4. 2025
Čas měření	12:00 – 12:30 (30 minut)
Počet připojených zařízení za dobu měření	0
Průměrný interval připojení	X

Zdroj: vlastní zpracování

Fotbalové hřiště TJ Sokol Tišice, zápas 26. 4. 2024

Měření proběhlo v areálu fotbalového hřiště TJ Sokol Tišice, kde zároveň funguje veřejně přístupná Hospoda na hřišti, a to během konání společenské akce, což se projevilo na vyšší koncentraci osob. Tabulka 16 prezentuje parametry tohoto měření. V průběhu měření se v prostoru pohybovalo odhadem 100 až 150 návštěvníků. Testovací zařízení vysílalo falešnou nezabezpečenou Wi-Fi síť, která mohla být vnímána jako případná síť provozovaná restaurací nebo areálem.

Přestože se v lokalitě vyskytovalo značné množství lidí a šlo o prostředí, kde je běžné používání mobilních telefonů (např. k focení, sdílení obsahu nebo komunikaci), pouze jedno zařízení se připojilo k falešné síti, a to navíc vědomě, bez aktivního automatického připojení. Tento výsledek může naznačovat, že většina přítomných zařízení byla buď správně zabezpečena, nebo že uživatelé raději využívali mobilní data, případně se k Wi-Fi vůbec nepřipojovali. Roli mohl sehrát i fakt, že většina návštěvníků tento prostor pravidelně navštěvuje a jsou seznámeni s faktem o nepřítomnosti oficiální bezdrátové sítě. I tak je třeba vnímat, že i jediné připojení k neznámé síti může představovat potenciální riziko, a to zejména v prostředí, kde si uživatelé nejsou jisti, která síť je oficiálně provozována. Výsledek měření, zobrazený v Tabulka 17, tedy poukazuje na relativně dobrou úroveň zabezpečení v praxi, ale zároveň připomíná, že i při vyšší účasti veřejnosti může podvržená síť nalézt své oběti.

Tabulka 16: Parametry měření na hřišti TJ Sokol Tišice

Parametr měření	Hodnota
Datum	26. 4. 2025
Čas měření	17:00 – 20:00 (180 minut)
Počet připojených zařízení za dobu měření	1
Průměrný interval připojení	Každých 180 minut

Zdroj: vlastní zpracování

Tabulka 17: Výsledky měření na hřišti TJ Sokol Tišice

Síťová adresa zařízení	Automatické připojování
04:4a:6c:7f:de:56	ne

Zdroj: vlastní zpracování

Domov pro seniory a Domov se zvláštním režimem „4“ Sokolov

Měření bylo provedeno v prostředí Domu pro seniory Čtyřka Sokolov s parametry v Tabulka 18, konkrétně ve společenské místnosti, kde se v době měření nacházelo přibližně 20 osob, z toho část tvořili senioři a část jejich rodinní příslušníci. Objekt disponuje vlastní zabezpečenou Wi-Fi sítí, která je určena pro obyvatele i návštěvy. Během hodinového měření byla vysílána falešná nezabezpečená Wi-Fi síť, jež mohla být vnímána jako alternativní nebo veřejná síť dostupná v prostorách zařízení. Přesto však nedošlo k žádnému připojení, a to ani automatickému, ani vědomému.

Tento výsledek lze hodnotit pozitivně, neboť naznačuje buď nízkou míru potřeby připojení v daném čase, nebo zodpovědný přístup přítomných osob k výběru důvěryhodných sítí. U seniorů je zároveň pravděpodobné, že mají své zařízení méně často u sebe nebo je používají omezeně. Zároveň lze ocenit, že ani žádný doprovod, často mladší osoby, se k falešné síti nepřipojil, což naznačuje buď preferenci mobilních dat, nebo opatrnost při výběru připojení. Měření tak doplnilo poznatky z jiných lokalit o specifické prostředí, kde riziko připojení k neznámé síti zůstává minimální, především díky omezenému používání zařízení i přítomnosti oficiální zabezpečené sítě.

Tabulka 18: Parametry měření 4 Sokolov

Parametr měření	Hodnota
Datum	11. 5. 2025
Čas měření	14:30 – 15:30 (60 minut)
Počet připojených zařízení za dobu měření	0
Průměrný interval připojení	X

Zdroj: vlastní zpracování

Kinosál společnosti Cinema City Czech s.r.o.

Měření bylo provedeno v kinosále společnosti Cinema City během dopoledního promítání dětského filmu s parametry, které jsou zobrazeny v Tabulka 19. V prostoru nebyla dostupná žádná oficiální Wi-Fi síť provozovaná společností Cinema City a testovací zařízení vysílající falešnou nezabezpečenou Wi-Fi síť zde fungovalo po celou dobu projekce. Během měření se k síti nepřipojilo žádné zařízení. V sále bylo přítomno přibližně 30 dospělých osob, převážně v roli doprovodu dětí, pro které byl film určen.

Tuto nulovou aktivitu lze s největší pravděpodobností přičíst tomu, že návštěvníci byli plně soustředěni na sledování filmu, případně se řídili pravidly kinosálu o omezení používání mobilních zařízení během promítání. Navíc dětské filmy obecně vyžadují aktivní přítomnost rodičů nebo doprovodu, což může omezovat prostor pro jiné aktivity, včetně snahy o připojení k Wi-Fi.

Tabulka 19: Parametry měření kinosál Cinema City

Parametr měření	Hodnota
Datum	18. 5. 2025
Čas měření	10:00 – 11:40 (100 minut)
Počet připojených zařízení za dobu měření	0
Průměrný interval připojení	X

Zdroj: vlastní zpracování

Obchodní centrum Letňany, food court

Měření proběhlo ve food courtu obchodního centra Letňany. Jednalo se o typicky rušné prostředí, kde se v době měření nacházelo přibližně 50 osob, převážně návštěvníků využívajících gastronomické služby obchodního centra. V prostoru byla dostupná oficiální Wi-Fi síť provozovaná samotným obchodním centrem, což mohlo ovlivnit rozhodování návštěvníků při výběru připojení. Během aktivního vysílání falešné nezabezpečené sítě byly zaznamenány čtyři připojení ze strany mobilních zařízení.

Pozitivním zjištěním je skutečnost, že žádné ze zařízení se k síti nepřipojilo automaticky, ve všech případech šlo o vědomé připojení uživatele. To ukazuje na skutečnost, že uživatelé si síť aktivně vybrali na základě jejího názvu, který pravděpodobně působil důvěryhodně díky podobnosti s názvem oficiální Wi-Fi sítě provozované obchodním centrem. Výsledky tak potvrzují, že i v prostředí s dostupnou legitimní sítí může podvržená síť nalézt své cíle, pokud není uživatel dostatečně obezřetný. Parametry a výsledky měření jsou zobrazeny v Tabulka 20 a Tabulka 21.

Tabulka 20: Parametry měření Food court OC Letňany

Parametr měření	Hodnota
Datum	18. 5. 2025
Čas měření	13:10 – 13:40 (30 minut)
Počet připojených zařízení za dobu měření	4
Průměrný interval připojení	Každých 7 minut a 30 sekund

Zdroj: vlastní zpracování

Tabulka 21: Výsledky měření Food court OC Letňany

Síťová adresa zařízení	Automatické připojování
9e:4b:77:f6:d8:dc	ne
96:cd:ba:24:ee:a4	ne
ea:f5:e1:69:f7:80	ne
22:3b:9c:b1:81:e7	ne

Zdroj: vlastní zpracování

Fotbalové hřiště TJ Sokol Tišice

Měření proběhlo v areálu fotbalového hřiště TJ Sokol Tišice v průběhu zápasu A-týmu s parametry v Tabulka 22, kdy se na místě nacházelo přibližně 70 osob různého věku, včetně dětí, dospělých i seniorů. Součástí areálu je také hospoda, která však neprovozuje žádnou oficiální Wi-Fi síť, což mohlo vést k vyšší náchylnosti návštěvníků k připojení na neznámé sítě v případě potřeby internetového připojení. Testovací zařízení po dobu měření vysílalo falešnou, nezabezpečenou síť, která mohla působit jako legitimní přístupový bod.

V průběhu testu bylo zaznamenáno jedno připojení k falešné síti, přičemž toto připojení proběhlo prvně manuálně a následně automaticky, tedy po zákazu zařízení a jeho následném povolení. Následné automatické připojení proběhlo bez vědomí uživatele. Tento výsledek, zobrazený v Tabulka 23, je varovným signálem, neboť ukazuje, že některá zařízení jsou stále nastavena tak, aby se připojovala k otevřeným sítím bez ověření jejich důvěryhodnosti. Toto měření dokazuje, že i v prostředí bez oficiální Wi-Fi, jako je tomu v tomto případě, může mít podvržená síť vysokou šanci na úspěch.

Tabulka 22: Parametry druhého měření na hřišti TJ Sokol Tišice

Parametr měření	Hodnota
Datum	18. 5. 2025
Čas měření	17:00 – 19:00 (120 minut)
Počet připojených zařízení za dobu měření	1
Průměrný interval připojení	Každých 120 minut

Zdroj: vlastní zpracování

Tabulka 23: Výsledky druhého měření na hřišti TJ Sokol Tišice

Síťová adresa zařízení	Automatické připojování
a2:a1:ca:63:4b:5c	ano

Zdroj: vlastní zpracování

Vlak ICC společnosti PKP Intercity S.A. na trase z Bydgoště do Vřeclavi

Měření probíhalo ve vlaku na trase Bydhošť – Praha na území Polska s parametry z Tabulka 24. Testovací zařízení bylo umístěno ve voze, který byl téměř zcela obsazený, přičemž většina

cestujících aktivně používala svá zařízení, včetně mobilních telefonů, notebooků a tabletů. Vlaková souprava byla vybavena oficiální Wi-Fi sítí provozovanou dopravcem, která vyžadovala přesměrování na webovou stránku pro přihlášení k připojení k internetu. Po celou dobu měření bylo aktivní vysílání falešné nezabezpečené sítě, přesto však nedošlo k žádnému připojení, ani automatickému, ani ručnímu.

Tento výsledek může být ovlivněn několika faktory. Jedním z nich je právě existence oficiální palubní Wi-Fi, která mohla pokrýt potřeby většiny uživatelů, ale zároveň může být důležité zohlednit i cenovou dostupnost mobilních datových tarifů v Polsku. Vzhledem k nižším cenám mobilního připojení v této zemi může být běžné, že uživatelé raději využívají vlastní data a veřejné Wi-Fi sítě příliš nevyhledávají. Tento aspekt je dále zohledněn v další části této práce. Přestože falešná síť nenalezla své „oběti“, měření potvrdilo vysokou míru využívání technologií na cestách, a tedy potenciální bezpečnostní rizika v jiných kontextech, kde připojení k neznámým sítím může být lákavější.

Tabulka 24: Parametry měření vlak ICC

Parametr měření	Hodnota
Datum	6. 6. 2025
Čas měření	8:30 – 9:00 (30minut)
Počet připojených zařízení za dobu měření	0
Průměrný interval připojení	X

Zdroj: vlastní zpracování

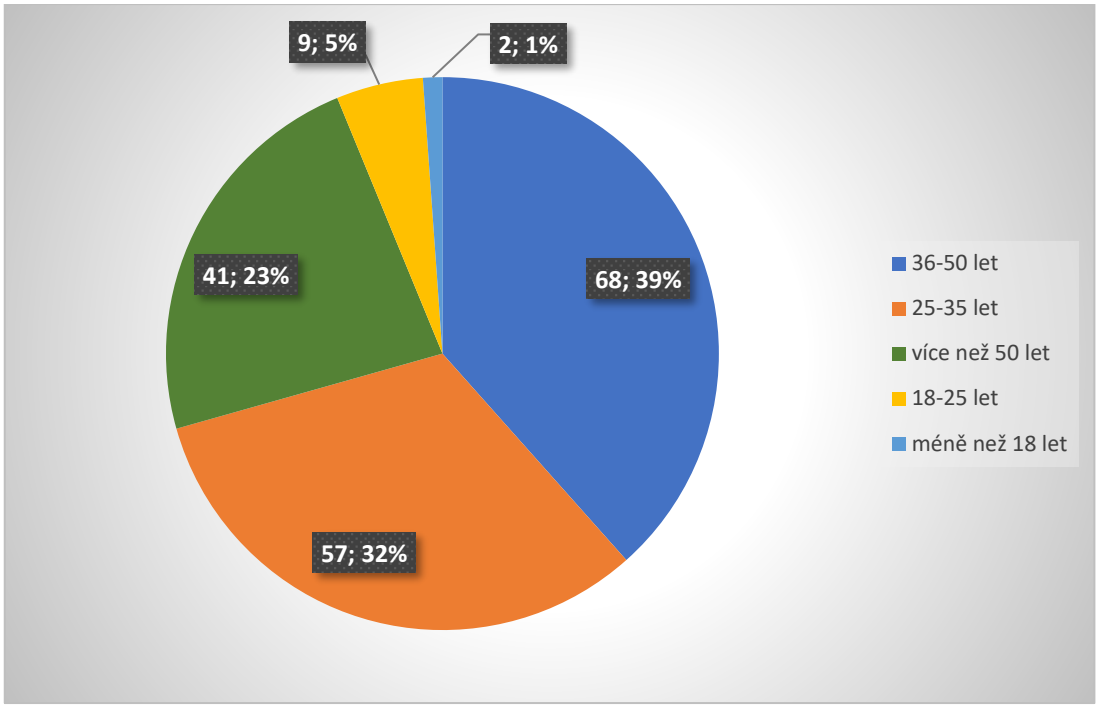
4.2 Výsledky průzkumu o vzdělanosti uživatelů

Cílem dotazníkového průzkumu bylo zjistit, jaké mají respondenti bezpečnostní návyky, jaká je jejich úroveň znalostí v oblasti ochrany dat, o rizicích spojených s používáním veřejných Wi-Fi sítí a jaká opatření při používání bezdrátových sítí uplatňují. Výsledky šetření doplňují poznatky získané z praktického experimentu a společně poskytují ucelený pohled na to, jak jsou uživatelé připraveni čelit hrozbám v prostředí veřejných bezdrátových sítí a jak moc by tedy pomohla edukace v této oblasti zvýšit jejich schopnost se ještě více bránit.

V období od 11. 3. 2025 do 30. 4. 2025 bylo získáno 177 responsí, přičemž návratnost dotazníků byla 75,7 %. To je, pro účely této práce, relevantní soubor respondentů.

Otázka č.1: Jaký je Váš věk?

První otázka byla jedna z demografických, a to konkrétně otázka na věk respondenta. Výsledky nám ukazuje Obrázek 3: Graf odpovědí na otázku č.1



Obrázek 3: Graf odpovědí na otázku č.1

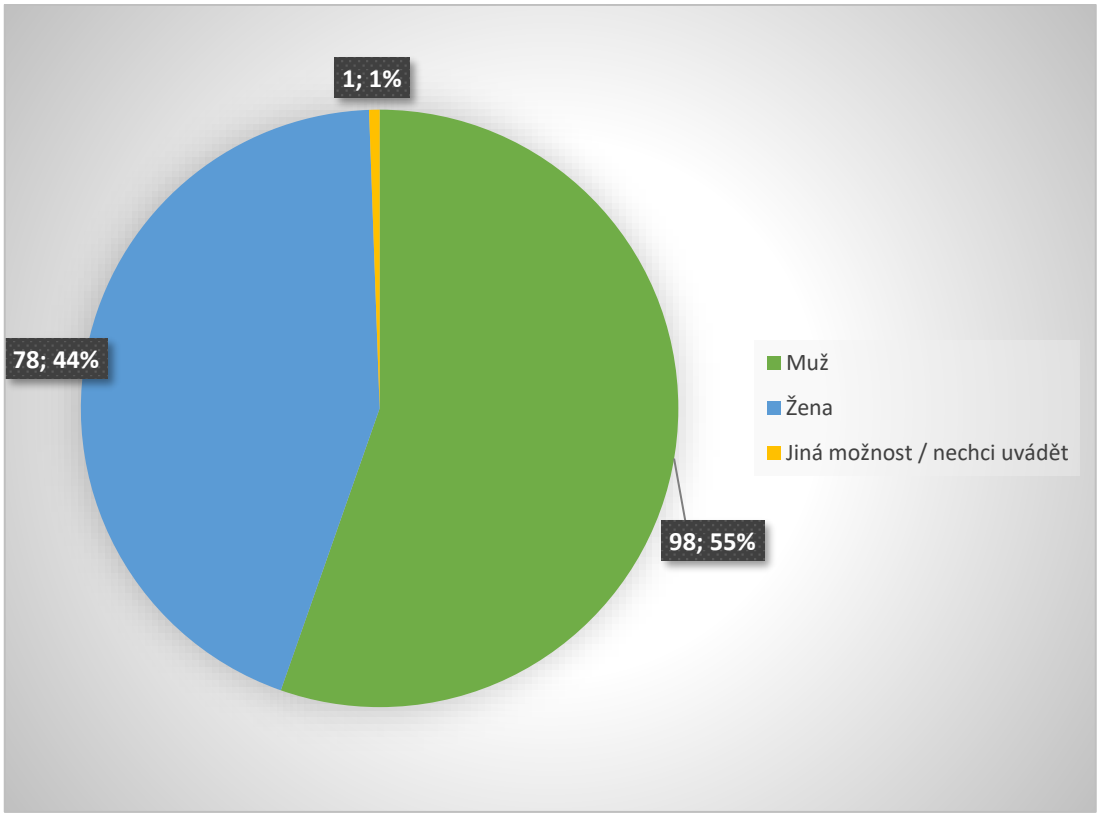
Zdroj: vlastní zpracování

Na základě výsledků dotazníkového šetření lze říct, že největší část respondentů tvořili jedinci ve věkové kategorii 36–50 let, kteří představovali více než třetinu všech odpovídajících (68 osob). Následuje skupina 26–35 let s 57 respondenty, což značí, že významná část účastníků dotazníku patří do produktivního věku, kdy mají tito uživatelé vysokou míru zapojení do technologií a pravděpodobně i pravidelný přístup k bezdrátovým sítím v zaměstnání i doma.

Skupiny více než 50 let a 18–25 let byly zastoupeny méně výrazně (41, respektive 9 respondentů), což může odrážet nižší míru technologického zapojení nebo menší ochotu zapojit se do výzkumu v těchto věkových skupinách. Nejnižší zastoupení měla kategorie méně než 18 let, kde odpověděli pouze 2 respondenti. Celkově složení vzorku naznačuje, že většina účastníků spadá do věkového rozmezí, které je technologicky aktivní a má reálnou zkušenost s využíváním Wi-Fi sítí, což zvyšuje relevanci získaných dat pro účely této práce.

Otázka č. 2: Jaké je Vaše pohlaví?

Druhá otázka řešila pohlaví respondenta. Výsledky jsou zobrazeny na Obrázek 4.



Obrázek 4: Graf odpovědí na otázku č.2

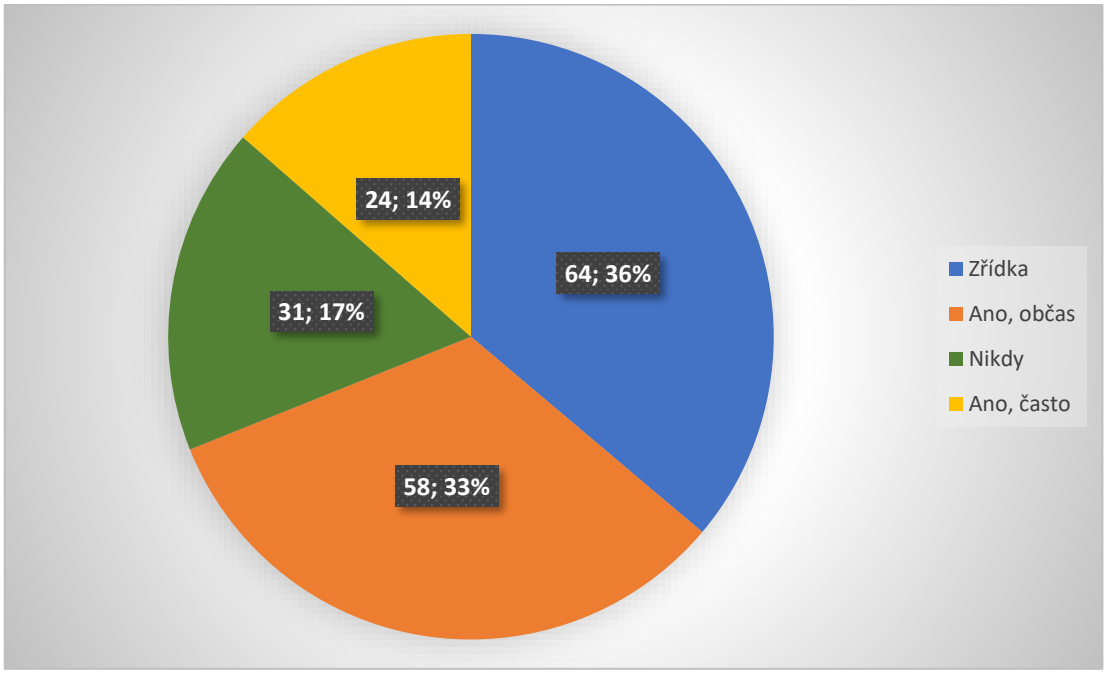
Zdroj: vlastní zpracování

Z hlediska pohlaví byl v dotazníkovém šetření zaznamenán mírně vyšší počet mužských respondentů, celkem 98 osob, zatímco žen se zúčastnilo 78. Pouze jeden respondent zvolil možnost „jiná možnost / nechci uvádět“, což ukazuje na minimální zastoupení mimo binární klasifikaci. Výsledky tedy ukazují, že se na průzkumu podílel poměrně vyrovnaný vzorek mužů a žen, s mírnou převahou mužů.

Toto rozložení odpovědí ukazuje, že průzkum oslovil dostatečně širokou škálu respondentů obou pohlaví, což přispívá k vyváženému pohledu na danou problematiku. Mírná převaha mužů může být v souladu s tím, že muži bývají častěji technicky zaměření a mají větší zájem o témata kybernetické bezpečnosti, což může ovlivnit i jejich ochotu zapojit se do výzkumu zaměřeného na tuto oblast. Na druhé straně vysoký počet odpovědí od žen naznačuje, že povědomí o bezpečnosti bezdrátových sítí není doménou pouze jedné skupiny, ale je důležitým tématem napříč pohlavími. Lze tak uzavřít, že odpovědi v této otázce podporují celkovou relevanci a reprezentativnost dat získaných z dotazníkového šetření.

Otázka č. 3: Připojujete se na veřejných místech (např. kavárny, nádraží, letiště) k bezdrátovým Wi-Fi sítím?

Třetí otázka už začíná řešit samotnou problematiku tohoto dotazníku a zjišťuje, jestli se respondent připojuje k Wi-Fi sítím na veřejně dostupných místech. Výsledky jsou zobrazeny na Obrázek 5.



Obrázek 5: Graf odpovědí na otázku č.3

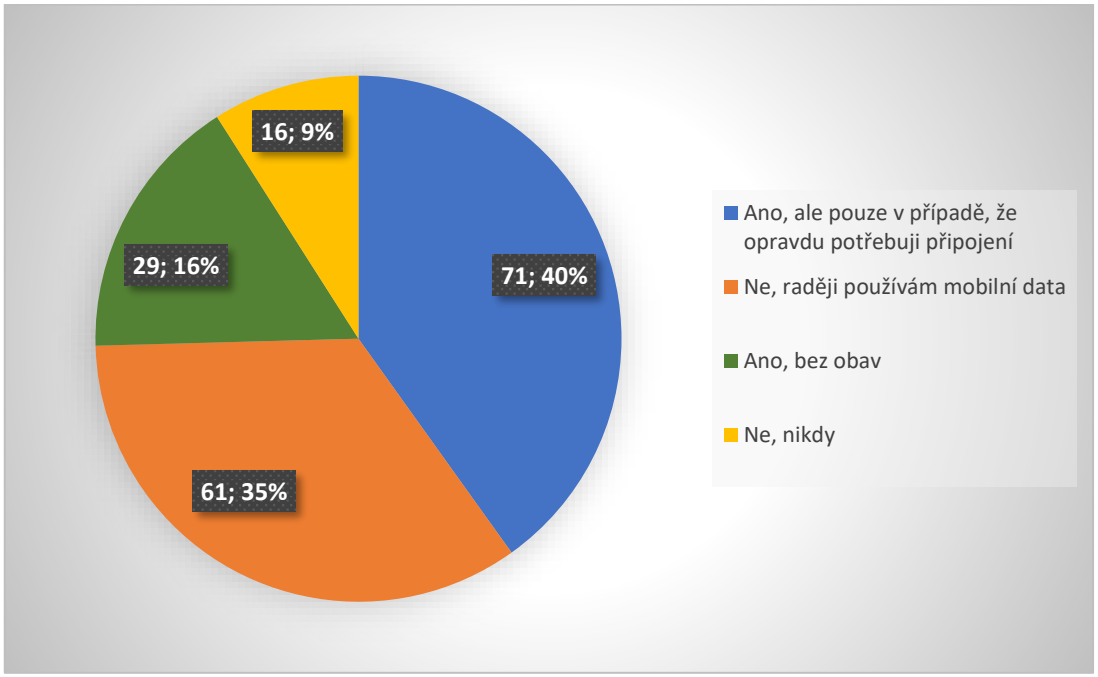
Zdroj: vlastní zpracování

Z výsledků dotazníkového šetření vyplývá, že většina respondentů se k Wi-Fi sítím na veřejně dostupných místech připojuje pouze zřídka, 64 odpovědí, nebo občas, 58 odpovědí. To značí určitou míru obezřetnosti vůči veřejným sítím, která může být způsobena buď povědomím o bezpečnostních rizicích, nebo preferencí mobilních dat. Naopak 31 respondentů uvedlo, že se k veřejným Wi-Fi nikdy nepřipojují, což lze považovat za bezpečnostně nejzodpovědnější přístup. 24 osob pak deklarovalo, že se k těmto sítím připojují často, což představuje nejzranitelnější skupinu uživatelů, pokud zároveň nevyužívají dodatečná ochranná opatření, jako je například VPN.

Z těchto údajů lze vyvodit, že značná část uživatelů si je alespoň částečně vědoma rizik spojených s připojením k veřejným sítím a přistupuje k nim s určitou mírou opatrnosti. Znepokojující však zůstává skutečnost, že přibližně jeden z deseti respondentů se k těmto sítím připojuje pravidelně, což vytváří potenciální prostor pro kybernetické útoky, jako jsou MITM útoky či odposlech přenosu. Tyto výsledky podtrhují důležitost vzdělávání uživatelů a šíření osvěty o bezpečnostních návycích při používání bezdrátových sítí na veřejných místech.

Otázka č. 4: Pokud jste na veřejném místě a k dispozici je otevřená (nezabezpečená) Wi-Fi síť, připojíte se k ní?

Tato otázka už řeší přímo problematiku nezabezpečených Wi-Fi sítí, a to konkrétně jestli se k ní respondent připojí, když nějakou takovou má k dispozici na veřejně dostupném místě. Výsledky jsou prezentovány na Obrázek 6.



Obrázek 6: Graf odpovědí na otázku č.4

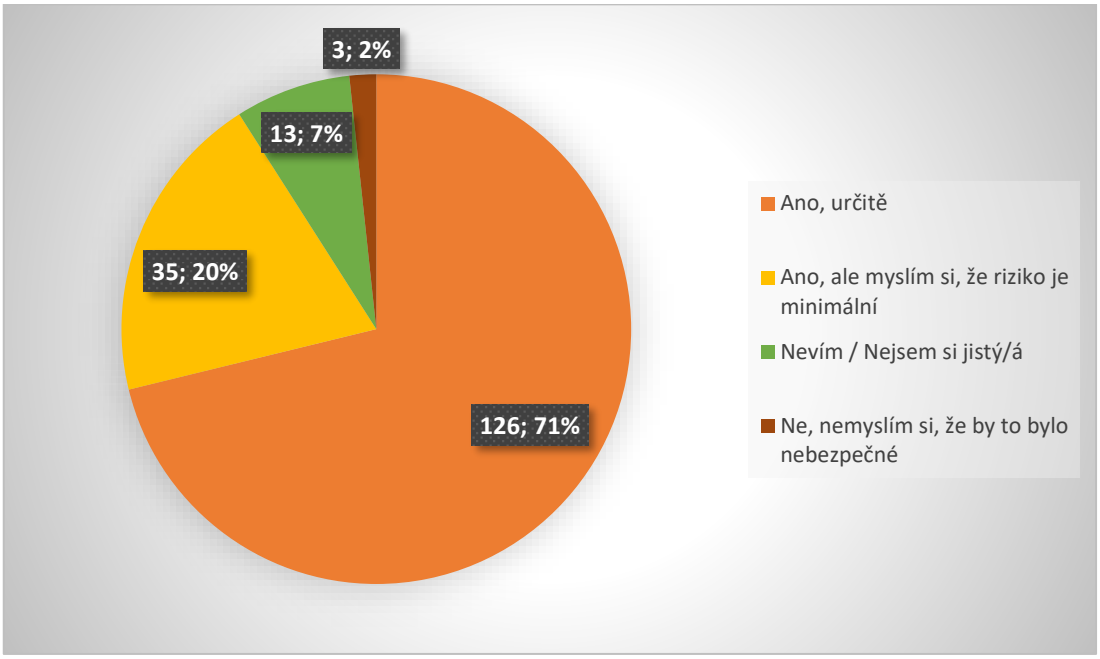
Zdroj: vlastní zpracování

Výsledky ukazují, že největší skupina respondentů, 71 osob, se k nezabezpečeným Wi-Fi sítím připojuje pouze v případě nutnosti, což naznačuje určitou míru obezřetnosti. 61 respondentů uvedlo, že raději využívají mobilní data, čímž se zcela vyhýbají rizikům spojeným s nezabezpečeným připojením. Tento přístup lze označit za výrazně bezpečnější, neboť eliminuje hrozby, jako jsou odposlech dat nebo připojení ke škodlivému přístupovému bodu.

Na druhou stranu 29 osob se připojuje k těmto sítím bez obav, což poukazuje na nízké povědomí o potenciálních rizicích nebo jejich podcenění. Alarmující je i to, že pouze 16 respondentů se nikdy k nezabezpečené síti nepřipojuje. Tyto výsledky potvrzují, že přestože část uživatelů jedná zodpovědně, stále existuje nezanedbatelná skupina, která se vystavuje vysokému bezpečnostnímu riziku.

Otázka č. 5: Věříte, že připojení k nezabezpečené Wi-Fi síti může představovat bezpečnostní riziko?

Otázka se respondenta ptá na to, jestli si uvědomuje, že nezabezpečená Wi-Fi síť může představovat riziko. Obrázek 7 nám prezentuje na získaná data.



Obrázek 7: Graf odpovědí na otázku č.5

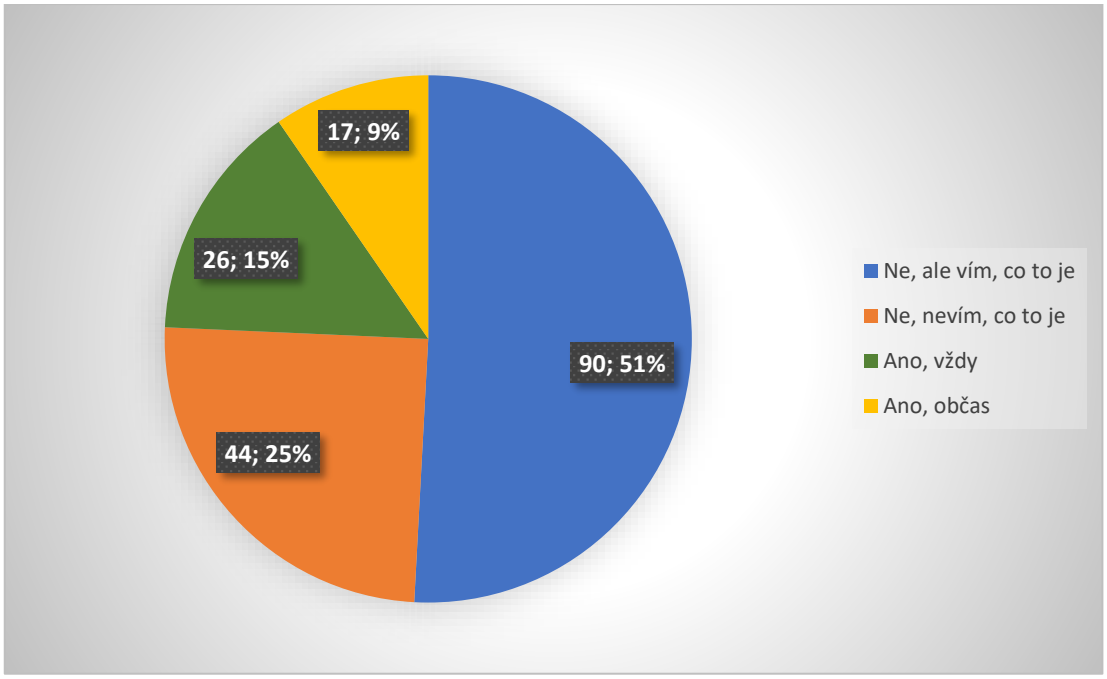
Zdroj: vlastní zpracování

Většina respondentů, 126 osob, uvedla, že si určitě uvědomují rizika spojená s připojováním k nezabezpečeným Wi-Fi sítím. To je pozitivní zjištění, které naznačuje, že základní povědomí o kybernetických hrozbách je mezi uživateli poměrně rozšířené. Dalších 35 respondentů sice riziko připouští, ale domnívají se, že je minimální, což ukazuje na částečné podcenění situace. Tito uživatelé sice mají obecnou představu o existenci hrozeb, ale pravděpodobně nemají dostatek informací o tom, jak snadno může být taková síť zneužita.

Naopak 13 respondentů uvedlo, že si nejsou jisti, a 3 osoby vůbec rizika nevnímají, což představuje potenciálně zranitelnou skupinu uživatelů. Přestože jejich podíl není významný, ukazuje se, že určité procento uživatelů stále postrádá dostatečné bezpečnostní povědomí. Celkově však výsledky této otázky potvrzují, že většina uživatelů chápe základní rizika spojená s nezabezpečeným připojením, což je důležitý předpoklad pro budování bezpečnějšího chování v oblasti bezdrátových sítí.

Otázka č. 6: Používáte při připojení k veřejným Wi-Fi sítím VPN?

Výsledky řešící otázku používání VPN při připojení k veřejným Wi-Fi sítím jsou zobrazeny na Obrázek 8.



Obrázek 8: Graf odpovědí na otázku č.6

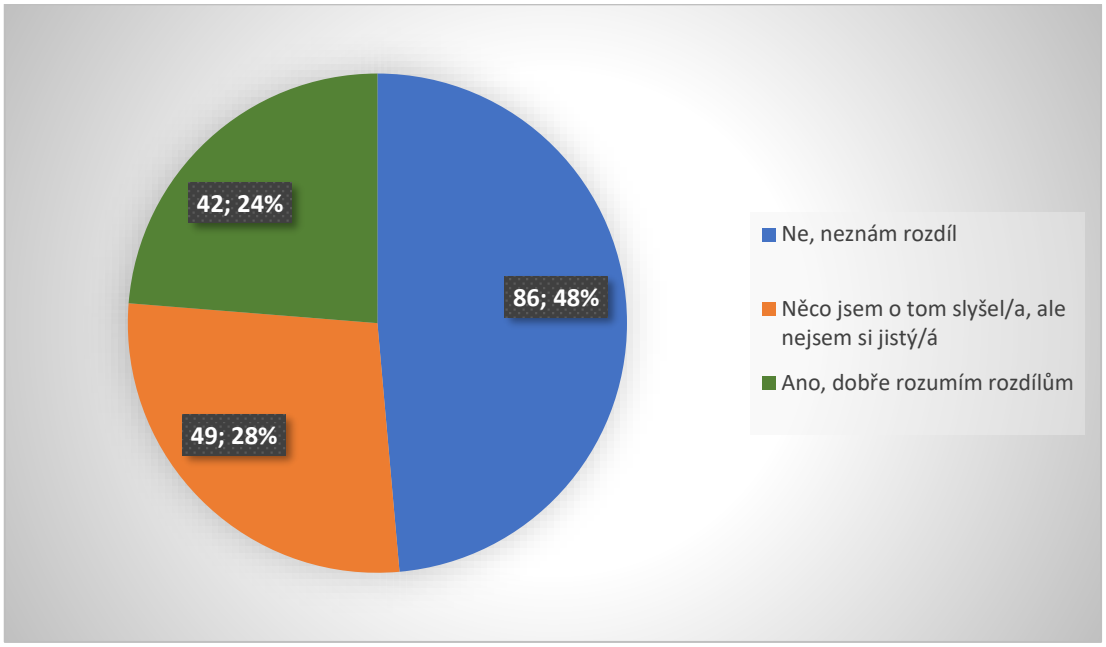
Zdroj: vlastní zpracování

Výsledky ukazují, že pouze menšina respondentů VPN aktivně využívá, 26 osob uvedlo, že ji používá vždy, a dalších 17 ji využívá občas. To dohromady představuje jen přibližně 24 % všech dotazovaných, což je poměrně nízké číslo vzhledem k tomu, že VPN je jedním z nejúčinnějších nástrojů pro ochranu soukromí a dat při používání veřejných Wi-Fi sítí. Tento výsledek poukazuje na prostor ke zlepšení v oblasti praktického uplatňování bezpečnostních opatření v reálném chování uživatelů.

Zajímavým zjištěním je, že většina respondentů, 90 osob, VPN nepoužívá, ale ví, o co se jedná, což naznačuje určitou úroveň informovanosti, avšak zároveň i nezájem nebo podcenění rizik. Ještě znepokojivější je, že 44 osob uvedlo, že o VPN vůbec neví, tedy přibližně pětina všech dotazovaných. To svědčí o tom, že osvěta v oblasti ochrany soukromí při připojování k veřejným sítím stále není dostatečná. Výsledky tak potvrzují potřebu zvýšit povědomí o výhodách VPN a motivovat uživatele k jejímu aktivnímu využívání.

Otázka č. 7: Znáte rozdíl mezi zabezpečením Wi-Fi pomocí WEP, WPA a WPA2/WPA3?

Další z technických otázek, která řeší znalosti mezi jednotlivými standardy zabezpečení WEP, WPA a následnými generacemi. Výsledky nám prezentuje Obrázek 9.



Obrázek 9: Graf odpovědí na otázku č.7

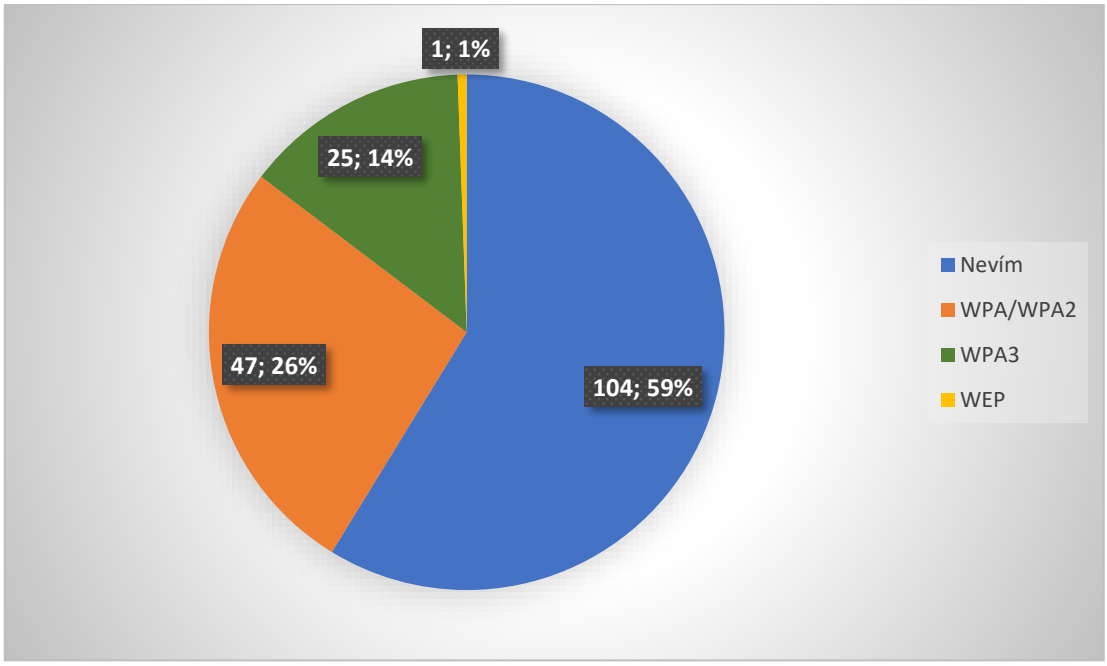
Zdroj: vlastní zpracování

Výsledky této otázky ukazují, že většina respondentů má velmi omezené znalosti o rozdílech mezi bezpečnostními standardy WEP, WPA, WPA2 a WPA3. Konkrétně 86 osob uvedlo, že rozdíly vůbec neznají, a dalších 49 respondentů si není jistých, přestože o těchto pojmech alespoň slyšeli. To znamená, že přibližně tři čtvrtiny dotazovaných nemají dostatečné povědomí o tom, jaké zabezpečení využívají a jak bezpečné je jejich připojení.

Pouze 42 respondentů uvedlo, že rozdílům mezi jednotlivými standardy dobře rozumí, což představuje necelou čtvrtinu vzorku. Tento výsledek je klíčový, protože volba bezpečnostního protokolu má přímý vliv na odolnost bezdrátové sítě vůči útokům. Nízká míra znalostí o základních bezpečnostních technologiích potvrzuje potřebu větší osvěty mezi uživateli, zejména v souvislosti s přechodem na modernější a bezpečnější standardy, jako je WPA3. Informovanost v této oblasti je zásadní pro to, aby uživatelé mohli činit kvalifikovaná rozhodnutí při nastavování svých sítí i při připojování k cizím.

Otázka č. 8: Jaký bezpečnostní protokol používá vaše domácí Wi-Fi síť?

Výsledky otázky ohledně použití konkrétního zabezpečení u domácích sítí respondentů jsou uvedeny na Obrázek 10.



Obrázek 10: Graf odpovědí na otázku č.8

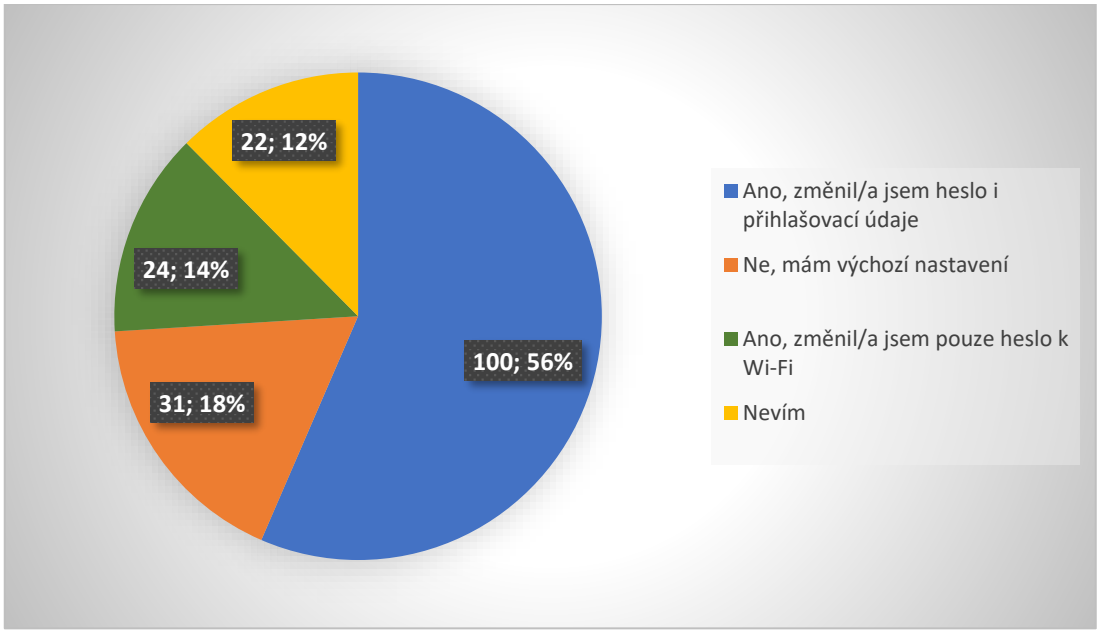
Zdroj: vlastní zpracování

Výsledky této otázky odhalují, že značná část respondentů (104 osob) neví, jaké zabezpečení používá jejich domácí Wi-Fi síť, což představuje více než polovinu dotazovaných. Tato skutečnost ukazuje na nízkou míru technického povědomí mezi běžnými uživateli a zároveň poukazuje na potenciální riziko, že domácí sítě nejsou dostatečně chráněny, případně používají zastaralé nebo nebezpečné metody zabezpečení bez vědomí uživatelů.

Pozitivní je, že 47 respondentů uvedlo použití WPA nebo WPA2, což jsou stále poměrně bezpečné standardy, a 25 osob již využívá WPA3, tedy nejnovější a nejbezpečnější šifrovací protokol. Alarmující je naopak zjištění, že jeden respondent stále používá WEP, který je považován za zcela nevyhovující a snadno prolomitelný. Celkově výsledky ukazují, že i když část uživatelů moderní zabezpečení používá, je zde silná potřeba zvyšovat informovanost veřejnosti o významu zabezpečení domácích sítí a podporovat jejich aktivní správu.

Otázka č. 9: Má vaše domácí Wi-Fi síť změněné výchozí přihlašovací údaje k routeru?

Tato otázka řešila zabezpečení domácích Wi-Fi routerů respondentů. Výsledky jsou uvedeny na Obrázek 11.



Obrázek 11: Graf odpovědí na otázku č.9

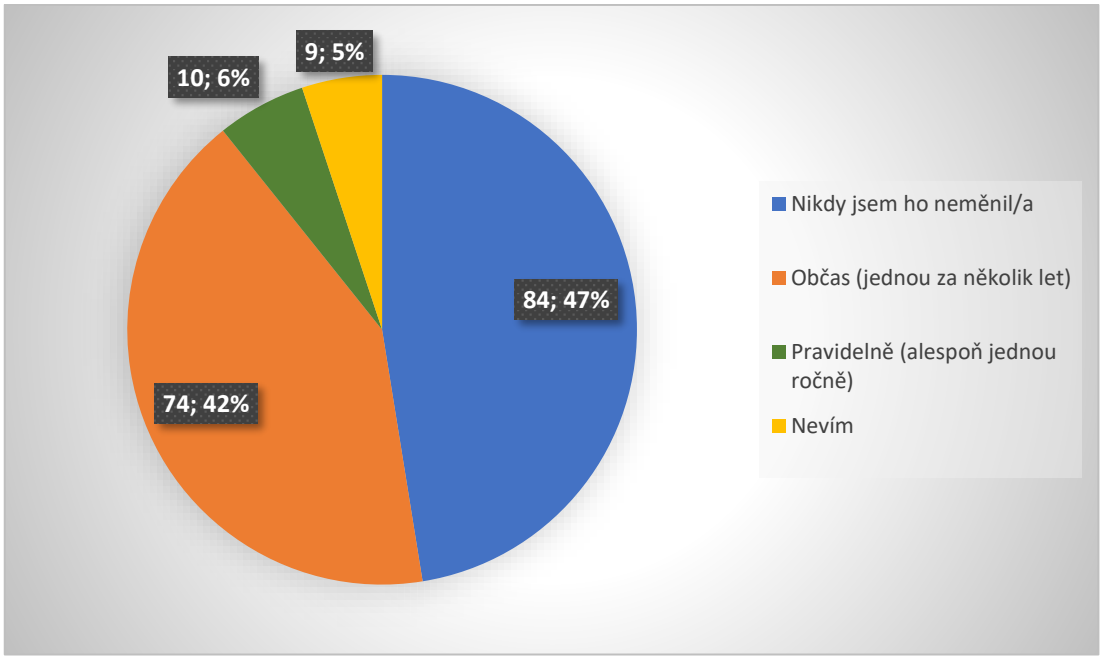
Zdroj: vlastní zpracování

Výsledky této otázky ukazují, že většina respondentů, 100 osob, přistoupila k odpovědné správě své domácí sítě a změnila nejen heslo k Wi-Fi, ale i přihlašovací údaje k administračnímu rozhraní routeru. To je pozitivní zjištění, neboť výchozí přihlašovací údaje bývají snadno dohledatelné a představují častý cíl útoků. Tento krok výrazně snižuje riziko neautorizovaného přístupu a ukazuje na dobrou míru bezpečnostního povědomí této skupiny uživatelů.

Naopak 31 respondentů uvedlo, že ponechali výchozí nastavení, což znamená, že jejich zařízení může být snadno zneužitelné, například prostřednictvím útoků na webové rozhraní routeru. Dalších 24 osob změnilo pouze heslo k Wi-Fi, ale administraci ponechali v původním stavu, což poskytuje částečnou ochranu, avšak stále ponechává otevřený prostor k potencionálnímu útoku. 22 respondentů neví, zda prováděli jakékoli změny, což ukazuje na nízkou úroveň zapojení do správy síťového zabezpečení. Tyto výsledky podtrhují důležitost osvěty o správné konfiguraci síťových zařízení a upozorňují na běžné chyby, které mohou oslabit celkovou bezpečnost domácího prostředí.

Otázka č. 10: Jak často měníte heslo k domácí Wi-Fi síti?

Výsledky na Obrázek 12 ukazují četnost změny hesla domácích Wi-Fi sítí u respondentů.



Obrázek 12: Graf odpovědí na otázku č.10

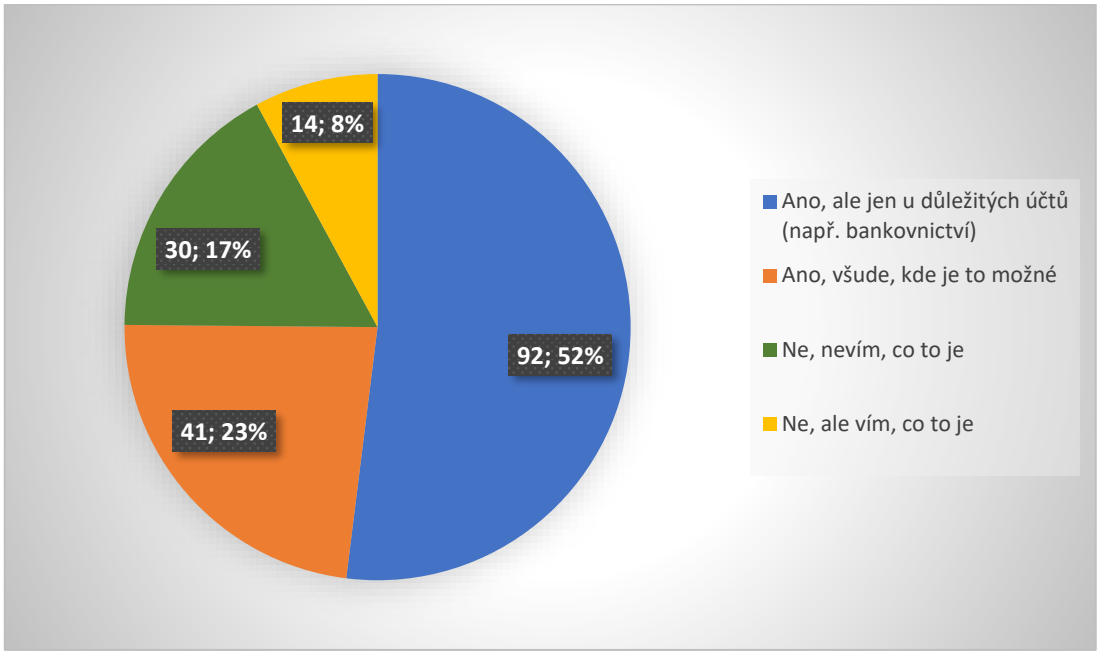
Zdroj: vlastní zpracování

Výsledky této otázky ukazují, že většina respondentů heslo ke své domácí Wi-Fi buď vůbec nemění, nebo pouze velmi zřídka. Konkrétně 84 osob uvedlo, že heslo nikdy neměnili, což představuje více než třetinu všech odpovídajících. Dalších 74 respondentů uvedlo, že heslo mění pouze občas, přibližně jednou za několik let, což je z hlediska kybernetické bezpečnosti stále velmi nízká frekvence. Tyto údaje naznačují, že uživatelé často přistupují ke správě své sítě pasivně a spoléhají na původní konfiguraci bez dalšího přehodnocení bezpečnosti.

Naopak pouze 10 osob mění heslo pravidelně, alespoň jednou ročně, což je sice bezpečnostně ideální přístup, ale je zcela výjimečný. 9 respondentů si navíc nebylo jistých, zda heslo vůbec měnili, což opět ukazuje na nedostatečné zapojení do správy vlastní sítě. Celkově tato data potvrzují, že frekventovaná obměna přístupových údajů k Wi-Fi síti není mezi uživateli běžnou praxí, ačkoli by mohla významně zvýšit ochranu před neoprávněným přístupem, zejména v prostředí, kde hrozí únik nebo zneužití hesla.

Otázka č. 11: Používáte dvoufaktorové ověřování (2FA) při přihlašování do online služeb?

Tato otázka řešila používání dvoufaktorového ověřování uživatelů pro přístup k online službám. Výsledky jsou zobrazeny na Obrázek 13.



Obrázek 13: Graf odpovědí na otázku č.11

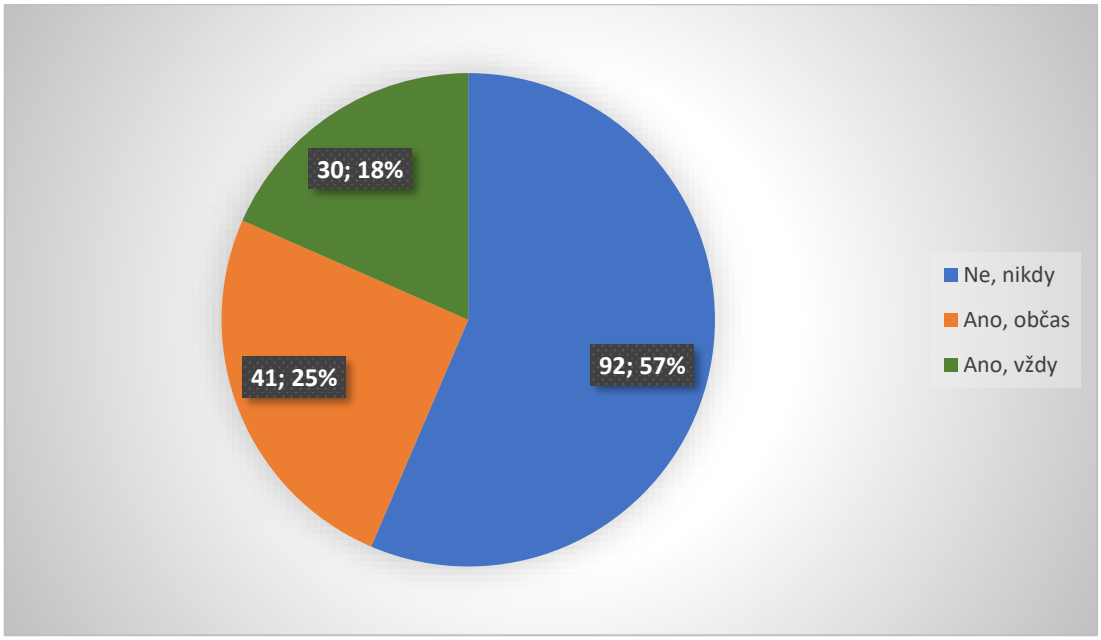
Zdroj: vlastní zpracování

Výsledky ukazují, že největší část respondentů, 92 osob, používá dvoufaktorové ověřování (2FA) alespoň u důležitých účtů, jako je například internetové bankovnictví. Tento přístup odráží základní bezpečnostní uvědomění, uživatelé si jsou vědomi citlivosti určitých služeb a snaží se je lépe chránit. Dalších 41 respondentů uvedlo, že využívají 2FA všude, kde je to možné, což představuje pokročilý a velmi zodpovědný přístup k ochraně svých online identit.

Na druhé straně 30 respondentů uvedlo, že vůbec neví, co dvoufaktorové ověřování je, a dalších 14 jej sice zná, ale nepoužívá, což tvoří dohromady téměř pětinu dotazovaných. Tato část populace je z pohledu kybernetické bezpečnosti nejzranitelnější, protože spoléhá výhradně na základní hesla, která mohou být snadno prolomena. Výsledky tedy ukazují pozitivní trend v rozšiřování použití 2FA, ale zároveň i značný prostor pro další edukaci, zejména mezi uživateli, kteří o této metodě vůbec neslyšeli. Vzhledem k rostoucímu počtu útoků na online účty by šíření povědomí o výhodách dvoufázové ochrany mělo být jednou z priorit v oblasti bezpečnostní osvěty.

Otázka č. 12: Když se připojíte k Wi-Fi síti, kontrolujete název sítě (SSID), abyste se ujistili, že se jedná o legitimní síť?

Otázka řešící kontrolu názvu sítě SSID, ke které se respondenti připojují, respektive kontrola legitimnosti názvu, například dle jejího umístění. Výsledky nám ukazuje Obrázek 14.



Obrázek 14: Graf odpovědí na otázku č.12

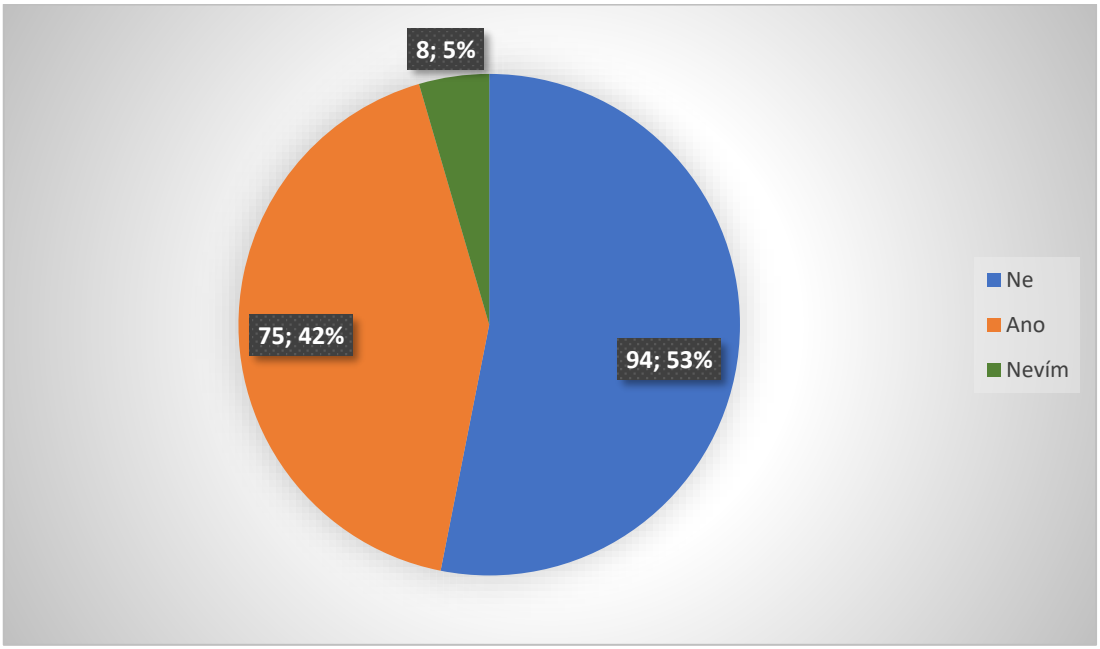
Zdroj: vlastní zpracování

Výsledky této otázky ukazují, že většina respondentů, 92 osob, nikdy nekontroluje název Wi-Fi sítě (SSID) před připojením, což představuje závažné bezpečnostní riziko. Právě podvržené přístupové body (tzv. „evil twin“) často spoléhají na důvěřivost uživatelů, kteří se připojují k síti pouze na základě známého názvu, aniž by ověřili její legitimitu (tohoto bylo využito při prvním průzkumu chování uživatelů bezdrátových sítí). Tento výsledek ukazuje na nízkou míru ostražitosti při připojování ke známým nebo veřejným sítím a zvyšuje riziko útoků typu Man-in-the-Middle nebo odposlechu.

Pouze 30 respondentů uvedlo, že SSID kontrolují vždy, což je z hlediska bezpečnosti ideální chování. Dalších 41 osob kontroluje název sítě pouze občas, což sice představuje určitý pokrok oproti zcela pasivnímu přístupu, ale stále není dostatečné. Celkově výsledky poukazují na to, že většina uživatelů se spoléhá na automatické připojení nebo známý název sítě, aniž by věnovali pozornost možnosti podvržení, což zdůrazňuje potřebu osvěty v této oblasti a důraz na aktivní kontrolu síťové identity před každým připojením.

Otázka č. 13: Máte ve svém mobilním zařízení nebo počítači zapnuté automatické připojování k Wi-Fi sítím?

Další poměrně důležitá otázka, a to konkrétně o nastavení automatického připojování k Wi-Fi sítím na mobilních zařízeních respondentů, na jejíž výsledky se můžeme podívat na Obrázek 15.



Obrázek 15: Graf odpovědí na otázku č.13

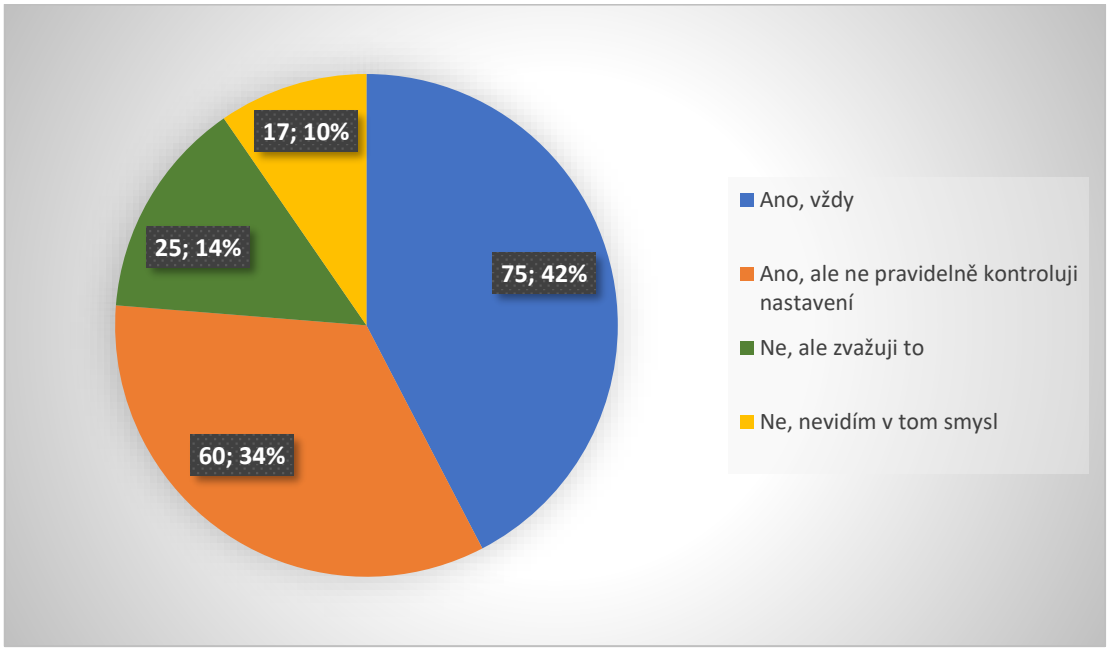
Zdroj: vlastní zpracování

Výsledky ukazují, že 94 respondentů má automatické připojování k bezdrátovým sítím vypnuté, což lze z hlediska bezpečnosti považovat za pozitivní zjištění. Tento přístup minimalizuje riziko samovolného připojení k neznámým nebo podvrženým Wi-Fi sítím, které mohou sloužit k odposlechu dat nebo provádění útoků typu Man-in-the-Middle. Vypnutí automatického připojování ukazuje na určitou míru bezpečnostního povědomí a opatrnosti při pohybu ve veřejném prostoru.

Naopak 75 respondentů přiznalo, že mají automatické připojování aktivní, což zvyšuje pravděpodobnost, že se jejich zařízení připojí bez vědomí uživatele k nezabezpečené či škodlivé síti. To může vést k nechtěnému sdílení dat, vystavení útokům nebo kompromitaci zařízení. Dalších 8 osob uvedlo, že si nejsou jisty nastavením svého zařízení, což signalizuje nedostatečnou orientaci v základních bezpečnostních funkcích systému. Tyto výsledky zdůrazňují nutnost edukace uživatelů o rizicích spojených s automatickým připojováním a o tom, jak si zabezpečit své zařízení jednoduchým krokem v nastavení.

Otázka č. 14: Používáte ve svém zařízení firewall nebo jiný bezpečnostní software pro ochranu před kybernetickými hrozbami?

Předposlední otázka dotazníku nám na Obrázek 16 objasňuje výsledky toho, jestli respondenti používají na svých zařízeních firewall nebo jiný ochranný software chránících je před kybernetickými hrozbami.



Obrázek 16: Graf odpovědí na otázku č.14

Zdroj: vlastní zpracování

Výsledky této otázky ukazují, že většina respondentů, 75 osob, na svých zařízeních pravidelně používá firewall nebo jiný bezpečnostní software, což je pozitivní zjištění a doklad základní kybernetické gramotnosti. Dalších 60 respondentů software také využívá, ale nevěnuje dostatečnou pozornost jeho nastavení, což může snižovat účinnost ochrany, např. pokud není aktivní aktualizace, detekce hrozeb nebo správné blokování přístupů. Tato skupina sice činí první krok k zabezpečení, ale její ochrana může být pouze formální.

Zbývajících 42 respondentů ochranný software zatím nepoužívá, 25 z nich to však zvažuje, což naznačuje otevřenost ke změně návyků, zejména pokud jim bude věnována osvěta. Naopak 17 osob nevěří v přínos těchto nástrojů, což ukazuje na nepochopení jejich role v ochraně zařízení a dat. Celkově lze říci, že více než dvě třetiny uživatelů mají alespoň základní formu softwarové ochrany, ale je nutné zdůraznit i význam její správné konfigurace a pravidelné údržby, aby plnila svůj účel skutečně efektivně.

Otázka č. 15: Jaká opatření by podle vás nejlépe zvýšila bezpečnost bezdrátových sítí?

Poslední otázka dotazníku je poměrně zásadní, jelikož v ní mohli respondenti navrhovat, kromě několika daných možností, i svá řešení pro zvýšení bezpečnosti bezdrátových sítí. Výsledky je možné vidět v Tabulka 25: Odpovědi na otázku č. 15

Podrobněji budou výsledky na tuto otázku rozebrány v kapitole 7 této práce, kam bezesporu většina těchto návrhů patří, obzvláště potom opatření s mobilními daty od operátora, což je bezesporu, společně s osvětou všech uživatelů, nejlepší prevence z hlediska bezpečnosti v oblasti používání bezdrátových sítí.

Tabulka 25: Odpovědi na otázku č. 15

Odpověď	Počet respondentů
Automatická detekce a blokování nebezpečných připojení	114
Lepší informovanost uživatelů o bezpečnostních rizicích	108
Používání silnějších šifrovacích protokolů	54
Povinné používání VPN při připojení k veřejným sítím	45
Nevím	2
Snížení cen mobilních dat by nenutila lidi se připojovat k veřejným sítím	1
Obejít se bez nich a nepoužívat je	1
Dostupnější mobilní data	1
Záleží na definici bezpečnosti, ale platí, že největší bezpečnostní riziko je vždy uživatel. Jo a taky online "smart" web-of-things cetky z Aliexpresu, poskytující přístupová místa do "zabezpečené" domácí sítě.	1
Nové bezpečnostní technologie, současné jsou příliš složité na použití.	1
Lepší informování prohlížečů o HTTPS	1
Nepoužívat veřejné Wi-Fi sítě, vždyť dneska už má každý data v mobilu a může si udělat hotspot pro notebook	1

Zdroj: vlastní zpracování

4.3 Zhodnocení výsledků obou průzkumů

Výsledky obou provedených průzkumů, experimentálního měření a dotazníkového šetření, poskytují komplexní pohled na chování uživatelů bezdrátových sítí v různých situacích a prostředích. Zatímco experimentální část práce simulovala přítomnost nezabezpečené podvržené Wi-Fi sítě a sledovala reakce zařízení v reálném čase, dotazníkové šetření odhalilo postoje, návyky a míru povědomí respondentů o rizicích spojených s používáním bezdrátového připojení.

Z hlediska praktického měření lze konstatovat, že reakce uživatelů byly značně ovlivněny prostředím, ve kterém se nacházeli. Nejvyšší počet připojených zařízení byl zaznamenán na veřejných místech s vyšší koncentrací osob a dostupností oficiálních Wi-Fi sítí, jako například v obchodním centru Letňany nebo na stadionu AC Sparta Praha. V těchto případech

se část uživatelů připojila vědomě na základě názvu sítě, který imitoval legitimní připojení. V několika případech došlo dokonce k automatickému připojení bez zásahu uživatele, což představuje závažné bezpečnostní riziko a potvrzuje, že někteří lidé mají stále zapnutou funkci automatického připojování k otevřeným sítím. Naopak v prostředích s nižší koncentrací osob (např. domov pro seniory, venkovské oblasti či místa bez oficiální Wi-Fi) byla ochota či schopnost zařízení navázat spojení s podvrženou sítí výrazně nižší či nulová.

Dotazníkové šetření potvrdilo, že velká část uživatelů si základních rizik vědoma je, zejména u nezabezpečených sítí. Přesto však praxe ukazuje, že i přes deklarované povědomí o hrozbách se část uživatelů stále chová rizikově. Příkladem může být nízké procento lidí, kteří používají VPN, i když se připojují na veřejné sítě, nebo fakt, že většina respondentů nikdy nezměnila heslo ke své domácí Wi-Fi a neví, jaký bezpečnostní standard jejich síť využívá. Dalším závažným zjištěním je, že přes 40 % respondentů ponechává výchozí přihlašovací údaje ke svému domácímu routeru, což výrazně zvyšuje riziko napadení sítě zvenčí.

Oba průzkumy se vzájemně dobře doplňují, zatímco dotazník odhalil, jak uživatelé o bezpečnosti přemýšlejí, praktická část ukázala, jak se skutečně chovají. Určitá nesrovnalost mezi vědomím a praxí je zřejmá a potvrzuje známý jev v oblasti kybernetické bezpečnosti: uživatelé sice často znají doporučení, ale nedodržují je v každodenním životě. Ukázalo se také, že míra rizika není konstantní, závisí na typu prostředí, technické konfiguraci zařízení i momentální pozornosti uživatele.

Výsledky obou šetření tak podtrhují potřebu pokračující osvěty, zjednodušení bezpečnostních nástrojů (např. jednodušší aktivace VPN nebo automatická kontrola SSID) a zejména výchovy k bezpečnému chování již od základní úrovně technického vzdělávání. Zároveň potvrdily, že přítomnost podvržených sítí není hypotetickým rizikem, ale reálně funkční metodou pro zachycení nepozorných nebo neinformovaných uživatelů.

Další výzkum by mohl pokračovat v bezpečnějších prostředích, například ve formě informovaného experimentu s dobrovolníky, nebo simulací v řízeném prostředí, kde lze provádět podrobnější analýzu bez právních rizik.

5. NÁVRH ŘEŠENÍ PRO ZVÝŠENÍ BEZPEČNOSTI BEZDRÁTOVÝCH SÍTÍ

Bezpečnost bezdrátových sítí zůstává i nadále jedním z klíčových témat v oblasti informačních technologií, zejména s ohledem na jejich rostoucí roli v každodenním životě. Jak ukázaly výsledky provedeného průzkumu i praktických měření, chování uživatelů je často v rozporu s obecně doporučovanými bezpečnostními zásadami. Mnoho uživatelů se připojuje k nezabezpečeným sítím, ignoruje nastavení automatického připojování, nebo nevyužívá dostupné ochranné nástroje, jako je VPN. Přestože si jsou vědomi určitých rizik, chybí jim konkrétní návyky nebo motivace, jak se chránit efektivněji.

Zvyšování bezpečnosti bezdrátových sítí je úzce spojeno s kombinací technických opatření a odpovědného chování uživatelů. I přes rostoucí dostupnost moderních technologií zůstává lidský faktor jedním z nejvýznamnějších prvků ovlivňujících úroveň ochrany. Správné nastavení zařízení, základní informovanost a uvědomění si rizik mohou výrazně snížit pravděpodobnost útoků. Bezpečnost tak často začíná u jednoduchých kroků, které mají zásadní dopad na ochranu dat a soukromí a není nutné, aby tyto kroky byly vždy nutně spojené s vysokými náklady nebo složitějšími technologiemi, mnohdy postačí správné nastavení zařízení, základní informovanost a změna běžných uživatelských návyků.

Navržená opatření jsou členěna do několika tematických okruhů, které reflektují nejčastější slabiny identifikované v dotazníkovém i praktickém šetření. Patří mezi ně technická doporučení, návrhy na zlepšení informovanosti uživatelů i systémová opatření, která mohou být realizována na úrovni poskytovatelů internetového připojení, školství či státní správy.

5.1 Technologická opatření

Technologická opatření představují základní stavební kámen každé strategie zabezpečení bezdrátových sítí. V prostředí, kde jsou bezdrátové přenosy stále více vystaveny neautorizovanému přístupu, odposlechu nebo manipulaci s daty, je důležité, aby zařízení i síťové prvky využívaly moderní a bezpečné nástroje pro ochranu komunikace. Technologická řešení mohou být aplikována jak na straně poskytovatele služby (například v rámci routerů, přístupových bodů nebo serverů), tak i na straně koncového uživatele, který by měl být schopen v rámci svého zařízení nastavit vhodné parametry ochrany.

Zásadním předpokladem bezpečného provozu je především výběr správných protokolů pro šifrování dat a autentizaci, stejně jako zajištění integrity komunikace. Neméně důležitou roli

však hrají i doplňková opatření, jako je využití VPN, pravidelná aktualizace softwaru, správné nastavení zařízení či omezení automatického připojování ke známým sítím. Kombinace těchto prvků tvoří robustní obranu, která významně snižuje pravděpodobnost úspěšného útoku.

5.1.1 Implementace moderních šifrovacích protokolů

Jedním ze zásadních kroků pro zvýšení bezpečnosti bezdrátových sítí je přechod na moderní a spolehlivé šifrovací protokoly. Zatímco starší standardy, jako je WEP, jsou již dnes považovány za nevyhovující a snadno prolomitelné, stále se v praxi objevují, zejména u starších zařízení nebo neaktualizovaných síťových prvků. Protokol WEP byl navržen v době, kdy útoky na bezdrátové sítě nebyly příliš rozšířené, a jeho konstrukce nepočítá s pokročilými metodami analýzy datového provozu.

Moderní protokoly jako WPA2 a zejména WPA3 přinášejí výrazně vyšší úroveň zabezpečení. WPA2 využívá šifrování AES, které je dodnes považováno za velmi silné, a přináší mechanismy pro ověřování integrity dat (například CCMP). Jeho nástupce WPA3 navíc přidává ochranu proti offline útokům prostřednictvím protokolu SAE, což zvyšuje odolnost proti prolomení hesla slovníkovým útokem.

Pro běžného uživatele znamená implementace těchto protokolů především nutnost zajistit, aby jeho domácí router nebo přístupový bod tyto standardy podporoval a měl je správně nastavené. To zahrnuje nejen volbu šifrovacího režimu (např. přepnutí z WPA/WPA2 mixed mode na čisté WPA2 nebo WPA3), ale také volbu dostatečně silného a unikátního hesla pro přístup k síti. V případě veřejných sítí, které jsou dnes stále často nezabezpečené nebo šifrovány pouze slabými metodami, je absence moderního protokolu rizikem, kterému se uživatelé mohou vyhnout právě výběrem jiného typu připojení.

5.1.2 Využití VPN a dalších ochranných mechanismů

Vedle správně nastaveného šifrování na úrovni samotné Wi-Fi sítě je klíčové i nasazení dalších ochranných vrstev, které působí nezávisle na kvalitě veřejné sítě. Nejdostupnějším a nejefektivnějším nástrojem je v tomto směru VPN, která umožňuje šifrování celého datového provozu mezi zařízením uživatele a vzdáleným VPN serverem. I když se uživatel připojí k nezabezpečené síti, třetí strana nemá možnost do šifrovaného přenosu nahlížet, a tedy ani odposlouchávat či měnit přenášená data.

Z průzkumu provedeného v rámci této práce však vyplývá, že VPN využívá pouze menšina respondentů, přestože značná část z nich ví, o jaký princip se jedná. Zde se ukazuje důležitost další osvěty i zpřístupnění kvalitních VPN služeb běžným uživatelům. V ideálním případě

by VPN měla být nastavena jako výchozí ochrana vždy, když se zařízení připojuje k veřejné Wi-Fi, například v kavárně, na letišti nebo v obchodním centru.

Za ještě bezpečnější alternativu však lze považovat vlastní mobilní datové připojení od operátora, které uživatele zcela vyvazuje z potřeby připojovat se k veřejným sítím. Mobilní data jsou přenášena přes šifrované mobilní kanály (např. LTE nebo 5G), jejichž bezpečnostní vrstvy jsou výrazně pokročilejší než u většiny otevřených Wi-Fi sítí. Navíc přístup ke službě je vázán na SIM kartu, což přidává další vrstvu autentizace.

Bohužel, v České republice zůstává vlastní mobilní připojení cenově náročnější než ve většině ostatních zemí Evropské unie. Zatímco v zemích jako Finsko, Estonsko, Švédsko nebo Polsko jsou neomezené nebo objemné datové tarify běžně dostupné i v nižších cenových kategoriích, v ČR se podobné služby stále pohybují na vyšší cenové hladině. To může vést ke snaze uživatelů snižovat své datové náklady připojováním k veřejným sítím, často bez ohledu na úroveň jejich zabezpečení. Tato situace je dlouhodobě kritizována odbornou veřejností a i samotnými uživateli, kteří by v případě dostupnějších tarifů zcela přirozeně preferovali bezpečnější mobilní připojení. [14]

Z hlediska návrhu řešení je tedy žádoucí, aby byla podpořena konkurence na trhu s mobilními daty a zároveň aby byla veřejnost lépe informována o možnostech, jak efektivně kombinovat mobilní data s dalšími nástroji, jako je VPN, pro zajištění maximální možné ochrany. Spojení těchto dvou přístupů, tedy šifrovaného připojení přes VPN a využití vlastních mobilních dat, představuje v současné době nejbezpečnější běžně dostupnou formu připojení k internetu, zejména v prostředí mimo domácí nebo pracovní síť.

5.2 Vzdělávání a osvěta uživatelů

Zatímco technologická opatření hrají klíčovou roli v ochraně bezdrátových sítí, jejich účinnost je z velké části podmíněna chováním a informovaností samotných uživatelů. I sebelepší šifrovací protokoly nebo zabezpečená síť mohou být zbytečné, pokud uživatel z neznalosti nebo nedbalosti umožní útočníkovi přístup ke svému zařízení, sdílí citlivé informace nebo se připojí k podvržené síti. Z tohoto důvodu je vzdělávání a osvěta nedílnou součástí strategie zvyšování kybernetické bezpečnosti.

Výsledky dotazníkového šetření realizovaného v rámci této práce potvrdily, že povědomí o základních hrozbách sice existuje, ale uživatelské návyky často zaostávají za jejich znalostmi. Mnoho respondentů například uvedlo, že vědí o rizicích veřejných Wi-Fi sítí, ale přesto se k nim připojují bez dalších ochranných opatření. Tento rozpor mezi věděním a chováním

je dobře známým fenoménem v oblasti kybernetické bezpečnosti a potvrzuje, že samotná informovanost nestačí a je třeba ji aktivně převádět do praxe.

5.2.1 Zvýšení povědomí o rizicích

Základním předpokladem změny uživatelského chování je pochopení konkrétních rizik, která při používání bezdrátových sítí hrozí. Mnoho uživatelů vnímá Wi-Fi připojení jako běžnou a neškodnou součást digitálního života, aniž by si uvědomovali, že v prostředí veřejných sítí mohou být jejich data snadno odposlouchávána, zachycena nebo zneužita. Příklady útoků typu Man-in-the-Middle, podvržených přístupových bodů (evil twin) nebo falešných captive portálů jsou přitom běžné a relativně snadno proveditelné.

Zvýšení povědomí by mělo probíhat vícero kanály a formami, od výuky v rámci základního a středního školství, přes firemní školení až po veřejné informační kampaně a jednoduché návody pro běžné uživatele. Klíčové je komunikovat hrozby srozumitelným jazykem a uvádět konkrétní scénáře, s nimiž se může uživatel setkat, například připojení k falešné síti v kavárně, přihlášení do banky přes nezabezpečenou Wi-Fi nebo sdílení soukromých souborů v otevřené síti.

Velkou roli zde mohou sehrát i samotní poskytovatelé připojení, mobilní operátoři nebo výrobci zařízení, kteří mohou uživatele upozorňovat na nezabezpečené sítě, nabízet výchozí nastavení se zvýšenou ochranou a poskytovat jasné návody pro bezpečné připojení, jako například v současné době společnost O2 se svým produktem O2 Security, který je bezplatný a je to souhrn doporučení pro všechna zařízení Android i Apple iOS. [15]

V podnikovém prostředí je relativně snadné zajistit systematické vzdělávání zaměstnanců v oblasti bezpečnostních rizik spojených s kyberkriminalitou. Díky centralizované infrastruktuře a interním komunikačním kanálům mohou organizace efektivně šířit osvětu, například formou pravidelných prezenčních školení, e-learningových kurzů zaměřených na bezpečnostní minimum, interaktivních workshopů s praktickými ukázkami nebo simulovaných phishingových kampaní, které pomáhají zaměstnancům rozpoznat podvodné praktiky v reálném čase. Kromě těchto metod lze využít i jednoduché, ale účinné nástroje, jako jsou bezpečnostní letáky nebo infografiky nastavené jako spořiče obrazovky na pracovních počítačích. Jeden takový leták, který je přiložen mezi přílohami této práce, upozorňuje na rizika spojená s připojováním k nezabezpečeným Wi-Fi sítím. Tyto vizuální prvky slouží jako každodenní připomínka důležitých pravidel a mohou významně přispět k budování bezpečnostního povědomí napříč celou organizací.

5.2.2 Doporučené postupy pro bezpečné připojování

Spolu s informováním o hrozbách je důležité uživatelům nabídnout i konkrétní doporučení, jak se bezpečně připojovat a minimalizovat rizika. Tato doporučení by měla být jednoduchá, snadno realizovatelná a přizpůsobená různým úrovním technických dovedností.

Mezi základní doporučení patří:

- Vyhýbat se nezabezpečeným Wi-Fi sítím, pokud není nezbytné se připojit.
- Nepřistupovat k citlivým službám (např. internetové bankovnictví, e-mail) přes veřejné Wi-Fi bez použití VPN.
- Vypnout automatické připojování k sítím, zejména pokud se jedná o známé názvy bez ověření autenticity.
- Pravidelně aktualizovat software a operační systém, protože mnoho útoků cílí na známé zranitelnosti.
- Používat silná hesla pro přístup k Wi-Fi a administračním rozhraním routerů, ideálně v kombinaci s vícefaktorovým ověřením.
- Zkontrolovat název sítě (SSID), ke které se uživatel připojuje, a ujistit se, že se nejedná o podvrženou síť.

Tyto kroky nejsou časově ani technicky náročné, přesto mohou výrazně zvýšit bezpečnost při používání bezdrátových sítí. Důležité je, aby se z těchto postupů stal běžný uživatelský standard, nikoli výjimka.

5.3 Návrh politik a pravidel pro správu bezdrátových sítí

Bezpečnost bezdrátových sítí není odpovědností pouze koncových uživatelů, zásadní roli hrají i správci sítí, provozovatelé přístupových bodů a organizace, které síťové připojení poskytují. Správná konfigurace zařízení, pravidelná údržba a jednoznačná pravidla připojení jsou základními pilíři zajištění bezpečného prostředí pro přenos dat. Tato část kapitoly se zaměřuje na návrh základních principů a politik, které by měly být uplatňovány při správě bezdrátových sítí ve veřejných, komerčních i školních zařízeních.

Jedním z klíčových doporučení je, aby každá bezdrátová síť měla definovanou bezpečnostní politiku, která stanoví, kdo se smí připojovat, jaká pravidla musí uživatelé dodržovat a jakým způsobem bude síť monitorována. Pro veřejné Wi-Fi sítě, jako jsou ty v kavárnách, obchodních centrech či na sportovištích, by měly být zcela standardními opatřeními alespoň základní formy šifrování (např. WPA2-Enterprise), omezená šířka pásma pro neautorizované přístupy, a oddělení veřejné a interní části sítě pomocí VLAN.

V prostředí firem a škol je vhodné zavést politiku víceúrovňového přístupu, kdy zaměstnanci nebo studenti používají jinou síť než návštěvníci. Tato segmentace snižuje riziko, že nezvaný uživatel získá přístup k interním zdrojům. Zároveň je důležité logovat a analyzovat síťový provoz, nikoli za účelem sledování jednotlivců, ale jako prevenci před podezřelou aktivitou, pokusy o průnik či šíření škodlivého softwaru.

Samostatnou oblastí je pak správa přístupových údajů a hesel. Správci by měli dbát na to, aby výchozí hesla nebyla ponechána aktivní a aby docházelo k jejich pravidelné obměně. Uživatelé by měli být motivováni používat silná a jedinečná hesla. Tam, kde to zařízení umožňuje, by mělo být povinné vícefaktorové ověření (2FA) pro přístup k administraci nebo ke klíčovým službám sítě.

V neposlední řadě je vhodné zavést pravidla pro vzdělávání uživatelů sítě, zejména v případě škol, univerzit, podniků a firem. Studenti, zaměstnanci i návštěvníci by měli být při prvním připojení informováni o zásadách bezpečného chování v síti (např. přes captive portál, informační e-mail nebo v bezpečnostní směrnici dostupné všem uživatelům). Pravidelné připomínání těchto zásad může přispět k vytvoření bezpečnostně uvědomělé komunity.

Celkově platí, že bezdrátová síť není statický prvek, ale živý systém, který se vyvíjí, a kterému je třeba věnovat průběžnou pozornost. Dobře navržená pravidla správy a provozu mohou významně snížit riziko útoku, zneužití sítě i úniku citlivých dat, a současně přispět k vyšší důvěře uživatelů ve službu jako takovou.

ZÁVĚR

Práce si kladla za cíl analyzovat chování uživatelů v souvislosti s používáním bezdrátových sítí, zhodnotit úroveň jejich povědomí o rizicích a navrhnout opatření, která mohou zvýšit celkovou úroveň bezpečnosti při práci s bezdrátovým připojením. Kombinací dotazníkového šetření a praktického experimentálního měření se podařilo získat ucelený přehled o tom, jak uživatelé reagují na reálné situace a jaké návyky si v oblasti kybernetické bezpečnosti osvojili.

Z výsledků vyplynulo, že ačkoli si většina uživatelů uvědomuje rizika spojená s připojováním k nezabezpečeným sítím, jejich skutečné chování často tomuto vědomí neodpovídá. Velká část respondentů například používá veřejné Wi-Fi bez jakékoli dodatečné ochrany, automatické připojování k sítím je běžně aktivní a mnoho uživatelů ani neví, jaký bezpečnostní standard využívá jejich domácí síť. Naopak pozitivním zjištěním je rostoucí povědomí o technologiích jako VPN a dvoufázové ověření, i když jejich praktické využívání je stále omezené.

Praktické měření připojení k podvrženým Wi-Fi sítím ukázalo, že reálné bezpečnostní hrozby existují, v několika případech se zařízení připojila automaticky, jindy uživatelé vybrali falešnou síť na základě zavádějícího názvu. Výsledky potvrzují, že zranitelnost uživatelů není jen teoretická, ale že lze relativně jednoduše simulovat útoky, které mohou ohrozit důvěrnost a integritu přenášených dat.

Na základě těchto poznatků byla v poslední části práce navržena konkrétní technologická a edukační opatření, která mohou přispět ke zlepšení stávající situace. Mezi nejefektivnější patří používání vlastního mobilního připojení (pokud to podmínky dovolí), implementace moderních šifrovacích protokolů, vypnutí automatického připojování a důsledná správa síťových zařízení. Zároveň byla zdůrazněna potřeba zvýšení dostupnosti datových tarifů a lepšího vzdělávání uživatelů, ať už ve formálním vzdělávání, nebo prostřednictvím veřejné osvěty.

Práce tak přináší nejen analýzu současného stavu, ale i návrh možných zlepšení, která mohou být aplikována jak jednotlivci, tak institucemi a poskytovateli připojení. Vzhledem k neustále se vyvíjejícím hrozbám v oblasti kybernetické bezpečnosti je nezbytné, aby bezpečnost bezdrátových sítí byla vnímána jako dlouhodobá priorita, nikoli pouze jako jednorázové nastavení.

POUŽITÁ LITERATURA

[1] LORENTZEN, Nils, SEIDLITZ, Leander. Evolution of Wireless Security. *www.net.in.tum.de.* [Online] [Citace: 20. 4 2025.] https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2024-09-1/NET-2024-09-1_14.pdf.

[2] GOODRICH, M.,TAMASSIA,R. *Introduction to Computer Security.* USA : Addison-Wesley Publishing Company, 2010.

[3] www.securityuncorked.com. A Brief History of Wireless Security: Open, WEP, WPA, WPA2 & 802.1X. *www.securityuncorked.com.* [Online] [Citace: 1. 5 2025.] https://securityuncorked.com/2008/08/history-of-wireless-security/.

[4] www.mycyberawareness.co.uk. From WEP to WPA3: The History of Wireless Security Protocols. *www.mycyberawareness.co.uk.* [Online] [Citace: 1. 5 2025.] https://mycyberawareness.co.uk/from-wep-to-wpa3-the-history-of-wireless-security-protocols/.

[5] MITCHELL, Bradley. 802.11 Wi-Fi Standards: Decoding 802.11be to 802.11a. *www.lifewire.com.* [Online] [Citace: 23. 4 2025.] https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553.

[6] BENTON, Kevin. The Evolution of 802.11 Wireless Security. *web.archive.org.* [Online] 18. 4 2010. [Citace: 25. 4 2025.] https://web.archive.org/web/20160302132133/http://homes.soic.indiana.edu/ktbenton/research/benton_wireless.pdf.

[7] SAI. WPA2 vs WPA3 (Full 2025 Comparison & Differences). *www.stationx.net.* [Online] [Citace: 29. 5 2025.] https://www.stationx.net/wpa2-vs-wpa3/.

[8] MONTGOMERY, David. Wireless Network Security in 2025 and Beyond. *www.medium.com.* [Online] [Citace: 21. 5 2025.] https://medium.com/%40dmontg/wireless-network-security-in-2025-and-beyond-71f7c13f9889.

[9] www.sentinelone.com. Cyber Security Best Practices for 2025. *www.sentinelone.com.* [Online] [Citace: 26. 5 2025.] https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-best-practices/.

[10] WHITE, Daniella. Top IoT Security Risks to Guard Against in 2024. *www.thedailyplaniot.com.* [Online] [Citace: 24. 4 2025.] https://thedailyplaniot.com/iot-security-risks/.

[11] CACHE, Johnny, WRIGT, Joshua, LIU, Vincent. *Hacking exposed wireless.* New York : The McGraw-Hill, 2010.

[12] ANDERSON, Ross. *Security engineering: a guide to building dependable distributed systems. Third edition.* Indianapolis : Wiley, 2020.

[13] www.cybersecura.com. WPA/WPA2 cracking, PMKID, Evil Twin... Overview of attacks and threats to Wi-Fi in 2022. *www.cybersecura.com.* [Online] [Citace: 2. 5 2025.] https://www.cybersecura.com/en/post/overview-of-attacks-and-threats-to-wifi-in-2022.

[14] BÖHM, Petr. *Analýza telekomunikačních služeb v České republice.* Diplomová práce. Přerov : Vysoká škola logistiky o.p.s., 2023.

[15] O2. O2 security. *O2.* [Online] [Citace: 3. 5 2025.] https://www.o2.cz/osobni/internet/o2security.

[16] BARKEN, Lee, VESELSKÝ, Jiří. *Wifi: jak zabezpečit bezdrátovou síť.* Brno : Computer Press, 2004.

[17] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace: jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G.* Brno : CP Books, 2005.

[18] GAST, Matthew. *802.11 wireless networks: the definitive guide.* Beijing : O´Reilly, 2002.

[19] EARLE, A.E. *Wireless Security Handbook.* USA : Auerlach Publications, 2005.

[20] PUŽMANOVÁ, Rita. Bepečnost WLAN podle IEEE. *Lupa.cz.* [Online] [Citace: 14. 2 2025.] https://www.lupa.cz/clanky/bezpecnost-wlan-podle-ieee/.

[21] KÖHRE, Thomas. *Stavíme si bezdrátovou síť Wi-fi.* Brno : Computer Press, 2004.

[22] ZANDL, Patrick. *Bezdrátové sítě WiFi: praktický průvodce : jak vybrat hardware a anténu : realizace a bezpečnost sítí WiFi : podpora WiFi v operačních systémech.* Brno : Computer Press, 2006.

[23] CARROLL, Brandon James. *Bezdrátové sítě Cisco Autorizovaný výukový průvodce.* Brno : Computer Press, 2011.

[24] Norton. Public Wi-Fi: A guide to the risks and how to stay safe. *www.trustedsec.com.* [Online] [Citace: 25. 4 2025.] https://trustedsec.com/blog/the-dangers-of-transition-mode.

[25] Okta. WPA3 Security: Benefits, Vulnerabilities & Comparison to WPA2. *www.netgear.com.* [Online] [Citace: 22. 4 2025.] https://www.netgear.com/hub/network/security/wpa3-encryption-secure-wifi.

[26] KRTEK, Václav. Zabezpečení Wi-Fi sítí (výsledky průzkumu). *www.vyplnto.cz.* [Online] 2025. https://81332.vyplnto.cz.

SEZNAM PŘÍLOH

PŘÍLOHA A: Dotazník vzdělanosti uživatelů

I. Demografické údaje

1. Jaký je váš věk?
   - Méně než 18 let
   - 18–25 let
   - 26–35 let
   - 36–50 let
   - Více než 50 let

2. Jaké je vaše pohlaví?
   - Muž
   - Žena
   - Jiná možnost / Nechci uvádět

II. Chování při připojování k bezdrátovým WI-FI sítím

3. Připojujete se na veřejných místech (např. kavárny, nádraží, letiště) k bezdrátovým WI-FI sítím?
   - Ano, často
   - Ano, občas
   - Zřídka
   - Nikdy

4. Pokud jste na veřejném místě a k dispozici je otevřená (nezabezpečená) Wi-Fi síť, připojíte se k ní?
   - Ano, bez obav
   - Ano, ale pouze v případě, že opravdu potřebuji připojení
   - Ne, raději používám mobilní data
   - Ne, nikdy

5. Věříte, že připojení k nezabezpečené Wi-Fi síti může představovat bezpečnostní riziko?
   - Ano, určitě
   - Ano, ale myslím si, že riziko je minimální
   - Nevím / Nejsem si jistý/á
   - Ne, nemyslím si, že by to bylo nebezpečné

6. Používáte při připojení k veřejným Wi-Fi sítím VPN?
   - Ano, vždy
   - Ano, občas
   - Ne, ale vím, co to je
   - Ne, nevím, co to je

III. Povědomí o bezpečnostních technologiích

7. Znáte rozdíl mezi zabezpečením Wi-Fi pomocí WEP, WPA a WPA2/WPA3?
   - Ano, dobře rozumím rozdílům
   - Něco jsem o tom slyšel/a, ale nejsem si jistý/á
   - Ne, neznám rozdíl

8. Jaký bezpečnostní protokol používá vaše domácí Wi-Fi síť?
   - WEP
   - WPA/WPA2
   - WPA3
   - Nevím

9. Má vaše domácí Wi-Fi síť změněné výchozí přihlašovací údaje k routeru?
   - Ano, změnil/a jsem heslo i přihlašovací údaje
   - Ano, změnil/a jsem pouze heslo k Wi-Fi
   - Ne, mám výchozí nastavení
   - Nevím

10. Jak často měníte heslo k domácí Wi-Fi síti?
    - Pravidelně (alespoň jednou ročně)
    - Občas (jednou za několik let)
    - Nikdy jsem heslo neměnil/a
    - Nevím

IV. Ochrana osobních údajů a bezpečnostní opatření

11. Používáte dvoufaktorové ověřování (2FA) při přihlašování do online služeb?
    - Ano, všude, kde je to možné
    - Ano, ale jen u důležitých účtů (např. bankovnictví)
    - Ne, ale vím, co to je
    - Ne, nevím, co to je

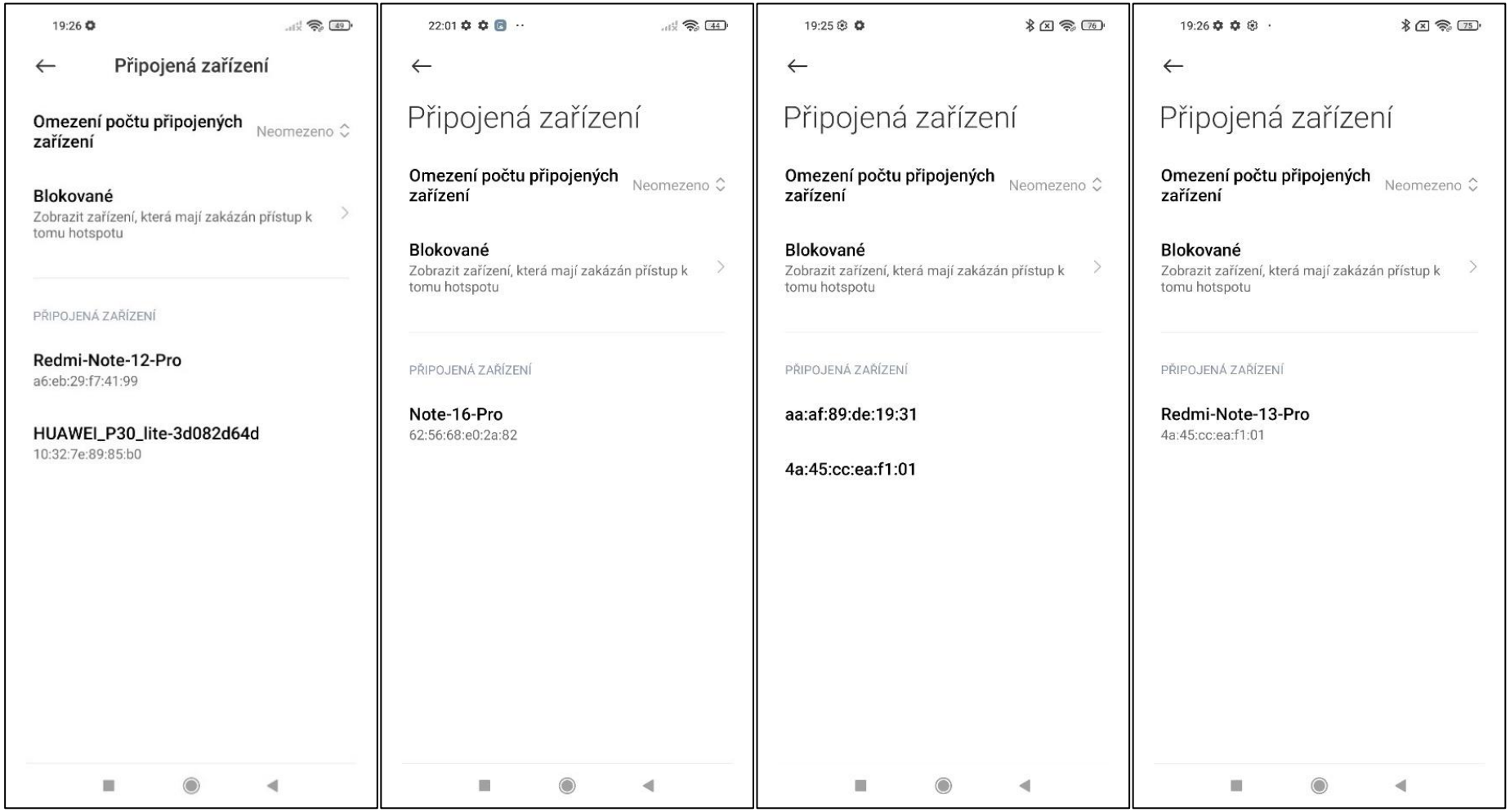
12. Když se připojíte k Wi-Fi síti, kontrolujete název sítě (SSID), abyste se ujistili, že se jedná o legitimní síť?
    - Ano, vždy
    - Ano, občas
    - Ne, nikdy

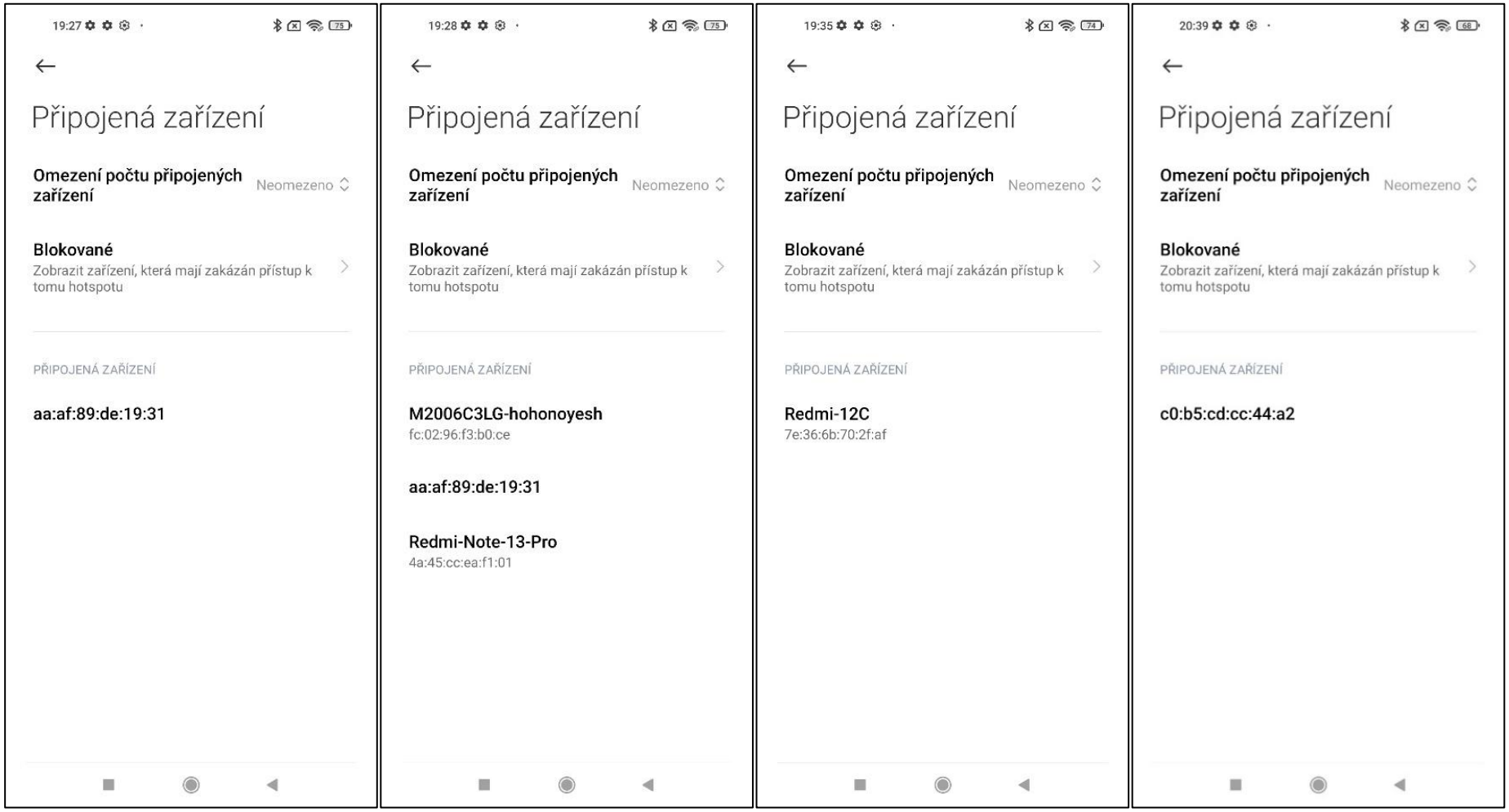
13. Máte ve svém mobilním zařízení nebo počítači zapnuté automatické připojování k Wi-Fi sítím?
    - Ano
    - Ne
    - Nevím

14. Používáte ve svém zařízení firewall nebo jiný bezpečnostní software pro ochranu před kybernetickými hrozbami?
    - Ano, vždy
    - Ano, ale ne pravidelně kontroluji nastavení
    - Ne, ale zvažuji to
    - Ne, nevidím v tom smysl

15. Jaká opatření by podle vás nejlépe zvýšila bezpečnost bezdrátových sítí? (můžete vybrat více možností)
    ☐ Lepší informovanost uživatelů o bezpečnostních rizicích
    ☐ Používání silnějších šifrovacích protokolů
    ☐ Povinné používání VPN při připojení k veřejným sítím
    ☐ Automatická detekce a blokování nebezpečných připojení
    ☐ Jiná možnost: _____

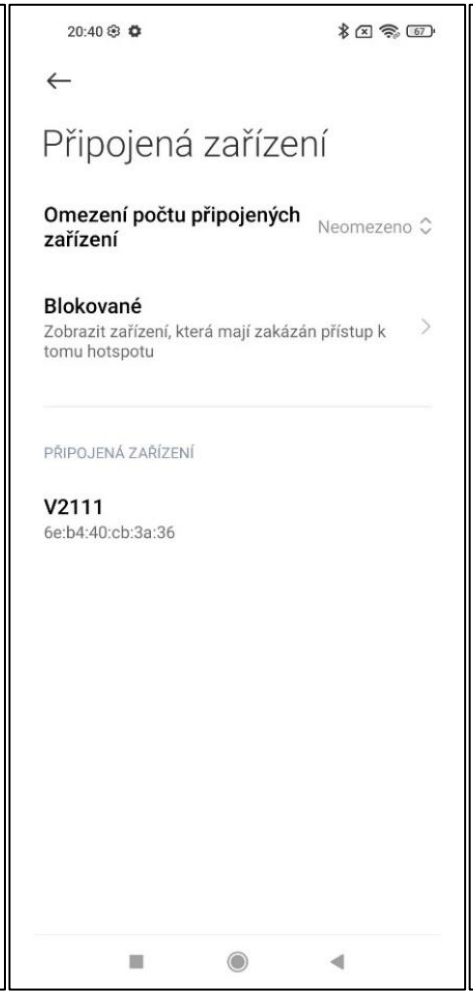
PŘÍLOHA B: Zachycené printscreeny z měření s falešnou Wi-Fi



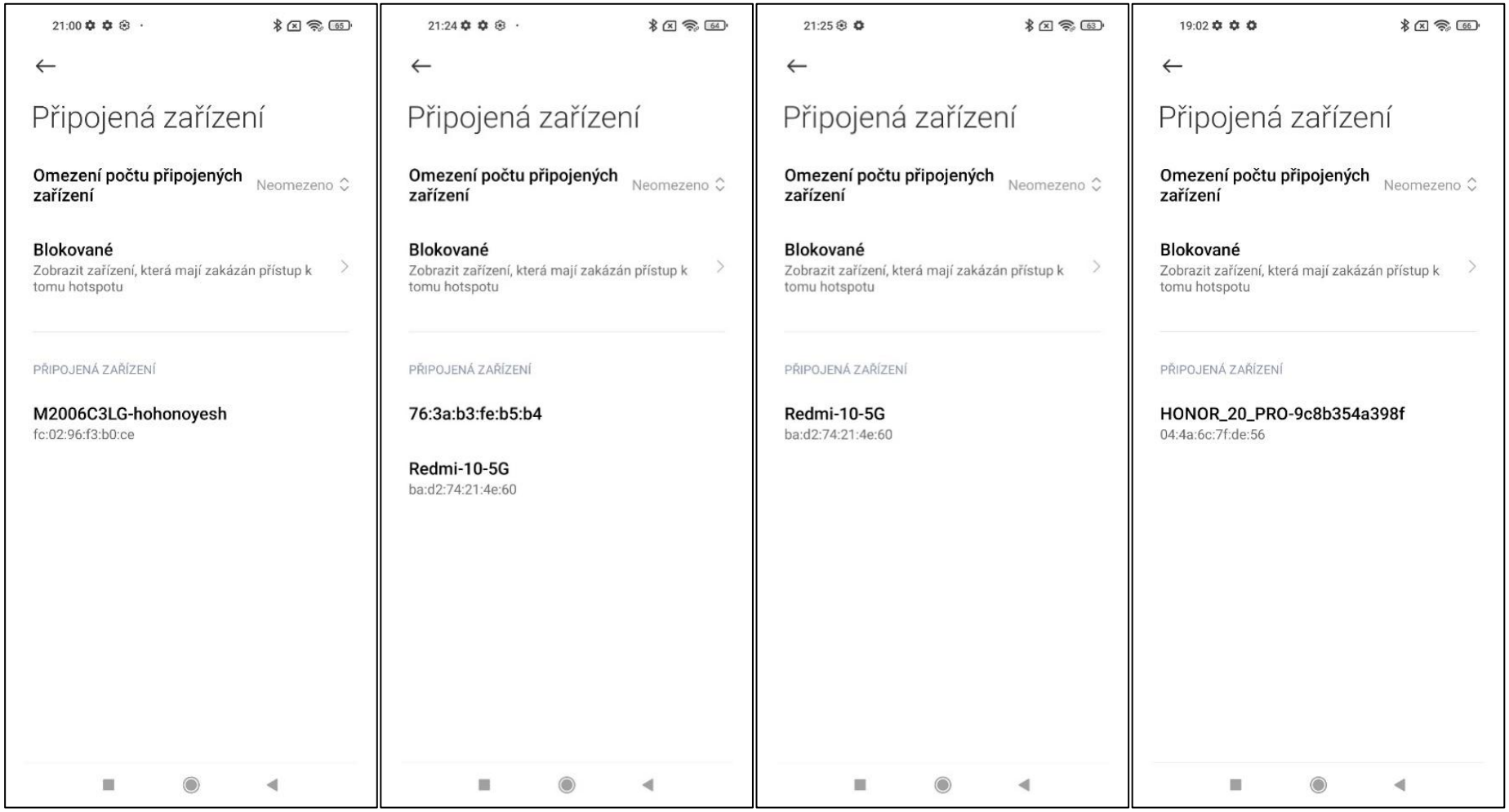

19:27
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
aa:af:89:de:19:31
19:28
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
M2006C3LG-hohonoyesh
fc:02:96:f3:b0:ce
aa:af:89:de:19:31
Redmi-Note-13-Pro
4a:45:cc:ea:f1:01
19:35
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
Redmi-12C
7e:36:6b:70:2f:af
20:39
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
c0:b5:cd:cc:44:a2

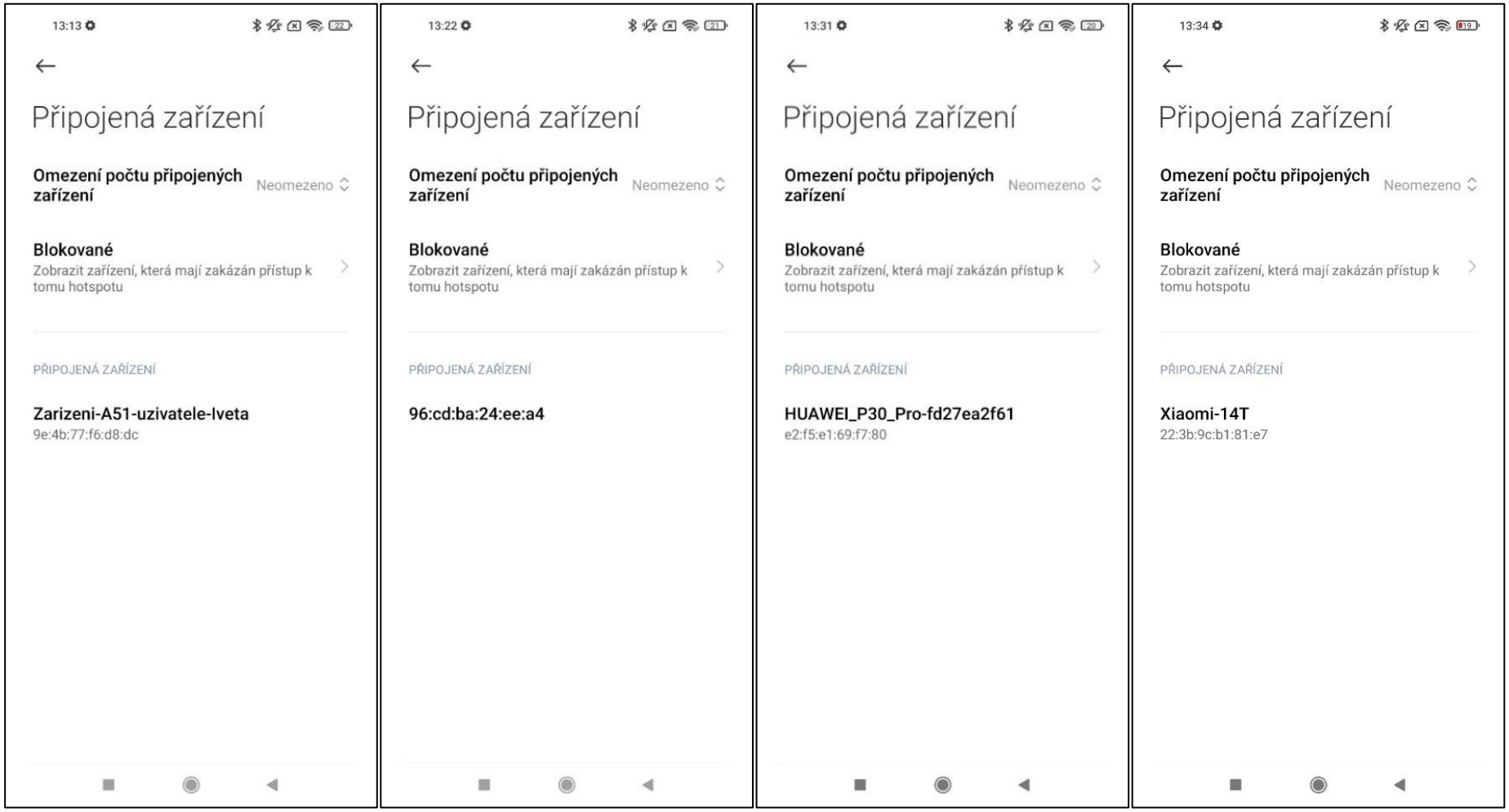

20:40
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
6e:b4:40:cb:3a:36

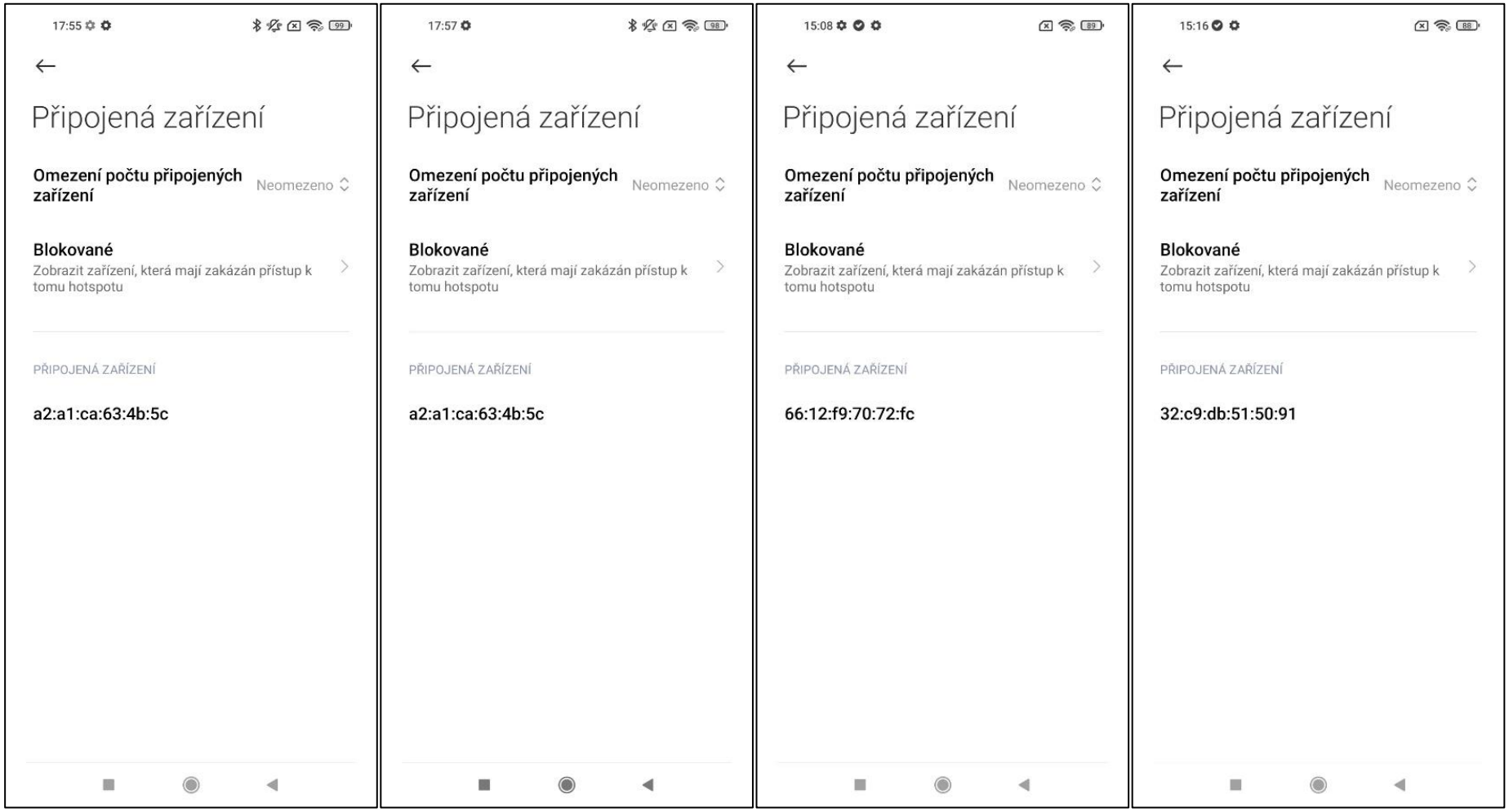

20:40
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
Galaxy-A70
e6:02:bc:88:64:9d
V2111
6e:b4:40:cb:3a:36

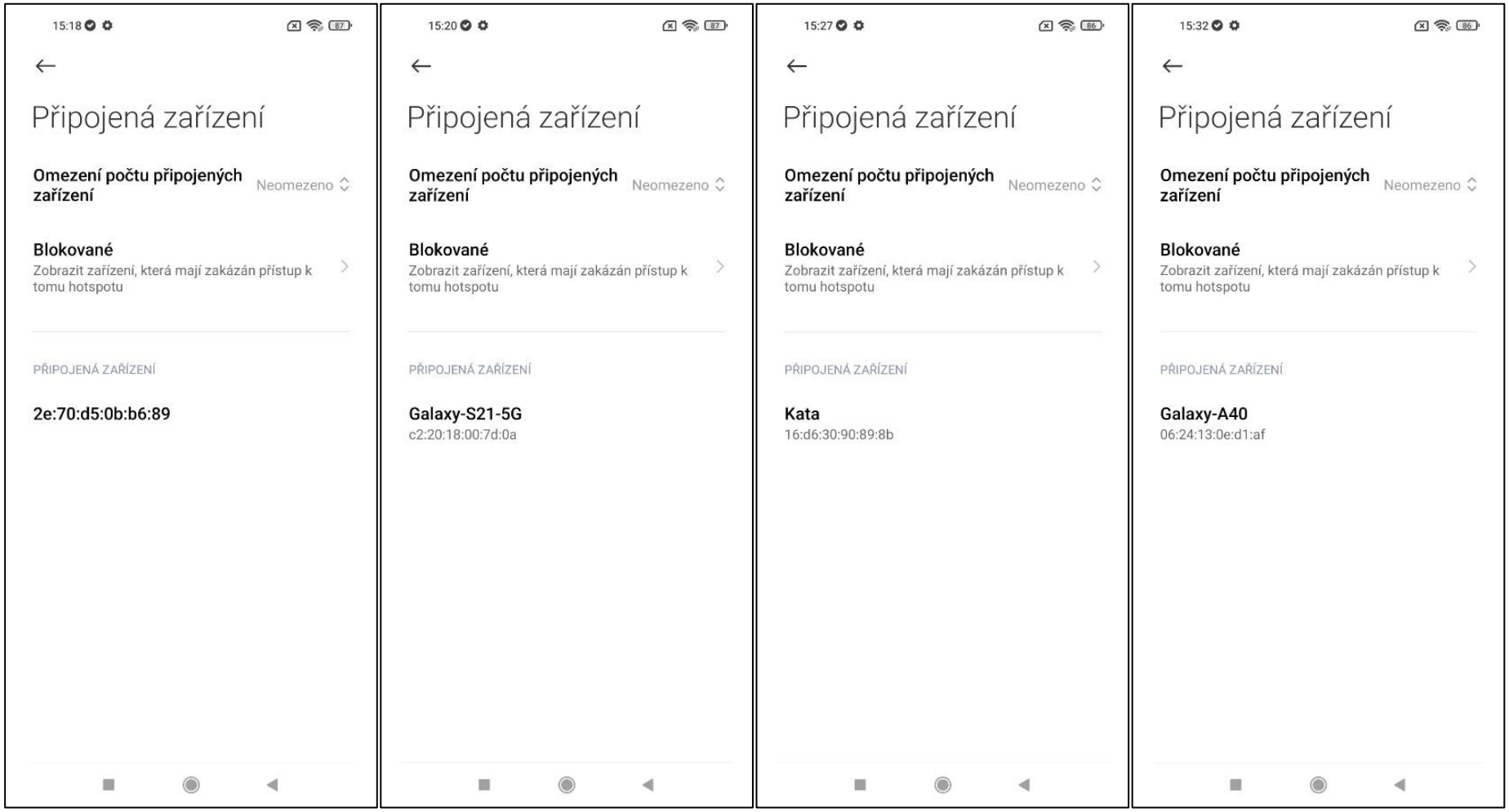

20:40
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
V2111
6e:b4:40:cb:3a:36


20:51
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
Redmi-12C
7e:36:6b:70:2f:af
aa:af:89:de:19:31


21:00
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
M2006C3LG-hohonoyesh
fc:02:96:f3:b0:ce
21:24
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
76:3a:b3:fe:b5:b4
Redmi-10-5G
ba:d2:74:21:4e:60
21:25
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
Redmi-10-5G
ba:d2:74:21:4e:60
19:02
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
HONOR_20_PRO-9c8b354a398f
04:4a:6c:7f:de:56


13:13
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
Zarizeni-A51-uzivatele-Iveta
9e:4b:77:f6:d8:dc
13:22
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
96:cd:ba:24:ee:a4
13:31
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
HUAWEI_P30_Pro-fd27ea2f61
e2:f5:e1:69:f7:80
13:34
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
Xiaomi-14T
22:3b:9c:b1:81:e7


17:55
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
a2:a1:ca:63:4b:5c
17:57
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
a2:a1:ca:63:4b:5c
15:08
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
66:12:f9:70:72:fc
15:16
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
32:c9:db:51:50:91


15:18
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
2e:70:d5:0b:b6:89
15:20
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
Galaxy-S21-5G
c2:20:18:00:7d:0a
15:27
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
Kata
16:d6:30:90:89:8b
15:32
Připojená zařízení
Omezení počtu připojených zařízení
Neomezeno
Blokované
Zobrazit zařízení, která mají zakázán přístup k tomu hotspotu
PŘIPOJENÁ ZAŘÍZENÍ
Galaxy-A40
06:24:13:0e:d1:af

PŘÍLOHA C: Leták s upozorněním na připojování k nezabezpečené Wi-Fi