VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

KYBERNETICKÁ BEZPEČNOST V ČESKÉ REPUBLICE

Autor práce: Josef Misar

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: prof. JUDr. Jozef Meteňko, PhD.

Katedra: Katedra právních oborů a bezpečnostních studií

2025

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucímu bakalářské práce prof. JUDr. Jozefovi Meteňkovi, PhD. za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

MISAR, J. Kybernetická bezpečnost v České republice: bakalářská práce. České Budějovice: Vysoká škola evropských a regionálních studií, 2025. 71 s. Vedoucí bakalářské práce: prof. JUDr. Jozef Meteňko, PhD.

V této bakalářské práci jsme se zabývali problematikou kybernetické bezpečnosti v České republice. Cílem práce bylo analyzovat aktuální stav kybernetické bezpečnosti, a to včetně legislativního rámce, vývoje kybernetických hrozeb, preventivních opatření a konkrétních případů kybernetických útoků.

V teoretické části jsme vymezili základní pojmy, popsali vývoj kybernetiky a kybernetické bezpečnosti, přiblížili právní aspekty a strategické dokumenty. V praktické části jsme realizovali kvantitativní výzkum formou dotazníkového šetření, jehož cílem bylo zjistit úroveň povědomí veřejnosti o kybernetické bezpečnosti a používaných bezpečnostních opatřeních. Získané výsledky nám umožnily identifikovat slabá místa ve znalostech respondentů a navrhnout doporučení, která mohou přispět ke zvýšení bezpečnosti jednotlivců i organizací. Práce poskytuje ucelený pohled na současný stav kybernetické bezpečnosti a její význam pro společnost v době rychlého technologického rozvoje.

Klíčová slova: kybernetická bezpečnost, kybernetické útoky, ochrana dat, bezpečnostní opatření, organizační bezpečnost

ABSTRACT

MISAR, J. Cybersecurity in the Czech Republic: Bachelor Thesis. České Budějovice: The College of European and Regional Studies, 2025. 71 pgs. Supervisor: prof. JUDr. Jozef Meteňko, PhD.

In this bachelor's thesis, we dealt with the issue of cybersecurity in the Czech Republic. The aim of the thesis was to analyse the current state of cybersecurity, including the legislative framework, the development of cyber threats, preventive measures, and specific cases of cyber-attacks.

In the theoretical part, we defined basic concepts, described the development of cybernetics and cybersecurity, and presented legal aspects and strategic documents. In the practical part, we conducted quantitative research in the form of a questionnaire survey, the aim of which was to determine the level of public awareness of cybersecurity and the security measures used. The results obtained allowed us to identify weaknesses in the respondents' knowledge and propose recommendations that can contribute to increasing the digital security of individuals and organizations. The work provides a comprehensive view of the current state of cybersecurity and its importance for society in an era of rapid technological development.

Key words: cybersecurity, cyber-attacks, data protection, security measures, organizational security

Obsah

Úvod

V digitální době, kdy se naše každodenní činnosti čím dál více přesouvají do online prostředí, je téma kybernetické bezpečnosti stále žádanějším tématem. S rostoucí mírou digitalizace společnosti a rychlým vývojem technologií vznikají nové formy kybernetických hrozeb, které musíme řešit nejen na úrovni jednotlivců, ale i na úrovni institucí a státu. Kybernetická bezpečnost je nezbytnou součástí ochrany informačních systémů a citlivých údajů.

Téma bakalářské práce jsme si zvolili především z osobního zájmu o oblast informačních technologií a bezpečnosti. Kybernetickou bezpečnost vnímáme jako jednu z klíčových součástí ochrany současné společnosti a věříme, že její hlubší porozumění nám umožní lépe čelit aktuálním i budoucím výzvám digitálního světa.

Hlavním cílem této práce bude analyzovat sociální a technologické dopady kybernetických hrozeb v České republice. Budeme se snažit identifikovat hlavní problémy v oblasti kybernetické bezpečnosti, vyhodnotit jejich dopad na společnost a navrhnout konkrétní opatření pro zlepšení ochrany.

V teoretické části budeme analyzovat odbornou literaturu, právní předpisy a strategické dokumenty. V praktické části provedeme dotazníkové šetření mezi uživateli internetu, abychom zjistili jejich povědomí o kybernetické bezpečnosti, osobní zkušenosti a přijatá bezpečnostní opatření. K dosažení tohoto cíle využijeme také kvantitativní výzkumnou metodu pomocí dotazníkového šetření. Výsledky výzkumu následně vyhodnotíme a na jejich základě navrhneme doporučení pro zlepšení situace.

V rámci této práce bude zkoumána problematika kybernetické bezpečnosti se zaměřením na její cíle, výzkumnou metodologii, základní pojmy a historický vývoj. Věnovat se bude rovněž prostředí České republiky, a to z hlediska současné situace, strategických přístupů i právního rámce. Dále budou popsány různé formy kybernetických útoků a analyzovány konkrétní případy, které dokumentují reálné hrozby v této oblasti. Součástí práce je také rozbor možností, jak těmto útokům předcházet a jakými prostředky lze posilovat ochranu. Závěr bude tvořit analýza výsledků získaných z dotazníkového šetření, jež ilustrují vnímání kybernetické bezpečnosti mezi běžnými uživateli internetu.

1 Cíl a metodika bakalářské práce

Kybernetická bezpečnost je v současné době klíčovou oblastí, která ovlivňuje jednotlivce, organizace i Českou republiku. S rostoucí digitalizací a zvyšujícím se počtem kybernetických hrozeb se stává ochrana informačních systémů nezbytnou součástí bezpečnostní strategie každého subjektu. Hlavním motivem pro volbu tématu bakalářské práce je osobní zájem o oblast informačních technologií a kybernetické bezpečnosti. Vnímám ji jako zásadní složku hybridních hrozeb a mám za to, že porozumění aktuálním kybernetickým rizikům přispěje k efektivnější ochraně jak na úrovni jednotlivců, tak ve veřejném a soukromém sektoru.

Hlavním cílem této bakalářské práce je analyzovat sociální a technologické dopady kybernetických hrozeb v České republice. Tento cíl vychází z oficiálního zadání bakalářské práce a zahrnuje identifikaci klíčových problémů souvisejících s kybernetickou bezpečností, jejich dopad na různá odvětví a návrh opatření ke zlepšení ochrany kybernetického prostředí.

V rámci práce bude nejprve vymezen pojem kybernetické bezpečnosti a analyzován její historický vývoj. Následně bude zmapován legislativní rámec kybernetické bezpečnosti v České republice a zhodnocena jeho účinnost. Důležitou částí analýzy bude identifikace hlavních typů kybernetických útoků a jejich dopad na jednotlivce, organizace a kritickou infrastrukturu. Empirická část práce se zaměří na analýzu úrovně povědomí o kybernetické bezpečnosti mezi veřejností a odborníky na základě dotazníkového šetření. Dalším cílem je porovnání expertního a uživatelského pohledu na kybernetické hrozby a bezpečnostní opatření. Na základě zjištěných dat budou formulována doporučení ke zlepšení kybernetické bezpečnosti v České republice.

Pro dosažení stanovených cílů budou použity různé výzkumné metody. Primární metodou bude analýza dokumentů a literatury, která zahrne studium odborných publikací, právních předpisů a aktuálních zpráv o kybernetických hrozbách. Další klíčovou metodou bude dotazníkové šetření mezi uživateli internetu a IT odborníky, jehož cílem je zhodnotit míru povědomí o kybernetických hrozbách a přijatých opatřeních. Empirická část bude dále doplněna analýzou vybraných kybernetických incidentů v České republice a jejich dopadů na vybrané sektory.

Očekávaným výsledkem této práce je vyhodnocení současného stavu kybernetické bezpečnosti v České republice na základě empirických dat. Výstupy zahrnují identifikaci klíčových nedostatků v bezpečnostních opatřeních a legislativním rámci. Na základě těchto poznatků bude formulován návrh konkrétních opatření pro zlepšení kybernetické bezpečnosti na individuální, firemní a státní úrovni. Práce může sloužit jako podklad pro odbornou i veřejnou sféru, zejména v oblasti prevence kybernetických útoků a zvyšování digitální gramotnosti.

2 Kybernetická bezpečnost

Kybernetická bezpečnost (z angličtiny „cyber security“) je soubor opatření, technik a postupů sloužících k ochraně počítačových systémů, sítí, elektronických zařízení a dat před neoprávněným přístupem, útoky, poškozením či zneužitím.

Kybernetická bezpečnost nemá jednotnou a obecně uznávanou definici. Tento koncept lze vnímat jako součást širšího rámce bezpečnosti, přičemž představuje jeho specifickou.[1]

Na kybernetickou bezpečnost může být nahlíženo z různých perspektiv. Práce vychází z definice, která považuje kybernetickou bezpečnost za součást informační bezpečnosti.

Kybernetická bezpečnost se zaměřuje na ochranu počítačových systémů a sítí před hrozbami pocházejícími z kyberprostoru. Na rozdíl od fyzických aktiv, kde se řeší jejich zničení, poškození či krádež, se v oblasti kybernetické bezpečnosti jedná o zajištění základních bezpečnostních atributů pro data a informace, které jsou v těchto systémech a sítích uloženy, zpracovávány nebo přenášeny.[2]

2.1 Vymezení základních pojmů

Jirovský popisuje kybernetickou kyberkriminalitu neboli **kybernalitu** jako činnost, kterou je porušován zákon nebo je v rozporu s morálními pravidly společnosti. Tato kriminalita může být namířena přímo proti počítačům, jejich hardwaru, softwaru, datům, sítím apod.[3]

Následující definice základních pojmů v této kapitole jsou čerpány z Výkladového slovníku kybernetické bezpečnosti.[4]

- **Kyberprostor:** Virtuální prostředí, ve kterém dochází k interakci mezi počítači, sítěmi a uživateli.

[1]KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity.* CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. s. 41. ISBN 978-80-88168-31-7.

[2]ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

[3]JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. s.19.ISBN 978-80-247-1561-2.

[4]JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti.* Páté doplněné a upravené vydání. Praha: Česká pobočka AFCEA, 2022. ISBN 978-80-908388-4-0.

- **Informační bezpečnost:** Širší pojem, který zahrnuje ochranu informací v jakékoli podobě (elektronické, tištěné, verbální).
- **Kybernetická hrozba:** Jakákoli událost nebo aktivita, která by mohla narušit kybernetickou bezpečnost.
- **Zranitelnost:** Slabina v systému, která může být zneužita útočníkem.
- **Kybernetický útok:** Cílená akce s cílem narušit kybernetickou bezpečnost.
- **Kybernetický incident:** Jakákoli událost, která narušila kybernetickou bezpečnost.
- **Malware:** Škodlivý software, který může infikovat počítač a způsobit škodu.
- **Phishing:** Podvodná technika, která se snaží vylákat od uživatele citlivé informace (hesla, čísla kreditních karet).
- **DDoS útok:** Útok na dostupnost služby, který se snaží zahltit server požadavky a znemožnit jeho fungování.
- **Sociální inženýrství:** Manipulace s lidmi s cílem získat přístup k informacím nebo systémům.
- **Šifrování:** Technika, která chrání data před neoprávněným přístupem.
- **Autentizace:** Ověření identity uživatele.
- **Autorizace:** Ověření oprávnění uživatele k přístupu k informacím nebo systémům.
- **Firewall:** Bezpečnostní systém, který chrání síť před neoprávněným přístupem.
- **Bezpečnostní audit:** Systematické posouzení kybernetické bezpečnosti.
- **Zálohování:** Pravidelné ukládání dat pro případ ztráty nebo poškození.
- **Hacking:** Hacking je aktivita, při které se útočník pokouší nalézt chyby systému.[5]

[5]PORADA, Viktor, 2019. *Bezpečnostní vědy: úvod do teorie, metodologie a bezpečnostní terminologie*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-758-0.

2.2 Definice kybernetiky

Norbert Wiener, americký matematik, poprvé použil termín „kybernetika“ jako název své knihy z roku 1948, v níž se zabýval samoregulačními mechanismy. Tento pojem odvodil z latinizované podoby starořeckého slova „kybernetes“, což znamená „kormidelník“. Pravděpodobně byl inspirován i francouzským termínem „cybernétique“, označujícím řízení a správu. Slovo „kybernetes“ vychází z řeckého slovesa „kybernan“, tedy „řídit“ nebo „kormidlovat“, jehož původ zůstává nejasný. V osmdesátých letech 20. století se předpona „cyber-“ začala používat ve spojení s výpočetní technikou, ačkoli šlo o chybnou reinterpretaci původního výrazu.[6]

Pojem kybernetiky se během desetiletí významně rozšířil a transformoval, což dokládá jeho vývoj od původního označení řízení a samoregulace až po moderní spojení s výpočetní technikou. Tato flexibilita v užívání slova naznačuje, že jazyk se neustále přizpůsobuje technickému pokroku a kulturním změnám. Wienerova definice se stala klíčovou pro mnoho oborů, včetně umělé inteligence, robotiky a teorie systémů, což potvrzuje trvalý význam kybernetiky v akademickém i praktickém kontextu.

Principy kybernetiky hrají klíčovou roli i v oblasti kybernetické bezpečnosti. Kybernetické systémy, jako jsou počítačové sítě, informační systémy a komunikační infrastruktura, jsou neustále vystaveny různým hrozbám. Kybernetika nabízí nástroje a metody pro analýzu těchto systémů, identifikaci zranitelností a navrhování opatření pro jejich ochranu, přičemž se zaměřuje především na digitální hrozby, ale může být využita i při řešení některých mechanických aspektů bezpečnosti. Například principy zpětné vazby se uplatňují při detekci a reakci na kybernetické útoky, kdy systémy automaticky analyzují a reagují na podezřelé aktivity.

Ačkoliv se kybernetika zrodila již v polovině 20. století, její principy jsou stále aktuální a nacházejí uplatnění v mnoha oblastech, včetně kybernetické bezpečnosti.[7]

[6]ALEKSIC, Adam. *CYBER-PILOT*. Online. The Etymology Nerd. Dostupné z: https://www.etymologynerd.com/blog/cyber-pilot. [cit. 2025-03-01].

[7]REJZEK, Jiří. *Český etymologický slovník*. 2., nezměněné vydání. Voznice: Nakladatelství LEDA, 2012. ISBN 978-80-7335-296-7.

Díky kybernetice můžeme lépe porozumět komplexním kybernetickým systémům, identifikovat jejich slabá místa a vytvářet efektivní strategie pro jejich ochranu před kybernetickými hrozbami.

2.3 Historie kybernetické bezpečnosti

Počátky kybernetické bezpečnosti sahají až do období druhé světové války, kdy se s vývojem výpočetní techniky objevila potřeba ochrany citlivých informací. V roce 1939 byl vyvinut Turingův stroj Bomba k dešifrování zpráv z německého šifrovacího stroje Enigma. V roce 1940 byl vytvořen Colossus, první programovatelný elektronický počítač, který k dešifrování Lorenzovy šifry používal elektronky.[8]

Poválečné období přineslo rozvoj počítačů s využitím tranzistorů a integrovaných obvodů. V 60. letech vznikla první čtyřuzlová síť, která se stala základem pro moderní internet.[9]

V 80. letech se objevily první počítačové viry. V roce 1988 byl vytvořen Morrisův červ, první červ, který se šířil po internetu.[10]

S nástupem internetu se tak kybernetické útoky staly čím dál tím častější a sofistikovanější.

V České republice se kybernetická bezpečnost stala prioritou až v posledních letech. Vláda přijala řadu opatření k posílení ochrany před kybernetickými útoky, včetně Strategie pro oblast kybernetické bezpečnosti České republiky. V roce 2017 byl zřízen Národní úřad pro kybernetickou a informační bezpečnost (NUKIB).[11]Dopad útoků se tak v kybernetickém prostoru v posledních letech výrazně zvýšil.

Podle Požárova teoretického vymezení lze bezpečnost chápat jako charakteristiku objektu či subjektu, která reflektuje úroveň jeho zabezpečení před

[8]FELL, Jade. *Hacking through the years: a brief history of cybercrime*. Online. The Institution of Engineering and Technology. 2017. Dostupné z: https://eandt.theiet.org/2017/03/13/hacking-through-years-brief-history-cyber-crime. [cit. 2025-02-09].

[9]ZELENÝ, Jaroslav a MANNOVÁ, Božená. *Historie výpočetní techniky*.1. vydání. Praha: Scientia, 2006. ISBN 80-86960-04-8.

[10]PAGE, Bob. *A Report on the internet Worm.* Online. Toronto Metropolitan University. 1988, 2024. Dostupné z: https://www.ee.torontomu.ca/~elf/hack/iworm.html. [cit. 2025-02-09].

[11]NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Slavnostní setkání k 5. výroční založení NÚKIB.* Online. 2022. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/1859-slavnostni-setkani-k-5-vyrocni-zalozeni-nukib/. [cit. 2025-02-09].

potenciálními hrozbami či škodlivými vlivy. Jinými slovy, míra bezpečnosti je vyjádřením rozsahu ochrany, již daný subjekt disponuje vůči identifikovaným rizikům.[12]

2.4 Kyberprostor

Kyberprostor se stal neodmyslitelnou součástí moderní společnosti a jeho fenomenální vliv na lidskou společnost neustále roste.

Pojem kyberprostor (Cyberspace), ačkoliv se s ním dnes setkáváme na denní bázi, nemá jednoznačnou a univerzálně přijímanou definici. Jeho původ sahá do 80. let 20. století, kdy jej spisovatel William Gibson ve svém díle Neuromancer zpopularizoval jako „sdílenou halucinaci“ – nehmotný svět propojených informací a komunikace.[13]

S rozvojem informačních a komunikačních technologií se kyberprostor stal nedílnou součástí moderní společnosti.

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti jej definuje jako digitální prostředí, které umožňuje vytváření, zpracovávání a sdílení informací prostřednictvím informačních systémů, elektronických komunikací a souvisejících služeb.[14]

Je důležité si uvědomit, že ačkoliv je kyberprostor nehmotný, jeho existence je pevně spjata s fyzickým světem a internetovou infrastrukturou. Často se setkáváme s nesprávným ztotožňováním kyberprostoru s internetem. Ve skutečnosti je kyberprostor širším pojmem, který internet zahrnuje, ale zároveň jej přesahuje o další aspekty digitální interakce.

Vznik a vývoj internetu, který tvoří materiální základnu kyberprostoru, se datuje do 50. let 20. století. Vznikl z vojenských a vědeckých projektů (ARPANET

[12]POŽÁR, Josef. *Informační bezpečnost*. Vysokoškolské učebnice. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. s.37.ISBN 80-86898-38-5.

[13]CHRISTENSSON, Per. *Cyberspace Definition*. Online. SHARPENED PRODUCTIONS. TechTerms.com. 2024. Dostupné z: https://techterms.com/definition/cyberspace. [cit. 2025-02-10].

[14]MINISTERSTVO VNITRA ČR. *Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).* 2014. Dostupné z: https://www.e-sbirka.cz/sb/2014/181?zalozka=text. [cit. 2025-02-09].

a NSFNET) a stále se jedná o decentralizovanou síť bez centrálního řízení a vlastnictví.[15]

Kromě pojmu kyberprostor se v odborné literatuře objevují i další související termíny, jako například digitální prostor (digital space) nebo informační prostředí (information environment). Zatímco kyberprostor klade důraz na propojenost informačních systémů a jejich interakci, digitální prostor se často zaměřuje na technologickou infrastrukturu a digitální obsah jako takový. Informační prostředí zase zahrnuje širší kontext, včetně sociálních, politických a ekonomických aspektů ovlivňujících tok informací.

Kyberprostor lze chápat jako „globální doménu, kde státy pronikají do počítačových sítí za účelem způsobení škody nebo narušení“, což jej odlišuje od užšího pojetí internetu a zdůrazňuje jeho strategický význam.[16]

Diskuze o těchto pojmech není pouze akademickou otázkou, ale má praktické důsledky pro oblast kybernetické bezpečnosti. Pokud například chápeme kyberprostor pouze jako synonymum pro internet, může to vést k podcenění rizik spojených s jinými digitálními interakcemi, jako jsou uzavřené sítě nebo IoT (Internet věcí). Osobně zastávám názor, že širší pojetí kyberprostoru, jak je definováno v českém zákoně o kybernetické bezpečnosti, je pro účely analýzy hrozeb v České republice přínosnější, protože zohledňuje komplexnost digitálního prostředí a jeho propojení s fyzickou infrastrukturou.

Podle studie od Libickiho, který se zabývá kyberprostorem z hlediska vojenské strategie, je kyberprostor tvořen třemi vrstvami: fyzickou (hardware a infrastruktura), syntaktickou (protokoly a kódy) a sémantickou (informace a jejich význam).[17]

Zmíněná studie tak zdůrazňuje, že kyberprostor není pouze technologickým fenoménem, ale i sociálním a informačním konstruktem. Tento přístup má význam i pro pochopení kybernetické bezpečnosti v České republice.

---

[15]KOLOUCH, Jan. *CyberCrime*. Online. CZ.NIC, 2016. ISBN 978-80-88168-15-7. Dostupné zhttps://knihy.nic.cz/cs/detail/14/. [cit. 2025-02-09].

[16]A. CLARKE, Richard a KNAKE, Robert. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Ecco, 2011. ISBN 978-0061962240.

[17]LIBICKI, Martin C. *Conquest in Cyberspace: National Security and Information Warfare.* New York: Cambridge University Press, 2007. ISBN 978-0-521-69214-4.

Například fyzická vrstva kyberprostoru, tedy kritická infrastruktura, je v ČR regulována Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB), zatímco sémantická vrstva – například dezinformace – představuje rostoucí hrozbu, která vyžaduje koordinaci mezi státními i nestátními aktéry. Libickiho model tedy nabízí užitečný rámec pro analýzu, protože ukazuje, jak různé aspekty kyberprostoru vyžadují odlišné přístupy k zajištění bezpečnosti. Z mého pohledu by tento vícevrstvý přístup mohl být v českém kontextu dále rozpracován, zejména s ohledem na rostoucí digitalizaci veřejné správy a její zranitelnost vůči hybridním hrozbám.

Zatímco v minulosti se kybernetická kriminalita soustředila především na narušení provozu počítačových systémů, zneužívání telefonních sítí, páchání podvodů či neoprávněné nakládání s osobními daty, současný vývoj ukazuje výrazný posun směrem k sofistikovanějším formám útoků. V současné době se kybernetická trestná činnost stále častěji zaměřuje na klíčové prvky státní správy a infrastruktury. Prostřednictvím moderních informačních a komunikačních technologií mohou útočníci zasahovat do fungování finančních institucí, energetických sítí, dopravních systémů či dokonce obranných struktur jiných států, čímž představují vážnou hrozbu pro národní i mezinárodní bezpečnost.[18]

[18]SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. s.105.ISBN 8073808498.

3 Kybernetická bezpečnost v České republice

Česká republika se v oblasti kybernetické bezpečnosti potýká se specifickými výzvami, které vyžadují komplexní a proaktivní přístup. Rostoucí propojenost digitálního a fyzického světa s sebou nese zvýšené riziko kybernetických útoků s potenciálně závažnými dopady na kritickou infrastrukturu, ekonomiku i společnost jako celek.

3.1 Vývoj kybernetické bezpečnosti v České republice

Vývoj kybernetické bezpečnosti v České republice prošel v posledních desetiletích dynamickým vývojem, reagujícím na rostoucí míru digitalizace společnosti a s ní spojená rizika.

V počáteční fázi, která se datuje do 90. let 20. století, se kybernetická bezpečnost v České republice teprve formovala. S rostoucí dostupností internetu a informačních technologií se začaly objevovat první kybernetické incidenty. V této době se jednalo spíše o ojedinělé případy s nízkou mírou sofistikovanosti, často motivované spíše zvědavostí a experimentováním než snahou o finanční zisk či způsobení škody.

Vláda a instituce si postupně začaly uvědomovat význam kybernetické bezpečnosti, avšak jejich reakce na nové hrozby v 90. letech byla pomalá. Přesto podnikaly první kroky k jejímu zajištění, například formou vzdělávacích programů a osvěty. V druhé polovině 90. let vyšla vláda ČR vstříc tlaku médií a schválila zákon o počítačové bezpečnosti. V roce 1997 vyšel v ČR první antivirový program, který měl ochraňovat počítače před šířením počítačových virů.[19]

Přelom tisíciletí přinesl nárůst kybernetické kriminality a sofistikovanějších útoků. Do popředí se dostaly hrozby jako krádeže identity, finanční podvody a útoky na dostupnost systémů (DDoS útoky). V této době se začal prosazovat mezinárodní bezpečnostní standard ISO/IEC 27002, který od roku 1995 neustále vylepšuje své postupy. Na přelomu tisíciletí také došlo k posunu v motivaci kybernetických útoků,

[19]ČESKÉ RADIOKOMUNIKACE A.S. *Kybernetická bezpečnost: Sedm fází kybernetického útoku*. Online. CRA.cz. 2021. Dostupné z: https://www.cra.cz/kyberneticka-bezpecnost-sedm-fazi-kybernetickeho-utoku. [cit. 2025-02-09].

od zvědavosti a experimentování v 90. letech k finančnímu zisku a způsobení škody.[20]

V dalších letech identifikoval NUKIB dva významné útoky na Českou republiku. Prvním byl útok botnetu Pony v březnu 2014, který ukradl uživatelská data z více než 700 000 účtů. Druhým byl útok spywaru Turla (Uroburos, Snake, Carbon) v březnu 2014, který ukradl data z potenciálně stovek počítačů ve více než 45 zemích.[21]

V roce 2010 Česká republika přijala usnesení o řešení problematiky kybernetické bezpečnosti a ustavila Ministerstvo vnitra České republiky jako autora a zároveň i autoritu kybernetické bezpečnosti. Téhož roku vláda přijala další usnesení, kterým se zřizuje Mezi-resortní koordinační rada pro oblast kybernetické bezpečnosti. Na konci roku 2010 vznikl Národní Computer Security Incident Response Team (Národní CSIRT), který poskytuje proaktivní služby v oblasti bezpečnosti, řešení a koordinaci řešení bezpečnostních incidentů, a hlavně osvětovou a školící činnost v oblasti kybernetické bezpečnosti. V roce 2011 bylo přijato usnesení vlády, kterým byla mimo jiné schválena Strategie pro oblast kybernetické bezpečnosti České republiky pro období 2011 až 2015.[22]

Významným milníkem byl rok 2014, kdy byl v České republice přijat již zmíněný zákon o kybernetické bezpečnosti. Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů je první komplexní právní úpravou v oblasti kybernetické bezpečnosti v České republice.[23]

Zákon mimo jiné určuje povinnosti pro vybrané veřejné a soukromé orgány a osoby k zajištění bezpečnosti jejich kybernetické a informační infrastruktury. Zákon také upravuje působnost NÚKIB v oblasti koordinace a dozoru nad zajištěním kybernetické bezpečnosti ČR. V Brně bylo také otevřeno Národní centrum kybernetické bezpečnosti (NCKB). Dopad kyberkriminality na české hospodářství se

[20]ČESKÉ RADIOKOMUNIKACE A.S. *Kybernetická bezpečnost: Sedm fází kybernetického útoku.* Online. CRA.cz. 2021. Dostupné z: https://www.cra.cz/kyberneticka-bezpecnost-sedm-fazi-kybernetickeho-utoku. [cit. 2025-02-09].

[21]*Osnova strategie kybernetické bezpečnosti České republiky: Zpráva o stavu kybernetické bezpečnosti České republiky 2014.* Online. 2014, s. 40. Dostupné z: NUKIB, https://nukib.gov.cz/download/publikace/zpravy_o_stavu/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2014.pdf. [cit. 2025-02-09].

[22]HOLAKOVSKÝ, Jiří. *Kybernetická bezpečnost v České republice*. Bakalářská práce, vedoucí Ing. Michaela Henzlová Ph.D. Praha: AMBIS vysoká škola, a.s, 2022. Dostupné také z: https://is.ambis.cz/th/auw08/Bakalarska_prace_-_Jiri_Holakovsky_.pdf.

[23]MINISTERSTVO VNITRA ČR. *Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. 2014. Dostupné z: https://www.e-sbirka.cz/sb/2014/181?zalozka=text. [cit. 2025-02-09].

v období let 2013–2017 zpětinásobil a v roce 2021 vzrostl o 600 procent. Zákon o kybernetické bezpečnosti byl novelizován v roce 2017 zákonem č. 205/2017 Sb.[24]

V posledních letech se kybernetické hrozby stávají stále sofistikovanějšími a komplexnějšími. V roce 2023 došlo k nárůstu kybernetických incidentů a státem podporovaných operací, což představuje významnou výzvu pro Českou republiku. Mezi aktuální trendy patří nárůst ransomwarových útoků, phishingových kampaní a zneužívání umělé inteligence k vytváření škodlivého kódu. Phishingové kampaně v roce 2023 dosáhly nové úrovně sofistikovanosti a rozšířily se do forem jako vishing, smishing a quishing. Konflikt na Ukrajině zhoršil geopolitické napětí a vedl k nárůstu sofistikovaných kybernetických útoků mimo jiné i na Českou republiku. V roce 2023 byla Česká republika svědkem rekordního počtu kybernetických bezpečnostních incidentů. Velkým nebezpečím zůstávají aktivity útočníků sponzorovaných státem, zejména z Ruska. Vláda a soukromé společnosti v ČR však podnikly kroky k posílení kybernetické bezpečnosti, například posílením zákona o kybernetické bezpečnosti a zahájením osvětových kampaní zaměřených na prevenci phishingu a ochranu proti DDoS.[25]

Příkladem závažného kybernetického incidentu v roce 2023 byl ransomwarový útok na Univerzitu obrany v Brně. Tento útok zdůraznil strategický význam cíle, evoluci ransomwarových taktik, důležitost robustních zálohovacích postupů a potenciální dlouhodobé bezpečnostní důsledky úniku citlivých dat.[26]

V roce 2023 došlo k výraznému nárůstu kybernetických útoků v České republice. NÚKIB zaznamenal celkem 262 incidentů. Hlavní příčinou tohoto nárůstu byly opakované vlny DDoS útoků, které byly vedeny především proruskými hacktivistickými skupinami.[27]

---

[24]MINISTERSTVO VNITRA ČR. *Zákon č. 205/2017 Sb.: Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů*. 2017. Dostupné z: https://www.e-sbirka.cz/sb/2017/205?zalozka=text. [cit. 2025-02-09].

[25]ORTMANN, Matyáš. *Kybernetická bezpečnost České republiky v roce 2023: Výzvy a trendy*. Online. CZECH ARMY & DEFENCE MAGAZINE. CZDEFENCE.cz. Praha, 2024. Dostupné z: https://www.czdefence.cz/clanek/kyberneticka-bezpecnost-ceske-republiky-v-roce-2023-vyzvy-a-trendy. [cit. 2025-02-09].

[26]ORTMANN, Matyáš. *Kybernetická bezpečnost České republiky v roce 2023: Výzvy a trendy*. Online. CZECH ARMY & DEFENCE MAGAZINE. CZDEFENCE.cz. Praha, 2024. Dostupné z: https://www.czdefence.cz/clanek/kyberneticka-bezpecnost-ceske-republiky-v-roce-2023-vyzvy-a-trendy. [cit. 2025-02-09].

[27]NÚKIB. NÚKIB v roce 2023 zaznamenal rekordní počet kybernetických incidentů. Online. NÚKIB. Praha, 2024. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/2073-nukib-v-roce-2023-zaznamenal-rekordni-pocet-kybernetickych-incidentu/. [cit. 2025-02-09].

Vývoj kybernetické bezpečnosti v České republice od 90. let prošel výraznou proměnou. Zpočátku šlo o izolované incidenty motivované zvědavostí, ale s rozvojem internetu a digitalizace narostla i sofistikovanost útoků, zaměřených na krádeže identity, finanční podvody a útoky na systémy. Vláda na situaci reagovala postupně – v roce 2010 vznikl Národní CSIRT a v roce 2014 byl přijat zákon o kybernetické bezpečnosti. Přesto se s rostoucím technologickým pokrokem ukazuje, že legislativa a bezpečnostní opatření jsou často o krok pozadu.

V posledních letech počet kybernetických incidentů narůstá, přičemž hlavními hrozbami jsou ransomwarové útoky, phishingové kampaně a Ruskem podporované hackerské aktivity. Konflikt na Ukrajině vedl i k nárůstu sofistikovaných útoků na české instituce, včetně škol a státních úřadů. Rekordní počet kybernetických útoků v roce 2023 ukázal závažnost problému. Vláda a soukromé firmy proto posilují obranná opatření, například novelizací zákona o kybernetické bezpečnosti a osvětovými kampaněmi, ale výzvy v oblasti kybernetické bezpečnosti stále rostou.

3.2 Národní strategie kybernetické bezpečnosti ČR 2021-2025

Problematika kybernetické bezpečnosti v České republice spadá od 1. srpna 2017 do kompetence samostatné instituce – Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Tento úřad vznikl vyčleněním oblasti kybernetické bezpečnosti z působnosti Národního bezpečnostního úřadu (NBÚ), čímž došlo k institucionalizaci specializovaného přístupu k této oblasti. NÚKIB od té doby zajišťuje veškeré úkoly a odpovědnosti, které dříve vykonávala jeho organizační složka působící pod NBÚ, konkrétně Národní centrum kybernetické bezpečnosti.[28]

Národní strategie kybernetické bezpečnosti ČR 2021-2025 představuje komplexní rámec pro zajištění bezpečnosti České republiky v kyberprostoru. Strategie si klade za cíl dosáhnout vysoké úrovně kybernetické bezpečnosti a vytvořit bezpečné digitální prostředí pro občany, podniky i státní instituce. Vychází ze tří základních vizí: **důvěra v kyberprostor**, **silná a spolehlivá partnerství** a **odolná**

[28]DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019.s.65. ISBN 978-80-88260-39-4.

Společnost 4.0. Tyto vize reflektují strategické směřování naší země s časovým horizontem sahajícím do nadcházejících let a zdůrazňují nezbytnost holistického přístupu ke kybernetické bezpečnosti.

Kromě zmíněných oblastí strategie zahrnuje i další důležitá hlediska, která jsou klíčová pro efektivní zajištění kybernetické bezpečnosti:

- **Technické:** Strategie klade důraz na modernizaci technické infrastruktury, zavádění nových bezpečnostních technologií a standardů, a také na rozvoj schopností detekce a reakce na kybernetické incidenty.
- **Personální:** Strategie si uvědomuje potřebu kvalifikovaných odborníků v oblasti kybernetické bezpečnosti. Proto podporuje vzdělávání a odbornou přípravu, a také rozvoj kariérních možností v tomto oboru.
- **Sociální:** Kybernetická bezpečnost není jen technická záležitost, ale také sociální. Strategie se proto zaměřuje na zvyšování povědomí o kybernetických hrozbách a na podporu bezpečného chování v online prostředí.
- **Legislativní:** Pro efektivní boj s kybernetickými hrozbami je nezbytný adekvátní právní rámec. Strategie proto usiluje o aktualizaci a harmonizaci legislativy v oblasti kybernetické bezpečnosti.
- **Vzdělávací:** Vzdělávání uživatelů internetu hraje zásadní roli. Zvyšuje se informovanost uživatelů, a tím se snižuje riziko napadení.[29]

Kyberprostor a moderní technologie se staly nedílnou součástí našich životů a v roce 2020 se zájmy České republiky staly vitálně závislé na bezpečném kyberprostoru. Strategie se zaměřuje na klíčové oblasti, jako je ochrana kritické infrastruktury, vzdělávání v oblasti kybernetické bezpečnosti a mezinárodní spolupráce. Klíčovým prvkem je budování národního přístupu ke kybernetické bezpečnosti, založeného na sdílení informací a spolupráci mezi všemi relevantními aktéry.

[29]MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR. *Národní strategie kybernetické bezpečnosti ČR 2021-2025*. Online. DATABÁZE STRATEGIÍ. Databaze-strategie.cz. Praha: Ministerstvo pro místní rozvoj ČR. Dostupné z: https://www.databaze-strategie.cz/cz/narodni-urad-pro-kybernetickou-a-informacni-bezpecnost/strategie/narodni-strategie-kyberneticke-bezpecnosti-cr-2021-2025?typ=struktura. [cit. 2025-02-10].

3.3 Právní aspekty kybernetické bezpečnosti

Právní aspekty kybernetické bezpečnosti v České republice jsou pevně ukotveny v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti.[30] Tento zákon definuje základní povinnosti pro subjekty kritické informační infrastruktury, jako jsou poskytovatelé energií, vodárenství, dopravy a dalších klíčových služeb. Zákon subjektům ukládá povinnost přijmout opatření k zajištění kybernetické bezpečnosti svých systémů a hlásit kybernetické incidenty NÚKIB.

Dále je nutné zmínit směrnici Evropské unie NIS2, která přináší nová pravidla pro kybernetickou bezpečnost a rozšiřuje okruh povinných subjektů.

Směrnice klade důraz na prevenci kybernetických útoků, řízení rizik a posílení odolnosti subjektů. Implementace směrnice NIS2 do českého právního řádu si vyžádá novelizaci stávajícího zákona o kybernetické bezpečnosti. Česká právní úprava v oblasti kybernetické bezpečnosti se neustále vyvíjí s ohledem na dynamický charakter kybernetických hrozeb a technologický pokrok.

[30]MINISTERSTVO VNITRA ČR. *Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).* 2014. Dostupné z: https://www.e-sbirka.cz/sb/2014/181?zalozka=text. [cit. 2025-02-09].

4 Kybernetické útoky

Kybernetické útoky představují stále závažnější hrozbu, přičemž jejich sofistikovanost se neustále vyvíjí. Útočníci stále častěji využívají umělou inteligenci k automatizaci útoků, vývoji pokročilého malwaru a zdokonalování technik sociálního inženýrství.

Motivace těchto útoků se pohybuje od finančního zisku přes kybernetickou špionáž až po prosazování geopolitických zájmů. Mezi nejrozšířenější formy kybernetických útoků patří malware, phishing, ransomware, DDoS útoky, spam a zneužití umělé inteligence k narušení bezpečnostních systémů.

4.1 Druhy kybernetických útoků

Kybernetické útoky lze rozdělit do několika kategorií. Mezi nejvýznamnější útoky v ČR podle NÚKIB patří **malware**, který zahrnuje škodlivé programy jako ransomware či trojské koně, jejichž cílem je narušit bezpečnost systémů. **Phishing** využívá falešné e-maily či weby k získání citlivých údajů, zatímco **DDoS** útoky přetížením serverů znemožňují dostupnost online služeb. **Spam** představuje masové rozesílání nevyžádaných zpráv, často obsahujících odkazy na podvodné weby. **Brute force útoky** se snaží prolomit hesla systematickým zkoušením kombinací. Moderní hrozbou jsou také útoky využívající **umělou inteligenci**, která umožňuje efektivnější manipulaci s uživateli a obcházení bezpečnostních opatření.[31]

Kybernetické útoky rozdělujeme podle jejich způsobu fungování. Malware zahrnuje škodlivé programy, které narušují bezpečnost systémů. Phishing se zaměřuje na získání citlivých údajů prostřednictvím falešných zpráv a webů. DDoS útoky přetěžují servery, čímž blokují přístup k online službám. Spam šíří nevyžádané zprávy s podvodnými odkazy a brute force útoky se snaží prolomit hesla opakovaným zkoušením.

Novou hrozbou je využití umělé inteligence, která umožňuje sofistikovanější způsoby manipulace a obcházení bezpečnostních opatření.

[31]NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022*. PDF. Praha, 2023. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf. [cit. 2025-03-02].

4.1.1 Malware

Malware neboli škodlivý software, představuje širokou škálu programů a kódů, jejichž primárním účelem je narušit integritu, důvěrnost nebo dostupnost informačních systémů. Tato hrozba zahrnuje viry, červy, trojské koně, ransomware, spyware a další formy škodlivého kódu. Analýza malwaru je klíčovým procesem v oblasti kybernetické bezpečnosti, který umožňuje identifikovat chování, původ a potenciální dopad škodlivého softwaru. Analýza malwaru se zaměřuje na zkoumání technik, které útočníci používají, a na vývoj metod pro rychlou identifikaci a neutralizaci hrozeb.[32]

Důležitým aspektem je proces rychlého posouzení a kategorizace malware, který umožňuje určit další kroky v reakci na incident.

4.1.2 Phishing

Phishing je kybernetický podvod zaměřený na získání citlivých údajů, jako jsou hesla či čísla platebních karet. Útočníci využívají psychologickou manipulaci, například naléhavé zprávy o výhrách či neuhrazených platbách. Phishingové e-maily často obsahují odkazy na falešné weby, kde oběti zadávají své údaje. Moderní útoky jsou sofistikované a obtížněji rozpoznatelné. Úspěšnost phishingu dosahuje až 65 %, což dokládá jeho nebezpečnost.[33]

Phishing je velmi nebezpečná forma online podvodu, která cílí na neopatrné uživatele internetu a využívá jejich důvěřivosti či strachu. Útočníci se vydávají za důvěryhodné instituce a lákají oběti na podvodné odkazy či falešné stránky, kde získávají citlivé údaje. Vzhledem k rostoucí sofistikovanosti těchto útoků je důležitá obezřetnost, ověřovat odesílatele e-mailů a nikdy nezadávat své přihlašovací údaje na podezřelých webech a aplikacích.

4.1.3 DDoS

DDoS útoky (Distributed Denial of Service) jsou koordinované kybernetické útoky, které využívají síť kompromitovaných zařízení k zahlcení cílového serveru

[32]BARKER, Dylan. *Malware Analysis Techniques: Tricks for the triage of adversarial software.* Birmingham: Packt, 2021. ISBN 978-1-83921-227-7.

[33]MATĚJÍČEK, Pavel. *SPAM versus Phishing a jejich problematika ve školním prostředí*. Online. MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY (MŠMT). EDU.cz. Dostupné z: https://edu.gov.cz/spam-versus-phishing-a-jejich-problematika-ve-skolnim-prostredi/. [cit. 2025-03-02].

nadměrným provozem, což vede k jeho nedostupnosti. Existují různé typy těchto útoků, včetně volumetrických, aplikačních a protokolových. Obrana spočívá v kombinaci filtrace, analýzy provozu a distribuovaných systémů mitigace, které pomáhají minimalizovat dopady útoku.[34]

Tyto útoky patří mezi nejzávažnější kybernetické hrozby, protože mohou zcela paralyzovat cílový server či síť. Útočníci využívají velké množství zařízení k vytvoření extrémního datového provozu, čímž způsobí přetížení a nedostupnost služby. Obrana proti těmto útokům vyžaduje pokročilé filtrační mechanismy a analýzu provozu, které pomáhají rozpoznat a zmírnit jejich dopad.

4.1.4 SPAM

SPAM je označení pro nevyžádané zprávy, které mohou být šířeny nejen prostřednictvím e-mailu, ale také přes sociální sítě, SMS nebo jiné komunikační kanály. Typickým příkladem jsou reklamní nabídky na různé produkty či služby. Název „SPAM“ pochází původně z USA, kde byl spojen s masovou distribucí reklam na šunku. Ačkoli je většina SPAMu neškodná, některé zprávy mohou obsahovat škodlivé odkazy nebo podvodné nabídky. Nejlepší obranou proti SPAMu je aktivní používání antispamových filtrů a označování nežádoucích zpráv, což pomáhá systémům v jejich efektivním rozpoznávání.[35]

Nevyžádaná pošta, označovaná jako spam, představuje nejen rušivý prvek pro příjemce, ale zároveň zatěžuje kapacity síťové infrastruktury a omezuje dostupné úložiště elektronické pošty. Její přítomnost negativně ovlivňuje efektivitu elektronické komunikace a může přispívat ke snížení celkového výkonu e-mailových systémů.[36]

SPAM je běžným problémem digitální komunikace, kdy uživatelé dostávají nevyžádané zprávy, často s reklamním nebo podvodným obsahem. Ačkoli většina těchto zpráv jen obtěžuje, některé mohou obsahovat škodlivé odkazy či malware.

[34]BHATTACHARYYA, Dhruba K. a KALITA, Jugal Kumar. *DDoS Attacks: evolution, detection, prevention, reaction, and tolerance*. Boca Raton: CRC Press, Taylor & Francis Group, 2016. ISBN 978-1-4987-2964-2.

[35]MATĚJÍČEK, Pavel. *SPAM versus Phishing a jejich problematika ve školním prostředí*. Online. MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY (MŠMT). EDU.cz. Dostupné z: https://edu.gov.cz/spam-versus-phishing-a-jejich-problematika-ve-skolnim-prostredi/. [cit. 2025-03-02].

[36]PANDE, J. *Introduction to Cyber Security*. Haldwani: Uttarakhand Open University, 2017, s. 23. ISBN 978-93-84813-96-3.

Proto je důležité využívat antispamové filtry a označovat podezřelé e-maily, aby se minimalizovalo jejich šíření a snížilo riziko kybernetických hrozeb.

4.1.5 Brute-force attack

Útok hrubou silou (brute-force attack) je kybernetická technika, při níž útočník automatizovaně testuje různé kombinace hesel či šifrovacích klíčů k prolomení zabezpečení. Tento typ útoku využívá výpočetní sílu k systematickému ověřování přihlašovacích údajů, dokud není nalezena správná kombinace. Mezi běžné metody patří jednoduché útoky hrubou silou, testující běžná hesla, slovníkové útoky, využívající databáze častých hesel, a hybridní útoky, které kombinují obě metody. Útočníci také používají reverzní útoky, kdy začínají známým heslem a hledají odpovídající účty. Obrana spočívá v používání silných hesel, vícefaktorové autentizace a omezení počtu přihlašovacích pokusů.[37]

Jde o významnou hrozbu pro kybernetickou bezpečnost, neboť útočníci využívají systematického testování přihlašovacích údajů k neoprávněnému přístupu do systémů. Jejich efektivita se odvíjí od výpočetního výkonu útočníka a síly použitých hesel. Vzhledem k rostoucímu využívání těchto technik je zásadní implementace preventivních opatření, například vícefaktorové autentizace, omezení přihlašovacích pokusů na zařízení a používání silných hesel, což výrazně snižuje riziko úspěšného útoku.

4.1.6 Útok s AI

Umělá inteligence (AI) v kybernetické bezpečnosti představuje klíčový nástroj pro detekci a prevenci kybernetických útoků. Díky schopnosti analyzovat velké množství dat a učit se z předchozích incidentů dokáže AI identifikovat podezřelé aktivity, detekovat phishingové útoky a rozpoznávat nové varianty malware. Její využití umožňuje rychlejší reakci na hrozby a posiluje obranyschopnost systémů proti „zero-day“ útokům, které využívají dosud neznámé zranitelnosti. AI však nepředstavuje pouze obranný mechanismus, ale může být i nástrojem kyberzločinců, kteří ji využívají k automatizaci útoků, generování škodlivého kódu a zvyšování efektivity phishingových kampaní. Rychlý

[37]FORTINET. *What Is A Brute Force Attack?* Online. Fortinet.com. Dostupné z: https://www.fortinet.com/resources/cyberglossary/brute-force-attack. [cit. 2025-03-01].

technologický vývoj naznačuje, že AI se v budoucnosti stane nejen nepostradatelným spojencem bezpečnostních expertů, ale i významnou výzvou pro ochranu digitálních systémů.[38]

Využití AI v kybernetické bezpečnosti představuje významný pokrok v detekci a eliminaci kybernetických hrozeb. Umožňuje efektivní analýzu dat, rozpoznávání vzorců útoků a rychlou reakci na nové hrozby, tím posiluje obranyschopnost digitálních systémů. Zároveň ale přináší i nové bezpečnostní výzvy, neboť její technologie mohou být zneužity kyberzločinci k automatizaci a škálování útoků. Vzhledem k neustálému vývoji je proto klíčové nejen rozvíjet její obranné schopnosti, ale také hledat účinné strategie pro minimalizaci jejího potenciálního zneužití.

4.2 Kdo je hacker a kdo je oběť kybernetických útoků

Globální společnost ESET, specializující se na digitální zabezpečení, definuje hackera následovně: *„Hacker je člověk, který využívá své počítačové znalosti a dovednosti k odhalování chyb a zranitelností v počítačových systémech“*.[39]

Oběť kybernetických útoků lze definovat jako subjekty, které v důsledku škodlivého jednání v kyberprostoru utrpěly materiální či nemateriální ztráty. Tato kategorie zahrnuje široké spektrum aktérů, od individuálních uživatelů internetu, kteří se stávají oběťmi phishingových útoků a krádeží identity, přes malé a střední podniky, jež jsou vzhledem k omezeným zdrojům často cílem ransomwarových útoků, až po velké korporace a státní instituce, které čelí sofistikovaným útokům na servery, průmyslové špionáži či DDoS útokům.[40]

Společnost ESET definuje hackera jako jedince využívajícího své znalosti k identifikaci zranitelností v počítačových systémech, což může mít jak legitimní, tak škodlivé využití.

Kybernetické útoky postihují široké spektrum subjektů, od jednotlivců vystavených phishingu a krádeži identity po korporace a státní instituce čelící

[38]BREJCHA, Pavel. *AI jako (ne)přítel v kybernetické bezpečnosti*. Online. MASARYKOVA UNIVERZITA. Security.muni.cz. 2024. Dostupné z: https://security.muni.cz/clanky/ai-jako-nepritel-v-kyberneticke-bezpecnosti. [cit. 2025-03-02].

[39]ESET. *Hacker: Kdo je hacker?* Online. ESET. Dostupné z: https://www.eset.com/cz/hacker/. [cit. 2025-03-02].

[40]ČESKÉ RADIOKOMUNIKACE a.s. *Kybernetická bezpečnost: Sedm fází kybernetického útoku*. Online. Dostupné z: https://www.cra.cz/kyberneticka-bezpecnost-sedm-fazi-kybernetickeho-utoku. [cit. 2025-03-02].

ransomwarovým a DDoS útokům. Vzhledem k rostoucí sofistikovanosti hrozeb je nezbytné rozvíjet efektivní a robustní strategie kybernetické obrany a prevence.

4.2.1 Hacker

Hacker využívá své znalosti informačních technologií k identifikaci a manipulaci s počítačovými systémy. V závislosti na motivech a způsobu činnosti se dělí do několika kategorií. **Black hat** hackeři zneužívají zranitelnosti systémů k nelegálním aktivitám, jako je krádež dat či sabotáže. Naopak **white hat** hackeři, známí také jako etičtí hackeři, testují zabezpečení systémů na žádost organizací s cílem posílit jejich obranu. Podobnou roli mají **blue hat** hackeři, kteří jako externí konzultanti prověřují zabezpečení systémů před jejich uvedením do provozu. **Red hat** hackeři bojují proti kyberzločincům, přičemž někdy využívají podobné metody jako black hat hackeři, což je staví na hranici legality. Existují i **gray hat** hackeři, kteří sice nejednají s úmyslem škodit, ale často obcházejí etické normy či zákony. Specifickou skupinu tvoří **green hat** hackeři, tedy začátečníci, kteří se učí principům hackingu a kybernetické bezpečnosti.[41]

Historicky je hackerství spojeno s inovacemi a technologickým průzkumem, avšak s postupem času došlo k rozdělení hackerů na etické odborníky a kyberzločince, což vedlo ke vzniku odlišných přístupů k využívání hackerských dovedností.

4.2.2 Oběť kybernetického útoku

Kybernetické útoky si nevybírají – obětí se může stát prakticky kdokoli, od jednotlivců a firem až po celý stát.[42]

Žádná společnost, instituce ani běžný uživatel internetu není vůči kybernetickým útokům zcela imunní. Tato realita potvrzuje, že otázka kybernetické bezpečnosti se týká každého bez ohledu na velikost či význam.

[41]ESET. *Hacker: Kdo je hacker?* Online. ESET. Dostupné z: https://www.eset.com/cz/hacker/. [cit. 2025-03-02].

[42]CZ.NIC. *O seriálu "Jak na internet": Máme se bát kybernetických útoků?* Online. Dostupné z: https://www.jaknainternet.cz/page/3031/mame-se-bat-kybernetickych-utoku/. [cit. 2025-03-02].

5 Kybernetické incidenty v České republice

Od roku 2020 čelí Česká republika rostoucímu počtu kybernetických útoků, které zasáhly klíčové instituce, jako jsou nemocnice, státní úřady či dopravní infrastruktura. Nejvážnějším případem byl útok na Fakultní nemocnici Brno, který ochromil její provoz během pandemie. Následovaly i špionážní a ransomwarové útoky, například na Ministerstvo vnitra nebo ŘSD.

Významným momentem byla také vlna DDoS útoků v roce 2022, za nimiž stála proruská skupina Killnet. Tyto incidenty ukázaly zranitelnost státní správy i důležitost posilování kybernetické bezpečnosti. Reakcí je větší důraz na prevenci, zapojení NÚKIB a posilování ochrany informačních systémů.

5.1 Kybernetický útok na Fakultní nemocnici Brno

V polovině března 2020 došlo k závažnému kybernetickému incidentu, který ochromil provoz jedné z největších zdravotnických institucí v České republice – Fakultní nemocnice Brno. Událost se odehrála krátce po vyhlášení nouzového stavu kvůli pandemii COVID-19 a výrazně narušila běžné fungování nemocnice.

Předmětem útoku byl ransomware, který útočníkům umožnil zašifrovat rozsáhlou část serverové infrastruktury. Dotčeny byly klíčové databáze a systémy zajišťující jak administrativní, tak medicínské procesy. Narušení provozu mělo okamžitý dopad – vedení bylo nuceno vypnout veškerou výpočetní techniku, přerušit plánované zákroky a přejít na krizový režim.

Zvláště závažným důsledkem útoku byla ztráta dat a nedostupnost záloh, což znemožnilo rychlou obnovu. I přes intenzivní snahu IT odborníků trvalo znovu zprovoznění základních systémů několik týdnů, přičemž úplná obnova trvala výrazně déle. Některé informace, zejména z oblasti ekonomické agendy, se nepodařilo zachránit vůbec. Finanční škody dosáhly výše desítek milionů korun.

Tento incident je často označován za dosud nejvážnější případ narušení kybernetické bezpečnosti ve zdravotnictví v historii České republiky. Vyšetřování,

které následovalo, pachatele sice neidentifikovalo, avšak analýzy bezpečnostních složek naznačily pravděpodobné zapojení aktérů ze zahraničí – konkrétně z ruského kyberprostoru.[43]

5.2 Kybernetický útok na e-mailové servery Ministerstva vnitra

V prvním čtvrtletí roku 2021 se Česká republika stala součástí rozsáhlé mezinárodní kybernetické kampaně, která zneužívala kritické bezpečnostní slabiny v poštovním systému Microsoft Exchange Server. Tato zranitelnost umožnila útočníkům získat neoprávněný přístup k e-mailovým schránkám a dalším vnitřním systémům několika organizací, včetně zdravotnického zařízení Ministerstva vnitra.

Dotčená instituce zpracovává důvěrné údaje související s příslušníky bezpečnostních složek, což činí tento incident obzvláště citlivým. Analýzy ukázaly, že cílem útoku bylo získání strategických informací bez vědomí napadené organizace – tedy forma kyberšpionáže. Útočníkům se podařilo do systému proniknout a vytvořit trvalý přístup, tzv. "backdoor", což by jim potenciálně umožnilo opakovaný přístup k citlivým datům.

Zásah bezpečnostních specialistů Ministerstva vnitra však vedl k včasné detekci útoku a přijetí protiopatření, čímž se předešlo rozsáhlejším škodám a úniku dat. Závěry odborných institucí, včetně Národního úřadu pro kybernetickou a informační bezpečnost, ukázaly na téměř jisté propojení útočníků s čínskými státními strukturami. Tento případ nejen potvrdil zranitelnost kritické infrastruktury vůči sofistikovaným hrozbám, ale rovněž podnítil potřebu systematického posílení bezpečnostních mechanismů v rámci veřejné správy.[44] Kybernetické útoky jsou stále častější a rozšířenější a nevyhýbají se ani významným institucím jako je Ministerstvo vnitra.

[43]AVAST THREAT LABS. *Nemocnice pod náporem hackerů: Jak proběhly nejznámější kyberútoky na české nemocnice?* Online. Avast. 2021. Dostupné z: https://blog.avast.com/cs/nemocnice-pod-naporem-hackeru-jak-probihajikyberutoky-na-ceske-nemocnice. [cit. 2024-03-15].

[44]RESPEKT. *Útok pokračuje. Hackeři si vzali na mušku zdravotnické zařízení ministerstva vnitra*. Online. Dostupné z: https://www.respekt.cz/agenda/utok-pokracuje-hackeri-si-vzali-na-musku-zdravotnicke-zarizeni-ministerstva-vnitra/.[cit. 2025-03-30].

5.3 Kybernetický útok na Ředitelství silnic a dálnic ČR

V polovině května 2022 došlo k významnému kybernetickému útoku na infrastrukturu Ředitelství silnic a dálnic České republiky. Útočníci využili ransomware – typ škodlivého softwaru, jehož cílem je zašifrovat data oběti a znemožnit tak jejich přístup, dokud nebude zaplaceno výkupné. V důsledku útoku došlo k zablokování interních informačních systémů organizace.

Incident vyhodnotil Národní úřad pro kybernetickou a informační bezpečnost jako velmi sofistikovaný, přičemž bylo zjištěno hluboké proniknutí do systémové infrastruktury. Identita pachatele zůstala neveřejná z důvodu taktické ochrany probíhajícího šetření. V důsledku narušení došlo k nedostupnosti webového rozhraní organizace, včetně portálu Dopravniinfo.cz, který poskytuje veřejnosti informace o dopravní situaci.

Výpadek informačních systémů způsobil zpoždění a zrušení některých veřejných zakázek a prodloužení lhůt v rámci běžných provozních agend. Náprava a plná obnova činnosti si vyžádala časový horizont několika týdnů až měsíců. Podle bezpečnostních expertů lze s vysokou pravděpodobností útok připsat organizované kriminální skupině, přičemž okolnosti odpovídají známým ransomwarovým kampaním.[45]

5.4 DDoS útoky na státní infrastrukturu

Na jaře roku 2022 čelila Česká republika koordinované sérii distribuovaných útoků typu DDoS (Distributed Denial of Service), jejichž účelem bylo přetížení cílových serverů a tím znemožnění přístupu k online službám. K nejintenzivnějším incidentům došlo v druhé polovině dubna, kdy byly po určitou dobu mimo provoz internetové portály několika státních institucí.

Mezi postižené subjekty patřily například Ministerstvo vnitra, Policie ČR, Hasičský záchranný sbor, ale i Úřad vlády, Národní úřad pro kybernetickou

[45]ČTK ČESKÉ NOVINY. *NÚKIB: Kyberútok na weby ŘSD byl profesionální, zašifroval data*. Online. 2022. Dostupné z: https://www.ceskenoviny.cz/zpravy/2208924#:~:text=Praha%20,%C3%BAtoku%20%C4%8Delilo%20%C5%98SD%20v%20%C3%BAter%C3%BD. [cit. 2025-03-30].

a informační bezpečnost (NÚKIB) či dopravní portál Českých drah. Útoky se dotkly rovněž některých regionálních letišť. Ačkoli nebyl zaznamenán průnik do vnitřních systémů, útoky významně narušily dostupnost důležitých informačních kanálů.

K odpovědnosti za tyto incidenty se přihlásila proruská hackerská skupina Killnet, která je součástí širšího spektra tzv. hacktivistických uskupení. Jejich aktivity byly vnímány jako reakce na veřejně deklarovanou podporu České republiky směrem k Ukrajině po zahájení ozbrojeného konfliktu na jejím území. NÚKIB v reakci na tuto hrozbu opakovaně varoval před zvýšeným rizikem podobných útoků a doporučil organizacím posílit síťovou ochranu, zefektivnit monitoring provozu a připravit krizové plány pro zajištění provozní kontinuity.[46]

[46]EKONOMICKÝ DENÍK. *Kybernetické útoky na české vládní weby pokračují. Stojí za nimi ruská hackerská skupin*. Online. 2022. Dostupné z: https://ekonomickydenik.cz/kyberneticke-utoky-na-ceske-vladni-weby-pokracuji-stoji-za-nimi-ruska-hackerska-skupina/. [cit. 2025-03-30].

6 PREVENCE A OCHRANA PŘED KYBERNETICKÝMI ÚTOKY

Účinná prevence kybernetických útoků spočívá v přijetí opatření reagujících na aktuální vývoj hrozeb v online prostředí. Většina incidentů vzniká kvůli důvěřivosti uživatelů při práci s e-maily či jinou komunikací, kdy nerozeznají podvodný obsah.

Nejzranitelnější jsou ti, kteří postrádají základní znalosti v oblasti kybernetické bezpečnosti, avšak ohroženi mohou být i zkušení uživatelé, například v důsledku nepozornosti. Následující část se věnuje preventivním krokům a možnostem obrany proti těmto útokům. Přestože jejich úplné odstranění není v současnosti reálné, osvěta a odpovědný přístup mohou výrazně snížit riziko.

6.1 Antivirový program

Vývoj softwarových nástrojů určených k ochraně před škodlivým kódem prošel v posledních desetiletích výraznou transformací. Zatímco dřívější antivirové aplikace byly zaměřeny primárně na identifikaci a odstranění známých forem malwaru, současná bezpečnostní řešení představují komplexní systémy s širokým spektrem funkcionalit. Moderní antivirový software již neslouží pouze k detekci hrozeb, ale aktivně brání pokusům o průnik do systému, čímž minimalizuje riziko napadení ještě před tím, než k němu dojde.[47]

Tyto nástroje bývají zpravidla vybaveny vícevrstvou ochranou, která umožňuje efektivní reakci na různé typy útoků v reálném čase. Kromě obrany proti klasickým virům zahrnují mechanismy pro odhalení phishingových pokusů, ochranu před ransomwarem, prevenci neoprávněného přístupu k osobním údajům nebo zabezpečení před tzv. cryptojackingem, tedy zneužitím výpočetního výkonu k těžbě kryptoměn. Podstatnou součástí bývá rovněž filtrování nevyžádané pošty a ochrana digitální identity uživatele. Díky těmto funkcím lze říci, že současné antivirové

[47]ESET. Phishing. [online]. eset.com [cit. 2024-12-12]. Dostupné z: https://www.eset.com/cz/phishing/

programy tvoří klíčový pilíř kybernetické bezpečnosti běžných uživatelů i organizací.

6.2 Zálohování dat

Jedním z nejúčinnějších nástrojů ochrany dat v prostředí digitálních hrozeb zůstává systematické zálohování. V kontextu kybernetické bezpečnosti představuje vytváření záloh základní strategii, jak předcházet trvalé ztrátě dat v důsledku útoků, jako je například ransomware. V případě, že jsou data uživatele pravidelně ukládána na nezávislé úložné jednotky, umožňuje to jejich obnovu i po jejich zašifrování nebo smazání, aniž by došlo k finančnímu či datovému vydírání ze strany útočníka. Tímto způsobem lze minimalizovat dopady incidentu na uživatele, byť často za cenu reinstalace operačního systému a konfigurace zařízení do původního stavu.

Za účelem zvýšení efektivity zálohovacích procesů je odborníky doporučováno řídit se zásadami tzv. 3-2-1 pravidla. Tento přístup spočívá v uložení tří kopií dat, přičemž dvě by měly být uchovány na rozdílných médiích a třetí na fyzicky odděleném místě. Tato diverzifikace záložních úložišť významně snižuje pravděpodobnost úplné ztráty dat v důsledku poruchy zařízení, havárie nebo živelných událostí. Přestože zavedení tohoto opatření může vyžadovat určité finanční investice, přináší výrazné zvýšení odolnosti vůči datovým ztrátám a je proto považováno za standard v oblasti datové bezpečnosti.[48]

5.4.1 Způsoby zálohování

Pomocí zařízení NAS – Servery NAS jsou další možností, jak vytvořit zálohu dat. Existují v různých velikostech pro domácí nebo firemní použití. Díky nim lze automaticky zálohovat data z všech zařízení do RAID pole. Hlavní předností serverů NAS je lokální uložení dat, ať už se nacházejí v domě nebo v kanceláři. Uživatel si tak zachovává plnou kontrolu nad daty a může k nim flexibilně přistupovat z dálky, podobně jako u cloudu.[49]

[48]KO, Matias. *Řešení zálohování dat s pravidlem 3-2-1*. cz.msi.com [online]. 2023 [cit. 2023-12-12]. Dostupné z: https://cz.msi.com/blog/a-backup-solution-for-you-with-3-2-1- data-backup-rule

[49]TÝM SYNOLOGY. *Co je to zálohování? Definice a podrobné vysvětlení*. blog.synology.com [online]. 17. 10. 2022 [cit. 2023-12-12]. Dostupné z: https://blog.synology.com/cs-cz/co-je-to-zalohovani-definice-a-podrobne-vysvetleni/

Do cloudu – Pojem cloud označuje síť vzájemně propojených vzdálených serverů, sloužících k úschově a sdílení dat nebo k využívání aplikací a softwaru. Data nejsou fyzicky uložena na disku počítače, nýbrž právě v cloudu neboli úložišti poskytovatele, do kterého má uživatel přístup kdykoliv, odkudkoliv s internetovým připojením a z jakéhokoliv zařízení. Poskytovatelé cloudových uložišť jsou zodpovědní za zajištění datových center poskytujících zabezpečení, kapacitu uložiště a výpočetní výkonnost.[50]

Na externí pevné disky – Důležité jsou také offline zálohy na externích discích, jako jsou flash disky a další druhy externích nosičů dat, jejichž výhoda spočívá právě v nezávislosti na internetovém připojení, což sebou přináší další výhodu v podobě ochrany před napadením. Samotná obnova je navíc v případě takto zálohovaných dat jednodušší, než např. z cloudových uložišť.

6.3 Institucionální rámec reakce na kybernetické hrozby

Jedním z charakteristických rysů kybernetické kriminality, který ji zásadně odlišuje od tradičních forem trestné činnosti, je její obtížná zjistitelnost v důsledku výrazné latentnosti a vysoké úrovně anonymity pachatelů. Tato skutečnost je dále umocněna nízkou mírou společenské citlivosti vůči kybernetickým útokům, přičemž samotní uživatelé často projevují nezájem nebo nedostatečnou informovanost. Z toho vyplývá nezbytnost posílení obranných mechanismů, zejména prostřednictvím zkvalitnění nástrojů pro identifikaci pachatelů a koordinaci reakcí na incidenty.

Důležitou roli zde hraje standardizace postupů a důraz na systematické vzdělávání uživatelů v oblasti rozpoznávání a předcházení kybernetickým hrozbám. V návaznosti na tyto požadavky dochází k rozvoji specializovaných struktur, jako jsou bezpečnostní týmy CERT a CSIRT, které poskytují odbornou podporu při řešení incidentů a přispívají k celkovému posílení kybernetické bezpečnosti.[51]

Odborné týmy zabývající se řešením kybernetických bezpečnostních incidentů jsou ve světové praxi označovány zkratkami CERT (Computer Emergency Response Team) a CSIRT (Computer Security Incident Response Team). Ačkoliv se

[50]ALGOTECH. *Jak funguje cloud? algotech.cz* [online]. [cit. 2023-12-12]. Dostupné z: https://www.algotech.cz/novinky/2021-10-27-jak-fungujecloud#:~:text=Co%20je%20to%20cloud%3F,p%C5%99%C3%ADstroji%2C%20n%C3

[51]KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019.s.505. ISBN 978-80-88168-31-7.

tyto pojmy historicky vyvíjely odděleně a jejich původní definice se mírně liší, v současném pojetí představují obdobné organizační jednotky. Jejich hlavním úkolem je aktivně reagovat na bezpečnostní incidenty v oblasti informačních technologií a poskytovat podporu v rámci své vymezené působnosti. Z pohledu jednotlivců, institucí nebo jiných bezpečnostních týmů fungují tyto jednotky jako kontaktní a koordinační místo, na které se lze obrátit v případě detekce kybernetické hrozby, za účelem konzultace, sdílení informací nebo navázání odborné spolupráce.[52]

6.4 Aktualizace softwaru

Kybernetické hrozby se v digitálním prostředí neustále proměňují a sofistikují, což klade zvýšené nároky na zabezpečení operačních systémů. Jedním z klíčových preventivních opatření je pravidelná instalace dostupných aktualizací, které reagují na nově objevené zranitelnosti. Vývojáři operačních systémů proto průběžně implementují úpravy, jež nejen zlepšují funkcionalitu, ale především posilují ochranu vůči aktuálním bezpečnostním rizikům.

Z hlediska charakteru lze aktualizace rozdělit na dvě hlavní skupiny. První skupinu tvoří rozsáhlé aktualizace, které mění samotnou verzi či edici operačního systému. Tyto změny jsou zpravidla spojeny s ukončením podpory starších verzí, jak je tomu například u Windows 10 verze 21H2, pro niž již nejsou plánovány další aktualizace základní verze. Druhý typ představují drobnější, ale neméně důležité aktualizace, které bývají často zaměřeny na opravy zjištěných zranitelností. I když tyto změny nemusí být uživateli vždy plně srozumitelné nebo viditelné, jejich instalace má zásadní význam pro udržení bezpečnosti systému.

Zranitelnosti mohou být odhaleny buď přímo vývojovým týmem během testovacích fází, nebo prostřednictvím externích odborníků, tzv. etických hackerů, kteří se zabývají testováním odolnosti systémů vůči narušení. Přestože někteří uživatelé mohou důležitost aktualizací podceňovat, jejich pravidelné zavádění je základním prvkem kybernetické hygieny.[53]

[52]KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., *2019.s.505. ISBN 978-80-88168-31-7.*

[53]*VÍMKAMKLIKÁM.CZ.* Proč a jak aktualizovat operační systém. vimkamklikam.cz [online]. 02.11.2017 [cit. 2023-12-12]. Dostupné z: https://www.vimkamklikam.cz/radya-tipy/proc-a-jak-aktualizovat-operacni-system

6.5 Osvěta a vzdělávání v oblasti kybernetické bezpečnosti

Přestože povědomí veřejnosti o základních principech kybernetických útoků, jako je například phishing, se postupně zvyšuje, schopnost jednotlivců tyto útoky v praxi rozpoznat a adekvátně na ně reagovat zůstává omezená. K efektivnímu posilování kompetencí v oblasti kybernetické bezpečnosti přispívají různé vzdělávací nástroje a programy, které jsou dostupné široké veřejnosti i specifickým cílovým skupinám.

Jedním z příkladů interaktivního vzdělávání je e-learningový kurz „Dávej kyber“, vyvinutý Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB), který slouží k procvičování dovedností potřebných k rozpoznání a eliminaci kybernetických hrozeb. Dalším cenným zdrojem je vzdělávací iniciativa spolku Zvol si info, zaměřená na podporu mediální gramotnosti na základních a středních školách, která rozšiřuje povědomí žáků o bezpečném chování v digitálním prostoru.

Pro technicky pokročilé studenty a mladé odborníky v oblasti informačních technologií byla vytvořena simulační hra *Deploy or Die*, jejímž cílem je rozvoj schopnosti rychle a správně reagovat na krizové situace v kybernetickém prostředí.

Zvyšování úrovně kybernetické gramotnosti v České republice závisí nejen na institucionálních aktivitách, ale také na zapojení jednotlivců – pedagogů, rodičů či dalších dospělých, kteří jsou ochotni věnovat svůj čas osvětě a sdílení těchto nástrojů s mladší generací.[54]

V rámci Evropského měsíce kybernetické bezpečnosti proběhla v České republice řada vzdělávacích a osvětových aktivit, mezi nimiž vynikl Festival bezpečného internetu, koordinovaný Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB). Do programu se zapojilo více než třicet subjektů z různých sektorů, přičemž NÚKIB se aktivně podílel na realizaci několika z nich. Důraz byl kladen na cílenou osvětu v různých oblastech společnosti – například

[54]KRESA, Dan. *Jak vzdělávat v oblasti kyberbezpečnosti na základních a středních školách? kybez.cz* [online]. 10. 3. 2021 [cit. 2023-12-12]. Dostupné z: https://kybez.cz/jak-vzdelavat-v-oblasti-kyberbezpecnosti-na-zakladnich-a-strednichskolach/

formou specializovaných kurzů pro seniory nebo informačních kampaní pro zdravotnický personál.[55]

[55]NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Festival bezpečného internetu* [online]. Brno: NÚKIB, 2022 [cit. 2025-03-30]. Dostupné z: https://www.nukib.cz/cs/informacni-servis/aktuality/1901-festival-bezpecneho-internetu-2022/

7 Analýza stavu kybernetické bezpečnosti

7.1 Metodologie výzkumu

Výzkum byl proveden kvantitativní metodou prostřednictvím anonymního online dotazníku. Dotazník byl zaměřen na zmapování vnímání kybernetické bezpečnosti mezi běžnými uživateli internetu. Respondenti odpovídali na otázky týkající se jejich online návyků, povědomí o kybernetických hrozbách a osobní nebo pracovní zkušenosti s bezpečnostními opatřeními.

7.2 Výzkumný nástroj – dotazník

Dotazník obsahoval 17 otázek, z toho většina uzavřených, což umožnilo snadnou kvantitativní analýzu odpovědí. Zaměřoval se na obecné používání internetu, základní orientaci v problematice kybernetické bezpečnosti a zkušenosti s konkrétními opatřeními, jako jsou silná hesla, zálohování dat nebo využívání dvoufázového ověřování.

7.3 Charakteristika respondentů

Výzkumného šetření se zúčastnilo 138 respondentů oslovených prostřednictvím veřejné skupiny na sociální síti Facebook, čítající 8,8 tisíc uživatelů. Tato skupina sdružuje běžné uživatele internetu napříč různými věkovými, profesními i geografickými skupinami. Záměrem bylo oslovit širokou veřejnost, nikoliv odborníky či osoby s hlubokým technickým zázemím. Díky tomu bylo možné zmapovat obecné povědomí o kybernetické bezpečnosti a získat představu o tom, jak se běžní uživatelé internetu chovají v online prostředí.

Z hlediska pohlaví byli respondenti téměř rovnoměrně zastoupeni. Tento fakt přispívá k vyváženosti výsledků a umožňuje analyzovat vnímání kybernetických rizik bez významného zkreslení v důsledku převahy jednoho pohlaví. Věkové rozložení bylo rovněž pestré, s převahou mladších a středně starých dospělých, kteří se nejčastěji pohybují ve světě digitálních technologií a jsou zvyklí pracovat

s internetem každodenně. Zároveň byly zastoupeny i starší věkové kategorie, což umožňuje zachytit rozdíly v chování a přístupu ke kybernetické bezpečnosti napříč generacemi.

Respondenti pocházeli z různých částí České republiky. Ve výzkumném vzorku byli zastoupeni obyvatelé měst i venkovských oblastí, včetně hlavního města Prahy. Tato různorodost zajišťuje, že výsledky nejsou ovlivněny pouze lokálním prostředím, ale odrážejí situaci v rámci celé republiky.

Z odborného hlediska lze konstatovat, že značná část respondentů aktivně využívá internet při svém zaměstnání, zatímco menší část jej používá výhradně pro osobní účely. To poukazuje na propojení osobního a pracovního života v digitálním prostředí a na důležitost prevence v rámci kybernetické bezpečnosti v obou sférách.

Celkově lze říci, že struktura respondentů odpovídá cíli výzkumu – zachytit postoje běžných uživatelů internetu bez odborného zaměření. Široké věkové i profesní rozvrstvení dodává výsledkům vysokou výpovědní hodnotu a poskytuje důvěryhodný základ pro následnou analýzu.

7.4 Realizace výzkumů

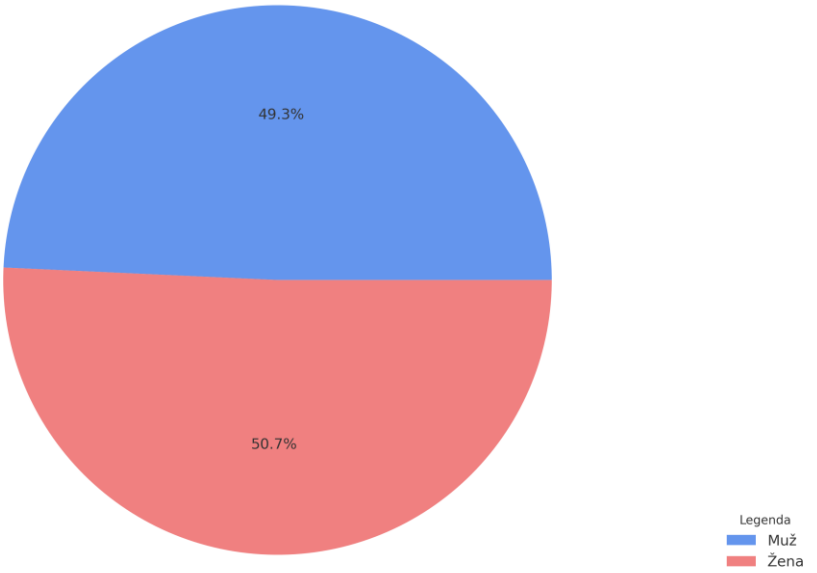
Sběr dat probíhal v první polovině března 2025. Dotazník byl dostupný online a distribuován do výše uvedené facebookové skupiny. Účast byla dobrovolná a anonymní, cílem bylo získat reprezentativní přehled o vnímání kybernetické bezpečnosti mezi běžnými uživateli internetu v ČR.

7.5 Vyhodnocení dotazníku

Otázka 1: Jaké je vaše pohlaví?

- Muž: 68 respondentů (49,3 %)
- Žena: 70 respondentů (50,7 %)

Graf 1: Pohlaví respondentů



Zdroj: Vlastní zpracování

Na otázku ohledně pohlaví odpovědělo všech 138 respondentů, přičemž 68 respondentů byli muži (49,3 %) a 70 ženy (50,7 %).

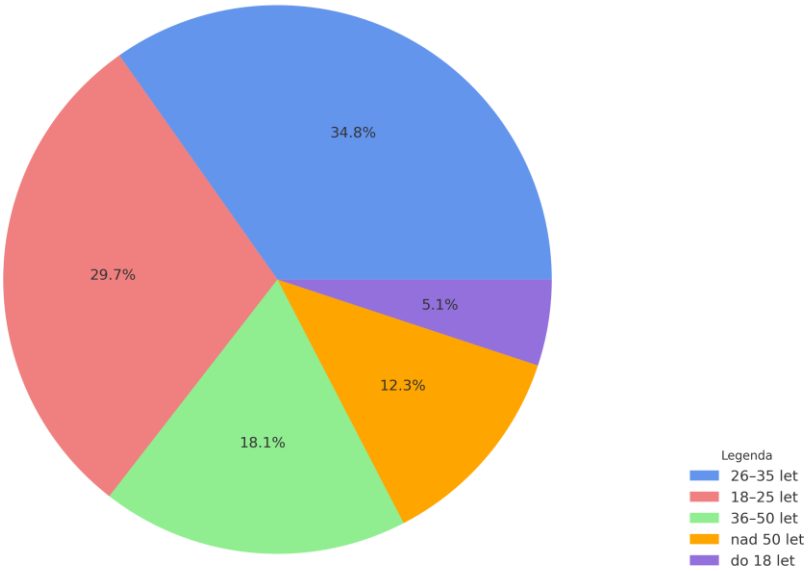
Vzorek je z hlediska genderu vyvážený, což zvyšuje relevanci dalších zjištění v rámci výzkumu.

Díky rovnoměrnému zastoupení je možné porovnávat odpovědi obou skupin bez potřeby statistického vyrovnání nebo úprav, a výsledky tak mohou lépe odrážet obecné trendy napříč celou populací.

Otázka 2: Do jaké věkové skupiny patříte?

- 26–35 let: 48 respondentů (34,8 %)
- 18–25 let: 41 respondentů (29,7 %)
- 36–50 let: 25 respondentů (18,1 %)
- nad 50 let: 17 respondentů (12,3 %)
- do 18 let: 7 respondentů (5,1 %)

Graf 2: Věk respondentů



Zdroj: Vlastní zpracování

Z věkového rozložení respondentů je patrné, že nejvíce odpovědí pocházelo od osob ve věku 26–35 let (34,8 %) a 18–25 let (29,7 %). Tyto dvě skupiny dohromady tvoří více než 64 % všech respondentů, což odpovídá vyšší aktivitě mladších dospělých na internetu.

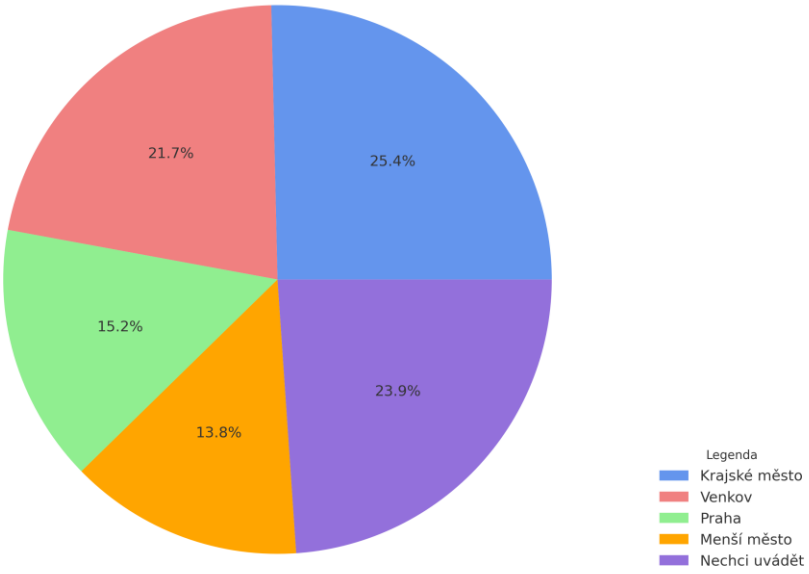
Věková skupina 36–50 let byla zastoupena z 18,1 %, uživatelé nad 50 let tvořili 12,3 %, a nejmenší zastoupení měla skupina do 18 let (5,1 %).

Výsledky tak odrážejí především pohled internetově aktivní generace, která je často vystavena nejčastějším kybernetickým rizikům.

Otázka 3: Odkud pocházíte?

- Krajské město: 35 respondentů (25,4 %)
- Venkov: 30 respondentů (21,7 %)
- Praha: 21 respondentů (15,2 %)
- Menší město: 19 respondentů (13,8 %)
- Nechci uvádět: 33 respondentů (23,9 %)

Graf 3: Místo bydliště respondentů



Zdroj: Vlastní zpracování

Z odpovědí na otázku týkající se místa bydliště vyplývá, že nejvíce respondentů pochází z krajských měst (25,4 %), těsně následovaných skupinou, která místo bydliště nechtěla uvést (23,9 %).

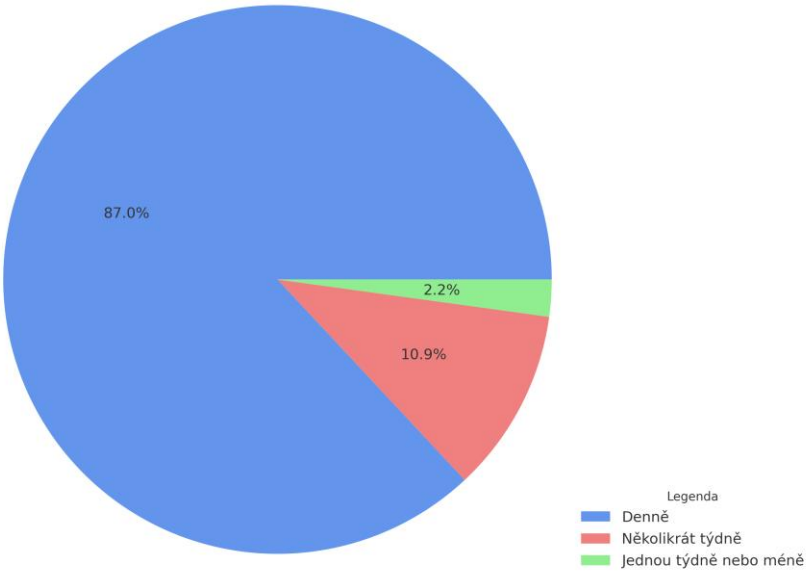
Poměrně vyrovnané zastoupení měly také venkovské oblasti (21,7 %) a Praha (15,2 %), zatímco menší města uvedlo 13,8 % dotázaných.

Tato různorodost ukazuje, že se do výzkumu zapojili uživatelé internetu z různých částí České republiky, což přispívá k pestřejšímu pohledu na vnímání kybernetické bezpečnosti napříč geografickými oblastmi. Významný podíl respondentů, kteří místo bydliště neuvedli, však mírně omezuje detailnější geografické srovnání.

Otázka 4: Jak často používáte internet?

- Denně: 120 respondentů (87,0 %)
- Několikrát týdně: 15 respondentů (10,9 %)
- Jednou týdně nebo méně: 3 respondenti (2,2 %)

Graf 4: Frekvence používání internetu respondenty



Zdroj: Vlastní zpracování

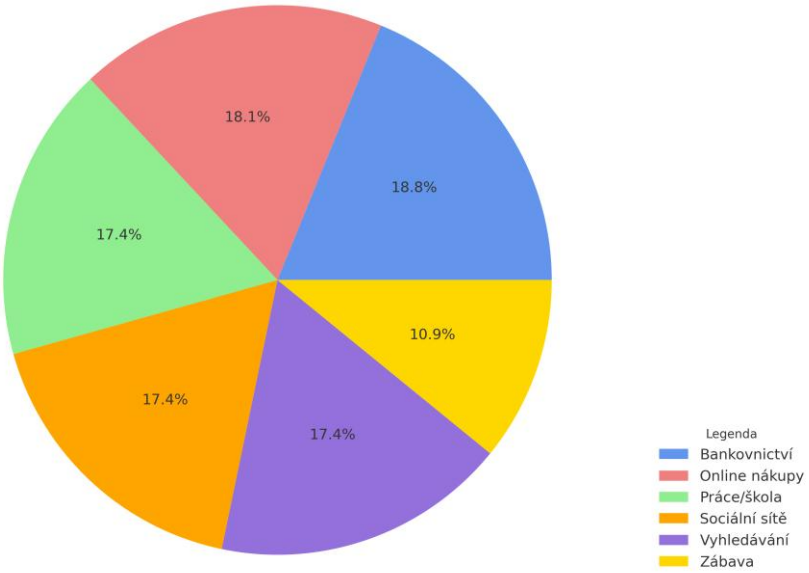
Výsledky ukazují, že naprostá většina respondentů (87,0 %) používá internet denně, dalších 10,9 % alespoň několikrát týdně. Pouze zanedbatelné množství (2,2 %) uvedlo, že internet využívá jednou týdně nebo méně.

Tento výsledek potvrzuje, že dotazovaní jsou aktivními uživateli internetu, což je klíčové pro hodnocení jejich postojů a chování v oblasti kybernetické bezpečnosti. Zároveň to naznačuje, že problematika online bezpečnosti se přímo dotýká každodenního života většiny respondentů.

Otázka 5: K jakým účelům nejčastěji používáte internet?

- Bankovnictví: 26 respondentů (18,8 %)
- Online nákupy: 25 respondentů (18,1 %)
- Práce/škola: 24 respondentů (17,4 %)
- Sociální sítě: 24 respondentů (17,4 %)
- Vyhledávání: 24 respondentů (17,4 %)
- Zábava: 15 respondentů (10,9 %)

Graf 5: Nejčastější účely využívání internetu



Zdroj: Vlastní zpracování

Odpovědi na tuto otázku ukazují, že využívání internetu je mezi respondenty rovnoměrně rozloženo mezi několik hlavních oblastí. Nejčastěji zmiňovanými účely byly bankovnictví (18,8 %) a online nákupy (18,1 %), těsně následované prací nebo školou, sociálními sítěmi a vyhledáváním informací (každé po 17,4 %). Zábava tvořila nejmenší podíl (10,9 %).

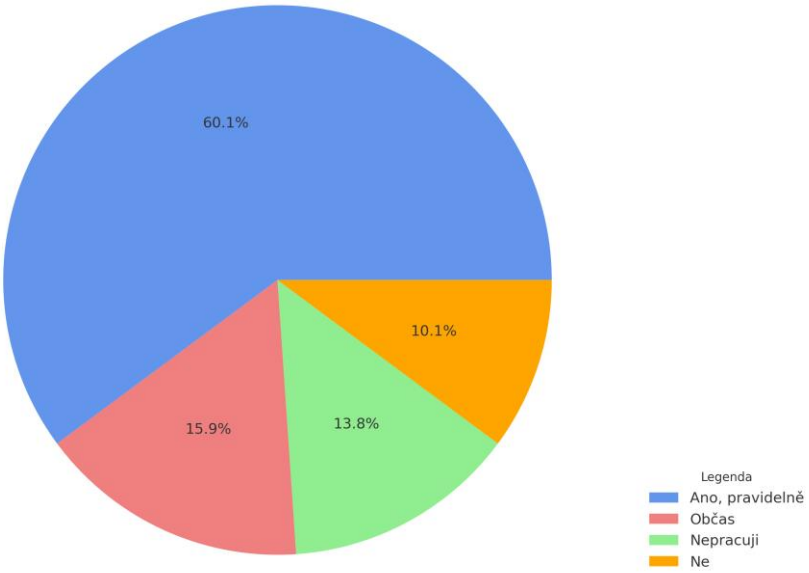
Tato rozmanitost využití potvrzuje, že internet hraje v každodenním životě respondentů důležitou roli – slouží nejen k pracovním a vzdělávacím účelům, ale i ke správě financí, nákupům, komunikaci a získávání informací.

Vzhledem k povaze těchto aktivit je zřejmé, že uživatelé se pohybují v prostředí, kde je zvýšené riziko kybernetických hrozeb (např. podvody, phishing, ztráta dat), což podtrhuje důležitost odpovědného a informovaného online chování.

Otázka 6: Využíváte při své práci připojení k internetu?

- Ano, pravidelně: 83 respondentů (60,1 %)
- Občas: 22 respondentů (15,9 %)
- Nepracuji: 19 respondentů (13,8 %)
- Ne: 14 respondentů (10,1 %)

Graf 6: Využívání internetu k práci



Zdroj: Vlastní zpracování

Z odpovědí vyplývá, že většina respondentů (60,1 %) využívá internet při své práci pravidelně, dalších 15,9 % alespoň občas. To znamená, že více než tři čtvrtiny dotázaných mají zkušenost s pracovním využíváním internetu.

Pouze 10,1 % respondentů uvedlo, že internet v rámci své pracovní činnosti vůbec nevyužívá, a 13,8 % nepracuje.

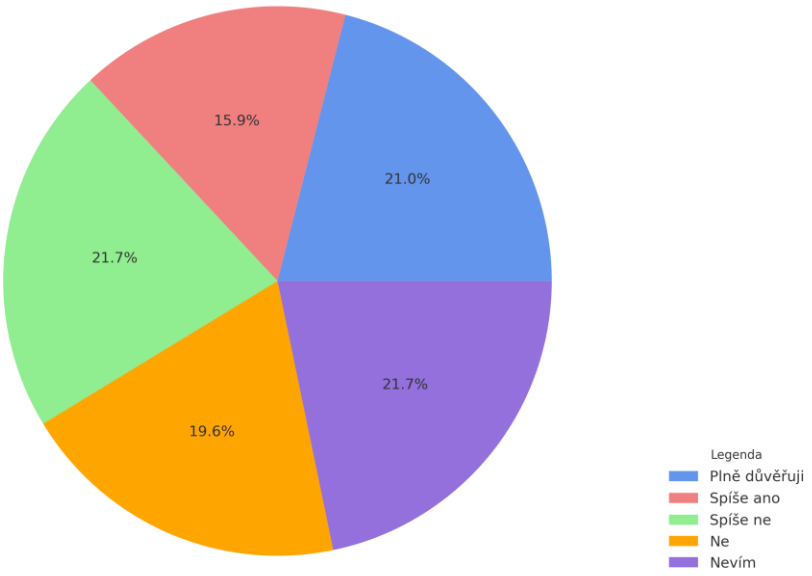
Tato čísla potvrzují, že internet hraje klíčovou roli nejen v soukromém, ale i v profesním životě většiny respondentů. Zároveň to naznačuje, že pro řadu z nich je kybernetická bezpečnost relevantní i z hlediska pracovního prostředí, kde mohou být vystaveni vyšším nárokům na ochranu dat a bezpečnou komunikaci.

Otázka 7: Domníváte se, že je vaše pracoviště dostatečně zabezpečeno proti kybernetickým útokům?

- Plně důvěřuji: 29 respondentů (21,0 %)
- Spíše ano: 22 respondentů (15,9 %)
- Spíše ne: 30 respondentů (21,7 %)
- Ne: 27 respondentů (19,6 %)

- Nevím: 30 respondentů (21,7 %)

Graf 7: Vnímání kybernetického zabezpečení pracoviště



Zdroj: Vlastní zpracování

Odpovědi na tuto otázku ukazují, že vnímání kybernetického zabezpečení na pracovišti je mezi respondenty značně rozdělené. Pouze 21 % dotázaných uvedlo, že svému pracovišti plně důvěřují, a dalších 15,9 % odpovědělo „spíše ano“. Naopak 21,7 % se vyjádřilo „spíše ne“ a 19,6 % odpovědělo jednoznačně „ne“.

Zajímavé je také vysoké procento nerozhodnutých – 21,7 % respondentů uvedlo, že nedokážou posoudit, zda je jejich pracoviště dostatečně zabezpečeno.

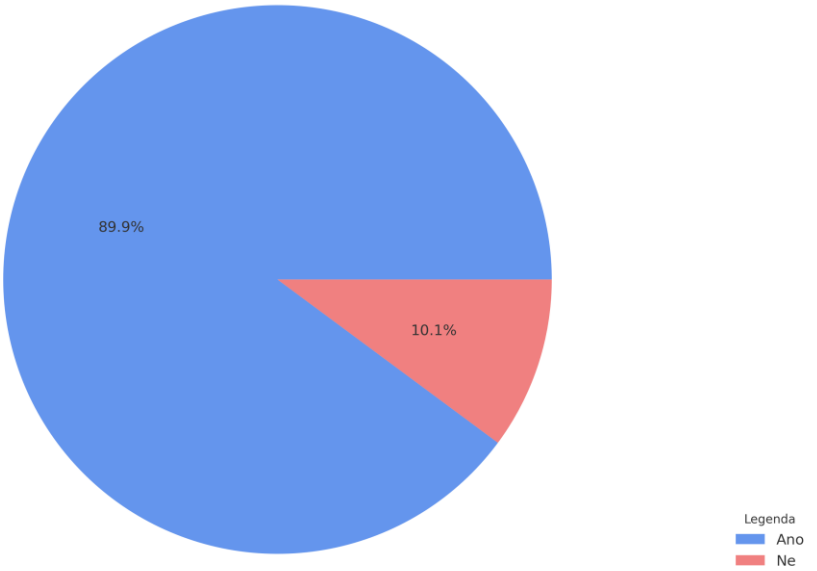
Tato nejistota a nedůvěra může signalizovat nedostatečnou komunikaci zaměstnavatelů směrem k zaměstnancům ohledně zabezpečení IT prostředí, případně i nízké povědomí zaměstnanců o opatřeních, která jsou v praxi realizována.

Zároveň výsledky poukazují na potřebu větší osvěty a školení v oblasti kybernetické bezpečnosti přímo na pracovištích.

Otázka 8: Setkali jste se někdy s pojmem kybernetická bezpečnost?

- Ano: 124 respondentů (89,9 %)
- Ne: 14 respondentů (10,1 %)

Graf 8: Povědomí o pojmu kybernetická bezpečnost



Zdroj: Vlastní zpracování

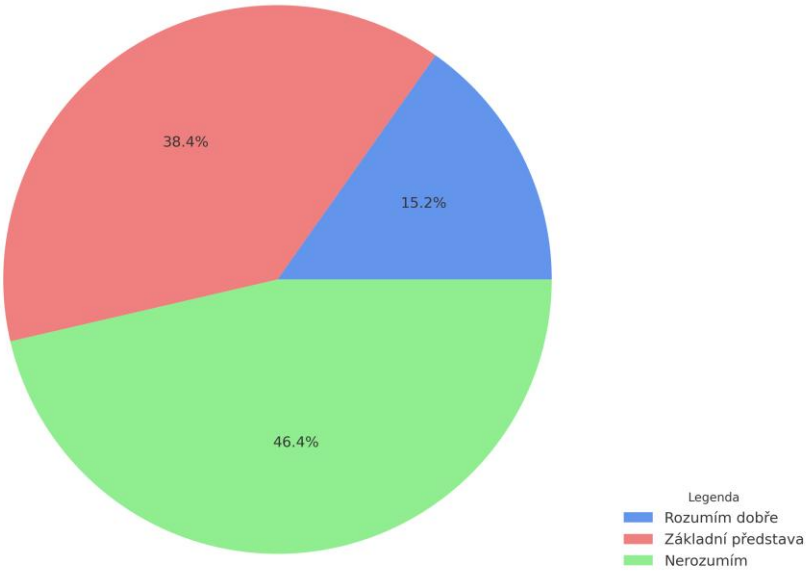
Většina respondentů (89,9 %, tedy 124 osob) uvedlo, že se již setkalo s pojmem kybernetická bezpečnost. Pouze 14 respondentů (10,1 %) uvedlo opak.

Tento výsledek ukazuje, že povědomí o dané problematice je mezi veřejností poměrně rozšířené. Zároveň to naznačuje, že téma je v informačním prostoru přítomné, ať už prostřednictvím médií, vzdělávání či osobní zkušenosti.

Otázka 9: Máte představu, co znamená pojem kybernetický útok?

- Rozumím dobře: 21 respondentů (38,4 %)
- Základní představa: 53 respondentů (46,4 %)
- Nerozumím: 64 respondentů (15,2 %)

Graf 9: Povědomí o významu kybernetického útoku



Zdroj: Vlastní zpracování

Z odpovědí na tuto otázku vyplývá, že většina respondentů má alespoň základní povědomí o tom, co znamená pojem *kybernetický útok*. Konkrétně 46,4 % uvedlo, že mají základní představu, a 38,4 % dokonce uvedlo, že pojmu rozumí dobře. To znamená, že dohromady více než 84 % respondentů má určitou míru porozumění tomuto pojmu.

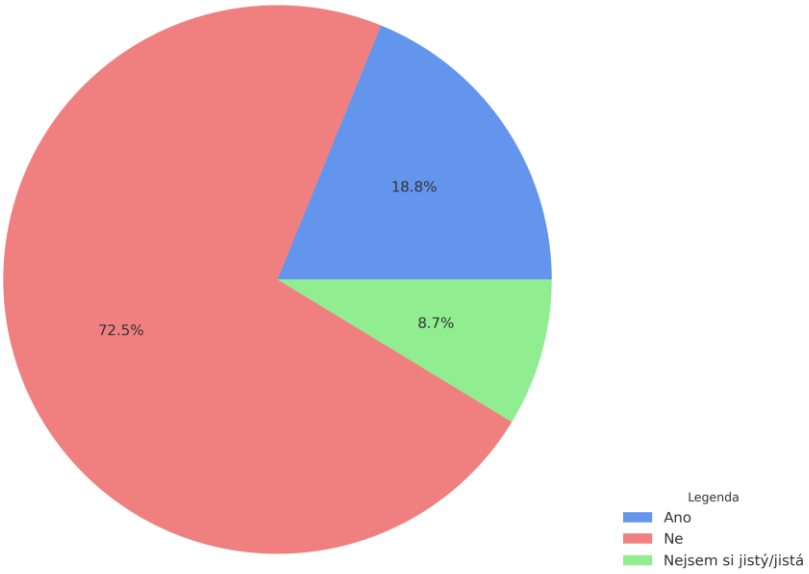
Pouze 15,2 % uvedlo, že významu nerozumí. Tento výsledek ukazuje na poměrně vysokou míru informovanosti mezi uživateli internetu. Zároveň ale naznačuje, že pro část populace může být problematika stále nejasná, což může mít negativní dopad na jejich schopnost rozpoznat hrozby a adekvátně na ně reagovat.

Osvěta a vzdělávání v této oblasti tak stále zůstávají důležitými nástroji.

Otázka 10: Stali jste se někdy cílem nebo obětí kybernetického podvodu či útoku?

- Ano: 26 respondentů (18,8 %)
- Ne: 100 respondentů (72,5 %)
- Nejsem si jistý/jistá: (12 respondentů 8,7 %)

Graf 10: Zkušenost s kybernetickým útokem



Zdroj: Vlastní zpracování

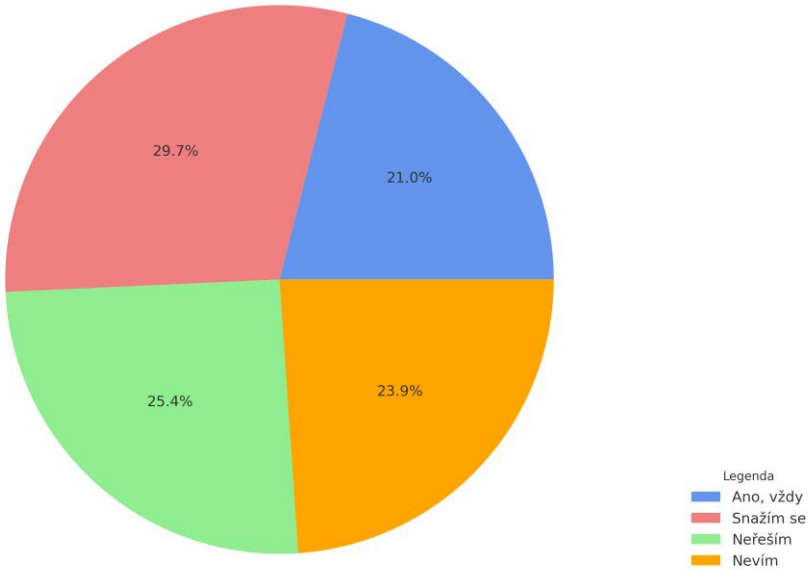
Z odpovědí vyplývá, že téměř pětina respondentů (18,8 %) má osobní zkušenost s kybernetickým podvodem nebo útokem, což je poměrně významné číslo, které ukazuje, že hrozby v online prostředí nejsou jen teoretické, ale pro část uživatelů velmi reálné.

Většina respondentů (72,5 %) uvedla, že se cílem útoku nestala, avšak 8,7 % si tím nebylo jistých. Právě tato nejistota může ukazovat na nedostatečné povědomí o formách kybernetických hrozeb nebo na neviditelnost některých typů útoků (např. sledování bez vědomí uživatele, phishing bez zjevných následků apod.).

Otázka 11: Používáte na internetu silná hesla?

- Ano, vždy: 29 respondentů 21,0 %
- Snažím se: 41 respondentů 29,7 %
- Neřeším: 35 respondentů 25,4 %
- Nevím: 33 respondentů 23,9 %

Graf 11: Využívání silných hesel na internetu



Zdroj: Vlastní zpracování

Odpovědi na otázku týkající se používání silných hesel ukazují, že přístup respondentů k této základní formě kybernetické ochrany je poměrně rozdělený. Pouze 21 % dotázaných uvedlo, že silná hesla používají vždy, a dalších 29,7 % se o to alespoň snaží. To znamená, že přibližně polovina respondentů si je vědoma významu silných hesel a do určité míry se jimi řídí.

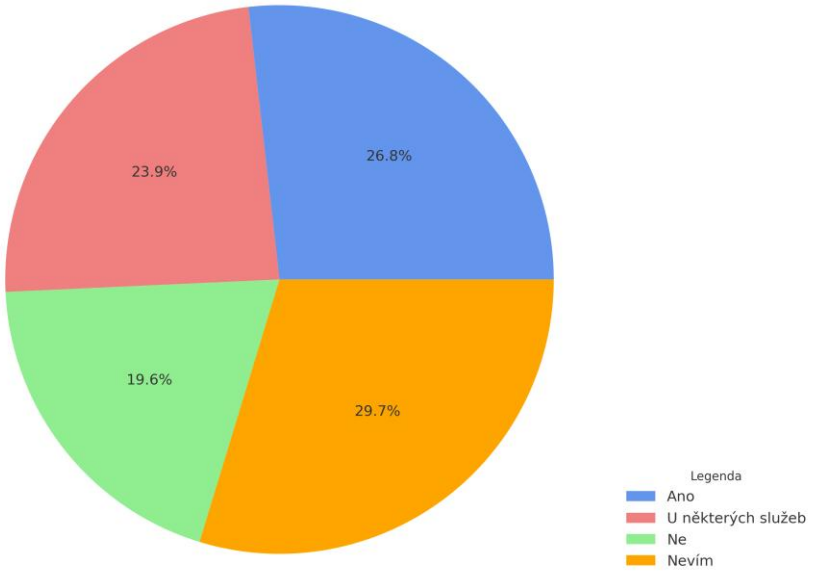
Na druhé straně však 25,4 % tuto problematiku vůbec neřeší a 23,9 % si ani není jistých, co silné heslo znamená. To představuje více než 49 % respondentů, kteří potenciálně používají slabá nebo opakovaně stejná hesla, čímž zvyšují své riziko kybernetického napadení.

Tento výsledek jasně ukazuje na potřebu větší osvěty a vzdělávání v oblasti bezpečného chování na internetu, konkrétně v tématu tvorby a správy hesel, které představují první linii obrany proti mnoha typům útoků.

Otázka 12: Používáte dvoufázové ověření (2FA)?

- Ano: 37 respondentů (26,8 %)
- U některých služeb: 33 respondentů (23,9 %)
- Ne: 27 respondentů (19,6 %)
- Nevím: 41 respondentů (29,7 %)

Graf 12: Používání dvoufázového ověření



Zdroj: Vlastní zpracování

Výsledky této otázky ukazují, že přibližně polovina respondentů (celkem 50,7 %) dvoufázové ověření (2FA) aktivně používá – buď u všech služeb (26,8 %), nebo alespoň u některých (23,9 %). To je pozitivní zjištění, protože 2FA patří mezi účinné způsoby ochrany uživatelských účtů před neoprávněným přístupem.

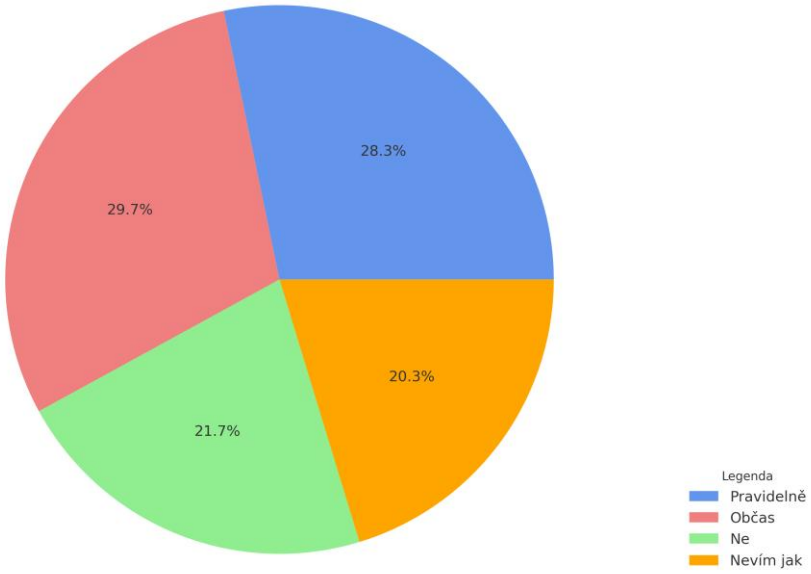
Zároveň však 19,6 % respondentů dvoufázové ověření vůbec nepoužívá a 29,7 % si ani není jistých, co tato funkce znamená. To znamená, že téměř polovina respondentů buď 2FA ignoruje, nebo o něm nemá dostatečné informace.

Tento výsledek poukazuje na nutnost další edukace veřejnosti o tom, jak důležitou roli 2FA hraje při ochraně osobních údajů a digitální identity. Zvýšení povědomí by mohlo přispět k většímu rozšíření tohoto bezpečnostního opatření mezi běžnými uživateli internetu.

Otázka 13: Zálohujete svá data?

- Pravidelně: 39 respondentů (28,3 %)
- Občas: 41 respondentů (29,7 %)
- Ne: 30 respondentů (21,7 %)
- Nevím jak: 28 respondentů (20,3 %)

Graf 13: Frekvence zálohování dat



Zdroj: Vlastní zpracování

Z výsledků této otázky vyplývá, že pouze 28,3 % respondentů pravidelně zálohuje svá data, což je relativně nízké číslo vzhledem k významu této činnosti v prevenci ztráty dat například při napadení malwarem či technickém selhání.

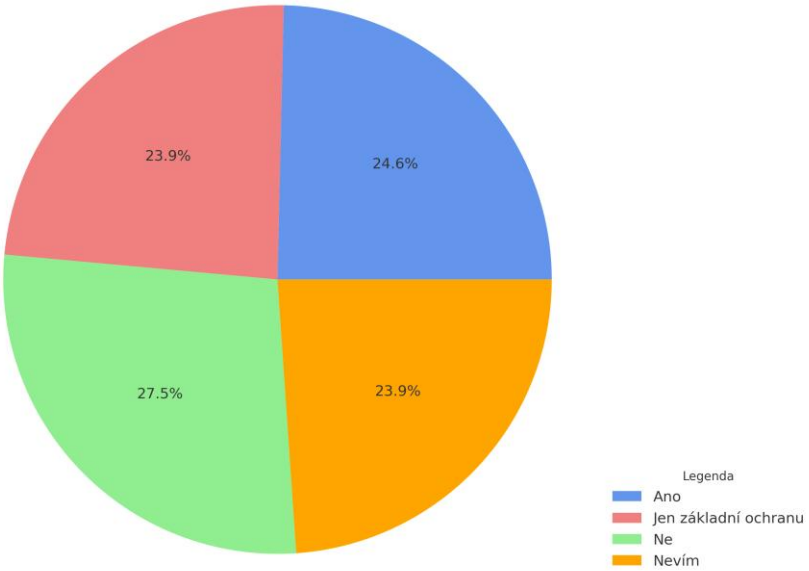
Dalších 29,7 % respondentů uvedlo, že data zálohují alespoň občas, zatímco 21,7 % zálohování vůbec neřeší. Znepokojující je také zjištění, že 20,3 % dotázaných vůbec neví, jak zálohování provádět. To znamená, že více než 40 % respondentů buď nezálohuje, nebo k tomu postrádá potřebné znalosti.

Tento výsledek poukazuje na slabé místo v osobní digitální bezpečnosti běžných uživatelů. Je patrné, že chybí dostatečné povědomí o významu pravidelného zálohování i o samotném způsobu jeho provedení. Vzdělávání v této oblasti by tak mohlo výrazně snížit riziko trvalé ztráty cenných osobních nebo pracovních dat.

Otázka 14: Máte na svém zařízení nainstalovaný antivirový program?

- Ano: 34 respondentů (24,6 %)
- Jen základní ochranu: 33 respondentů (23,9 %)
- Ne: 38 respondentů (27,5 %)
- Nevím: 33 respondentů (23,9 %)

Graf 14: Používání antivirového programu



Zdroj: Vlastní zpracování

Výsledky ukazují, že pouze čtvrtina respondentů (24,6 %) má na svém zařízení nainstalovaný antivirový program. Dalších 23,9 % spoléhá pouze na základní ochranu, která bývá součástí operačního systému. Největší podíl odpovědí ale tvoří skupiny uživatelů, kteří buď žádný antivirus nemají (27,5 %), nebo si nejsou jistí, zda ho jejich zařízení obsahuje (23,9 %).

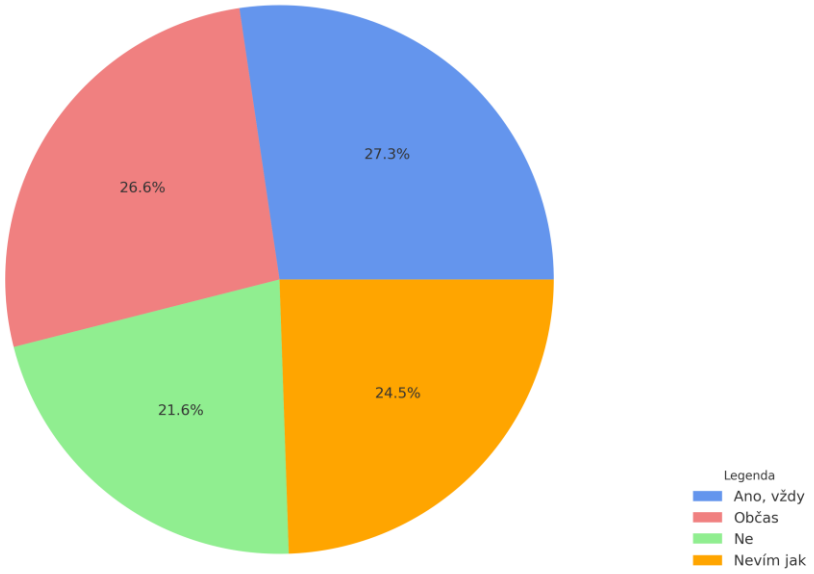
Celkově tedy téměř polovina respondentů (51,4 %) buď nemá dostatečnou antivirovou ochranu, nebo o ní nemá přehled. To je z hlediska kybernetické bezpečnosti alarmující zjištění, protože absence nebo podcenění antivirové ochrany zvyšuje riziko napadení malwarem, phishingem či jinými hrozbami.

Tento výsledek opět poukazuje na potřebu zvyšovat povědomí veřejnosti o důležitosti antivirových programů a obecně o technických opatřeních, která by měla být samozřejmou součástí každodenního používání internetu.

Otázka 15: Ověřujete si pravost e-shopů, e-mailů nebo odkazů?

- Ano, vždy: 38 respondentů (27,5 %)
- Občas: 37 respondentů (26,8 %)
- Ne: 30 respondentů (21,7 %)
- Nevím jak: 34 respondentů (23,9 %)

Graf 15: Ověřování pravosti online zdrojů



Zdroj: Vlastní zpracování

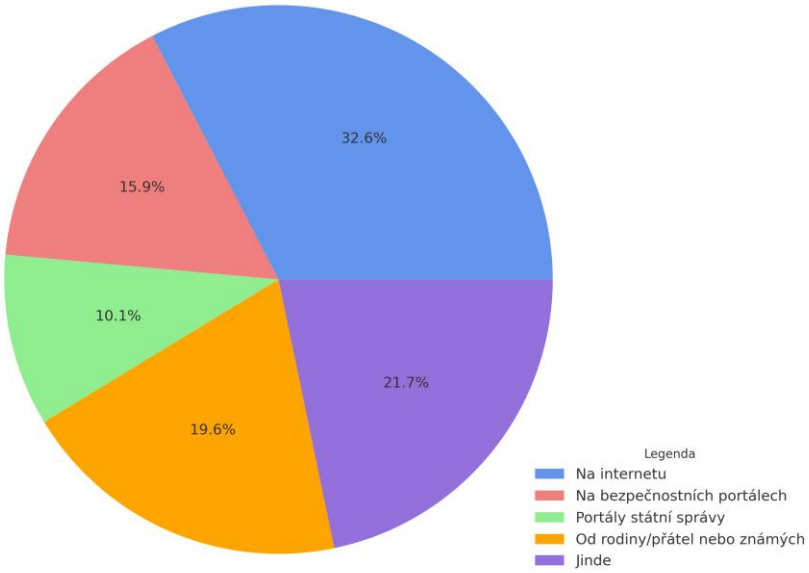
Výsledky této otázky ukazují, že pouze 27,5 % respondentů si pravost e-shopů, e-mailů nebo odkazů ověřuje vždy, což je méně než třetina. Dalších 26,8 % uvedlo, že tak činí občas. Zbylá téměř polovina respondentů přiznala, že si odkazy a elektronické komunikace neověřuje vůbec (21,7 %), nebo ani neví, jak na to (23,9 %).

To znamená, že až 45,6 % respondentů může být při pohybu na internetu výrazně zranitelných vůči phishingu, podvodným e-shopům či falešným odkazům. Výsledek tak odhaluje značné rezervy v oblasti preventivního chování uživatelů a zároveň upozorňuje na potřebu jednoduše dostupného vzdělávání a osvěty o základních principech ověřování online obsahu.

Otázka 16: Kde získáváte informace o tom, jak se bezpečně chovat na internetu?

- Na internetu: 45 respondentů (32,6 %)
- Na bezpečnostních portálech: 22 respondentů (15,9 %)
- Portály státní správy: 14 respondentů (10,1 %)
- Od rodiny/ přátel nebo známých: 27 respondentů (19,6 %)
- Jinde: 30 respondentů (21,7 %)

Graf 16: Zdroje informací o bezpečném chování na internetu



Zdroj: Vlastní zpracování

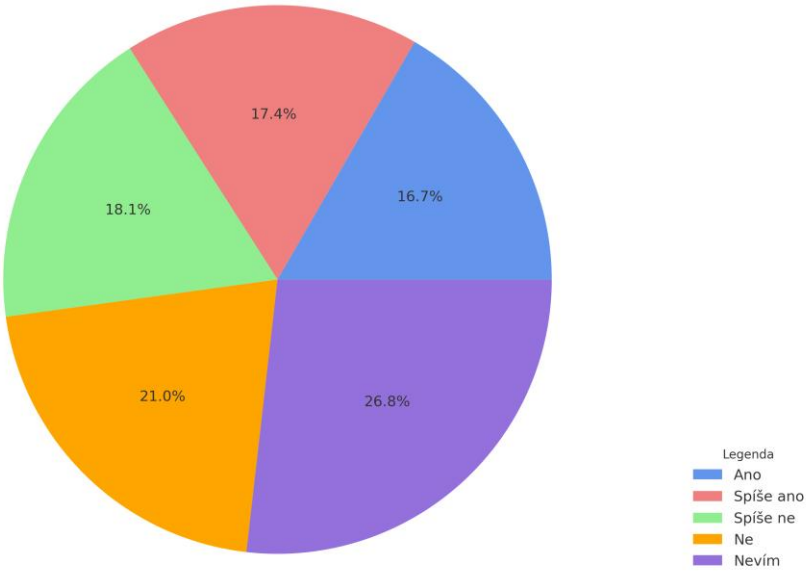
Výsledky ukazují, že největší část respondentů (45 osob, 32,6 %) získává informace přímo na internetu, například prostřednictvím článků nebo videí. Dalších 27 respondentů (19,6 %) čerpá informace od rodiny, přátel nebo známých. Bezpečnostní portály využívá 22 osob (15,9 %) a portály státní správy 14 respondentů (10,1 %). Odpověď „jinde“, která může zahrnovat například školu, práci nebo média, uvedlo 30 respondentů (21,7 %).

Z výsledků vyplývá, že formální a oficiální zdroje informací jsou využívány méně než neformální a volně dostupné kanály. To potvrzuje důležitost zvyšování informovanosti veřejnosti a podpory oficiálních edukačních iniciativ v oblasti kybernetické bezpečnosti.

Otázka 17: Myslíte si, že Česká republika je dostatečně připravená na kybernetické hrozby?

- Ano: 23 respondentů (16,7 %)
- Spíše ano: 24 respondentů (17,4 %)
- Spíše ne: 25 respondentů (18,1 %)
- Ne: 29 respondentů (21,0 %)
- Nevím: 37 respondentů (26,8 %)

Graf 17: Vnímání připravenosti ČR na kybernetické hrozby



Zdroj: Vlastní zpracování

Výsledky ukazují, že důvěru v připravenost České republiky vyjádřilo pouze 34,1 % respondentů, zatímco 39,1 % ji vnímá spíše negativně.

Téměř 27 % dotázaných se nedokázalo vyjádřit. Tyto údaje ukazují na rozdělené vnímání veřejnosti a zároveň na značnou míru nejistoty ohledně státní připravenosti čelit kybernetickým hrozbám.

Celkové vyhodnocení dotazníku

Výsledky ukazují, že povědomí o kybernetické bezpečnosti sice mezi veřejností existuje (přes 89 % zná pojem), nicméně praktické zabezpečení je často nedostatečné. Méně, než třetina respondentů používá dvoufázové ověření nebo pravidelně zálohuje data. Silná hesla používá jen pětina dotázaných a antivirovou ochranu nemá zhruba 28 %.

Z hlediska vnímání připravenosti České republiky na kybernetické hrozby převažuje spíše nedůvěra nebo nerozhodnost – jen třetina dotázaných se vyjádřila pozitivně, zatímco 39 % uvedlo spíše negativní názor a 27 % nevědělo. To naznačuje, že kybernetická bezpečnost zůstává pro mnoho lidí abstraktním nebo nedostatečně komunikovaným tématem.

Celkově výsledky ukazují na potřebu zlepšení osvěty v oblasti kybernetické bezpečnosti, a to nejen ze strany státu, ale i prostřednictvím vzdělávacích a mediálních kanálů. Veřejnost má sice určité povědomí o rizicích, ale často neví, jak se konkrétně chránit.

Závěr

V této bakalářské práci jsme se zaměřili na analýzu kybernetické bezpečnosti v České republice z teoretického i praktického hlediska. V teoretické části jsme vymezili základní pojmy, popsali vývoj kybernetické bezpečnosti a přiblížili legislativní rámec České republiky, včetně platné národní strategie. Zabývali jsme se také nejčastějšími typy kybernetických útoků a konkrétními případy incidentů, které v posledních letech výrazně ovlivnily chod některých institucí a organizací.

Zaměřili jsme se na komplexní analýzu kybernetické bezpečnosti v České republice, a to jak z teoretického, tak praktického hlediska. V teoretické části jsme nejprve vymezili základní pojmy související s kybernetikou, kyberprostorem a kybernetickou bezpečností. Popsali jsme historický vývoj této oblasti a následně jsme se zaměřili na současné trendy v kybernetických hrozbách, typologii útoků a na klíčové pojmy, jako je malware, phishing, DDoS útoky nebo zneužití umělé inteligence. Dále jsme přiblížili právní rámec České republiky, včetně zákona o kybernetické bezpečnosti a Strategie kybernetické bezpečnosti ČR pro období 2021–2025. Věnovali jsme se rovněž analýze konkrétních případů kybernetických incidentů, které v uplynulých letech zasáhly státní i veřejné instituce.

V praktické části jsme provedli kvantitativní výzkum formou online dotazníkového šetření mezi uživateli internetu v České republice. Cílem bylo zjistit, jak veřejnost vnímá kybernetickou bezpečnost, jaká opatření ve svém online chování uplatňuje a jaké má zkušenosti s kybernetickými hrozbami. Získané odpovědi od 138 respondentů nám umožnily provést důkladnou analýzu. Zjistili jsme, že i když povědomí o problematice existuje, v praxi je často nedostatečné – mnoho uživatelů nevyužívá dvoufázové ověření, pravidelně nezálohuje data, ani si neověřuje pravost e-mailů a odkazů. Zároveň jsme identifikovali určitou míru nedůvěry ve schopnost České republiky efektivně čelit kybernetickým hrozbám.

Na základě výsledků výzkumu jsme dospěli k závěru, že kybernetická bezpečnost je sice vnímána jako důležité téma, ale existují značné mezery v informovanosti, digitálních návycích i ve vzdělávání veřejnosti. Nejvíce zranitelnou skupinu tvoří uživatelé, kteří se v prostředí internetu pohybují denně, ale přesto nemají dostatečné znalosti o základních principech kybernetické ochrany. To

představuje reálné riziko nejen pro ně samotné, ale i pro instituce, v nichž pracují nebo s nimiž přicházejí do kontaktu.

Závěrem navrhujeme následující doporučení ke zlepšení současné situace kybernetické ochrany v ČR. Mezi nejdůležitější doporučení patří zvýšení investic do osvěty a vzdělávání, začlenění tématu kybernetické bezpečnosti do školních osnov, pravidelná školení zaměstnanců ve firmách i veřejných institucích a větší důraz na propagaci bezpečnostních nástrojů, jako je dvou faktorová autentizace nebo antivirová ochrana. Významnou roli by měl sehrávat i stát, který by měl jasněji komunikovat svá opatření a strategie směrem k veřejnosti, a tím zvýšit důvěru v úroveň národní kybernetické bezpečnosti.

Tato práce přispěla k hlubšímu pochopení problematiky a může sloužit jako výchozí podklad pro další výzkum, odbornou diskusi i navrhování praktických opatření v oblasti kybernetické bezpečnosti v České republice.

Seznam literatury

BARKER, Dylan. Malware Analysis Techniques: *Tricks for the triage of adversarial software.* Birmingham: Packt, 2021. ISBN 978-1-83921-227-7.

BHATTACHARYYA, Dhruba K. a KALITA, Jugal Kumar. *DDoS Attacks: evolution, detection, prevention, reaction, and tolerance*. Boca Raton: CRC Press, Taylor & Francis Group, 2016. ISBN 978-1-4987-2964-2.

CLARKE, A. Richard a KNAKE, Robert. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Ecco, 2011. ISBN 978-0061962240.

DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti.* Páté doplněné a upravené vydání. Praha: Česká pobočka AFCEA, 2022. ISBN 978-80-908388-4-0.

JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. s.19. ISBN 978-80-247-1561-2.

KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity.* CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. s. 41. ISBN 978-80-88168-31-7.

LIBICKI, Martin C. *Conquest in Cyberspace: National Security and Information Warfare.* New York: Cambridge University Press, 2007. ISBN 978-0-521-69214-4.

PANDE, J. *Introduction to Cyber Security*. Haldwani: Uttarakhand Open University, 2017, s. 23. ISBN 978-93-84813-96-3.

PORADA, Viktor, 2019. *Bezpečnostní vědy: úvod do teorie, metodologie a bezpečnostní terminologie.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-758-0.

POŽÁR, Josef. *Informační bezpečnost*. Vysokoškolské učebnice. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

REJZEK, Jiří. *Český etymologický slovník*. 2., nezměněné vydání. Voznice: Nakladatelství LEDA, 2012. ISBN 978-80-7335-296-7.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN 8073808498.

ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

ZELENÝ, Jaroslav a MANNOVÁ, Božená. *Historie výpočetní techniky*.1. vydání. Praha: Scientia, 2006. ISBN 80-86960-04-8.

Internetové zdroje:

ALEKSIC, Adam. *CYBER-PILOT*. Online. The Etymology Nerd. Dostupné z: https://www.etymologynerd.com/blog/cyber-pilot. [cit. 2025-03-01].

AVAST THREAT LABS. *Nemocnice pod náporem hackerů: Jak proběhly nejznámější kyberútoky na české nemocnice?* Online. Avast. 2021. Dostupné z: https://blog.avast.com/cs/nemocnice-pod-naporem-hackeru-jak-probihajikyberutoky-na-ceske-nemocnice. [cit. 2024-03-15].

ČESKÉ RADIOKOMUNIKACE A.S. *Kybernetická bezpečnost: Sedm fází kybernetického útoku*. Online. CRA.cz. 2021. Dostupné z: https://www.cra.cz/kyberneticka-bezpecnost-sedm-fazi-kybernetickeho-utoku. [cit. 2025-02-09].

FELL, Jade. *Hacking through the years: a brief history of cybercrime*. Online. The Institution of Engineering and Technology. 2017. Dostupné z: https://eandt.theiet.org/2017/03/13/hacking-through-years-brief-history-cyber-crime. [cit. 2025-02-09].

HOLAKOVSKÝ, Jiří. *Kybernetická bezpečnost v České republice*. Bakalářská práce, vedoucí Ing. Michaela Henzlová Ph.D. Praha: AMBIS vysoká škola, a.s, 2022. Dostupné také z: https://is.ambis.cz/th/auw08/Bakalarska_prace_-_Jiri_Holakovsky_.pdf.

CHRISTENSSON, Per. *Cyberspace Definition*. Online. SHARPENED PRODUCTIONS. TechTerms.com. 2024. Dostupné z: https://techterms.com/definition/cyberspace. [cit. 2025-02-10].

KOLOUCH, Jan. *Cybercrime*. Online. CZ.NIC, 2016. ISBN 978-80-88168-15-7. Dostupné z https://knihy.nic.cz/cs/detail/14/. [cit. 2025-02-09].

MINISTERSTVO VNITRA ČR. *Zákon č. 205/2017 Sb.: Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů*. 2017. Dostupné z: https://www.e-sbirka.cz/sb/2017/205?zalozka=text. [cit. 2025-02-09].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Slavnostní setkání k 5. výroční založení NÚKIB.* Online. 2022. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/1859-slavnostni-setkani-k-5-vyrocni-zalozeni-nukib/. [cit. 2025-02-09].

ORTMANN, Matyáš. *Kybernetická bezpečnost České republiky v roce 2023: Výzvy a trendy*. Online. CZECH ARMY & DEFENCE MAGAZINE. CZDEFENCE.cz. Praha, 2024. Dostupné z: https://www.czdefence.cz/clanek/kyberneticka-bezpecnost-ceske-republiky-v-roce-2023-vyzvy-a-trendy. [cit. 2025-02-09].

PAGE, Bob. *A Report on the Internet Worm*. Online. Toronto Metropolitan University. 1988, 2024. Dostupné z: https://www.ee.torontomu.ca/~elf/hack/iworm.html. [cit. 2025-02-09].

RESPEKT. *Útok pokračuje. Hackeři si vzali na mušku zdravotnické zařízení ministerstva vnitra*. Online. Dostupné z: https://www.respekt.cz/agenda/utok-pokracuje-hackeri-si-vzali-na-musku-zdravotnicke-zarizeni-ministerstva-vnitra/.[cit. 2025-03-30].

Seznam grafů

Seznam příloh

Příloha č. 1 – Dotazník – Vnímání kybernetické bezpečnosti mezi uživateli internetu

1. Jaké je vaše pohlaví?

a) Muž

b) Žena

2. Do jaké věkové skupiny patříte?

a) do 18 let

b) 18–25 let

c) 26–35 let

d) 36–50 let

e) nad 50 let

3. Odkud pocházíte?

a) Hlavní město Praha

b) Krajské město

c) Menší město

d) Venkov / obec

e) Nechci uvádět

4. Jak často používáte internet?

a) Denně

b) Několikrát týdně

c) Jednou týdně nebo méně

d) Nepoužívám internet

5. K jakým účelům nejčastěji používáte internet? (možné více odpovědí)

a) Sociální sítě (např. Facebook, Instagram)

b) Nakupování online

c) Práce / škola

d) Zábava (YouTube, Netflix apod.)

e) Bankovnictví a finance

f) Vyhledávání informací

g) Jiné: _____

6. Využíváte při své práci připojení k internetu?

a) Ano, pravidelně

b) Občas

c) Ne

d) Nejsem ekonomicky aktivní / nepracuji

7. Domníváte se, že je vaše pracoviště (firma, organizace) dostatečně zabezpečeno proti kybernetickým útokům?

a) Ano, plně důvěřuji nastavení bezpečnosti

b) Spíše ano, ale jsou možné rezervy

c) Spíše ne, zabezpečení není dostatečné

d) Ne, zabezpečení je slabé

e) Nedokážu posoudit

8. Setkali jste se někdy s pojmem kybernetická bezpečnost?

a) Ano

b) Ne

9. Máte představu, co znamená pojem kybernetický útok?

a) Ano, rozumím tomu dobře

b) Mám základní představu

c) Ne, nerozumím tomu

10. Stali jste se někdy cílem nebo obětí kybernetického podvodu či útoku?

a) Ano

b) Ne

c) Nejsem si jistý/jistá

11. Používáte na internetu silná hesla (kombinace velkých a malých písmen, čísel, znaků)?

a) Ano, vždy

b) Snažím se o to

c) Neřeším to

d) Nevím, co je považováno za silné heslo

12. Používáte dvoufázové ověření (např. SMS kód nebo ověřovací aplikaci)?

a) Ano

b) U některých služeb

c) Ne

d) Nevím, co to je

13. Zálohujete svá data (např. fotografie, dokumenty)?

a) Ano, pravidelně

b) Občas

c) Ne

d) Nevím, jak se to dělá

14. Máte na svém zařízení (počítači, notebooku, telefonu) nainstalovaný antivirový program?

a) Ano

b) Jen základní ochranu (např. Windows Defender)

c) Ne

d) Nevím

15. Ověřujete si pravost e-shopů, e-mailů nebo odkazů, na které klikáte?

a) Ano, vždy

b) Občas

c) Ne

d) Nevím, jak to poznat

16. Kde získáváte informace o tom, jak se bezpečně chovat na internetu? (možné více odpovědí)

a) Z médií

b) Od přátel nebo rodiny

c) Ze školy nebo práce

d) Ze sociálních sítí

e) Nezjišťuji si tyto informace

f) Jinde: _____

Otázka 17: Myslíte si, že Česká republika je dostatečně připravená na kybernetické hrozby?

a) Ano

b) Spíše ano

c) Spíše ne

d) Ne

e) Nevím