Srovnání mezigeneračních pohledů na kyberbezpečnost

Jakub Výkruta

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Jakub Výkruta**
Osobní číslo:	**L21534**
Studijní program:	**B1032A020002 Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Srovnání mezigeneračních pohledů na kyberbezpečnost**

Zásady pro vypracování

1. Zpracujte literární rešerši na dané téma a to včetně vymezení právního rámce se zaměřením na dokumenty z předmětné oblasti.
2. Proveďte dotazníkové šetření za účelem zjištění povědomí o problematice kybernetických hrozeb.
3. Proveďte analýzu nad získanými daty, a to i v souvislosti s vybranými dříve provedenými výzkumy.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. 1.vyd. Praha: CZ. NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
2. MITNICK, Kevin a Robert VAMOSI. *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data*. New York: Back Bay Books, Little, Brown and Company, 2019. ISBN: 978-0-316--38052-2.
3. SILBERBERG, Adam. *Všichni máme právo na soukromí: Konspirativní techniky*. V prvním vydání. Praha: Restart project, 2018. ISBN 978-80-270-4239-5.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Pavel Tomášek, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2023**
Termín odevzdání bakalářské práce: **3. května 2024**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 4. prosince 2023

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 3. 5. 2024

Jméno a příjmení studenta: Jakub Výkruta

.....
podpis studenta

ABSTRAKT

Tato bakalářská práce se soustředí na srovnání mezigeneračních pohledů na kyberbezpečnost. Práce je rozdělena na dvě části – teoretickou a praktickou. Teoretická část práce vymezuje pojmy jako kyberbezpečnost a její problematiku obecně a charakterizuje jednotlivé generace. Praktická část práce nabízí analýzu získaných dat od respondentů pomocí dotazníkové metody.

Klíčová slova: generace, kyberbezpečnost, kybernetická obrana, kybernetická ochrana, kybernetická kriminalita

ABSTRACT

This bachelor's thesis focuses on comparing intergenerational perspectives on cybersecurity. The thesis is divided into two parts – theoretical and practical. The theoretical part of the thesis defines concepts such as cybersecurity and its issues in general and characterizes individual generations. The practical part of the thesis offers an analysis of the data obtained from respondents using a questionnaire method.

Keywords: generation, cyber security, cyber defence, cyber protection, cyber crime

Rád bych poděkoval vedoucímu mé bakalářské práce, panu Ing. Pavlu Tomáškovi, Ph.D. za jeho cenné rady a připomínky, které mi ochotně dával po celou dobu kompletování bakalářské práce. Také bych chtěl poděkovat všem respondentům, kteří si udělali čas a odpověděli na otázky v mém dotazníkovém šetření. Rovněž bych chtěl poděkovat své přítelkyni Lucii, která se mnou po celou dobu studia měla nesmírnou trpělivost a poskytovala mi podporu.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Téma kybernetické bezpečnosti bylo pro tuto bakalářskou práci zvoleno z více důvodů. Jedním z nich je bezpochyby ten, že se jedná o nadčasové a stále se proměňující téma, které se kontinuálně rozvíjí spolu s vývojem informačních technologií obecně. Dále je zde patrná i spojitost s oborem Ochrana obyvatelstva, jejíž je kybernetická bezpečnost neodmyslitelnou součástí. Ve středu zájmu oboru Ochrana obyvatelstva stojí nejen ochrana osob a majetku ve fyzické rovině, ale i jejich ochrana v kyberprostoru. Zároveň se jedná o oblast, do které se vývojem společnosti i technologií zapojuje stále více lidí různých generací, a tudíž je důležité tyto vědomosti šířit mezi odbornou i laickou veřejnost.

Spolu s tématem kybernetické bezpečnosti se práce soustředí na její interakci s generacemi X, Y a Z. Porozumění jednotlivým generačním teoriím s sebou totiž přináší možnosti, jak efektivně pracovat s jejími příslušníky ve spojitosti s kybernetickou bezpečností. Cílem mé bakalářské práce je porovnat jednotlivé přístupy těchto generací. Dílčími cíli je pak jim porozumět a zmapovat, jaké jsou dosavadní znalosti jejich příslušníků ohledně kybernetické bezpečnosti. Na základě těchto vědomostí pak lze s těmito příslušníky cíleně pracovat a jejich informovanost prohlubovat.

Tato bakalářská práce je rozdělena na část teoretickou a praktickou. Teoretická část práce popisuje legislativní ukotvení kybernetické bezpečnosti v České republice. Následuje kapitola věnovaná charakteristice generací X, Y a Z, přičemž se budeme soustředit zvlášť i na jejich přístup ke kyberbezpečnosti. Poslední teoretická kapitola je zaměřená na kybernetické hrozby a bezpečnost samotnou, přičemž jsou zde uvedeny i konkrétní příklady kybernetických útoků.

Praktická část práce je rovněž rozdělena do několika částí – metodologické, analytické a diskuzní. V první zmíněné je popsán výzkumný cíl práce spolu s výzkumnými otázkami a hypotézami. Dále zde je vybrán design práce, výzkumná metoda a vzorek respondentů, se kterým je dále pracováno. Zvolenou výzkumnou metodou je dotazník. Analytická část práce je věnována rozboru získaných dat, které zde jsou porovnány s již provedenými (zahraničními) výzkumy na totožné či příbuzné téma. Závěrečná kapitola je věnována shrnutí výsledků dotazníkového šetření, a také odpovědím na výzkumné otázky a hypotézy.

I. TEORETICKÁ ČÁST

1 LITERÁRNÍ REŠERŠE A VYMEZENÍ PRÁVNÍHO RÁMCE

V následující kapitole je představen právní rámec a legislativní vymezení problematiky kybernetické bezpečnosti. V rámci této bakalářské práce je pozornost soustředěna pouze na tuto problematiku v tuzemském prostředí, a tudíž je zde vymezen právní rámec zahrnující pouze Českou republiku. V následujícím textu jsou uvedeny pouze klíčové zákony a vyhlášky, neboť jde o problematiku velmi rozsáhlou.

1.1 Právní rámec problematiky kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti – je legislativní dokument stanovující práva a povinnosti orgánů veřejné moci a osob v oblasti kybernetické bezpečnosti v České republice. Nevztahuje se však na informační nebo komunikační systémy, které pracují s utajovanými informacemi. V zákoně jsou vymezeny základní pojmy, bezpečnostní opatření a jejich úrovně. (Česko, 2014)

Ze základních pojmů je na místě zmínit definici pojmu bezpečnost informací, čímž tento zákon rozumí „*zajištění důvěrnosti, integrity a dostupnosti informací a dat*“ (NÚKIB, nd.). Domnívám se, že nezbytné je zmínit také samotný pojem kybernetického prostoru, jenž zákon vymezuje jako „*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací*“. (NÚKIB, nd.)

Jedná se o základní pojmy, které jsou v tomto zákoně popisovány velmi široce. V rámci této bakalářské práce je mým cílem zjistit, jakým způsobem se dotázaní respondenti orientují v problematice kybernetické bezpečnosti. Výsledky dotazníku by současně měly dokládat to, jakým způsobem se respondenti chovají v kybernetickém prostoru, ať už se jedná o citlivé prostředí (např. internetové bankovnictví, elektronická pošta) nebo rozhraní sociální sítí.

Zákon č. 205/2017 Sb., Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony – implementuje požadavky směrnice NIS, upravuje oblasti jako obsah a strukturu bezpečnostní dokumentace, rozsah bezpečnostních opatření, hodnocení a hlášení kybernetických bezpečnostních incidentů. (Česko, 2017a)

Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) - implementuje Směrnici Evropské Unie (EU) o bezpečnosti sítí a informačních systémů (Směrnici NIS) do českého právního řádu. (Česko, 2018)

Zákon č. 110/2019 Sb., Zákon o zpracování osobních údajů – fyzická bezpečnost je relevantní i podle zákona č. 110/2019 Sb., který se týká ochrany osobních údajů. Tento právní předpis identifikuje fyzickou bezpečnost jako jedno z hledisek ochrany osobních údajů. Podle tohoto zákona je fyzická bezpečnost definována jako opatření zabezpečující budovy, místnosti, skříně, archivy a zařízení, jako jsou počítače, servery a mobilní telefony, kde jsou uloženy osobní údaje, aby se zabránilo neoprávněnému přístupu, manipulaci, poškození nebo ztrátě těchto údajů. Zákon specifikuje, že správci a zpracovatelé osobních údajů mají povinnost zajistit fyzickou bezpečnost těchto objektů a zařízení. (Česko, 2019)

Zákon č. 297/2016 Sb., Zákon o službách vytvářejících důvěru pro elektronické transakce – tento zákon vymezuje postupy a požadavky na služby vytvářející důvěru, rovněž upravuje sankce, které viníka postihují v případě porušení povinností v této oblasti. Zároveň se soustředí na působnost Digitální a informační agentury. (Česko, 2016)

Zákon č. 250/2017 Sb., Zákon o elektronické identifikaci – tento zákon hovoří o jejím využití, možných přestupcích a dále o působnosti Digitální a informační agentury. Zákon také vymezuje pojem akreditace, povinnosti kvalifikovaného správce, držitele nebo kvalifikovaného poskytovatele. (Česko, 2017b)

Zákon č. 12/2020 Sb., Zákon o právu na digitální služby a o změně některých zákonů – jedná se o velmi rozsáhlý zákon, který se v několika částech soustředí na změnu zákona o svobodném přístupu k informacím, na obecné právo na digitální služby nebo změnu zákona o informačních systémech veřejné správy. (Česko, 2020)

1.2 Literární rešerše problematiky kybernetické bezpečnosti

Kybernetická (ne)bezpečnost. Problematika bezpečnosti v kyberprostoru – v publikaci je pojem kybernetické bezpečnost popsán v širších souvislostech a pojat z pohledu aktuální bezpečnostní situace v kyberprostoru, vývoje nových technologií a systémové integrace. (Konečný a Sedlák, 2021)

Routledge Handbook of International Cybersecurity – příručka zabývající se kybernetickou bezpečností na mezinárodní úrovni. Zahrnuje národní, regionální a globální přístupy k otázkám kybernetické bezpečnosti. Zahrnuje diskuze ohledně role Organizace spojených národů (OSN), mezinárodního práva a kybernetických konfliktů v oblasti kybernetické bezpečnosti. (Tikk a Kerttunen, 2020)

Social Engineering Hacking Systems, Nations, a Societies – kniha zdůrazňuje nedostatky lidského článku v oblasti kybernetické bezpečnosti. Popisuje způsoby předvídání a předcházení kybernetických útoků prováděných sociálním inženýrstvím. Podtrhuje kritickou roli lidského jednání v případě kybernetického útoku a poskytuje strategie, které je možné použít pro obranu před těmito útoky. (Erbschloe, 2019)

Cybersecurity – v knize jsou objasněny základní dovednosti, které jsou nezbytné k bezpečnému chování v kyberprostoru. Dále v knize můžeme najít bližší vysvětlení některých právních norem vztahujících se k této problematice. (Kolouch a Bašta, 2019)

The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data – kniha od jednoho z největších expertů na kybernetickou bezpečnost současnosti je určena pro širokou veřejnost. Autor se v knize snaží vysvětlit, jak důvody nezbytnosti anonymního a bezpečného chování na internetu, tak i postupy, jak výše zmíněného dosáhnout. (Mitnick a Vamosi, 2019)

Všichni máme právo na soukromí: Konspirativní techniky – v této knize je možné najít podrobný popis různých možností a způsobů odposlouchávání a jiných zásahů do soukromí, jakož i způsoby obrany pro každého člověka v kyberprostoru. (Silberberg, 2018)

2 ROZDĚLENÍ GENERACÍ

Následující kapitola se soustředí na představení jednotlivých generací, které jsou předmětem této bakalářské práce. Na začátku kapitoly je věnován prostor rozdělení jednotlivých generací obecně, posléze jsou podkapitoly věnovány každé generaci a jejím specifikům zvlášť.

Než se budeme zabývat popisem jednotlivých generací, je potřeba, abychom porozuměli samotnému pojmu generace. Obecně můžeme říct, že se jedná o sociologický pojem, který sdružuje, a také rozděluje členy společnosti do několika (věkových) skupin. (Betz, 2019) Zmiňované rozdělení do skupin, generací, je ale obtížné sjednotit. Některé studie popisují generace na základě společných hodnot a životních priorit, které příslušníci v rámci konkrétní generace sdílí. Současné moderní studie ale dávají přednost stanovení příslušnosti k dané generaci dle roku narození jedince. Také se můžeme setkat i s alternativním rozdělením generací na základě například stylu komunikace nebo přístupu k pracovnímu životu. Tato rozdělení jsou ale využitelná spíše pro výzkum v oblasti humanitních věd, což se ale neshoduje se zaměřením této bakalářské práce.

V odborné literatuře se spíše setkáme s tím, že studie jsou zaměřené pouze na jednu z generací, které se věnují do hloubky. Bohužel už najdeme méně těch, které by nabízely přehled všech generací. Pokud už nějaký ucelený systém najdeme, jednotliví autoři se mezi sebou odlišují tím, jak k členění generací přistupují. Neexistuje žádné oficiální rozdělení generací, které by ostatní zaštiťovalo a s jistotou a přesností rozdělovalo jednotlivé generace. Generaci je třeba vnímat jako živý a stále se proměňující pojem, tudíž není výjimkou ani to, když se jednotlivé generace a roky, dle kterých se jejich příslušnost rozděluje, překrývají. (Dimock, 2023)

V této práce bude použito rozdělení dle Pew Research Center:
Generace X: 1965–1980
Generace Y: 1981–1996
Generace Z: 1997–2012
(Dimock, 2019).

Zároveň se také můžeme setkat s rozdílným pojmenováním jednotlivých generací ve srovnání se zahraniční a českou odbornou literaturou. Například, generace X je termín, který označuje skupinu lidí narozenou v letech 1965–1980 v USA. Tento pojem bychom

samozřejmě mohli užívat i v českém kontextu, nicméně využívá se i pojem tzv. generace Husákových dětí. (ČSÚ, 2014) Této generaci se budeme podrobně věnovat v následující podkapitole.

2.1 Generace X

Generace X označuje skupinu lidí, která se narodila v letech 1965–1980. Setkáváme se u ní s rozdílným pojmenováním generací ve srovnání se zahraniční a českou odbornou literaturou. Generace X je termín, který označuje skupinu lidí narozenou v letech 1965–1980 v USA. Tatáž věková skupina lidí je označována v českém kontextu jako tzv. generace Husákových dětí. V České republice tím nazýváme generační vlnu, která přicházela na svět na přelomu 70. let 20. století vlivem propopulační státní politiky, která vzešla spolu s nástupem prezidenta Gustava Husáka, od nějž se název generace odvozuje. (Klímová, 2022)

Cílem propopulační politiky bylo motivovat obyvatelstvo k vyšší porodnosti a podpoře rodin obecně. Silný populační nárůst s sebou přinesl několik důsledků – rodiny obvykle vychovávají více dětí, ve školách se zvyšuje počet dětí ve třídách a později se zvyšuje i počet zaměstnanců na pracovišti. Ačkoliv se nám to zpočátku nemusí jevit jako pozitivní, generace Husákových dětí dokázala tyto zkušenosti později využít ku svému prospěchu. Vlivem toho, že mnoho z nich vyrůstalo s více sourozenci a jednoduše ve skupině více lidí, musel se každý, kdo chtěl něčeho dosáhnout, umět prosadit. Když se pak v roce 1989 vyskytla možnost svobodného podnikání, Husákovy děti věděly, jak přitáhnout pozornost ostatních ve svůj prospěch. (ČSÚ, 2014) V současné době je generace Husákových dětí na pomezí produktivního a předdůchodového věku. S ohledem na jejich četné zastoupení ve společnosti a stále se snižující porodnost lze očekávat problémy ve spojitosti s jejich finančním zajištěním v důchodovém věku. I přesto, že se s jejich odchodem do starobního důchodu uvolní mnoho pracovních míst, můžeme předpokládat potíže se zajištěním takového množství penzistů.

Přesto, že se jedná o jednu z nejvzdělanějších generací, směrem k technologiím jsou její příslušníci hodně skeptičtí a spíše pragmatičtí. Z hlediska učení se ale jedná o velmi tvárné jedince, kteří rádi vyhledávají způsoby toho, jak svou práci mohou udělat chytřeji a rychleji. Co se týče jejich pohybu na webových stránkách, například během online nakupování, mají tendence ignorovat reklamu mířenou přímo na jejich věkovou skupinu. Dávají přednost

prozkoumávání a hodnocení dostupného zboží „na vlastní pěst“. Zároveň ze všech generací nejvíce tíhnou k návštěvám internetových poraden a různých názorových webů, kde si mohou přečíst recenze a při výběru produktu se inspirovat i zkušeností ostatních uživatel. (Klímová, 2022)

2.2 Generace Y

Pojmem generace Y je nazývána skupina lidí narozena mezi lety 1981–1996. Jak už bylo řečeno výše, časová ohraničení jednotlivých generací se můžou napříč odbornými zdroji různit. Nicméně, společným jmenovatelem této generace je spojitost se vstupem do nového milénia, tedy rokem 2000. I z tohoto důvodu se často setkáváme s označením „generace Mileniálů“, což je jen další z názvů pro generaci Y. V rámci generační hierarchie můžeme Mileniály popsat jako potomky generace X, a zároveň jako generaci předcházející generaci Z. (Dimock, 2019)

Jedním z nejvýznamnějších charakteristických rysů generace Y je ten, že se jedná o první generaci, která vyrůstala v době rozšíření internetu a jeho personifikované podoby do běžných domácností. I to je důvod, proč je pro Mileniály přirozené využívat jeho služeb na denní bázi – ať už pro komunikaci s přáteli, ale i pro nakupování, hledání zaměstnání, nebo jako zábavnou platformu pro sledování videí, filmů nebo poslouchání hudby. Neopomenutelný je i význam sociálních sítí, které nám umožňují zůstávat v kontaktu s našimi blízkými, ale i seznamovat se s novými lidmi pomocí aplikací, jako je třeba Tinder, Bumble nebo Hinge. (Zelazko, 2024)

Seznamovací aplikace nabízí svým uživatelům zábavný způsob, jakým mohou poznávat hned několik potencionální partnerů najednou – rychle, snadno a třeba přímo z pohodlí vlastního domova. K seznámení se s přitažlivým protějškem uživateli stačí pouhý pohyb prstu, zleva doprava, po displeji mobilního telefonu. S užíváním seznamovacích aplikací se ale pojí několik rizik, která už sice nejsou natolik poutavá nebo zábavná, ale je o to více je třeba zvyšovat o nich povědomí. (Zelazko, 2024)

V roce 2018 byla provedena studie s názvem Are You Dating Danger? An Interdisciplinary Approach to Evaluating the (In) Security of Android Dating Apps, která se podrobně věnuje problematice nebezpečí skrze seznamovací aplikace. Možná nebezpečí spojená s jejich užíváním rozděluje na fyzická a psychická. Mezi ta fyzická řadí například vraždu, stalking nebo sexuální napadení, mezi ta psychická pak krádež identity, obtěžování nebo cyber-

stalking. Studie upozorňuje zejména na špatně navržené mobilní aplikace a nedostatečné bezpečnostní mechanismy daných aplikací. Ve studii bylo přímo demonstrováno to, jak snadné je prostřednictvím tzv. dating app získat přístupové tokeny v prostém textu. Ty pak může případný útočník využít nejen k získání citlivých informací skrze seznamovací aplikaci, ale třeba také skrze účet na sociální síti Facebook. Autoři studie tedy apelují nejen na vývojáře seznamovacích aplikací, ale také na zvýšené povědomí a vzdělávání uživatelů těchto aplikací ohledně nebezpečí, kterým se mohou vystavovat. (Shetty et al., 2021)

2.3 Generace Z

Generací Z nazýváme skupinu lidí narozenou v 1997–2012. V rámci hierarchie jednotlivých generací se jedná již o třetí v pořadí, která ve svém názvu nese písmeno (X, Y, Z). Zároveň se jedná o koncové písmeno abecedy, tudíž generace, která bude následovat, ponese název generace Alfa, což je první písmeno abecedy řecké, která na ni navazuje. (Dimock, 2019)

Co se týče její charakteristiky, jedná se o skupinu mladých lidí s velmi širokou škálou toho, co vnímají jako standartní. Mnoho z nich vyrostlo v prostředí, které je formovalo k otevřenosti vůči různým situacím nebo okolnostem, které by pro předcházející generace byly nepřijatelné. Mezi mnohými můžeme jmenovat například akceptující postoj k LGBTQ+ komunitě, rodinám, které jsou tvořeny pouze jedním rodičem s dětmi nebo jedinců, kteří se při identifikaci svého pohlaví nevejdou do škatulky muž, či žena. Významnou událostí bylo rovněž zvolení amerického prezidenta Baracka Obamy, coby prvního amerického prezidenta s černou barvou pleti. (Eldridge, 2024)

Generace Z je první generací, která prožila a stále žije svůj život s naprostým spojením s digitální světem. Většina jejích příslušníků si ani nemůže pamatovat svět před chytrými telefony a sociálními sítěmi. Ve srovnání s předchozí generací Y, která tíhne spíše k využívání sociálních sítí jako Facebook a Twitter, generace Z dává přednost Instagramu a Snapchatu. Příslušníci generace Y preferují tyto sociální sítě, kde prezentují svůj osobní obsah, který se rozhodli sdílet se svými přáteli, nebo celým internetovým světem. Kdežto generace Z, spíše využívá pseudo-anonymity a krátkého trvání poskytnutých informací, na což je aplikace Snapchat jako stvořená. Zmiňovaná sociální síť totiž nabízí tu výhodu, že pomocí ní můžeme ostatním posílat zprávy a fotografie, které se v historii chatu trvale neuloží. Osobě, která ji obdrží, je přístupná pouze omezenou dobu, a poté zmizí, pokud si je dotyčná osoba nestihne rychle uložit. (Eldridge, 2024)

Právě taková možnost v sobě ale skrývá mnohá nebezpečí a pokušení. Mladým lidem se najednou nemusí zdát tolik nebezpečné někomu poslat někomu své nahé fotky, když přece budou přístupné jen pár vteřin. Je třeba mezi mladými lidmi šířit povědomí o tom, že i jen pár vteřin pro ně může mít fatální následky, pokud narazí na člověka, který se rozhodne jejich lehkomyslnosti zneužít. (Eldridge, 2024)

Tato kapitola byla věnována charakteristice generací X, Y a Z, přičemž byl zvláštní fokus mířen na jejich přístup ke kyberbezpečnosti a online prostoru obecně. V následující kapitole bude pozornost věnována konkrétním typům kybernetických hrozeb.

3 KYBERNETICKÉ HROZBY

Kybernetické hrozby představují jednu z největších bezpečnostních výzev současnosti. S rostoucím počtem zařízení připojených k internetu a neustálým rozvojem digitálních technologií se objem a složitost těchto hrozeb neustále zvyšuje. Kybernetické útoky mohou mít mnoho forem a cílů, od krádeže citlivých informací po narušení klíčových infrastruktur.

Základem pochopení kybernetických hrozeb je poznání jejich rozmanitosti a proměnlivosti. Každý typ hrozby má specifické charakteristiky, které ovlivňují způsob, jakým může být na hrozbu reagováno nebo jak ji lze předcházet. Z tohoto důvodu je důležité, aby organizace a jednotlivci rozpoznali široké spektrum možných hrozeb a přizpůsobili své obranné strategie tak, aby byly co nejúčinnější.

Kategorizace těchto hrozeb je klíčová pro jejich efektivní řízení a prevenci. Bez porozumění různým formám a taktikám kybernetických útoků mohou být obranná opatření neúčinná nebo nedostatečná. Důležité je také sledovat neustálý vývoj a inovace v oblasti kybernetické bezpečnosti, což umožňuje lepší předvídání a reakci na nově vznikající hrozby. (Microsoft, ©2024a)

V následujících kapitolách budou tyto hrozby podrobněji rozebrány, což umožní hlubší pochopení každého specifického typu a jeho potenciálního vlivu na digitální bezpečnost.

3.1 Malware

Malware, zkratka pro "malicious software" (škodlivý software), je jakýkoliv software navržený k narušení, poškození nebo neoprávněnému přístupu k počítačovým systémům. Jeho hlavním účelem je infikovat, špehovat, poškodit nebo vykrást data z cílových systémů. Malware může přijít v mnoha formách, včetně virů, červů, trojských koní, spyware, adware a ransomware. (Microsoft, ©2024f)

Malware se může šířit různými způsoby, například formou e-mailových příloh, stahování software z neověřených zdrojů, infikovaných USB disků nebo prostřednictvím zranitelností v operačním systému či aplikacích. Útočníci také často využívají sociální inženýrství, jako je phishing, aby přiměli uživatele ke stáhnutí a instalaci malware. (Microsoft, ©2024f)

3.1.1 Spyware

Spyware lze obecně definovat jako druh malware, jehož cílem je sledování činnosti uživatele při práci na počítači. Jak už napovídá jeho název odvozený od anglického slova spy, tedy špión, dokáže se nepozorovaně dostat do operačního systému počítače a napáchat zde velké škody. Jeho hlavním cílem není přímo poškodit zařízení počítače, nicméně shromažďovat citlivá osobní data uživatele, která poté nezřídka kdy poskytuje třetí straně. Nebezpečí tkví právě v tom, že se takto děje často za (ne)vědomosti uživatele, který spyware zpřístupnil cestu skrze nainstalování aplikace, která v sobě skrývala dodatek o tom, že jejím obsahem může být i jmenovaný druh malware. (Aira Group s.r.o., ©2022)

Odhalit přítomnost spyware v počítači může být někdy obtížné. Některé jeho druhy, obzvláště pak ty, které jsou skutečně dobře navržené, dokážou v tichosti pracovat uvnitř zařízení a nepozorovaně sbírat citlivé informace uživatele. Existuje však i několik výstražných znamení, která nás mohou upozornit na možnou přítomnost spywaru v našem zařízení. Patří mezi ně například: zpomalení operačního systému nebo dalších programů, nepředvídatelné a nevyžádané přesměrovávání webového prohlížeče nebo odesílání spamů prostřednictvím vaší emailové adresy. (Eset, ©1992 – 2024a)

Pokud bychom měli jmenovat několik druhů spyware, lze zmínit například keylogger, jehož hlavní funkcí je shromažďování znaků, které uživatel stiskne na klávesnici. S touto funkcí je úzce spojen i infostealer, jenž dokáže snímat činnost uživatele ne skrze webkameru, ale právě díky keyloggeru. Významný je také password stealer, který, jak už napovídá název, dokáže ukrást hesla uživatele, která si automaticky ukládá ve webovém prohlížeči. Zákeřnost spyware dobře reprezentuje fake spyware removal tool, který se na první pohled prezentuje jako nástroj, jehož úkolem je spyware eliminovat, nicméně jeho cílem je ho naopak do zařízení nainstalovat. (Eset, ©1992 – 2024a)

Účinnou ochranou proti spyware je zcela jistě užívání antivirového programu. Do dalších obecných zásad patří například nenavštěvování webů s vyskakovacími okny nebo nestahování souborů z neověřených internetových zdrojů. Samozřejmostí zůstává i neotevírání podezřelých emailů od neznámých odesilatelů nebo příloh s příponou .exe. (Kaspersky, ©2024a)

3.1.2 Viry a červy

Než se budeme věnovat srovnání těchto dvou malware, představíme si je každého zvlášť. Počítačový virus je možné popsat jako „*škodlivý program, který se sám šíří bez vědomí uživatele kopírováním do jiného spustitelného programu nebo dokumentu*“ (Eset, ©1992 – 2024b). Jeho cílem je ovládnout napadené zařízení a získat citlivá a osobní data jeho uživatele. Jedním z nejčetnějších způsobů, jakým lze zapříčinit výskyt viru v našem zařízení, je prostřednictvím otevření zavirované emailové přílohy. V té nalezneme odkaz na nakaženou webovou stránku, ze které už vede přímá cesta viru do našeho zařízení. Podobně jako spyware, i virus dokáže pracovat postupně, tiše, nerušeně a hlavně netušeně, zatímco uživatel nadále pracuje na svém zařízení. Jeho úskalí spočívá právě v tom, že přítomnost viru v počítači se projeví až ve chvíli, kdy už je většinou pozdě. Do té doby nerušeně pracuje na získávání dat, a v okamžiku, kdy se nasycen, předává štafetu zpět původnímu programu. (Eset, ©1992 – 2024b)

Červ pracuje v počítači podobně jako virus. Je ale na místě vyzvednout rozdíl mezi nimi, tedy hlavně v ten ve způsobu, jakým se v zařízení šíří. Červ na rozdíl od viru nevyžaduje přímou účast uživatele na svém šíření. Stačí mu jedinkrát zpřístupnit cestu do našeho počítače, nejčastěji opět skrze síťové připojení nebo stažený soubor, a o zbytek se už postará sám. Nevyžaduje už další asistenci uživatele nebo znovuotevření infikovaného souboru. Dokáže se sám šířit a podobně jako virus v lidském těle, dál rozšiřuje své působení nejen v rámci konkrétního zařízení, ale i v rámci sítě, ze které původně vzešel. (Kaspersky, ©2024b)

Pokud se tedy budeme ptát, který z těchto dvou malware je nebezpečnější, přirozeně vyplývá, že odpovědí bude právě červ. Hlavním důvodem je právě jeho zmiňovaná samostatnost a nezadržitelné šíření, kterého je schopen i bez asistence a podpory uživatele. S tím úzce souvisí i škody, kterých díky této dovednosti dokáže napáchat mnohonásobně více, než tomu je u virů. (Latto, 2020)

3.1.3 Trojský kůň

Jak už napovídá název tohoto druhu malware, jeho chování je provázáno s historickou událostí z období starověkého Řecka. Báje vypráví o tom, jak řečtí bojovníci s pomocí bohyně Athény vybudovali dutého, dřevěného koně, kterého dopravili před brány města Trója. Doposud se jim nepodařilo brány města překonat, nicméně tehdy Trojané přijali sochu

koně jako dar a symbol příměří a sami si jej za brány města vtáhli. Netušili, že uvnitř koně čekají schovaní řečtí bojovníci, kterým se díky této lsti podařilo město dobýt. Na podobném principu funguje i stejnojmenný malware, kterému se nyní budeme podrobněji věnovat. (Eset, ©1992 – 2024c)

Vyznačuje se tím, že na první pohled působí velmi důvěryhodně. I to je totiž součástí jeho plánu – vypadat neškodně, nevzbuzovat v uživateli jakékoliv podezření, aby si sám do svého zařízení tento malware vpustil, podobně jako Trojané. Ve chvíli, kdy se ale v zařízení rozšíří, začne páchat škody dle toho, jakým způsobem byl naprogramovaný. Ve většině případů jde o zneužití dat uživatele, získání kontroly nad konkrétním počítačem či zpřístupnění zařízení pro další škodlivé softwary. (Eset, ©1992 – 2024c)

Jak už bylo zmíněno, každý trojský kůň je naprogramovaný k něčemu jinému. Nicméně, pro jejich účely je můžeme rozdělit do několika kategorií. Například, Rookit dokáže v našem zařízením skrýt některé činnosti, aby tak dopřál malware více prostoru pro nerušenou práci a šíření se. Backdoor je označen za jeden z nejnebezpečnějších, jelikož umožňuje jeho tvůrci na dálku ovládat, mazat nebo přeposílat soubory, tudíž je lehce zneužitelný pro trestnou činnost. Obecně platí, že trojské koně bývají zneužívané za cílem zcizit osobní údaje a zneužít je pro získání finančního obnosu. Ransomware bývá naprogramovaný právě k tomu, aby zablokoval přístup uživatele ke konkrétním částem počítače. Pokud chce uživatel omezení zrušit, jediným způsobem je uhrazení částky, kterou si stanoví ten, kdo malware naprogramoval. (Glamolija, 2024)

Rafinovanost trójského koně se projeví i v jeho působení přímo v zařízení. Dokáže v něm až měsíce setrvat, aniž by si jeho přítomnosti uživatel všimnul. Nicméně, pokud bychom měli jmenovat některé projevy jeho výskytu v zařízení, půjde o nenadálé změny v nastavení počítače, snížení jeho výkonu a výskyt dosud nezvyklé aktivity. Spolehlivým určením, zda se v zařízení opravdu nachází trójský kůň, je použití speciálního zařízení, tzv. Trojan scanner. (Fortinet, ©2024a)

3.1.4 Botnet

Botnet je možné popsat jako jeden z druhů malwaru, jehož fungování si lze představit jako rybářskou síť. Centrální zařízení, nazývané jako bot, je hlavním aktérem celého procesu, neboť v tomto procesu stojí za nastražením sítě. Uvnitř ní metaforicky rozhazuje škodlivý malware, většinou formou spamových emailů, a čeká, kdo z oslovených uživatelů se do sítě

chytí. Je důležité zmínit, že mezi oslovenými nemusí být pouze počítač, ale veškerá zařízení s přístupem na internet (smartphony, chytré televize apod.) Účinnou ochranou i v tomto případě může zaručit antivir. (Otoupal, ©2024)

V kontextu botnetu rozlišujeme dva odborné pojmy – bot heder, tedy kybernetický útočník (ten, kdo rozhazuje síť) a zombies, tedy zařízení, která má v plánu infikovat. Pokud se to útočníkovi podaří, může i na dálku získat plnou kontrolu nad daným zařízením. Zombies pak bývají často využíváni k tomu, aby se dostavili na konkrétní místo na webu, kde dostává úkoly od útočníka, které plní. Jejich obsahem jsou pak citlivé informace, které zasílají zpět bot hederovi. (Eset, ©1992 – 2024d)

3.2 ZPŮSOBY PROVEDENÍ KYBERNETICKÉHO ÚTOKU

V této podkapitole je představen pojem kybernetický útok a dále jeho příklady. Mezi všemi existujícími (například: DoS a DDoS útoky, zero-day exploit, sql injekce, atd.) byly zvoleny phishing a pharming, jelikož se jedná o jedny z nejrozšířenějších druhů útoků i v povědomí laické veřejnosti, a proto jim je věnováno nejvíce prostoru i v rámci této bakalářské práce.

Než bude pozornost podrobněji věnována jednotlivým druhům kybernetických útoků, je třeba, aby bylo definováno, co je tímto pojmem myšleno. Kybernetický útok lze popsat jako nedovolené a anonymní vniknutí do počítače nebo jiného výpočetního systému, jehož cílem je poškodit jeho uživatele. Konkrétním cílem může být třeba odcizení a zneužití citlivých dat, deaktivace zařízení nebo zneužití zařízení pro páchání dalších kyberútoků. Za těmito útoky může stát jak jednotlivec, tak celá skupina útočníků, kteří bývají nazýváni jako hackeři nebo hacktivisté. S vývojem společnosti nabývají i kybernetické útoky na promyšlenosti a důmyslnosti ze strany útočníků. Čím dál častěji bývají využívány jako nástroje ohrožující národní bezpečnost konkrétních států. Jejich motivem může být špionáž, krádež citlivých informací nebo jiné podvody. (Legislativa s.r.o., 2022)

Sílícímu vlivu kybernetických útoků přispívá samozřejmě i celková modernizace a digitalizace naší společnosti. Čím více prvků lidského života se přesouvá do online prostředí, přímo úměrně tím přibývá i potencionálních cílů, které mohou být napadeny hackery. O to více je třeba upozorňovat na to, jakými způsoby se lze před zcizením informací a kybernetickými útoky obecně chránit. „*Kybernetická bezpečnost se tak stala klíčovým aspektem digitálního věku*“ (Microsoft, ©2024a)

Útoky obecně je možné rozdělit na tři základní skupiny podle toho, na co cílí. Jedná se o útoky, které cílí na důvěrnost, tedy jejich snahou je získání citlivých informací uživatelů. (Microsoft, ©2024a)

Další skupinou jsou útoky mířené na integritu, které se snaží o zneužití konkrétních dat. Poslední skupinou jsou ty útoky, jejichž náplní je zamezení přístupu uživatelů k jejich osobním datům. (Legislativa s.r.o., 2022)

3.2.1 Phishing

Jedná se o zvláštní druh kybernetického útoku, který cílí na citlivé údaje uživatele spojené s jeho financemi. Většinou se pomocí nevyžádaného emailu snaží získat přístup k internetovému bankovnictví a žádá uživatele, aby mu poskytl své přihlašovací údaje. Setkat se ale lze i s variantou, kdy je cílem útoku infiltrace škodlivého kódu do uživatelova počítače. K šíření se tedy nevyužívá pouze prostředí elektronické pošty, ale i různé sociální sítě. (Eset, ©1992 – 2024e)

Ačkoliv je někdy obtížné rozpoznat, zda se jedná, či nejedná o phisingový útok, existuje několik obecných zásad, které při rozhodování mohou pomoci. První z nich je kontrola toho, z jaké emailové adresy byl konkrétní email odeslán – tady si lze všimnout toho, že útočníci posílají podezřelou poštu z adres, které sice vypadají na první pohled oficiálně, ale při bližším zkoumání si lze všimnout odchylek a překlepů. Překlepy a gramatické chyby v textu jsou dalším výstražným znamením. Stejně tak tomu je, pokud se jedná o zprávu, ve které odesílatel oznamuje, že příjemce vyhrál neobyčejně enormní sumu peněz nebo jiné velmi výhodné zboží. Posledním bodem je skutečnost, když se v emailu pokouší útočník vyvolávat nátlak – urguje, aby příjemce na jeho zprávu odpověděl co nejdříve. (Moneta, ©2024)

Jak se proti phishingu lze bránit? Je na místě být obezřetný a kontrolovat, kam zadávám své citlivé a přihlašovací údaje. Ty bychom mimo jiné neměli nikomu sdělovat, a tak se chránit před jejich zneužitím. Také se doporučuje neotevírat přílohy podezřelých emailů a už vůbec na ně reagovat. Univerzálním bodem ochrany zůstává pravidelná aktualizace softwaru a antivirového programu v našem zařízení (Moneta, ©2024)

3.2.2 Pharming

Pharming je typ kybernetického útoku, kdy při pokusu o připojení se k legitimní webové stránce dojde k přesměrování oběti na falešnou webovou stránku, která je vytvořena tak, aby

co nejvíc působila jako legitimní stránka, ke které se oběť snažila připojit. (Executech, ©2022.)

Pharmingový útok je proveden jedním ze dvou způsobů. Prvním způsobem je instalace malwaru na zařízení oběti, který má za cíl přesměrovat oběť na falešnou stránku, kde útočník vidí veškerá osobní data jako jsou přihlašovací údaje, které oběť vloží. (Insights Desk, 2023)

Druhým způsobem je napadení DNS serveru, který za normálních okolností slouží k přesměrování na legitimní webovou adresu. Nicméně po jeho napadení je žádost o přesměrování pozměněna tak, aby byla oběť přesměrována na alternativní nebo falešnou webovou stránku, kde je opět cílem získat osobní údaje oběti. (Fortined, ©2024b)

Účinnou obranou proti pharmingu je kontrolovaní Uniform Resource Locator (URL). Pokud je URL odlišná, byť jen jedním znakem, je nejlepší ze stránky odejít. Při kontrolování URL je také dobré neopomenout kontrolu internetového protokolu. Pouze stránky, které mají https protokol, umožňují zabezpečenou komunikaci. (Fortinet, ©2024b)

4 KYBERNETICKÁ BEZPEČNOST

Kapitola číslo čtyři je soustředěna na kybernetickou bezpečnost. V jejím úvodu je pracováno se samotným pojmem kybernetická bezpečnosti, a poté s jednotlivými technikami, které lze pro kybernetickou bezpečnost uplatňovat.

Kybernetická bezpečnost, nebo také digitální bezpečnost, se zabývá ochranou digitálních informací, zařízení a aktiv. Ve spojitosti s kybernetickou bezpečností je na místě zmínit zkratku „CIA“, která vyjadřuje tři pilíře kybernetické bezpečnosti:

Confidentiality (důvěrnost) – Je důležité, aby k datům a účtům měli přístup pouze autorizované osoby.

Integrity (integrita) – Zajištění toho, že data nebudou nikým pozměňována nebo odstraňována a nebude k nim vkládáno nic dalšího bez vědomí.

Access (přístup) – Mít jistotu neustálé možnosti přístupu k údajům a systémům. (Microsoft, ©2024b)

Zabezpečení našich zařízení a dat může být softwarové i nesoftwarové povahy. Správná kybernetická bezpečnost však využívá jak softwarové, tak nesoftwarové zabezpečení. Je skvělé mít zapnutou bránu firewall a nainstalovaný antivirový software, ale bez správných návyků a dostatečných znalostí to jednoduše stačit nemusí. (Microsoft, ©2024b)

V této kapitole jsou zmíněny pouze vybrané ochranné strategie, ačkoliv jich existuje velké množství (například: aktualizace softwaru zařízení z důvodu zero-day exploit, prohlubování vlastních znalostí kybernetických hrozeb a kybernetického prostředí, atd.). S ohledem na rozsah bakalářské práce se věnuji následujícím.

4.1 Zálohování dat

Data jsou to, co je ukládáno na našich zařízeních. Může se jednat o obrázky, videa, excelové tabulky, prezentace nebo například kvalifikační práce. I přes dodržení všech správných návyků, postupů a využívání antivirových softwarů není zaručeno, že zůstanou v bezpečí. Zařízení je možné nahradit, naše nezálohovaná data však nikoliv. (Lenovo, ©2024)

Nyní vyvstává otázka, jak často by bylo dobré důležitá data zálohovat. Většina zdrojů se shoduje na vhodnosti vytváření zálohy dat přinejmenším jednou týdně, ale ideálně každých 24 hodin. Tohle samozřejmě nemusí být nezbytné pro běžného uživatele, který nevytváří

důležitá data každý den. Nicméně, je možné říct, že pokud nahraji na některé ze svých zařízení data, o která nechci přijít, je dobré vytvořit jejich zálohu. (Lenovo, ©2024)

4.2 Silná hesla, jejich používání a vícefaktorové ověřování totožnosti

Každý člověk, který má vytvořenou emailovou adresu, účet na sociálních sítích, používá služby elektronického bankovnictví atd., je nucen si vytvořit minimálně jedno heslo, aby k těmto službám mohl mít přístup. Bohužel nežijeme ve světě, kde by nikdo jiný neměl zájem na znalosti tohoto hesla a je tedy nutné, aby toto heslo nebylo lehce prolomitelné.

Silné heslo by mělo mít dostatečný počet znaků a obsahovat velká i malá písmena, číslice a speciální znaky. Ideálně by takové heslo nemělo být lehce uhodnutelné, nemělo by nést jiný význam než náhodnou směs znaků a číslic. (EC-Council University, 2023)

Zapamatovat si takové heslo ale samozřejmě není jednoduché, a to i v případě, že bychom používali pouze jedno heslo pro každý účet. Většina z uživatelů internetu však nevyužívá pouze jeden účet a je doporučeno používat unikátní heslo pro každý z vlastněných účtů a zařízení. V případě, že chceme, aby naše hesla byla jedinečná, silná a těžce uhodnutelná, je dobré využívat software určený ke správě hesel jako je například KeePassX. (KeePassX, ©2005-2021) Tyto aplikace mohou hesla vytvářet, ale jejich hlavní účel je jejich bezpečné a šifrované ukládání, aby si uživatel nemusel pamatovat nesmyslné kombinace a neustále hesla obnovovat. (Mitnick a Vamosi, 2019)

Existují případy, kdy uživateli na jeho datech opravdu záleží a nechce riskovat jejich ztrátu nebo zneužití při kompromitaci našeho hesla. V takovém případě je na místě používání vícefaktorového ověření identity. Vícefaktorové ověření je něco, s čím se bez pochyby každý z uživatelů s přístupem k internetu setkal a jen o tom možná nepřemýšlel. (Microsoft, ©2024c)

Jako příklad je možné uvést elektronické bankovnictví. Pro přihlášení uživatel potřebuje své identifikační údaje (jméno a heslo), popřípadě PIN kód a unikátní kód zaslaný na emailovou adresu nebo telefonní číslo. Je mnoho možností vícefaktorového ověření identity a nemusí se jednat pouze o potvrzovací kódy zaslané na emailovou adresu nebo telefonní číslo. Může jít i o biometrické ověření totožnosti, jako je například otisk prstu nebo vytvořený vzorec. (Eset, ©1992 - 2024f)

4.3 Virtuální privátní síť (Virtual Private Network – VPN)

VPN vytváří šifrované spojení mezi zařízením a serverem provozovaným službou VPN, který poté provoz pošle dál na veřejné internetové sítě. Data, která se vracejí zpět na zařízení, podstoupí stejnou cestu přes šifrované spojení a zpět na zařízení. (Max a Stobing, 2023)

Používání VPN je obzvlášť vhodné v případě využívání veřejných sítí. Například při využívání veřejné WIFI v kavárně má každý, kdo tuto síť využívá potencionální schopnost zachytit a zneužít nejen citlivá data. (Microsoft, ©2024d)

Při využívání VPN je provoz na internetu šifrovaný a IP adresa maskována. Neznamená to však naprostou anonymitu. Webové stránky používají cookies, textové soubory zaznamenávající interakce na dané stránce, s jejichž pomocí utváří online profil. V podstatě jde o výměnu anonymity za používání služeb jako je emailová adresa, nebo účet na Amazonu. (Mitnick a Vamosi, 2019)

4.4 Antivirový software

Antivirem lze označit bezpečnostní program, jehož úkolem je vyhledávat kybernetické hrozby a účinně před nimi chránit konkrétní zařízení. (Eset, ©1992 - 2024g)

Pokud bychom se ale vrátili zpět v čase, zjistili bychom, že dříve se pod označením antivir skrýval pouze jednoduchý program, který dokázal počítačové viry snadno detekovat, popřípadě je odstranit. Souběžně s vývojem moderních technologií jsou ale dnešní antivirové programy mnohem výkonnější. Nabízí ochranu zařízení hned v několika vrstvách, a tím poskytují i účinnější ochranu nejen proti škodlivým kódům, ale také zabraňují prolomení hesel, krádeži uživatelských účtů a odcizení citlivých údajů. Dalším benefitem moderních antivirů je bezesporu i to, že dokáží chránit uživatele před spamem, spywarem nebo phishingem. V tomto ohledu zvládnou ochránit konkrétní zařízení nejen před škodlivými kódy, ale i před celými aplikacemi, které můžou negativně ovlivnit chod zařízení (např. snížit výkon, zobrazovat nevyžádaných obsah). (Eset, ©1992 - 2024g)

II. PRAKTICKÁ ČÁST

5 PRAKTICKÁ ČÁST

Obsahem praktické části práce je popis výzkumného plánu, metodologie výzkumu a jeho dílčích částí, kterými jsou výzkumný problém a výzkumné otázky, cíl práce, hypotézy a charakteristika výzkumného vzorku.

5.1 Výzkumný problém a cíl práce

Téma kybernetické bezpečnosti není zrovna novým pojmem. Jeho první použití lze najít již v roce 1971, kdy programátor Bob Thomas vytvořil virus, který měl odhalit systémové chyby a zranitelná místa. (MonroeCollege, ©2024)

Přesto se však nejedná o pojem, který by ztrácel na aktuálnosti. Pravda je opakem. V dnešním světě můžeme vidět snahu nahradit i běžné věci za technologicky vyspělejší elektronická zařízení. Jinými slovy – síť věcí, které jsou vybaveny softwarem, sensory a jinými technologiemi. Pro tato zařízení se ujal pojem Internet of Things (IoT), nebo česky internet věcí. Většina z nás nežije soběstačně odloučena od společnosti, a ať si to již uvědomujeme nebo ne, tak s IoT přicházíme do kontaktu na denní bázi. (Oracle, ©2024)

Je pro každého z nás přirozené chránit si svůj majetek. Na dveřích bytu nebo domu máme zámek, naše klíče od auta bychom nenechali bez dozoru ležet na kapotě a spousta z nás má na svém smartphonu kryt, který ho chrání před otřesy a pády. Nechráníme však pouze fyzické věci. Náš PIN od kreditní karty neříkáme nahlas a naše osobní citlivé údaje, jako jsou rodná čísla, čísla občanského průkazu nebo naše přihlašovací údaje, také neodhalujeme komukoliv. Tedy do chvíle, kdy si uvědomujeme, že tak nečiníme. Částka na našem bankovním účtu může převyšovat hodnotu našich hmotných statků a naše data pro nás mohou znamenat soukromí, kterého bychom se nechtěli vzdát. Ukradený počítač nebo telefon je nahraditelný, pokud ovšem máme vytvořenou zálohu. Nicméně, bez dostatečného zabezpečení zařízení má k těmto datům potencionální přístup kdokoliv, kdo ho zrovna drží v rukou. Bohužel, naše data nejsou zcela v bezpečí, i když máme svá zařízení přímo ve svých rukou. Tedy, pokud nemáme správný přístup ke kybernetické bezpečnosti.

Cílem práce je srovnat rozdíly v přístupech ke kybernetické bezpečnosti u generací X (viz podkapitola 2.1), Y (viz podkapitola 2.2) a Z (viz podkapitola 2.3) pomocí dotazníkového šetření.

5.2 Výzkumné otázky

Cílem praktické části této bakalářské práce je zjistit pomocí dotazníkového šetření, jak se liší přístup k bezpečnostním hrozbám v kyberprostoru mezi příslušníky generace X, Y a Z. Pro naplnění cíle praktické části byla stanovena hlavní výzkumná otázka a jedna vedlejší výzkumná otázka.

- Hlavní výzkumná otázka: Jakým způsobem reagují příslušníci jednotlivých generací na přítomnost kybernetických hrozeb?
- Vedlejší výzkumná otázka: Jakými způsoby se příslušníci jednotlivých generací chrání před kybernetickými hrozbami?

5.3 Hypotézy výzkumu

Pro výzkum jsem stanovil následující hypotézy:

- H1: Příslušníci generace X by častěji otevřeli přílohu zaslanou z neznámé emailové adresy než příslušníci generací Y a Z.
- H2: Respondenti všech generací budou mít častěji nastavené automatické přihlášení na stolním počítači/notebooku než na smartphonu/tabletu.

5.4 Charakteristika výzkumného vzorku

Výzkumný vzorek byl stanoven pouze na základě věkových kritérií. Jinými slovy, byli pro dotazníkové šetření vybráni pouze lidé narozeni v období od roku 1965 do roku 2012, tedy věkové rozmezí pro generace X, Y a Z.

5.5 Metodologie výzkumu

Před prací na praktické části své bakalářské práce jsem stanovil výzkumný plán. Prvním krokem bylo stanovení výzkumného problému a samotného cíle práce, na který dále navazují výzkumné otázky. Dalším krokem bylo zvolení designu práce a metody sběru dat. Souběžně byl záměrným výběrem stanovený výzkumný vzorek, se kterým bylo pracováno.

Chráska (2016) hovoří o rozdílnosti kvantitavního a kvalitativního výzkumu. Na základě účelu této práce jsem se rozhodl zvolit kvantativní design, který dokáže pracovat s velkým množstvím respondentů, což zároveň koresponduje s mým výzkumným cílem. Na tento design práce nasedá volba výzkumné metody, jako kterou jsem zvolil dotazník. Gavora (2010) popisuje dotazník jako ekonomicky velmi výhodnou metodu, jelikož dokáže za

krátký čas zpracovat velké množství dat od mnoha respondentů, což znovu odpovídá mému výzkumnému cíli.

Výzkumný vzorek byl stanoven na základě záměrného výběru. Gavora (2010) o něm mluví jako typu výběru, který pro který je vhodné vybrat pouze některé zástupce z celkového, tedy základního souboru. Pro svůj výzkum jsem stanovil kritéria účasti na základě generačních teorií. Podmínkou zapojení se do výzkumu tedy bylo to, aby respondenti věkově odpovídali buďto generaci X, Y, nebo Z.

Dotazník byl mezi respondenty rozšířen pomocí online prostoru, tedy skrze sociální sítě a další dostupné platformy, které jeho nasdílení umožňovaly. Zároveň jsem požádal o pomoc s nasdílením své blízké, ať už vrstevníky nebo své rodiče, aby se dotazník mohl dostat k co nejvíce lidem různého věku. Dotazník má celkem 27 položek a pro jeho sestavení byla využita platforma Google Forms, jelikož nabízí možnost přesměrování respondenta do příslušné části dotazníku na základě jeho odpovědi. Tato funkce je tedy při srovnávání výsledků několika skupin respondentů velmi dobrým pomocníkem. Sběr dat probíhal v termínu od 25.2.2024 do 19.3.2024.

V úvodu dotazníku bylo umístěno krátké představení výzkumníka a bakalářské práce. Při procesu sdílení dotazníku bylo potencionální respondentům sděleno, že účast ve výzkumu je zcela dobrovolná a mají možnost kdykoliv vyplňování dotazníku zanechat. Zároveň byla respondentům zaručena anonymita, neboť dotazník nevyžaduje žádné přihlášení či sdělení osobních údajů.

5.6 Předvýzkum

V rámci dotazníkového šetření byl proveden i předvýzkum. Dotazník jsem zaslal několika svým přátelům a mému otci, abych získal pohled více generací. Vysvětlil jsem jim cíle mého dotazníkového šetření a požádal je o zpětnou vazbu ohledně struktury a srozumitelnosti dotazníku.

Na základě zpětné vazby jsem poupravil, přidal a odebral některé otázky z dotazníkového šetření. Zpětná vazba se týkala především nesprávné formulace některých otázek, popřípadě jejich přílišné složitosti a možnosti potencionálního nepochopení otázky respondentem. Výsledná podoba dotazníku, který byl spuštěn k sesbírání dat od respondentů je přiložen jako příloha PI.

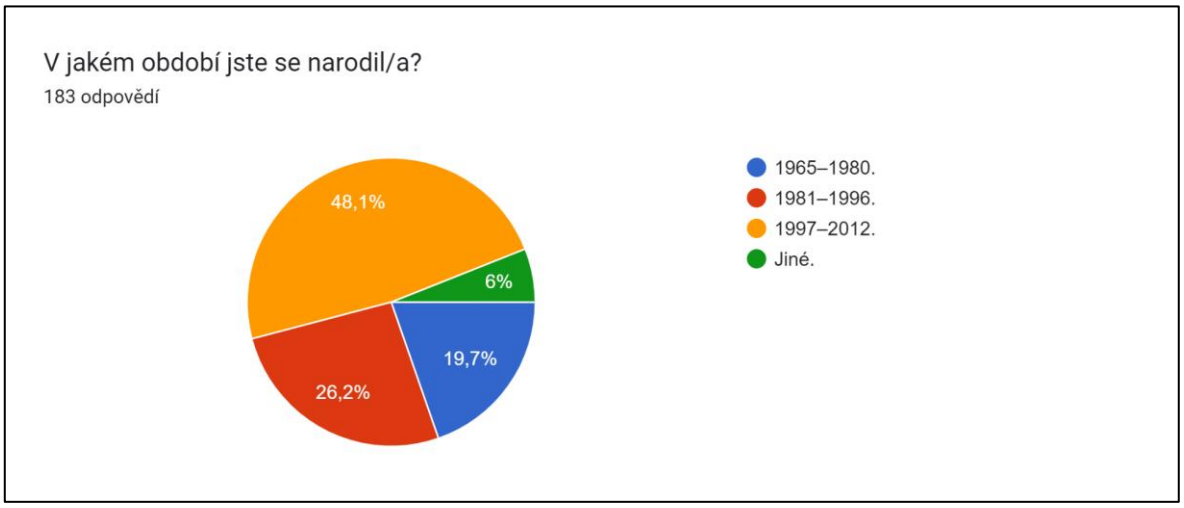
6 ANALÝZA VÝSLEDKŮ DOTAZNÍKOVÉHO ŠETŘENÍ

Následující kapitola se podrobně věnuje výsledkům dotazníkového šetření a zpracovává získaná data. Ta jsou následně konfrontována s již provedenými výzkumy podobného zaměření, ať už tuzemskými, či zahraničními.

Z důvodu vysokého počtu položek v dotazníku (celkem 27) budou v této kapitole představeny pouze jeho vybrané otázky. Zbytek otázek je vložen k nahlédnutí v příloze PI.

Otázka č. 1:

Dílčí výsledky dotazníkového šetření byly roztříděny pomocí vstupní otázky „V jakém období jste se narodil/a?“. Respondenty, kteří na tuto otázku zvolili možnost Jiné, dotazník automaticky přesměroval na konec dotazníku a dále tázáni nebyli.



Obrázek 1: Procentuální zastoupení věkových kategorií respondentů dotazníkového šetření

Největší počet respondentů byl z generace Z (1997–2012), který tvořil 92 z celkového počtu 183 odpovědí (48,1 %). Druhou nejvíce zastoupenou skupinou byla generace Y (1981–1996), jejíž příslušníci odeslali celkem 48 odpovědí (26,2 %). Poslední dotazovanou skupinou byla generace X (1965–1980) se zastoupením 36 odpovědí (19,7 %).

Otázka č. 2:

Po otázce týkající se období narození respondentů následovala otázka týkající se jejich pohlaví. Otázka sloužila k tomu, aby byl výsledný počet respondentů z každé generace rovnoměrně zastoupen z hlediska pohlaví. Tohoto dílčího cíle bylo nutné dosáhnout filtrováním respondentů a zasíláním dotazníků cíleně pouze těm, kteří byli potřební pro dosažení tohoto poměru. Výsledkem je, že každá generace má v dotazníku 50% zastoupení respondentů ženského pohlaví a 50 % respondentů mužského pohlaví.

Dle demografických dat z ČSÚ (2020) bylo obyvatelstvo ČR v roce 2020 rozprostřeno na 51 % žen a 49 % mužů. Procentuální rozdělení je rozdílné u různých věkových kategorií. Pro účely této bakalářské práce bylo uměle docíleno a dále pracováno s rovnoměrným zastoupením respondentů, tedy 50 % z nich byli muži a 50 % ženy napříč všemi dotazovanými generacemi.

Otázka č. 3:

Dotazovaní měli v této otázce subjektivně posoudit své znalosti z oblasti kyberbezpečnosti.

Obrázek 2: Vlastní zhodnocení znalostí kyberbezpečnosti u příslušníků generace X

Obrázek 3: Vlastní zhodnocení znalostí kyberbezpečnosti u příslušníků generace Y

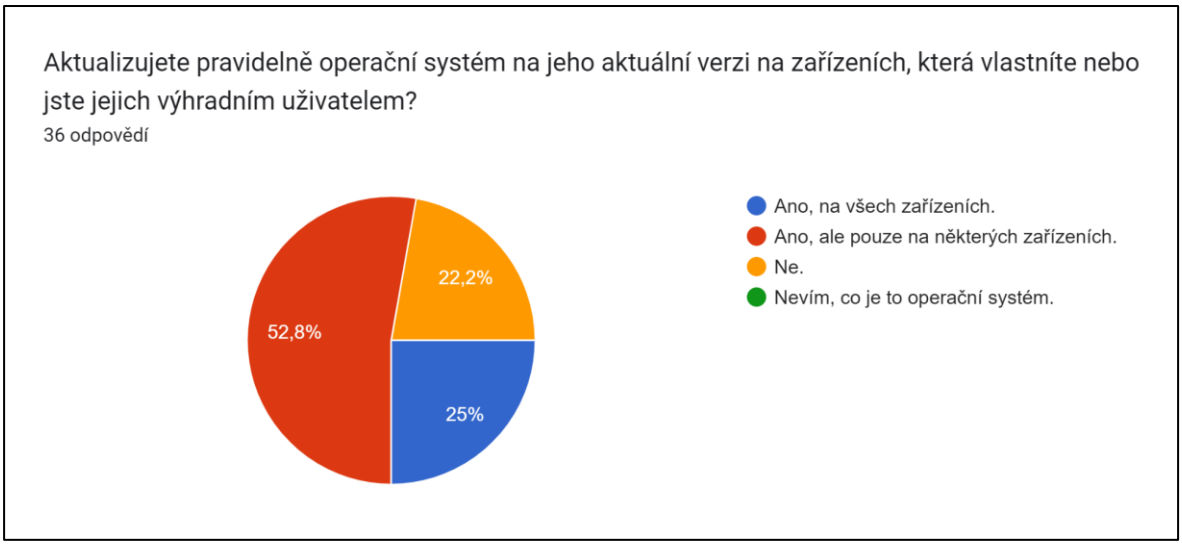
Obrázek 4: Vlastní zhodnocení znalostí kyberbezpečnosti u příslušníků generace Z

Z grafů vyplývá, že příslušníci generace X své znalosti v této oblasti nejčastěji hodnotí jako Průměrné až Nadprůměrné. Zajímavým zjištěním je, že své schopnosti shodně hodnotila i generace Z, kde převažovaly rovněž odpovědi Průměrné a Nadprůměrné. Ovšem, 10,9 % respondentů této generace (Z) se ohodnotila sebekriticky, neboť z možností zvolilo Velmi podprůměrné. Oproti tomu u generace Y bylo velké procentuální zastoupení (celkem 20,8 %) respondentů, kteří nemají tak velkou víru ve své znalosti a ohodnotili by je jako Podprůměrné.

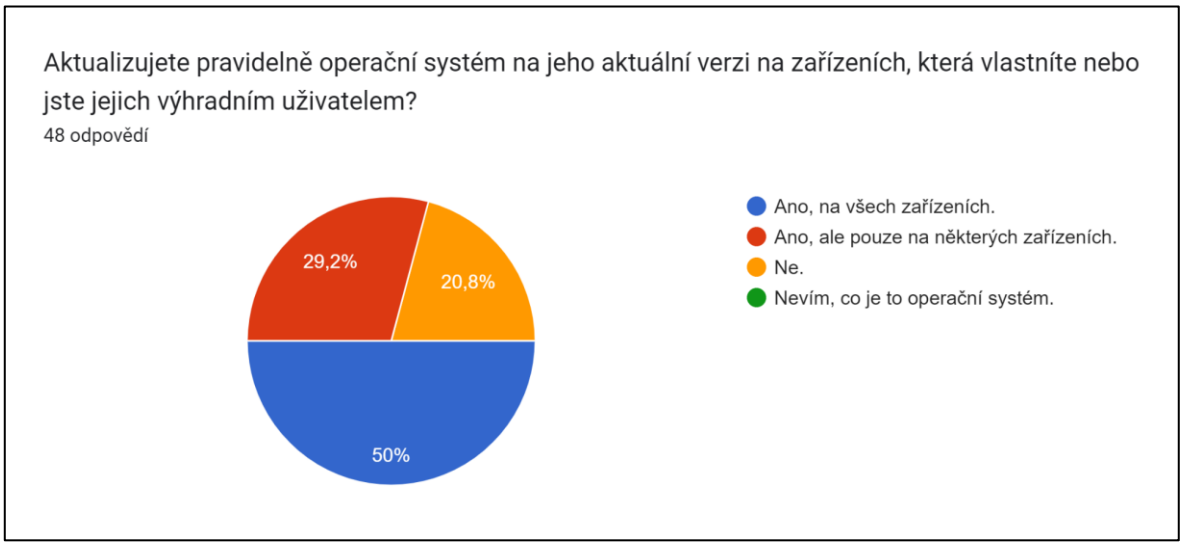
Otázka č. 4:

Ve čtvrté otázce byli respondenti tázáni na jejich přístup k provádění pravidelných aktualizací operačních systémů na jejich aktuální verzi.

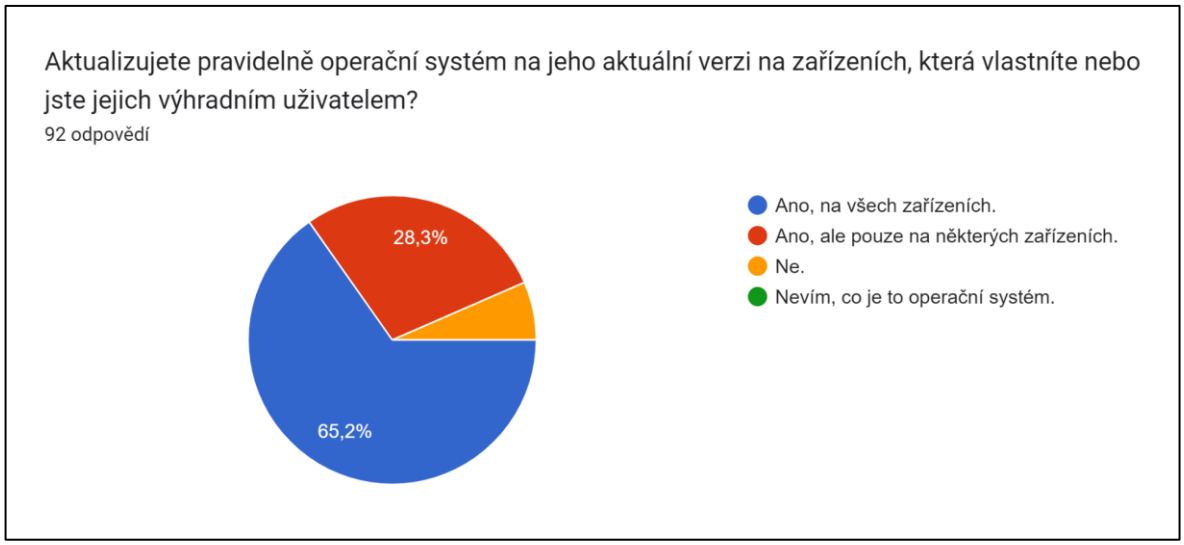
Pravidelná aktualizace operačních systémů je důležitá především z důvodu přidání bezpečnostních záplat u odhalených zranitelných míst. Ty chrání uživatele před zneužitím těchto zranitelných míst kybernetickými zločinci.



Obrázek 5: Odpovědi generace X týkající se jejich přístupu k aktualizování operačního systému



Obrázek 6: Odpovědi generace Y týkající se jejich přístupu k aktualizování operačního systému



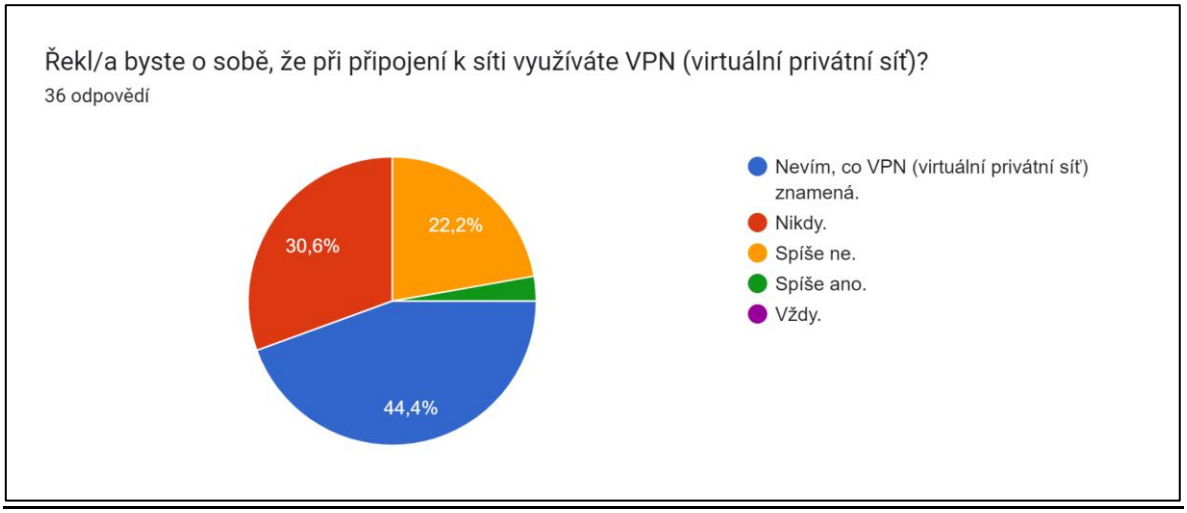
Obrázek 7: Odpovědi generace Z týkající se jejich přístupu k aktualizování operačního systému

Z dotazníkového šetření vyplývá, že nejčastěji udržují operační systém aktuální na všech svých zařízeních příslušníci generace Z, kdy takto odpovědělo 65,2 % respondentů. Pouze 6,5 % respondentů z generace Z odpovědělo, že svůj operační systém pravidelně neaktualizují. V opozici stojí příslušníci generací X a Y, kteří svůj operační systém neaktualizují pravidelně. Konkrétně u generace X to bylo 22,2 % respondentů a u generace Y 20,8 % respondentů. Je na místě zde poukázat na paradox, že ačkoliv generace X označuje své znalosti kyberbezpečnosti především jako Průměrné a Nadprůměrné, jejich přístup k aktualizaci operačního systému toto přesvědčení ale nepodporuje.

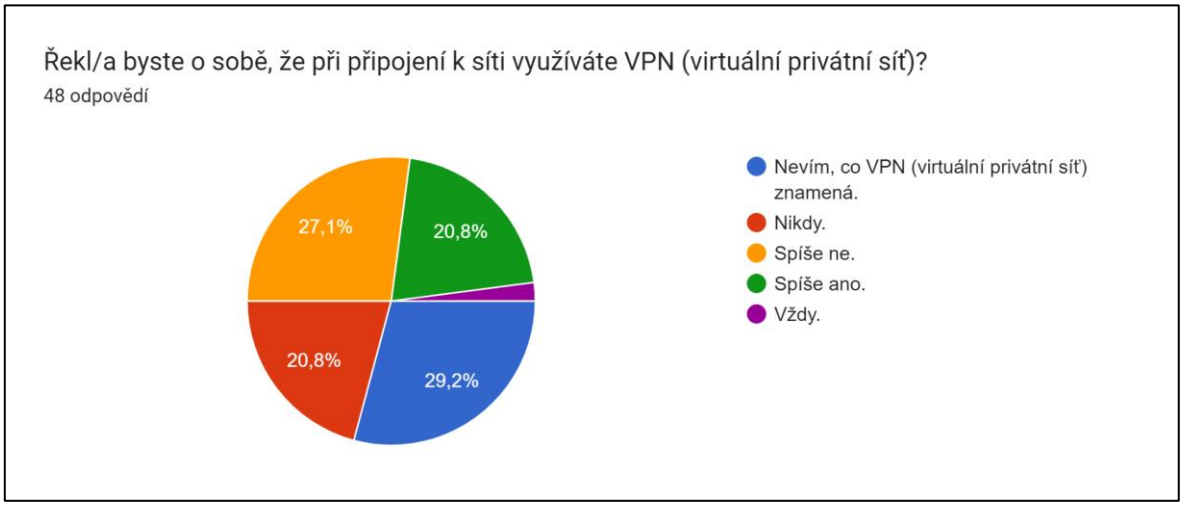
American International University – Bangladesh (AIUB) provedla v prosinci 2023 studii, ve které zkoumala povědomí generace Z ohledně kyberbezpečnosti. (Subhani et al., 2023) V této studii byla respondentům položena otázka týkající se jejich přístupu k pravidelnému aktualizování softwaru zařízení. Ve studii bylo zjištěno, že 81 % všech respondentů pravidelně aktualizuje software jejich zařízení. Toto zjištění tedy koresponduje i s výsledky mého výzkumu, kdy byla generace Z tou, která ze všech generací věnovala pozornost aktualizaci nejvíce.

Otázka č. 5:

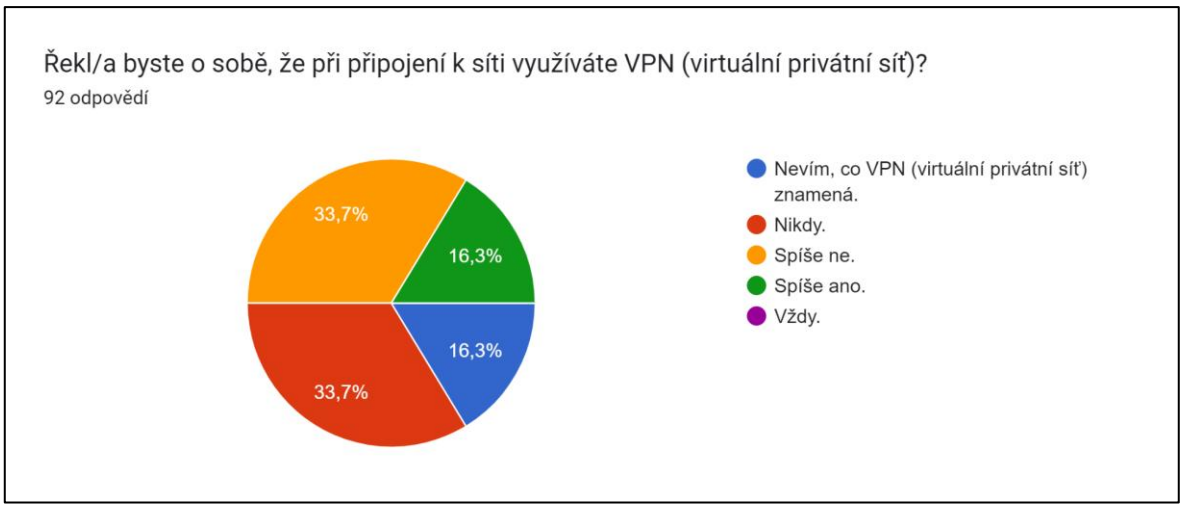
Mnoho odborníků na kybernetickou bezpečnost se shoduje v otázce týkající se důležitosti používání VPN. VPN nám umožňuje maskovat náš provoz na síti, a tím značně ztížit práci potencionálním útočníkům. Mimo to nabízí i částečnou ochranu našeho soukromí, kdy se náš provoz na internetu stává více anonymní.



Obrázek 8: Odpovědi příslušníků generace X týkajících se jejich využívání VPN



Obrázek 9: Odpovědi příslušníků generace Y týkajících se jejich využívání VPN



Obrázek 10: Odpovědi příslušníků generace Z týkajících se jejich využívání VPN

Poměrně překvapivé bylo velké procentuální zastoupení odpovědí Nevím, co VPN (virtuální privátní síť) znamená u respondentů všech generací. Pro generaci X to bylo dokonce 44,4 %, což činí téměř polovinu této skupiny respondentů. Druhá polovina respondentů, která pojem VPN zná, se rozložila tak, že tuto síť buď nevyužívají (30,6 %) anebo spíše nepoužívají (22,2 %). Zůstává tedy hodnota 2,8 % respondentů, kteří síť VPN skutečně využívají.

U respondentů z řad generace Y jsou všechna data, s výjimkou odpovědi Vždy, poměrně rovnoměrně rozprostřena. Smutným zjištěním je, že respondenti z řad generace Z sice většinou vědí, k čemu slouží VPN, ale spíše ji nepoužívají (33,7 %), nebo ji nepoužívají vůbec (33,7 %).

V souvislosti s dotazníkem provedeným týmem z All About Cookies (Koebert, 2023), který získal data od 1000 dospělých respondentů ze Spojených států amerických, můžeme srovnat jimi získané výsledky týkající se používání VPN, s výsledky získanými tímto dotazníkovým šetřením. Dotazník byl proveden v říjnu roku 2023.

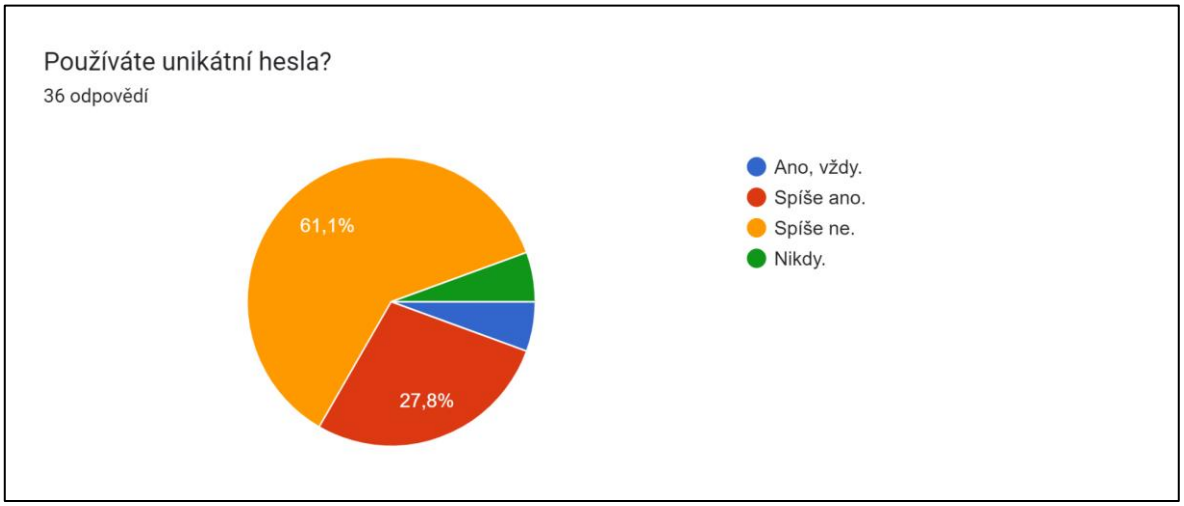
V témže dotazníku byla položena otázka, zda respondenti v současné době používají VPN. 37 % respondentů z generace X odpovědělo, že ano. Stejně tak vypovědělo i 42 % respondentů z generace Y a 40 % z generace Z.

Data získané z mého dotazníkového šetření se ve výsledcích liší, kdy pouze 25 % respondentů generace X odpovědělo, že VPN používá. Pro generaci Y toto číslo bylo vyšší

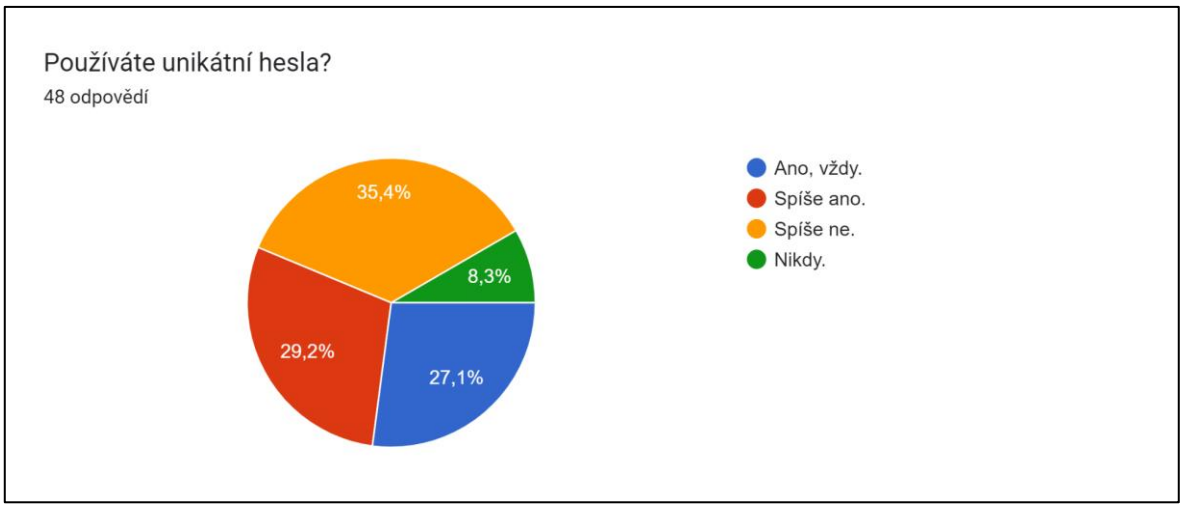
než v dotazníku provedeném týmem z All About Cookies (šlo o 50 % dotázaných). Vyšší počet uživatelů VPN byl zpozorován i u generace Z (rovněž 50 %).

Otázka č. 6:

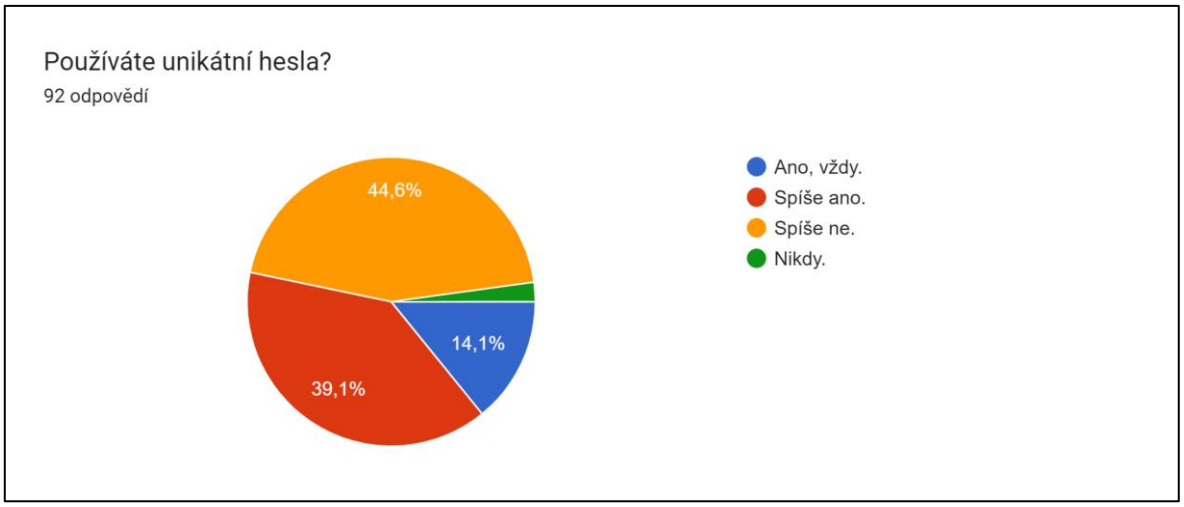
Používání unikátních hesel může být bez použití softwaru určeného pro správu hesel velmi náročné. To však neznamená, že není důležité. Pokud bychom používali pouze jedno heslo pro každý z našich účtů, dojde při jeho kompromitaci k potencionální ztrátě všech našich účtů.



Obrázek 11: Graf popisující používání unikátních hesel u příslušníků generace X



Obrázek 12: Graf popisující používání unikátních hesel u příslušníků generace Y



Obrázek 13: Graf popisující používání unikátních hesel u příslušníků generace Z

Největší procentuální zastoupení u odpovědí Ano, vždy můžeme vidět u respondentů generace Y (27,1 %). Nicméně, největší procentuální zastoupení u všech generací má odpověď Spíše ne, kdy takto odpovědělo 61,1 % respondentů generace X, 35,4 % respondentů generace Y a 44,6 % respondentů generace Z.

Pozitivním zjištěním je, že obecně velmi malé procentuální zastoupení u všech generací tvořila odpověď Nikdy. Nicméně, nejčastěji se takto vyjádřili příslušníci generace Y, konkrétně 8,3 % z nich. V kontextu předchozích odpovědí jde ale o velmi nemilé číslo, pokud vezmeme v potaz, že pouze jeden příslušník této generace výše ohodnotil své znalosti kyberbezpečnosti odpovědí jako Žádné. Zbývající část respondentů své znalosti považovala za Podprůměrné, či lepší.

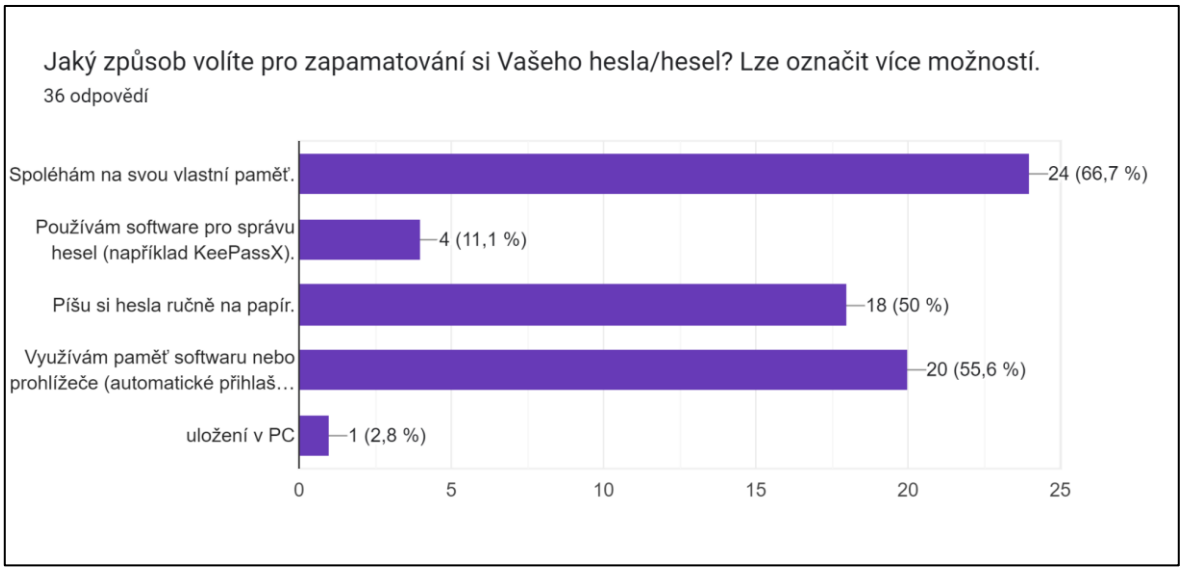
Studie publikovaná v Journal of Advanced Research in Social Sciences and Humanities (Subhani et al., 2023), která mimo jiného zkoumala i používání stejných hesel pro více účtů jednoho uživatele, získala výsledky od respondentů patřících do generace Z, kteří mají mezi 17 a 21 lety.

V této studii výzkumníci zjistili, že 38 % všech respondentů používá alespoň pro dva ze svých účtů stejné heslo. V porovnání s výsledky získanými pomocí dotazníkového šetření si můžeme všimnout toho, že mnou dotazovaní využívají stejná hesla mnohem častěji, neboť pouze 14,1 % respondentů této generace vždy používá unikátní hesla.

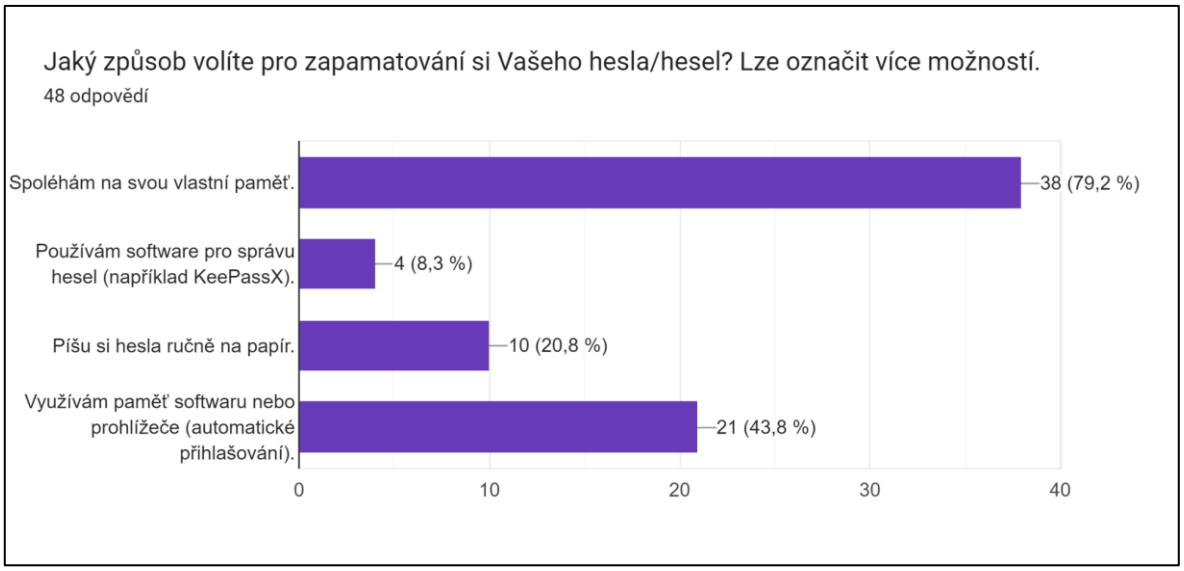
Otázka č. 7:

Jak již bylo zmíněno, používání unikátních hesel je nesmírně podstatnou součástí správného přístupu ke kybernetické bezpečnosti. Nicméně, i pokud bychom měli ta nejsložitější hesla a měli je zapsaná na lepícím papírku na našem zařízení, tak se rázem stávají velmi jednoduchými pro kohokoliv, kdo si je na něm přečte. Nejvíce bezpečným způsobem pro správu hesel je samozřejmě naše vlastní paměť, ale není možné v ní udržet všechny unikátní a silná hesla, která používáme k přihlášení k našim účtům.

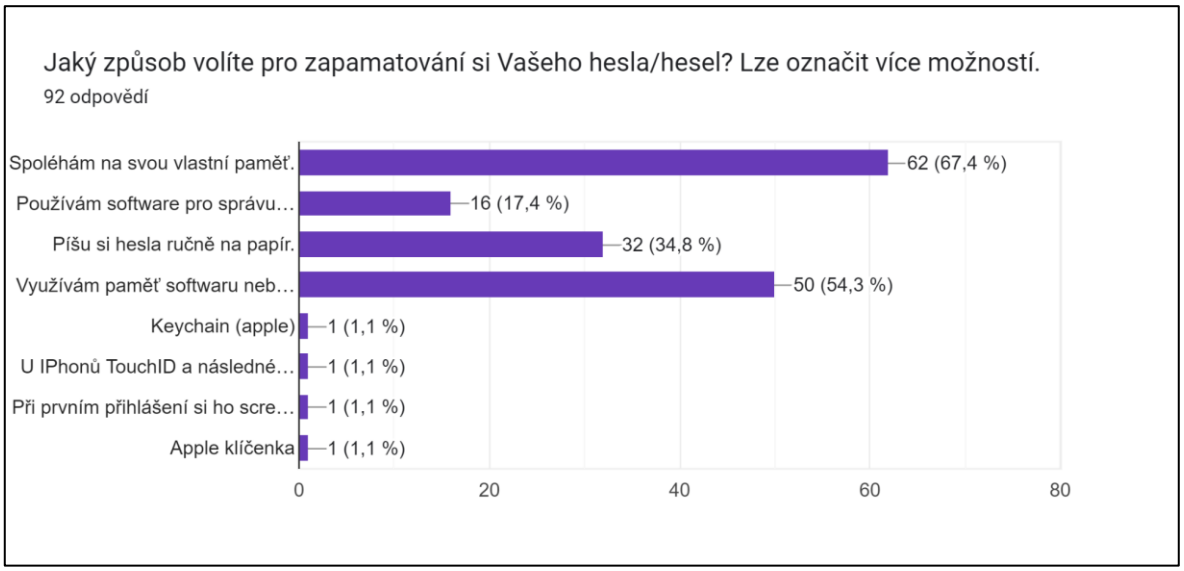
V této otázce měli respondenti možnost zvolit více možností. Nejčastěji volenou možností v každé generaci bylo Spoléhám se na svou vlastní paměť, která měla u všech generací zároveň poměrně podobné procentuální zastoupení. Druhou nejčastěji volenou možností u všech generací byla Využívám paměť softwaru nebo zařízení, která měla u všech generací opět velmi podobné procentuální zastoupení.



Obrázek 14: Otázka týkající se managementu hesel u generace X



Obrázek 15: Otázka týkající se managementu hesel u generace Y



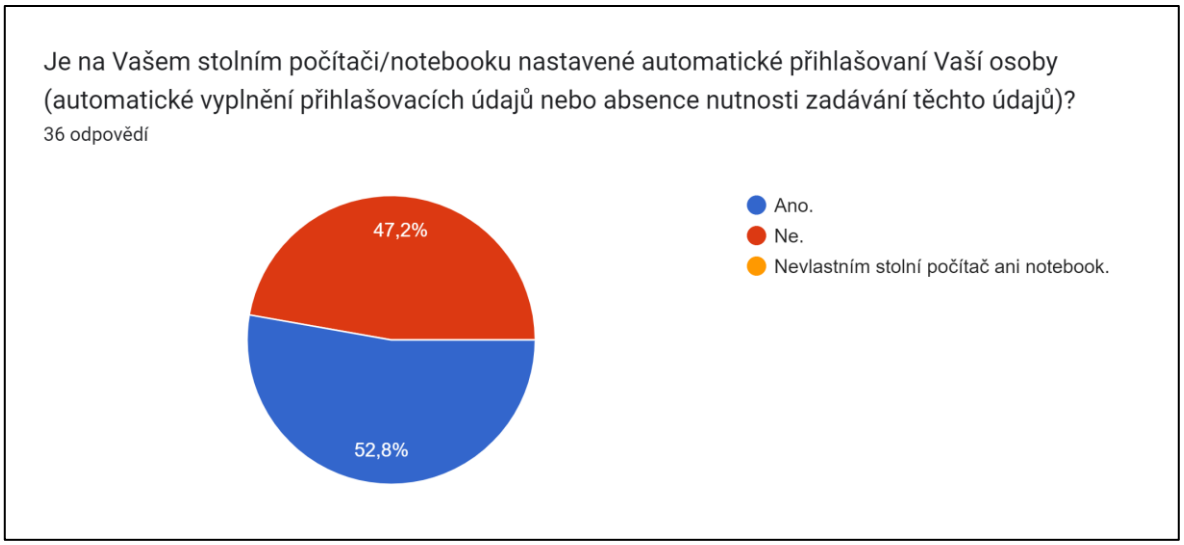
Obrázek 16: Otázka týkající se managementu hesel u generace Z

Větší výkyv nastal u odpovědi Píšu si hesla ručně na papír. Tuto možnost nejčastěji volili respondenti z generace X, kdy ji zvolilo 50 % těchto respondentů. U generace Y byla tato možnost zvolena 20,8 % respondentů a u generace Z 34,8 % respondentů. Experty doporučovanou variantu Používám software pro správu hesel volili nejčastěji respondenti generace Z, kde byla zastoupena 17,4 %. Pro generaci X to bylo 11,1 % a pro generaci Y 8, 3 %.

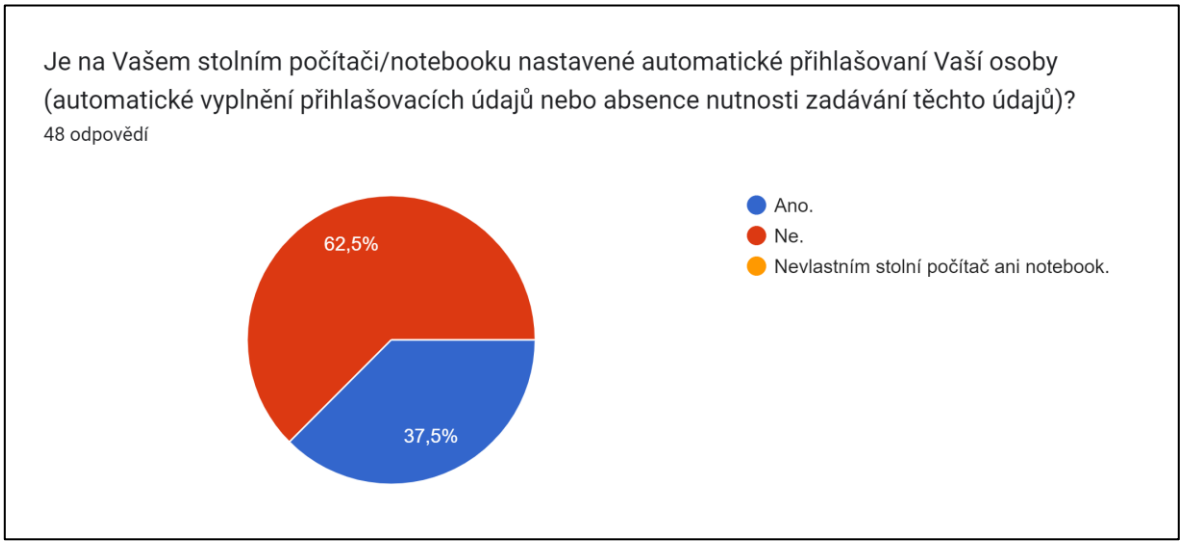
Na tuto otázku v zásadě neexistují špatné odpovědi, i přesto je příjemným zjištěním, kolik respondentů napříč všemi generacemi uchovává svá hesla pouze uvnitř své paměti, tedy mimo dosah okolních vlivů. Spoléhání se na svou paměť není v podstatě špatné. Je ale důležité zmínit, že mnohem ideálnějším řešením by bylo, kdyby si každý z nás dokázal zapamatovat i složitější hesla složená z kombinací velkých i malých písmen, čísel a speciálních znaků.

Otázka č. 8:

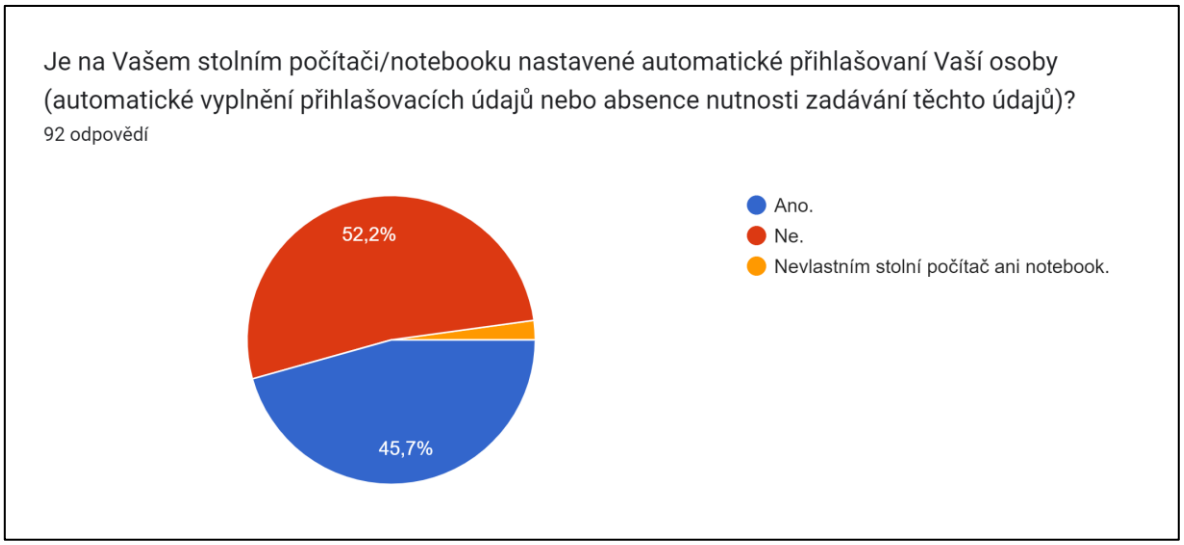
Automatické přihlášení do našich zařízení je sice uživatelsky pohodlné, ale zároveň velmi riskantní. Pokud někdo získá přístup k našemu zařízení, získá tak přístup i ke všem našim datům, která nevyžadují další přihlášení.



Obrázek 17: Automatické přihlášení na stolním počítači/notebooku u respondentů generace X



Obrázek 18: Automatické přihlášení na stolním počítači/notebooku u respondentů generace Y



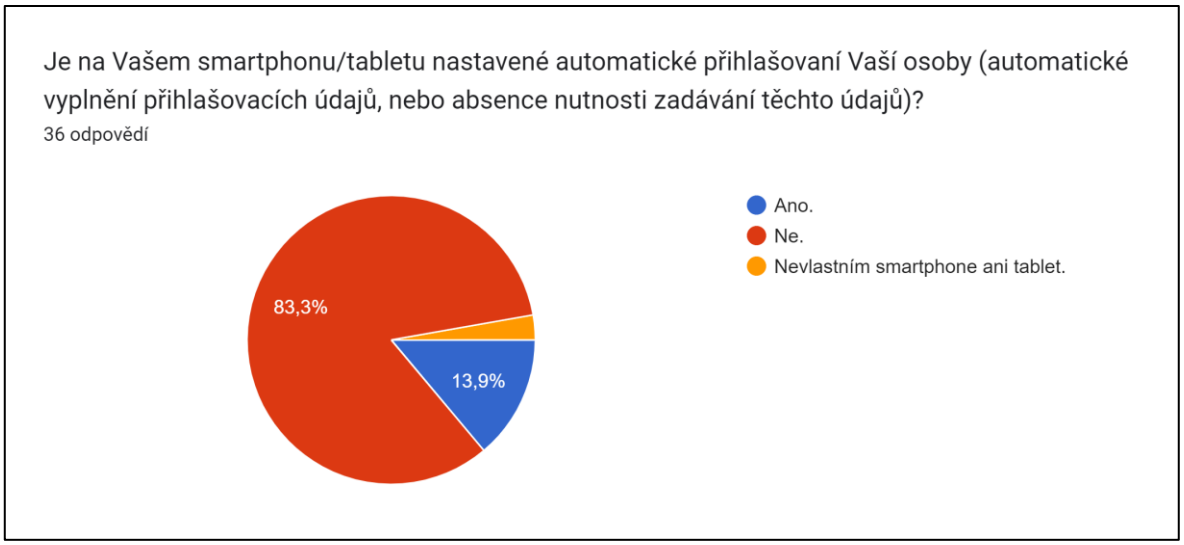
Obrázek 19: Automatické přihlášení na stolním počítači/notebooku u respondentů generace Z

Z otázky vyplývá, že nejvíce volí komfort před bezpečností při zadávání přihlašovacích údajů ke stolnímu počítači/notebooku generace X, konkrétně 52,8 % těchto respondentů. U generace Z byla zaznamenána rovněž téměř polovina respondentů, přesněji 45,7 %. Nejnižší hodnotu, a tudíž nejbezpečnější chování projevila generace Y s 37,5 % respondentů, kteří zvolili možnost Ano.

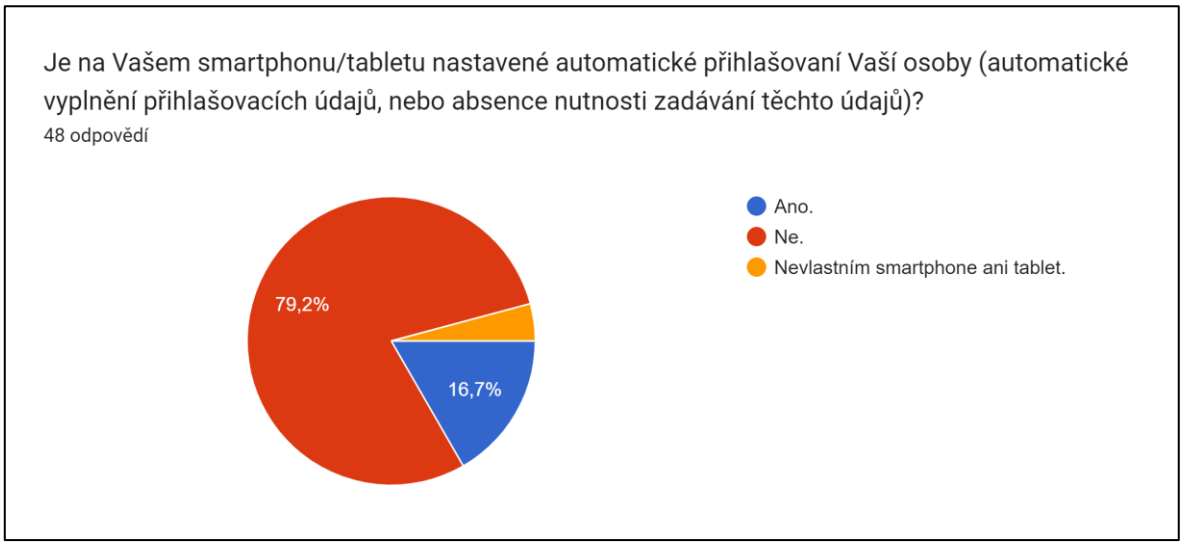
Otázka je myšlena jako navázání na předchozí otázku Používáte unikátní hesla? Pokud bychom měli na každý náš uživatelský účet používat unikátní hesla, je pro průměrného člověka téměř nemožné si je všechna zapamatovat. I proto velká část respondentů v každé generaci odpověděla, že se při správě hesel spoléhá jak na svou paměť, tak i na paměť softwaru nebo zařízení, tedy automatické vyplnění hesla při zapnutí zařízení nebo softwaru, který vyžaduje přihlášení uživatele.

Otázka č. 9:

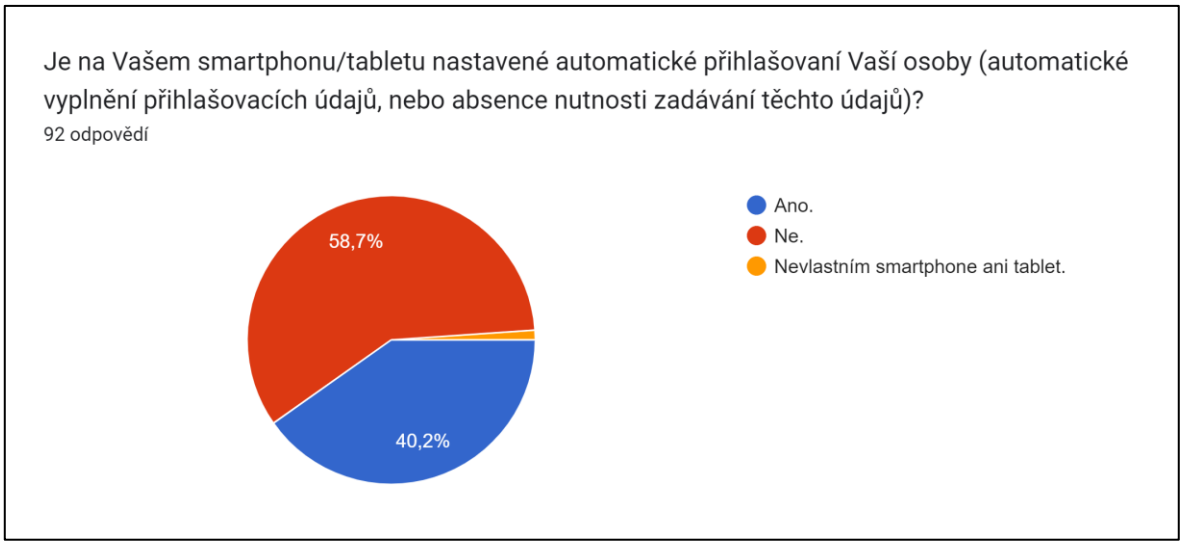
V deváté otázce je respondentům položena otázka týkající se jejich přístupu k automatickému přihlašování. Konkrétněji automatickému přihlašování na smartphony/tablety, které vlastní nebo jejichž jsou výhradními uživateli.



Obrázek 20: Automatické přihlášení na smartphonu/tabletu u respondentů generace X



Obrázek 21: Automatické přihlášení na smartphonu/tabletu u respondentů generace Y



Obrázek 22: Automatické přihlášení na smartphonu/tabletu u respondentů generace Z

Tato otázka se snaží podpořit odpověď na hypotézu: Respondenti všech generací budou mít častěji nastavené automatické přihlášení na stolním počítači/notebooku než na smartphonu/tabletu. Tato hypotéza byla na základě odpovědí respondentů potvrzena. Zároveň tato otázka nabídla zajímavě rozevřené nůžky při srovnání generací X a Y. U generace X si můžeme všimnout pouhých 16,7 % respondentů, kteří takto jednají, kdežto u generace Mileniálů se takto chová až 40,2 % dotazovaných.

Při propojení s výsledky předchozí otázky jde o zajímavé zjištění z toho důvodu, jelikož automatické přihlašování na stolním počítači/tabletu nezaznamenalo u generací X a Y takové rozdíly. Proč tomu tak je? Právě proto by toto zjištění zcela jistě stálo za hlubší prozkoumání, tudíž vytváří pole působnosti pro další výzkumy zabývající se touto problematikou.

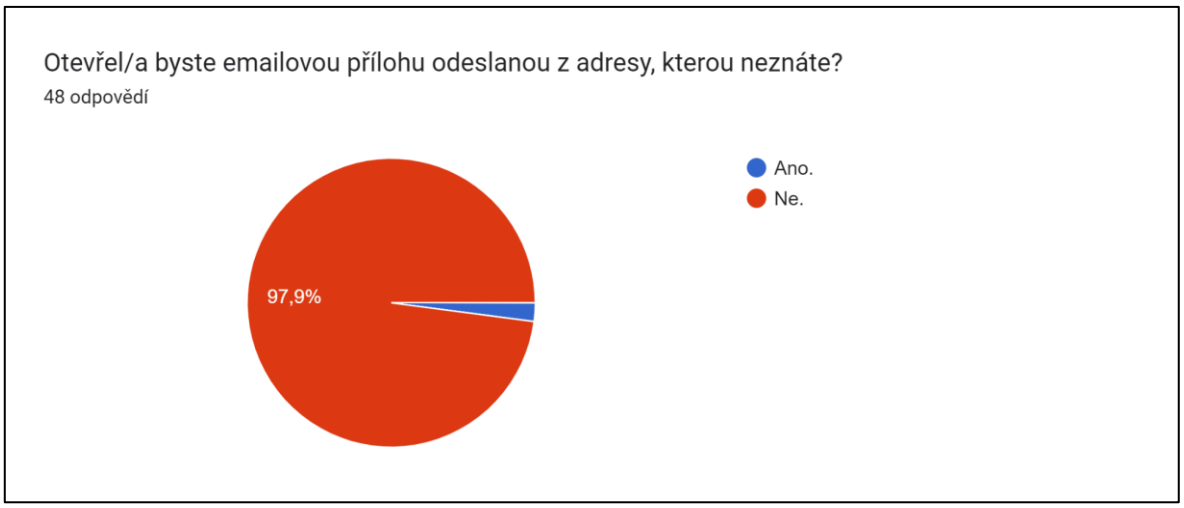
Faktem zůstává, že automatickým přihlašováním k smartphonu/tabletu neohrožujeme pouze sami sebe. Pokud dostane naše nezabezpečené zařízení do rukou zločinci, dostane tak přístup i k našim kontaktům. Prostřednictvím sociálního inženýrství se poté může pomocí phishingu pokusit o útok na osoby v našich kontaktech, kde pro něj bude snazší předstírat naši identitu.

Při výsledné analýze dat a konzultaci s vedoucím práce jsme ale dospěli k závěru, že u respondentů mohlo dojít k neúplnému pochopení položené otázky. Šedou zónou může být biometrické přihlášení uživatele, přičemž jde o způsob přihlášení, během kterého nedochází k přímému zadávání hesla.

Otázka č. 10:

Otevírání emailových příloh odeslaných z neznámých emailových adres je jedním ze způsobů, který může útočník zvolit k infikování zařízení oběti. Je proto doporučováno tyto přílohy neotevírat. V desáté otázce jsou respondenti tázáni, jak by se v této situaci zachovali.

Obrázek 23: Jak často by respondenti generace X otevřeli emailovou přílohu odeslanou z neznámé adresy.



Obrázek 24: Jak často by respondenti generace Y otevřeli emailovou přílohu odeslanou z neznámé adresy.

Obrázek 25: Jak často by respondenti generace Z otevřeli emailovou přílohu odeslanou z neznámé adresy.

U otázky Otevřel/a byste emailovou přílohu odeslanou z adresy, kterou neznáte, odpověděla naprostá většina respondentů Ne. Pro generaci X to bylo dokonce 100 % všech dotazovaných. U generace Y se našel pouze jeden respondent, který by byl ochotný takovou přílohu otevřít. V této otázce jsme tedy měli možnost získat odpověď na hypotézu, jejíž obsahem bylo tvrzení, že příslušníci generace X by častěji otevřeli emailovou přílohu odeslanou z neznámé adresy. Jak již výsledky napovídají, tato hypotéza byla těmito výsledky vyvrácena.

Otázka, která byla v mém dotazníkovém šetření položena respondentům generací X, Y a Z, byla položena i v dotazníku v diplomové práci (Malát, 2023). Tato diplomová práce se zaměřila na rizikové chování v kyberprostoru a mediální gramotnost u adolescentů. Respondenti tedy nemohli být starší než příslušníci generace Z.

Na otázku týkající se otevírání odkazů z neznámých emailových adres uvedlo téměř 81 % všech respondentů, že tyto odkazy nikdy neotvírá. Rozdíl více než 16 % je zde vcelku značný.

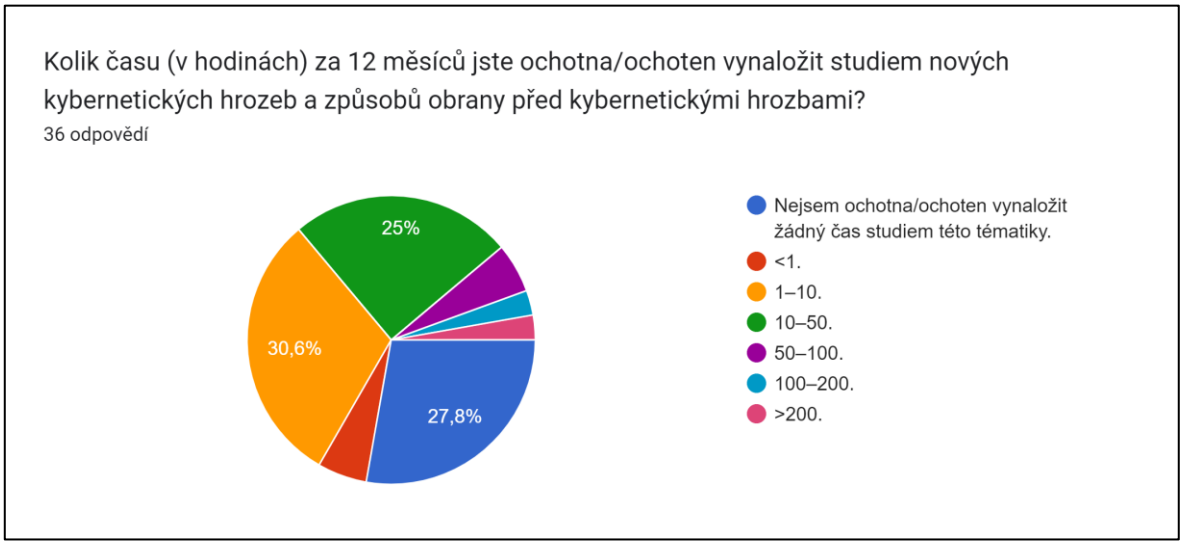
Studie publikovaná v SN Computer Science Journal (Carroll et al., 2022) srovnávala schopnost účastníků rozlišit phishingové emaily různých typů a různého stáří. Výsledky studie ukázaly, že její účastníci jsou nejčastěji schopni odhalit starší typy phishingových emailů na základě výrazných gramatických chyb, které se v emailech vyskytovaly.

U novějších typů phishingových emailů účastníci projevovali přehled a rozlišování v menší míře.

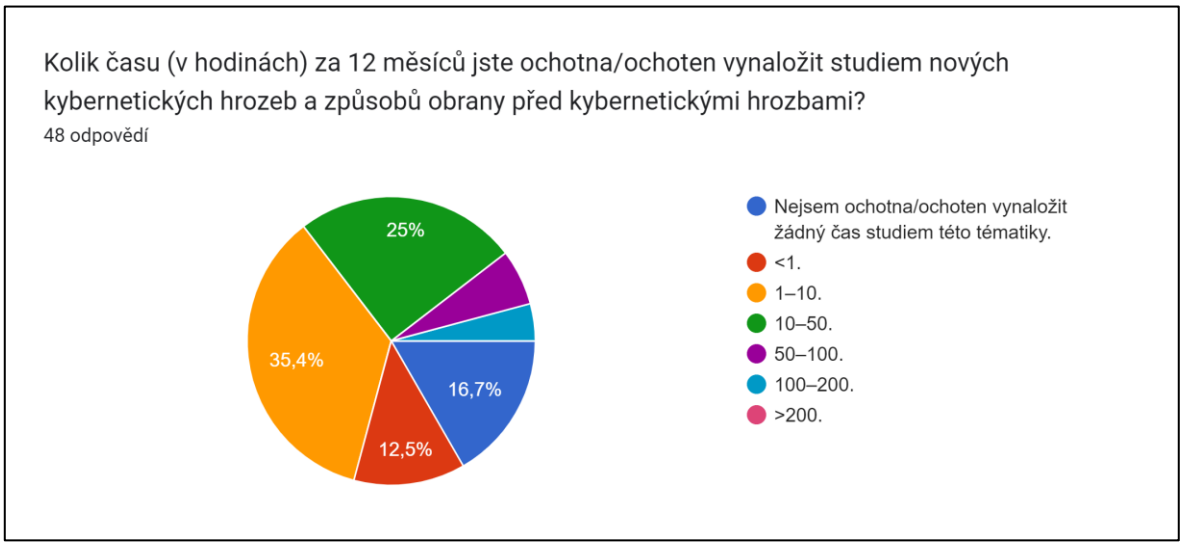
Studie publikována výzkumníky z University of Florida a New York University (Oliveira et al., 2017) se zaměřila na rozbor zranitelnosti mladších a starších lidí vůči spear phishingovým emailům. Studie se účastnilo 158 respondentů, kterým bylo v průběhu 21 dní zasláno několik phishingových emailů. Studie ukázala, že mladší účastníci byli mnohem náchylnější k jedinečnosti phishingového emailu a jednali více na základě impulzivních rozhodnutí. Starší účastníci studie byli oproti tomu mnohem více náchylnější kliknout na opakující se emaily. Celkově 43 % účastníků studie kliknulo alespoň na jeden odkaz zaslaný ve phishingovém emailu. Výzkumníci, kteří tuto studii vytvořili v závěru s ohledem na výsledky studie doporučují přistupovat k osvětě ohledně tématiky phishingových útoků cíleně s ohledem na věk jednotlivých příjemců.

Otázka č. 11:

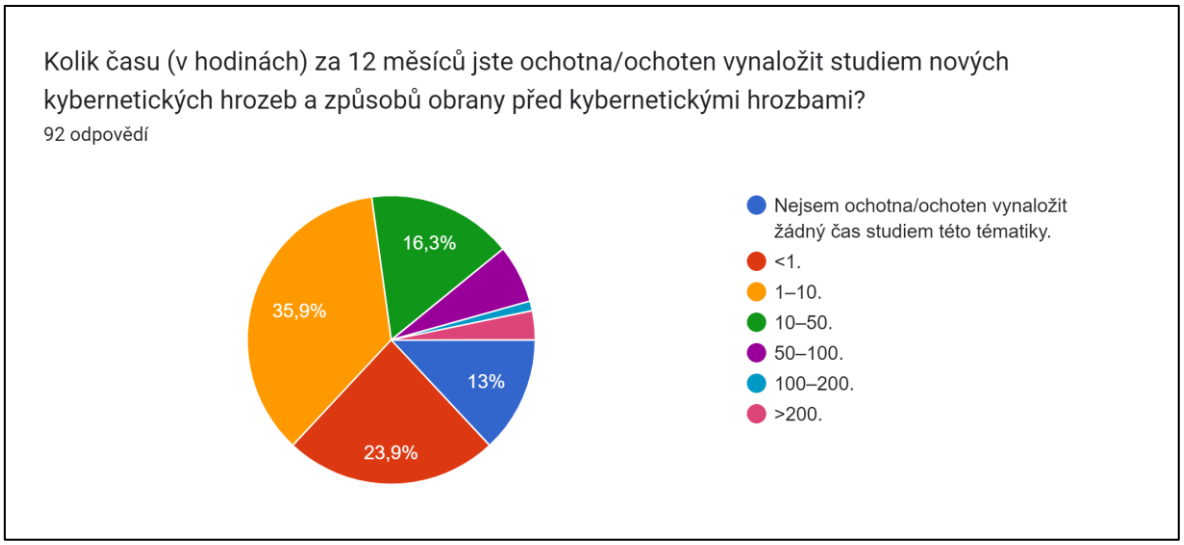
Problematika kybernetické bezpečnosti prochází neustálými změnami. S vývojem malwaru a sofistikovaností sociálního inženýrství se ale vyvíjí i způsoby obrany. Jinými slovy můžeme říct, že to, co platí dnes nemusí platit zítra a je potřebné udržovat naše znalosti aktuální. V této otázce se respondenti měli zamyslet nad tím, kolik času by byli ochotni za 12 měsíců věnovat studiu nových kybernetických hrozeb a ochranou před kybernetickými hrozbami.



Obrázek 26: Ochota respondentů generace X vynaložit čas na vzdělávání se v oblasti kyberbezpečnosti



Obrázek 27: Ochota respondentů generace Y vynaložit čas na vzdělávání se v oblasti kyberbezpečnosti



Obrázek 28: Ochota respondentů generace Z vynaložit čas na vzdělávání se v oblasti kyberbezpečnosti

Většina respondentů z každé generace odpověděla, že je ochotna se touto problematikou zabývat méně než 10 hodin za 12 měsíců.

Více než čtvrtina (27,8 %) respondentů generace X uvedla, že není ochotna vůbec vynakládat čas na tuto problematiku. Neochota vynaložit jakýkoliv čas pro studium této problematiky následně u dalších generací byla ještě nižší. Pro generaci Y to bylo 16,7 % a pro generaci Z 13 %. Nicméně, respondenti z generace X se mnohem častěji vyhnuli odpovědi <1 (5,6 %), kterou naopak volilo 12,5 % respondentů generace Y a 23,9 % respondentů generace Z.

U všech generací bylo velmi podobné procentuální zastoupení respondentů, kteří by byli ochotni vynaložit více než 10 hodin za 12 měsíců studiem této problematiky.

Studie, která se mimo jiné týkala ochoty vzdělávání se v oblasti kyberbezpečnosti byla publikována v Journal of Advanced Research in Social Sciences and Humanities (Subhani et al., 2023). Cílovou skupinou se stali pouze příslušníci generace Z, ve věkovém rozmezí 17-21 let, kteří odpovídali na otázku týkající se touhy učení se o kyberbezpečnosti. 90 % těchto respondentů odpovědělo, že by rádi získávali další informace z této oblasti. Na základě tohoto zjištění můžeme rovněž konstatovat velkou podobnost s výsledky mého výzkumu, kde takto odpovědělo 87 % respondentů z generace Z.

Otázka č. 12:

Odkazy na sociálních sítích nás velmi často přesměrují tam, kam skutečně míříme. Pokud tento odkaz však nevidíme, nebo tuto adresu neznáme, můžeme pouze doufat v to, že s námi tvůrce příspěvku nemá špatné úmysly. Je tedy vhodné neklikat na všechny odkazy, které na internetu jsou. Mohou se pod nimi skrývat URL, ze kterých se do našich zařízení stáhne malware, nebo může jít i o promyšlenou formu phishingu.

Obrázek 29: Přístup k neznámým odkazům na sociálních sítích u respondentů generace X

Obrázek 30: Přístup k neznámým odkazům na sociálních sítích u respondentů generace Y

Obrázek 31: Přístup k neznámým odkazům na sociálních sítích u respondentů generace Z

Neznámé odkazy na sociálních sítích by nejčastěji rozklikli respondenti generací Z a Y. Respondenti generace X projevili v rámci dotazníkového šetření vyšší míru obezřetnosti v ohledu na potencionální nebezpečí, které sociální sítě ukrývají.

7 SHRNUTÍ VÝSLEDKŮ DOTAZNÍKOVÉHO ŠETŘENÍ

V následující kapitole budou představeny celkové výsledky výzkumu a odpovědi na výzkumné otázky spolu s hypotézami.

7.1 Vyhodnocení výzkumných otázek

- **Hlavní výzkumná otázka: Jakým způsobem reagují příslušníci jednotlivých generací na přítomnost kybernetických hrozeb?**

  Příslušníci generace X své znalosti z oblasti kyberbezpečnosti nejčastěji ze všech respondentů, hodnotili jako průměrné. Rovněž se jedná o generaci, která ***nejméně používá antivirové softwary*** na svých zařízeních a pro více než polovinu jejích respondentů by nebyla příliš podstatná aktuální verze operačního systému. Tato generace má také ***největší zastoupení respondentů, kteří si nezálohují data,*** jak na stolním počítači/notebooku, tak na smartphonu/tabletu. Nicméně, respondenti generace X by dle dat získaných z dotazníkového šetření ***projevili větší obezřetnost, než respondenti generace Y a Z při odesílání citlivých údajů,*** otevírání příloh z neznámých adres, klikáním na neznámé odkazy na sociálních sítích a nejméně častým sdílením svých hesel.

  Příslušníci generace Y mají nejmenší procentuální zastoupení respondentů, kteří by nijak nezvyšovali své znalosti v oblasti kybernetické bezpečnosti. Také se jedná o generaci, která má ***největší procentuální podíl respondentů, kteří uvedli, že vždy používají unikátní hesla*** a její respondenti mají na svých zařízeních ***nejméně nastaveno automatické připojování*** k veřejným bezdrátovým sítím.

  Příslušníci generace Z jsou nejmladší zkoumanou generací v tomto dotazníkovém šetření. Respondenti této generace si nejvíce ze všech generací nenechávají zapnutou bránu firewall. Oproti zbylým dvěma generacím však mají na zařízeních, které vlastní nebo jsou jejich výhradními uživateli, ***častěji nainstalovaný antivirový software***. Z dotazníkového šetření také vyplynulo, že tato generace má ***nejmenší procentuální podíl respondentů, kteří nikdy nezálohují svá data***, jak na stolním počítači/notebooku, tak i na smartphonu/tabletu. ***Největší procentuální podíl*** u generace Z byl zaznamenán i v otázce týkající se ***vícefaktorového ověřování identity.***

- **<u>Vedlejší výzkumná otázka</u>: Jakými způsoby se příslušníci jednotlivých generací chrání před kybernetickými hrozbami?**

  Příslušníci generace X se před kybernetickými hrozbami chrání více svou obezřetností při pohybu v kyberprostoru než příslušníci generací Y a Z. Respondenti generace X ke svojí ochraně nejčastěji využívají ***prostředky anebo metody, které nejsou zpoplatněné***, popřípadě jsou zpoplatněny jednorázovým poplatkem. Většina respondentů generace X si zvyšuje své znalosti z oblasti kyberbezpečnosti z knih, článků, rozhovorů s odborníky nebo při školeních v práci. Respondenti generace X mají ***nejčastěji zapnutou bránu firewall.***

  Respondenti generace Y a Z se před kybernetickými hrozbami chrání velmi podobně. Oproti generaci X mají ***vyšší procentuální podíl respondentů***, kteří používají ***antivirový software*** na zařízeních, které vlastní nebo jsou jejich výhradními vlastníky, ***častějším zálohováním dat*** na těchto zařízeních a ***častějším používáním VPN.***

7.2 Vyhodnocení hypotéz

Pro výzkum jsem stanovil následující hypotézy:

- **H1: Příslušníci generace X by častěji otevřeli přílohu zaslanou z neznámé emailové adresy než příslušníci generací Y a Z.**

Ze získaných dat vyplynulo, že 100 % respondentů generace X uvedlo, že by neotevřelo přílohu zaslanou z neznámé emailové adresy. Oproti tomu tutéž odpověď uvedlo pouze 97,9 % příslušníků generace Y a 97,8 % respondentů z generace Z. Na základě těchto zjištění hypotézu č. 1 není možné zcela zamítnout, jelikož je rozdíl v odpovědích jen minimální.

- **H2: Respondenti všech generací budou mít častěji nastavené automatické přihlášení na stolním počítači/notebooku než na smartphonu/tabletu.**

Z odpovědí můžeme vyvodit závěr, jehož obsahem je tvrzení, že respondenti všech generací mají na stolních počítačích/noteboocích, které vlastní, nebo jimiž jsou výhradními uživateli, častěji nastavené automatické přihlašování. Na základě zjištěného tudíž hypotézu č. 2 přijímám.

Na základě zjištěných dat a jejich závěrečné interpretace došlo k porovnání přístupů jednotlivých generací, co se týče jejich přístupu ke kyberbezpečnosti. Na základě tohoto si dovoluji říci, že výzkumný cíl této bakalářské práce byl splněn.

7.3 Limity výzkumu

Jsem si kriticky vědom toho, že provedené dotazníkové šetření má mnohé limity. Zcela jistě při něm může nastat situace, kdy má respondent tendenci odpovídat takovým způsobem, který považuje za správný, i když ne zcela odpovídá realitě toho, jakým způsobem daný respondent přistupuje k chování v kyberprostoru. Při sběru dat se tedy spoléháme na přístup respondentů a to, že při jeho vyplňování skutečně odpovídali pravdivě.

Sběr dat probíhal necelý měsíc, a tedy byl pro účely této bakalářské práce časově omezen. Pokud bychom této problematice mohli věnovat více času, jistě bychom zajistili i vyšší počet respondentů, a tím i reálnější obrázek o přístupech ke kyberbezpečnosti u jednotlivých generací.

ZÁVĚR

Tato bakalářská práce byla zaměřena na srovnání mezigeneračních přístupů ke kyberbezpečnosti. Nejdříve se tomuto tématu věnovala z teoretické a dále i praktické perspektivy. V teoretické rovině byl vymezen právní rámec této problematiky a byly zde uvedeny jednotlivé typy kybernetických útoků. Současně byla zapojena i kapitola charakterizující generace od X po Z. V praktické části byl uveden výzkumný plán spolu s výzkumnými otázkami a hypotézami. Po analýze dat bylo provedeno zodpovězení zmiňovaných otázek a hypotéz.

Jak už bylo řečeno, v praktické části práce byla provedena analýza získaných dat pomocí dotazníkové metody. Ačkoliv má výzkum své limity, jeho výsledky přináší zajímavá zjištění na poli mezigeneračního přístupu ke kyberbezpečnosti. Za velmi zajímavé považuji zjištění, jehož obsahem je kontrast mezi tím, jak kriticky přistupuje generace X ke svých znalostem ohledně kyberbezpečnosti, zatímco výsledky ukazují jejich zdatnost a dobrou orientaci v mnoha oblastech tohoto tématu. Příslušníci generace X tímto potvrzují zmiňovanou vytrvalost a schopnost ověřování toho, co stojí ve středu jejich zájmů, jak bylo uvedeno i v teoretické části práce.

V rámci bakalářské práce byly uvedeny odpovědi na výzkumné otázky i hypotézy. Vyhodnocení dat ovšem proběhlo pouze deskriptivně, a tak by bylo jistě zajímavé pro další výzkum zpracovat data více do hloubky a hypotézy ověřit i statisticky. Zároveň se nabízí varianta výzkumu, která by nejdříve zmapovala chování respondentů pomocí dotazníku, a později prakticky ověřila pravdivost jejich tvrzení, například prostřednictvím zasílání vykonstruovaných spear phishingových emailů. Získaná data by poté byla předložena ke srovnání, zda respondenti dostojí svých teoretických odpovědí i po praktickém ověření jejich postojů.

Na základě zjištěného považuji cíl této bakalářské práce za splněný.

SEZNAM POUŽITÉ LITERATURY

AIRA GROUP S.R.O., ©2022, *Spyware.* Online. ©2022. Dostupné z: https://www.sprava-site.eu/spyware/. [citováno 2024-03-26].

BETZ, Cecily L., 2019. Generations X, Y, and Z. Online. In: *Journal of Pediatric Nursing*. 2019. Dostupné z: https://www.pediatricnursing.org/article/S0882-5963(18)30631-6/fulltext. [citováno 2024-03-26].

CARROLL, Fiona; ADEYOBI, John Ayooluwa a MONTASARI, Reza, 2022. How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society. Online. SN Computer Science. In: *A Springer Nature Journal*, 2022. Dostupné z: https://doi.org/https://doi.org/10.1007/s42979-022-01069-1. [citováno 2024-04-19].

ČESKO, 2014. 181/2014 Sb. ZÁKON o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. 2014, částka 75. ISSN 1211-1244. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181 .

ČESKO, 2016. Zákon č. 297/2016 Sb. Zákon o službách vytvářejících důvěru pro elektronické transakce. In: *Sbírka zákonů České republiky*. 2016, částka 115. ISSN 1211-1244. Dostupné také z: https://www.zakonyprolidi.cz/cs/2016-297 .

ČESKO, 2017 a. Zákon č. 205/2017 Sb. Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony. In: *Sbírka zákonů České republiky*. 2017, částka 74. ISSN 1211-1244. Dostupné také z: https://www.zakonyprolidi.cz/cs/2017-205 .

ČESKO, 2017 b. Zákon č. 250/2017 Sb. Zákon o elektronické identifikaci. In: *Sbírka zákonů České republiky*. 2017, částka 89. ISSN 1211-1244. Dostupné také z: https://www.zakonyprolidi.cz/cs/2017-250 .

ČESKO, 2018. 82/2018 Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti

kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). Online. In: Zákony pro lidi. AION CS, ©2010–2024, částka 43. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82 . [citováno 2024-03-23].

ČESKO, 2019. Zákon č. 110/2019 Sb. Zákon o zpracování osobních údajů. In: *Sbírka zákonů České republiky*. 2019, částka 47. ISSN 1211-1244. Dostupné také z: https://www.zakonyprolidi.cz/cs/2019-110 .

ČESKO, 2020. Zákon č. 12/2020 Sb. Zákon o právu na digitální služby a o změně některých zákonů. In: *Sbírka zákonů České republiky*. 2020, částka 5. ISSN 1211-1244. Dostupné také z: https://www.zakonyprolidi.cz/cs/2020-12 .

ČESKÝ STATISTICKÝ ÚŘAD [ČSÚ], 2014. *"Husákovy" versus „Havlovy děti"*. Online. Český statistický úřad, 2014. Dostupné z: https://www.czso.cz/csu/czso/52002e2055 . [citováno 2024-03-25].

Český statistický úřad [ČSÚ], 2020. *ŽENY A MUŽI V DATECH 2020*. Online. Praha: Český statistický úřad, 2020. ISBN 978-80-250-3065-3. Dostupné z: https://www.czso.cz/documents/10180/151439704/30000420.pdf/5f24abfc-dbb8-4be6-98f6-1d9acff33e56?version=1.3. [citováno 2024-04-19].

DIMOCK, Michael, 2019. *Defining generations: Where Millennials end and Generation Z begins*. Online. Pew Research Center, 2019. Dostupné z: https://www.pewresearch.org/short-reads/2019/01/17/where-millennials-end-and-generation-z-begins/. [citováno 2024-03-26].

DIMOCK, Michael, 2023. *5 things to keep in mind when you hear about Gen Z, Millennials, Boomers and other generations.* Online. Pew Research Center, 2023. Dostupné z: https://www.pewresearch.org/short-reads/2023/05/22/5-things-to-keep-in-mind-when-you-hear-about-gen-z-millennials-boomers-and-other-generations/. [citováno 2024-03-25].

EC-COUNCIL UNIVERSITY, 2023. *The Importance of Strong Passwords and How to Create Them.* Online. 2023. Dostupné z: https://www.eccu.edu/blog/technology/the-importance-of-strong-secure-passwords/ . [citováno 2024-03-26].

EDDY, Max a Chris STOBING, 2023. *Why You Need a VPN, and How to Choose the Right One.* Online. In: PcMag, 2023. Dostupné z: https://www.pcmag.com/how-to/what-is-a-vpn-and-why-you-need-one . [citováno 2024-03-26].

ELDRIDGE, Alison. BRITANNICA, 2024. *Generation Z demographic group.* Online. In: Encyclopedia Britannica. 2024. Dostupné z: https://www.britannica.com/topic/Generation-Z. [citováno 2024-03-26].

ERBSCHLOE, Michael, 2019. *Social Engineering Hacking Systems, Nations, and Societies.* Online. Boca Raton: CRC Press, 2019. ISBN 978-0-367-31337-1. Dostupné z: https://doi.org/https://doi.org/10.1201/9780429322143. [citováno 2024-04-17].

ESET, ©1992–2024a. *Spyware*. Online. Eset, ©1992–2024. Dostupné z: https://www.eset.com/cz/spyware/. [citováno 2024-03-26].

ESET, ©1992–2024b. *Co je počítačový virus + druhy virů.* Online. Eset, ©1992–2024. Dostupné z: https://www.eset.com/cz/virus/. [citováno 2024-03-26].

ESET, ©1992–2024c. *Trojský kůň*. Online. Eset, ©1992–2024. Dostupné z: https://www.eset.com/cz/trojsky-kun/. [citováno 2024-03-26].

ESET, ©1992–2024d. *Botnet.* Online. Eset, ©1992–2024. Dostupné z: https://www.eset.com/cz/botnet/. [citováno 2024-03-26].

ESET, ©1992–2024e. *Phishing.* Online. Eset, ©1992–2024. Dostupné z: https://www.eset.com/cz/phishing/. [citováno 2024-03-26].

ESET, ©1992–2024f. *Vícefázové ověření.* Online. Eset, ©1992–2024. Dostupné z: https://www.eset.com/cz/vicefazove-overeni-a-zabezpeceni-firemnich-hesel/. [citováno 2024-03-26].

ESET, ©1992–2024g. *What is antivirus software?* Online. Eset, ©1992–2024. Dostupné z: https://www.eset.com/uk/what-is-antivirus/. [citováno 2024-03-26].

EXECUTECH, ©2022. *What is a pharming attack? : Pharming Definition* Online. Executech, ©2022. Dostupné z: https://www.executech.com/insights/what-is-a-pharming-attack/ . [citováno 2024-03-26].

FORTINET, ©2024a. *Trojan Horse Virus.* Online. Fortinet, ©2024. Dostupné z: https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus . [citováno 2024-03-26].

FORTINET, ©2024b. *What Is Pharming?.* Online. Fortinet, ©2024. Dostupné z: https://www.fortinet.com/resources/cyberglossary/pharming [citováno 2024-03-26].

GAVORA, Peter, 2010. *Úvod do pedagogického výzkumu.* 2., rozš. české vyd. Brno: Paido. ISBN 978-80-7315-185-0.

GLAMOSLIJA, Katarina, 2024. *Co je to trojský kůň a jak ho chránit.* Online. In: Safetydetectives.com. 6.2.2024. Dostupné z: https://cs.safetydetectives.com/blog/co-je-to-trojsky-ku%CC%8An-a-jak-ho-chranit/. [citováno 2024-03-26].

CHRÁSKA, Miroslav, 2016. *Metody pedagogického výzkumu: základy kvantitativního výzkumu.* Praha: Grada. ISBN 978-80-247-5326-3.

INSIGHTS DESK, 2023. *Understanding Pharming Attack: A Sneaky Cyber Threat* Online. 2023. Dostupné z: https://www.itsecuritydemand.com/insights/security/understanding-pharming-attack-a-sneaky-cyber-threat/ . [citováno 2024-03-26].

KASPERSKY, ©2024a. *Spyware: What It Is and How to Protect* Yourself. Online. Kaspersky, ©2024b. Dostupné z: https://usa.kaspersky.com/resource-center/threats/spyware. [citováno 2024-03-26].

KASPERSKY, ©2024b. *What's the Difference between a Virus and a Worm?* Online. Kaspersky, ©2024. Dostupné z: https://www.kaspersky.com/resource-center/threats/computer-viruses-vs-worms. [citováno 2024-03-26].

KEEPASSX, ©2005-2021. *The Official KeePassX Homepage.* Online. KeePassX, ©2005-2021. Dostupné z: https://www.keepassx.org/ . [citováno 2024-03-26].

KLÍMOVÁ, Zuzana, 2022. *Generace X, Y nebo Z 1. díl.* Online. In: Orange Academy. 1.1.2022. Dostupné z: https://orangeacademy.cz/clanky/generace-x/. [citováno 2024-03-26].

KOEBERT, Josh, 2023. *Just 55 % of People Actually Know What VPNs Do.* Online. All About Cookies, 2023. Dostupné z: https://allaboutcookies.org/vpn-usage-survey . [citováno 2024-03-26].

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

LATTO, 2020. Nica. *Worm vs. Virus: What's the Difference and Does It Matter?* Online. In: Avast. 13.4.2020. [cit. 2024-03-26]. Dostupné z: https://www.avast.com/c-worm-vs-virus. [citováno 2024-03-26].

LEGISLATIVA S.R.O, 2022. *Kybernetický útok (kyberútok). Definice, typy, následky a prevence.* Online. 13.9.2022. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok . [citováno 2024-03-26].

LENOVO, ©2024. *What is backup?* Online. Lenovo, ©2024. Dostupné z: https://www.lenovo.com/us/en/glossary/backup/?orgRef=https%253A%252F%252Fwww.google.com%252F . [citováno 2024-03-26].

MALÁT, David, 2023. *Rizikové chování v kyberprostoru a mediální gramotnost adolescentů* Online. Diplomová práce. Ústí nad Labem: Univerzita Jana Evangelisty Purkyně v Ústí nad Labem, Pedagogická fakulta, 2023. Dostupné z: https://theses.cz/id/w1vvbi/. [citováno 2024-03-27].

MICROSOFT, ©2024a. *Co je kybernetický útok?* Online. Microsoft, ©2024. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-a-cyberattack . [citováno 2024-03-26].

MICROSOFT, ©2024b. *Co je: Vícefaktorové ověřování.* Online. Microsoft, ©2024. Dostupné z: https://support.microsoft.com/cs-cz/topic/co-je-v%C3%ADcefaktorov%C3%A9-ov%C4%9B%C5%99ov%C3%A1n%C3%AD-e5e39437-121c-be60-d123-eda06bddf661 . [citováno 2024-03-26].

MICROSOFT, ©2024c. *Create and use strong passwords.* Online. Microsoft, ©2024. Dostupné z: https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb . [citováno 2024-03-26].

MICROSOFT, ©2024d, *What is a VPN?* Online. Microsoft, ©2024. Dostupné z: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn . [citováno 2024-03-26].

MICROSOFT, ©2024e. Co je malware? Online. Microsoft, ©2024. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-malware . [citováno 2024-03-27].

MITNICK, Kevin a Robert VAMOSI, 2019. *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data.*

MONETA, ©2024. *Co je to phishing?* Online. Moneta, ©2024. Dostupné z: https://www.moneta.cz/slovnik-pojmu/detail/phishing . [citováno 2024-03-26].

MONROECOLLEGE, ©2024. *CYBERSECURITY HISTORY: HACKING & DATA BREACHES.* Online. ©2024. Dostupné z: https://www.monroecollege.edu/news/cybersecurity-history-hacking-data-breaches . [cit. 2024-03-26].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST [NÚKIB], nd. *Legislativa KB.* Online. NÚKIB. nd., Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/ . [citováno 2024-03-27].

New York: Back Bay Books, Little, Brown and Company. ISBN: 978-0-316-38052-2
OLIVEIRA, Daneila; ROCHA, Harold; YANG, Huizi; ELLIS, Donovan a DOMMARAJU, Sandeep, 2017. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. Online. New York: Association for Computing Machinery. *Older Adults and Computers*. Dostupné z: https://doi.org/https://dl.acm.org/doi/10.1145/3025453.3025831. [citováno 2024-04-19].

ORACLE, ©2024. *What is IoT?* Online. ©2024. Dostupné z: https://www.oracle.com/cz/internet-of-things/what-is-iot/. [citováno 2024-03-26].

OTOUPAL, Jiri, ©2024. *Lekce 1 – BOTNET.* Online. In: ITnetwork, ©2024. Dostupné z: https://www.itnetwork.cz/site/botnet/botnet-uvod . [citováno 2024-03-26].

SHETTY, Rushank, George GRISPOS a Kim-Kwang Raymond CHOO, 2021. Are You Dating Danger? An Interdisciplinary Approach to Evaluating the (In)Security of Android Dating Apps. IEEE Transactions on Sustainable Computing. Online. In: *IEEE Transactions on Sustainable Computing*. 2021, s. 197-207. ISSN 2377-3782. Dostupné z: https://doi:10.1109/TSUSC.2017.2783858. [cit. 2024-03-26].

SILBERBERG, Adam, 2018. *Všichni máme právo na soukromí: Konspirativní techniky*. V prvním vydání. Praha: Restart project. ISBN 978-80-270-4239-5.

SUBHANI, Arshiya, Iftikhar ALAM KHAN a Usman AHMAD, 2023. Importance of Conducting Cyber Security Awareness Sessions among Undergraduate Students. Online. In: *Journal of Advanced Research in Social Sciences and Humanities,* 2023. ISSN 25977040. Dostupné z: https://doi:10.26500/JARSSH-08-2023-0202 . [citováno 2024-03-27].

TIKK, Eneken a KERTTUNEN, Mika, 2020. *Routledge Handbook of International Cybersecurity*. Online. Londýn: Routledge. ISBN 978-1-351-03890-4. Dostupné z: https://doi.org/https://doi.org/10.4324/9781351038904. [citováno 2024-04-17].

ZELAZKO, Alicia, 2024. *Millennial demographic group.* Online. In: Encyclopedia Britannica. 1.2.2024. Dostupné z: https://www.britannica.com/topic/millennial. [citováno 2024-03-26].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

DDoS	Distributed Denial of Service
DoS	Denial of Service
EU	Evropská unie
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OSN	Organizace spojených národů

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

Nenalezena položka seznamu obrázků.

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK

Srovnání mezigeneračních pohledů na kyberbezpečnost
V tomto dotazníku, sloužícím k účelům mojí bakalářské práce, budete tázáni na problematiku týkající se kybernetické bezpečnosti a Váš přístup k této problematice.

Otázka č. 1: V jakém období jste se narodil/a?

- ○ 1965–1980.
- ○ 1981–1996.
- ○ 1997–2012.
- ○ Jiné.

Otázka č. 2: Jaké je Vaše pohlaví?

- ○ Muž.
- ○ Žena.

Otázka č. 3: Jak byste zhodnotil/a své celkové znalosti v oblasti kyberbezpečnosti?

- ○ Žádné.
- ○ Velmi podprůměrné.
- ○ Průměrné.
- ○ Nadprůměrné.
- ○ Vysoce nadprůměrné.

Otázka č. 4: Aktualizujete pravidelně operační systém na jeho aktuální verzi na zařízeních, která vlastníte nebo jste jejich výhradním uživatelem?

- ○ Ano, na všech zařízeních.
- ○ Ano, ale pouze na některých zařízeních.
- ○ Ne.
- ○ Nevím, co je to operační systém.

Otázka č. 5: Řekl/a byste o sobě, že při připojení k síti využíváte VPN (virtuální privátní síť)?
Nevím, co VPN (virtuální privátní síť) znamená.

- ○ Nikdy.
- ○ Spíše ne.
- ○ Spíše ano.
- ○ Vždy.

Otázka č. 6: Používáte unikátní hesla?

- ○ Ano, vždy.
- ○ Spíše ano.
- ○ Spíše ne.
- ○ Nikdy.

Otázka č. 7: Jaký způsob volíte pro zapamatování si Vašeho hesla/hesel? Lze označit více možností.

- ○ Spoléhám na svou vlastní paměť.
- ○ Používám software pro správu hesel (například KeePassX).
- ○ Píšu si hesla ručně na papír.
- ○ Využívám paměť softwaru nebo prohlížeče (automatické přihlašování).
- ○ Jiná:

Otázka č. 8: Je na Vašem stolním počítači/notebooku nastavené automatické přihlašovaní Vaší osoby (automatické vyplnění přihlašovacích údajů nebo absence nutnosti zadávání těchto údajů)?

- ○ Ano.
- ○ Ne.
- ○ Nevlastním stolní počítač ani notebook.

Otázka č. 9: Je na Vašem smartphonu/tabletu nastavené automatické přihlašovaní Vaší osoby (automatické vyplnění přihlašovacích údajů, nebo absence nutnosti zadávání těchto údajů)?

- ○ Ano.
- ○ Ne.
- ○ Nevlastním smartphone ani tablet.

Otázka č. 10: Otevřel/a byste emailovou přílohu odeslanou z adresy, kterou neznáte?

- ○ Ano.
- ○ Ne.

Otázka č. 11: Kolik času (v hodinách) za 12 měsíců jste ochotna/ochoten vynaložit studiem nových kybernetických hrozeb a způsobů obrany před kybernetickými hrozbami?
Nejsem ochotna/ochoten vynaložit žádný čas studiem této tématiky.

- ○ <1.
- ○ 1–10.
- ○ 10–50.
- ○ 50–100.
- ○ 100–200.
- ○ >200.

Otázka č. 12: Kliknul/a byste na krátké URL odkazy sdílené na sociálních sítích, pokud byste nevěděl/a, kam Vás přesměrují?

- ○ Ano.
- ○ Ne.

Otázka č. 13: Máte na Vašem stolním počítači/notebooku zapnutou ochranu pomocí brány firewall?

- ○ Ano.
- ○ Ne.
- ○ Nevím, co je to firewall.

Otázka č. 14: Používáte vícefaktorové ověření (například kombinace hesla a otisku prstu) při využívání zařízení nebo aplikací s přístupem k Vašim citlivým datům nebo finančním prostředkům?

- ○ Ano, vždy.
- ○ Ne, nikdy.
- ○ Ano, používám vícefaktorové ověření, ale pouze pro některé vybrané účty nebo zařízení.

Otázka č. 15: Máte ve Vašem zařízení nastavené automatické připojení k veřejným bezdrátovým sítím, ke kterým jste se již v minulosti připojil/a? (Například veřejná bezdrátová síť v kavárně).

- ○ Ano.
- ○ Ne.
- ○ Nevím.

Otázka č. 16: Představte si situaci, kdy si pořizujete nový operační systém pro Váš stolní počítač nebo notebook. Jak moc podstatná je pro Vás jeho aktuálnost?

- ○ Není podstatná.
- ○ Spíše není podstatná.
- ○ Spíše je podstatná.
- ○ Je podstatná.
- ○ Nepřemýšlím o tom.

Otázka č. 17: Sdílíte některé ze svých přihlašovacích údajů s jinou osobou?

- ○ Ano.
- ○ Ne.

Otázka č. 18: Odeslal/a jste někdy citlivé informace (například přihlašovací údaje, heslo/a, PIN kód/y) emailem, nebo přes sociální sítě?

- ○ Ano.
- ○ Ne.
- ○ Nejsem si jistá/jistý.

Otázka č. 19: Na kterém z těchto zařízení máte nainstalovaný antivirový software? Lze označit více možností.

- ○ Smartphone.
- ○ Stolní počítač.
- ○ Notebook.
- ○ Tablet.
- ○ Na žádném z výše uvedených zařízení nemám nainstalovaný antivirový software.
- ○ Nevlastním ani nejsem výhradním uživatelem žádného z výše uvedených zařízení.
- ○ Nevím, co je to antivirový software.

Otázka č. 20: Jaké zdroje informací používáte ke zvyšování svých znalostí o kyberbezpečnosti? Lze označit více možností.

- ○ Nijak své znalosti v této oblasti nezvyšuji.
- ○ Knihy a/nebo časopisy.
- ○ Články.
- ○ Rozhovory s odborníky.
- ○ Kurzy.
- ○ Workshopy.
- ○ Jiné:

Otázka č. 21: Jaké z těchto zařízení s přístupem k internetu vlastníte/jste jeho výhradním uživatelem? Lze označit více možností.

- ○ Smartphone.
- ○ Stolní počítač.
- ○ Notebook.
- ○ Tablet.
- ○ Žádné z výše uvedených nevlastním/nejsem jeho výhradním uživatelem.

Otázka č. 22: Jak často provádíte zálohování pro Vás důležitých dat na stolním počítači/notebooku, jehož jste vlastníkem nebo výhradním uživatelem?

- ○ Nikdy.
- ○ Méně než 1krát za 12 měsíců.
- ○ 1krát za 12 měsíců.
- ○ 2–3krát za 12 měsíců.
- ○ 3–4krát za 12 měsíců.
- ○ Více než 4krát za 12 měsíců.
- ○ Vždy, když vytvořím a/nebo nahraji data, o která nechci přijít.
- ○ Nevlastním, ani nejsem výhradním uživatelem žádného z těchto zařízení.

Otázka č. 23: Jak často provádíte zálohování pro Vás důležitých dat na smartphonu/tabletu, jehož jste vlastníkem nebo výhradním uživatelem?

- ○ Nikdy.
- ○ Méně než 1krát za 12 měsíců.
- ○ 1krát za 12 měsíců.
- ○ 2–3krát za 12 měsíců.
- ○ 3–4krát za 12 měsíců.
- ○ Více než 4krát za 12 měsíců.
- ○ Vždy, když vytvořím a/nebo nahraji data, o která nechci přijít.
- ○ Nevlastním, ani nejsem výhradním uživatelem žádného z těchto zařízení.

Otázka č. 24: Jakou částku jste ochotna/ochoten vynaložit na softwarové zabezpečení všech svých zařízení a dat před kybernetickými útoky za 12 měsíců? (Čísla vyjádřena v českých korunách.)

- ○ Nejsem ochotna/ochoten vynakládat své finanční zdroje pro tyto účely.
- ○ <100.
- ○ 100–500.
- ○ 500–1000.
- ○ 1000–1500.
- ○ 1500–2000.
- ○ >2000.

Otázka č. 25: Představte si situaci, kdy si pořizujete nový operační systém pro Váš stolní počítač nebo notebook. Jak moc podstatná je pro Vás jeho aktuálnost?

- ○ Není podstatná.
- ○ Spíše není podstatná.
- ○ Spíše je podstatná.
- ○ Je podstatná.
- ○ Nepřemýšlím o tom.

Otázka č. 26: Kontrolujete si správnost URL adresy před zadáváním citlivých údajů? (Například před zadáváním platebních údajů.)

- ○ Nikdy.
- ○ Spíše ne.
- ○ Spíše ano.
- ○ Vždy.

Otázka č. 27: Uveďte, jaký/jaké operační systém/y používáte na stolním počítači/notebooku jehož jste vlastníkem/výhradním uživatelem? (Například: Windows 11, Linux Ubuntu, apod.)