Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra jazyků

Bakalářská práce

Počítačová kriminalita jako hrozba pro demokracii a hospodářský rozvoj

Matěj Strnad

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Matěj Strnad

Informatika

Název práce

Počítačová kriminalita jako hrozba pro demokracii a hospodářský rozvoj

Název anglicky

Cybercrime as a Threat to Democracy and Economic Development

Cíle práce

Bakalářská práce se zabývá problematikou počítačové kriminality a jejím vlivem na ekonomiku a demokracii. Cílem práce je identifikovat nové formy počítačové kriminality, jako jsou deepfake a AI generování škodlivého obsahu, a vyhodnotit škodlivou činnost v této oblasti, včetně phishingu a jiných podvodů. V části věnované negativním dopadům na demokracii se práce zaměřuje hlavně na dezinformace. Práce se věnuje vyhodnocení dopadů počítačové kriminality na různé ekonomické sektory, jako jsou například finanční instituce, obchodní společnosti nebo obyvatelstvo.

Metodika

Teoretická část:

V této části práce bude pozornost věnována kritické analýze odborné literatury, věnující se obecnému tématu počítačové kriminality a jejímu dopadu na demokracii a ekonomiku. Budou prozkoumány hlavní trendy a aktuální problémy v této oblasti a rozebrány jejich důsledky.

Praktická část:

V praktické části práce budou analyzovány technologie pro tvorbu deepfake. Budou prezentovány výsledky analýzy a bude rozebíráno, jak se tato technologie může použít v počítačové kriminalitě. Bude proveden průzkum mezi studenty ohledně jejich povědomí o počítačové kriminalitě, který poskytne informace pro analýzu dopadu počítačové kriminality na ekonomiku.

Doporučený rozsah práce

30 – 40

Klíčová slova

počítačová kriminalita, demokracie, deepfaky, preventivní opatření

Doporučené zdroje informací

BASTA, P., KROPACOVA, A., KUNC, M., a KOLOUCH, J. 2019. CyberSecurity. 1. vyd. Praha: CZ.NIC. 556 s. ISBN 978-80-88168-32-4.

KOLOUCH, J. 2016. CyberCrime. 1. vyd. Praha: CZ.NIC.528 s. ISBN 978-80-88168-15-7.

MATEJKA, J. 2013. Internet jako objekt práva. Praha: CZ.NIC. 262 s. ISBN 978-80-905802-2-0.

SAK, P. 2018. Úvod do teorie bezpečnosti. 1. vyd. Praha: Petrklíč. 271 s. ISBN 978-80-7229-793-1.

YOUNG, N. (2019). DeepFake Technology. 1. vyd. Amazon Digital Services LLC – KDP Print US. 158 s. ISBN 978-1078494694.

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Ivan Hrbek

Garantující pracoviště

Katedra jazyků

Elektronicky schváleno dne 9. 6. 2023

PhDr. Mgr. Lenka Kučírková, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 18. 11. 2023

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Počítačová kriminalita jako hrozba pro demokracii a hospodářský rozvoj." jsem vypracoval(a) samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14.03.2024 _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu práce Ing. Ivanu Hrbkovi za podporu a vedení během mé bakalářské práce.

Počítačová kriminalita jako hrozba pro demokracii a hospodářský rozvoj

Abstrakt

Práce zkoumá, jak počítačová kriminalita ovlivňuje ekonomiku a demokracii. Zaměřuje se na nové formy kriminality, jako je vytváření falešného obsahu pomocí umělé inteligence ať už přes deepfake nebo přes programy, které dokážou udělat model hlasu člověka z krátké nahrávky jeho hlasu, což se může použít k dezinformacím. Práce analyzuje také již známé formy kriminality jako je phishing, různé druhy virů, ať je cílem získat osobní údaje oběti nebo například využít počítač nebo jiné zařízení k těžbě kryptoměn bez vědomí oběti. Řeší i nebezpečí, které vzniká z potvrzení cookies. Analyzuje také, jak tyto činy škodí občanům a různým obchodním sektorům. Práce se soustředí na identifikaci rizik spojených s podvodnými aktivitami a negativními dopady na společnost. Snaží se zhodnotit, jak tyto hrozby mohou ohrozit demokratické procesy a ekonomickou stabilitu, a navrhnout preventivní postupy k ochraně osobních údajů.

Klíčová slova: malware, hacker, kyberkriminalita, demokracie, virus, prevence, AI, dezinformace, phishing, podvody

Cybercrime as a Threat to Democracy and Economic Development

Abstract

The thesis examines how cybercrime affects the economy and democracy. It focuses on new forms of crime, such as the creation of fake content using artificial intelligence, either through deepfakes or programs that can make a model of a person's voice from a short recording of their voice, which can be used for disinformation. The thesis also analyses already known forms of crime such as phishing, various types of viruses, whether it is to obtain the victim's personal data or, for example, to use a computer or other device to mine cryptocurrencies without the victim's knowledge. It also addresses the danger that arises from cookie confirmation and analyses how these acts harm citizens and various business sectors. The work focuses on identifying risks associated with fraudulent activities and negative impacts on society. It seeks to evaluate how these threats can jeopardise democratic processes and economic stability, and propose preventive procedures to protect personal data.

Keywords: Malware, Hacker, Cybercrime, Democracy, Virus, Prevention, AI, Disinformation, Phishing, Fraud

Obsah

1 Úvod

V dnešní době je už většina zařízení „chytrá“, což znamená, že je lze ovládat pomocí počítače, nebo klidně i telefonu. Je možné třeba změnit teplotu vody v bojleru, zhasnout světlo, kontrolovat venkovní kamery, přepínat programy televize, klimatizace, pračky. To život značně usnadňuje, ale zároveň vytváří to prostor pro různé kriminální chování.

Nejsou to ale pouze domácí spotřebiče, co v dnešní době počítače ovládají. Ty jsou nedílnou součástí různých oblastí vědeckého výzkumu, zdravotnictví, obchodu, vzdělávání, průmyslu, bezpečnostních sil. Riziko kybernetických útoků na tyto oblasti značí velké ohrožení a obrana těchto sektorů je nesmírně důležitá.

Od doby, kdy se počítače staly běžnou součástí lidských životů, se možnosti kyberkriminality značně rozšířily. V současné době panuje nedůvěra v online prostředí. Lidé nevědí, zda mohou věřit informacím prezentovaným na sociálních sítích, obávají se zadávání údajů o kreditní kartě na internetových stránkách a s obavami otevírají přílohy v e-mailech. I zdánlivě banální akce, jako je otevření PDF souboru od neznámého odesílatele, může mít vážné následky. Například tím může odcizit takzvaný section token, který v prohlížeči slouží k identifikaci uživatele a následnému přihlášení.

Tyto hrozby se netýkají jen individuálních uživatelů, ale i různých firem, které kvůli jednomu špatnému kliknutí mohou ztratit až miliardové částky. Je tedy při klikání na odkazy důležité dbát na bezpečnost a důkladně zabezpečovat účty jakéhokoliv typu. Důraz by měl být kladen na obezřetnost i při potvrzování cookies, protože existují určitá rizika spojená s jejich používáním a shromažďováním osobních údajů. S rozvojem doby se objevují stále nové a hůře rozpoznatelné hrozby.

Nejnovějším fenoménem je v této době AI a deepfake. Obě tyto hrozby se dají použít k tvorbě dezinformací a kvůli tomu je čím dál tím obtížnější rozpoznat „fake“ od reality. Tyto technologie nemusí být vytvořeny jen k tvorbě dezinformací, lze vytvořit například model hlasu zpěváka a zjistit, jak by zazpíval nějakou hudební skladbu od jiného interpreta. Můžeme tak například znovu slyšet hlas našeho oblíbeného, již zesnulého zpěváka. V práci je zkoumáno, zda-li tento fenomén přijde lidem obecně nemorální nebo ho považují za zajímavý a nemají s ním problém.

2 Cíl práce a metodika

Cíl práce

Cílem práce je představit nové formy počítačové kriminality, jako jsou deepfake a AI generování škodlivého obsahu a vyhodnotit škodlivou činnost v této oblasti, včetně phishing a jiných podvodů. V části věnované negativním dopadům na demokracii se práce zaměřuje hlavně na dezinformace. Práce se věnuje vyhodnocování dopadů počítačové kriminality na různé ekonomické sektory, jako jsou například finanční instituce, obchodní společnosti nebo obyvatelstvo.

Metodika

Teoretická část:

- V této části práce je pozornost věnována kritické analýze odborné literatury, věnující se obecnému tématu počítačové kriminality a jejímu dopadu na demokracii a ekonomiku.
- Jsou prozkoumány hlavní trendy a aktuální problémy v této oblasti a rozebírány jejich důsledky.

Praktická část:

- V praktické části práce jsou analyzovány technologie pro tvorbu deepfake.
- Jsou prezentovány výsledky analýzy a bude rozebíráno, jak se tato technologie může použít v počítačové kriminalitě.
- Je proveden průzkum mezi respondenty ohledně jejich povědomí o počítačové kriminalitě, který poskytnuje informace pro analýzu dopadu počítačové kriminality na ekonomiku.

3 Kyberkriminalita

3.1 Definice kyberkriminality

„Kyberkriminalita je jev bez jednoznačné a přímé definice“ (Phillips, 2022).

Je to proto, že kyberkriminalita zahrnuje širokou škálu činností a technologie používané k páchání těchto zločinů se neustále vyvíjejí. V důsledku toho je snaha definovat kyberkriminalitu komplexním úkolem. Historie kyberkriminality sahá až do roku 1834, kdy dva zloději infiltrovali francouzský telegrafní systém a získali přístup k finančním trhům, aby mohli posílat falešné zprávy o změnách cen akcií. Tento čin je definován jako první zločin kyberkriminality, protože využívá kybernetický systém (Bluevoyant, 2022).

Kyberkriminalita existuje z několika důvodů:

- **Finanční zisk:** útočníci se snaží ukrást obětem osobní údaje a díky tomu se obohatit. Příkladem je skandál z roku 2018, kdy Facebook-Cambridge Analytica neoprávněně shromažďoval údaje z profilů přibližně 87 milionů uživatelů Facebooku (Hinds, 2020).
- **Vandalismus:** někdy jsou kyberútoky prováděny jen s vidinou něco poškodit. To může zahrnovat ničení dat nebo sítí.
- **Kyberšikana:** ta má za cíl ponižovat nebo emocionálně škodit jednotlivcům nebo skupinám.
- **Moc a sabotáž:** to zahrnuje útoky na vládní instituce, firmy nebo jednotlivce z politických nebo ideologických důvodů. Tomuto druhu kyberkriminality se říká kyberterorismus.

3.2 Kyberterorismus

Ministerstvo vnitra České republiky definuje kyberterorismus jako „*souhrnný název pro teroristické aktivity, jejichž cílem útoku, použitým prostředkem nebo přenašečem je tzv. „kyberprostor“, neboli jde o teroristické aktivity zaměřené proti a prováděné prostřednictvím počítačové sítě a touto sítí řízených systémů“* (Ministerstvo vnitra, 2024). Kyberterorismus využívá počítačových sítí, informačních technologií a internetu k provádění teroristických útoků nebo k podpoře teroristických činností. Například 24. listopadu 2014 byli zaměstnanci Sony Pictures America nakaženi ransomware a po příchodu do práce našli obrázek kostlivce na monitorech. Na tomto obrázku byla zpráva od skupiny, která si říkala „Guardians of Peace“ a výhružka, že vypustí terabajty dokumentů Sony mediím, pokud studio nezruší vydání akční komedie Interview, ve které šlo o atentát na nejvyššího vůdce Korejské lidově demokratické republiky Kim Čŏng-una (Israel, 2015).

Obrázek 1: Zpráva, která se objevila na obrazovkách počítačů zaměstnanců společnosti Sony Pictures https://shorturl.at/sDJO5

Obrázek 2: Zpráva, která se objevila na obrazovkách počítačů zaměstnanců společnosti Sony Pictures https://shorturl.at/sDJO5

3.3 Kyberkriminalita v České republice

V roce 2022 tvořila s 18,5 tisíci případy více než 10 % z celkové registrované kriminality v České republice. Meziročně tato kriminalita vzrostla takřka o 100 % (94,9 %).
V minulém roce byly nejčastější útoky na přihlašovací údaje k bankovním účtům, přesně cílené ransomware útoky pomocí e-mailu nebo SMS, útoky DoS (záplava dat znemožňující přístup k webu/serveru), DDoS (záplava dat z mnoha zdrojů znemožňující přístup k webu/serveru), nebo útoky pomocí škodlivých kódů s cílem krádeže dat a účtů uživatelů (Dlubalová, 2023).

3.4 Legislativa a právní aspekty kyberkriminality

Zákony a mezinárodní dohody týkající se kyberkriminality se v průběhu let rozvinuly kvůli rostoucí hrozbě kybernetických útoků. Nejdůležitější z nich je Budapešťská úmluva o kyberkriminalitě. Je to první mezinárodní dohoda vytvořená Radou Evropy, která se zaměřuje na boj proti kybernetické kriminalitě a zavádí opatření pro prevenci, vyšetřování a trestání kybernetických útoků a podvodů. Tato úmluva byla podepsána v roce 2001 a má za cíl koordinovat mezinárodní úsilí v oblasti kybernetické bezpečnosti, poskytovat rámcové směrnice pro spolupráci mezi různými zeměmi a zajišťovat harmonizaci právních nástrojů pro boj proti kybernetické kriminalitě (Tapia, 2022).

4 Online podvody

Online podvody se stávají globálním problémem, který se stále zvětšuje a stává se sofistikovanějším. Existují různé typy online podvodů, včetně phishing, „podvodů láskou“, investičních podvodů, a jiných. Oběti těchto podvodů jsou často vystaveny riziku, protože jsou zranitelní. Technologie se používá v centrální roli, a to jak podvodníky, tak oběťmi. Falešné webové stránky, phishing e-maily a malware jsou vytvářeny a distribuovány s pomocí technologií, které používají podvodníci, zatímco oběti technologie používají k ochraně před podvody, k jejich detekci a nahlášení. Boj proti kybernetickým podvodům je obtížný, protože se neustále vyvíjejí a pachatelé se často nacházejí v zahraničí. Vlády, orgány činné v trestním řízení a finanční instituce spolupracují na vývoji nových strategií, jak bojovat proti kybernetickým podvodům (Button, 2017).

4.1 Druhy podvodů

- Podvody láskou jsou druh, při kterém podvodníci vytvářejí falešné online profily a vydávají se za někoho, kdo je atraktivní a zajímavý. Tito podvodníci se pak spojí s obětí a vybudují si s ní vztah. Jakmile si získají důvěru oběti, začnou po ní žádat peníze nebo jiné výhody, jako je placení předplatného, dary apod (Bentham Science Publishers and BioMed Central, 2020).
- Investiční podvod je druh podvodu, při kterém podvodníci nabízejí falešné investiční příležitosti, které lákají na svou údajnou výhodnost. Tyto příležitosti často slibují vysoké zisky s minimálním rizikem. Oběti, které se rozhodnou investovat, nakonec o své peníze přijdou (Kieffer, 2017).
- **Phishing**: útok, při kterém se útočníci vydávají za důvěryhodné osoby nebo organizace a snaží se získat citlivé informace, jako jsou hesla nebo bankovní údaje. Botnety lze použít k šíření malware prostřednictvím phishingových e-mailů nebo využitím SMS. MMS, falešných aplikací a jiných.

„*Podstatou phishingu je využívání sociálního inženýrství“* (Kolouch, 2016, str. 246). Jedná se o podvodnou techniku, která je předpokladem pro to, aby byl phishing úspěšný. Je to psychologická manipulace tím, že obelstí uživatele k zadání citlivých informací. Phishing cílí na relativně neurčitý okruh obětí s nadějí, že se trefí do „někoho“.

4.2 Typy phishing

1. **Page hijacking:** oběť rozklikne stránku, která ho nasměruje na falešnou verzi např. facebooku, oběť tam zadá své přihlašovací údaje a útočník je ukradne.
2. **Whaling:** phisingové útoky, které cílí na tzv. velryby čili velmi bohaté lidi, jakými jsou např. majitelé firem či ředitelé.
3. **Email phising:** způsob, který platí pro většinu phishingových útoků, které jsou zasílány e-mailem a jsou šířeny hromadně. Způsob se dá také označit jako bulk phishing.
4. **Spear phising:** útok je cílený. Útočník dopředu získá informace o oběti a vytvoří zprávu na míru pro ni tak, aby jí podlehla. (Kolouch, 2016)
5. **CEO fraud:** útočník se tváří jako manažer a cílí na zaměstnance, kteří jsou pod ním.

4.3 Rozpoznaní phisingu a prevence

- Selský rozum
- Nepřesná URL adresa či e-mailová adresa – pokud URL nebo e-mailová adresa přesně neodpovídájí tomu, jaký je originál, tak se s velkou pravděpodobností jedná o phishingovou hrozbu, například místo originálu Facebook.com je URL adresa stránky Face-book.com
- Špatná gramatika – špatná čeština je signálem, že je něco špatně. Určitě by například z banky nepsali hrubky.
- Až moc výhodná nabídka – zprávy jako: „iPhone 15 za korunu!“, nebo „Vyhráli jste 1 000 000 Kč!“ To jsou typické podvodné zprávy pro phishing.

4.4 Online podvody jako hrozba pro ekonomiku

Podle Federálního obchodního úřadu (FTC) ztratili jen američtí spotřebitelé v roce 2023 kvůli podvodům více než 8,8 miliardy dolarů, což je o více než 30 % více než ve srovnání s rokem 2021 (FEDERAL TRADE COMMISION, 2023).

Z výše uvedeného vyplývá, že podvody jsou vážnou hrozbou pro ekonomiku a mají negativní dopady na hlavní aktéry ekonomiky.

Dopad na jednotlivce

Oběti podvodů mohou přijít o své peníze, osobní údaje nebo dokonce o důvěru v sebe sama.

Dopad na společnost

Podvody způsobují ztráty zisků, poškození reputace a snížení důvěry spotřebitelů.

Dopad na vládu

Online podvody mají také negativní dopad na vládu. Mohou vést k prodlevám v rozsahu daní, poškození veřejného majetku a snížení důvěry ve vládu.

5 Softwarové Hrozby

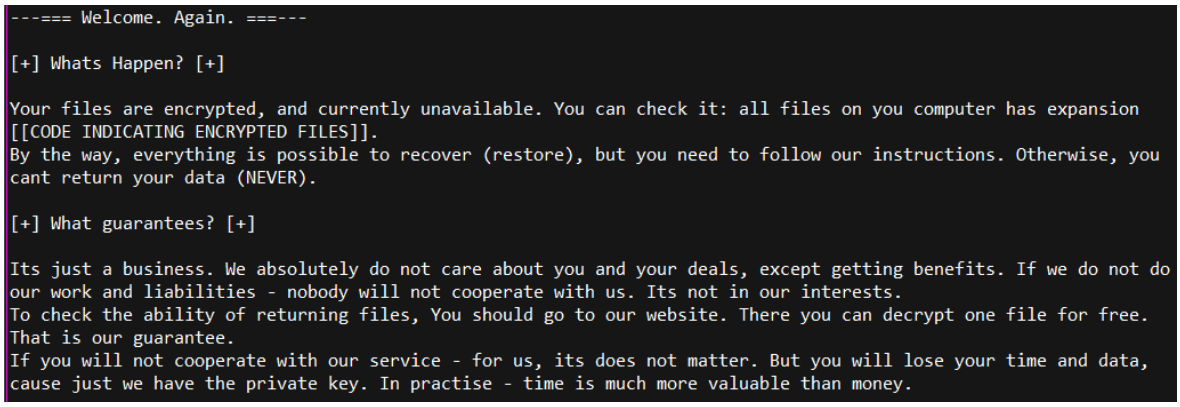
Pascal Maniriho definuje malware jako software, který je navržen k poškození počítačového systému nebo k získání neoprávněného přístupu k jeho datům (Maniriho, 2022). Tato definice je důležitá, protože nám pomáhá si uvědomit, že malware může být skrytý v jakémkoliv souboru.

5.1 Trojské koně

Skrývají se jako legální software, přičemž v pozadí po spuštění provádí škodlivé akce zadané útočníkem. Jako je krádež dat, instalace dalšího škodlivého software, nebo může rovněž sloužit k vytvoření botnet (Kolouch, 2016).

5.2 Ransomware

Blokuje přístup k počítači, většinou vyžaduje platbu za odemknutí počítače pod podmínkou, která je časově omezená, kdy v případě, že oběť nezaplatí, všechna data z počítače budou smazána a počítač bude nepoužitelný (Kolouch, 2016).
Velmi známá v Rusku založená hackerská skupina s názvem REvil, se zaměřuje na RaaS operace, což je obchodní model, v jehož případě se zaplatí za to, že tato skupina odešle ransomware útok na cílovou osobu (Li, 2021).



Obrázek 3: Ransomware zpráva od skupiny REvil https://shorturl.at/orDU0

Jan Kolouch rozděluje ransomware na dva hlavní druhy podle toho, jak zasahují do systému:

1. **Ransomware blokující systém**

Tento typ znemožní používání celého počítače. Buď zabrání spuštění operačního systému, nebo zamkne systémovou obrazovku a zobrazí zprávu s požadavkem na výkupné. Příkladem je "Policejní ransomware", který se tváří, že je od policie a obviňuje uživatele z nelegální činnosti. (Kolouch, 2016)

2. **Ransomware šifrující data**

Ponechává počítač funkční, ale zamkne a zašifruje data uživatele. Ten tak ztratí přístup k souborům, fotkám, dokumentům a dalším důležitým datům. Útočník pak požaduje výkupné za jejich dešifrování (Kolouch, 2016).

5.3 Ostatní malware

Spyware: software, který tajně shromažďuje data o aktivitách uživatele bez jeho vědomí. Tato data pak mohou být zneužita k reklamním účelům, krádeži identity nebo jiným kriminálním aktivitám. (Jirásek, 2015)

Worm: samostatně se šířící malware, který se replikuje v síti a může způsobit přetížení. Worm se šíří využitím zranitelností v operačním systému nebo síťových protokolech.

Keylogger: software zaznamenávající stisknutí kláves. Tím krade hesla a platební informace. (Jirásek, 2015)

Rootkit: malware umožňující se maskovat a skrýt před uživatelem vybrané běžící procesy (Jirásek, 2015). Umožňuje útočníkovi ovládnout počítač získáním root privilegia. Root = superuživatel, který má nejvyšší oprávnění v systému, to znamená, že může provádět libovolné akce, a to i změny v systémových souborech a konfiguraci.

6 Botnet

Vědci z Amerického Institutu elektrotechniky a elektroniky (IEEE) definovali botnet jako síť zkompromitovaných zařízení, která jsou ovládána útočníkem. Těmito zařízeními mohou být počítače, mobilní telefony, síťová nebo jiná zařízení připojená k internetu. Útočník může ovládat botnet k provádění různých útoků, včetně *DDoS* útoků, krádeží dat nebo šíření malware (al., 2020).

6.1 Životní cyklus

V první fázi (infekce) hacker (neboli boter) najde zranitelný bod buď na webové stránce, v aplikaci nebo v chování uživatele, aby ho vystavil malware. Záměrem útočníka je, aby si uživatelé nebyli vědomi svého rizika a případné nákazy malware. Může využívat bezpečnostních problémů v software nebo na webových stránkách, aby mohl malware doručit prostřednictvím e-mailů, stahování z disků nebo trojských koní.

Ve druhé fázi (spojení a kontrola) jsou zařízení obětí infikována malware, který může převzít kontrolu. Počáteční infekce malware umožňuje hackerům vytvořit „zombie“ zařízení pomocí technik, jako jsou stahování z webu, exploit kity (sada nástrojů k automatickému zneužívání zranitelností v systémech a šíření malware)., vyskakovací reklamy nebo přílohy e-mailů. Pokud se jedná o centralizovaný botnet, boter nasměruje infikované zařízení na C&C server (řídící server, se kterým komunikuje malware a ze kterého dostává pokyny k dalším aktivitám). Pokud se jedná o botnet P2P (Peer-to-peer, síťová architektura, kde počítače sdílí mezi sebou data a zdroje bez nutnosti centrálního serveru), začíná vzájemné šíření a „zombie“ zařízení se snaží spojit s dalšími infikovanými zařízeními.

Ve třetí fázi (útok a zneužití), potom, co boter infikuje dostatečné množství botů (bot = infikovaný počítač v rukou botera), může mobilizovat své útoky. „Zombie“ zařízení si pak stáhnou nejnovější aktualizaci z kanálu C&C a obdrží její příkaz. Bot pak pokračuje v plnění svých příkazů a zapojuje se do škodlivých aktivit. Boter může nadále vzdáleně spravovat a rozšiřovat svůj botnet a provádět různé nekalé praktiky. Botnety se nezaměřují na konkrétní osoby, protože cílem botera je infikovat co nejvíce zařízení, aby mohl provádět nebezpečné útoky (Avast Academy, 2024).

6.2 Řízení botnetů

- **Cetralizovaný model klient-server:** první generace botnetů fungovala na architektuře klient-server, kdy jeden server C&C (command-and-control) řídil celý botnet. Nevýhodou použití centralizovaného modelu oproti modelu P2P je vzhledem k jeho jednoduchosti náchylnost k selhání jednoho bodu (Kolouch, 2016).
    - **IRC (Internet Relay Chat) botnet:** IRC botnety patří mezi nejstarší typy botnetů a jsou řízeny na dálku pomocí předem nakonfigurovaného IRC serveru a kanálu. Boti se připojují k serveru IRC a čekají na příkazy strážce botů.
    - **HTTP botnet:** botnet HTTP je webový botnet, jehož prostřednictvím boter používá k odesílání příkazů protokol HTTP. Boti pravidelně navštěvují server, aby získali aktualizace a nové příkazy. Použití protokolu HTTP umožňuje boterovi maskovat své aktivity za běžný webový provoz.
- **Decentralizovaný model Peer-to-Peer:** novou generací botnetů je typ peer-to-peer, v rámci kterého si boti navzájem sdílejí příkazy a informace a nejsou v přímém kontaktu se serverem C&C. V případě botnetů typu peer-to-peer se jedná o tzv. P2P botnety, které je obtížnější implementovat než botnety IRC nebo HTTP, ale jsou také odolnější, protože nespoléhají na jeden centralizovaný server. Místo toho každý bot pracuje nezávisle jako klient i server a koordinovaně aktualizuje a sdílí informace mezi zařízeními v botnetu. (Kolouch, 2016)

7 Další kybernetické hrozby

- **Advanced Persistent Threats (APTs)**: dlouhodobé, sofistikované útoky, které cílí na specifické organizace nebo osoby s cílem dlouhodobého sledování a odcizení citlivých informací. Provedení útoku APT vyžaduje více úsilí než útok tradiční, protože může trvat od několika měsíců až po řadu let. Útočníci jsou obvykle dobře financovaní a mají zkušené týmy hackerů, kteří se zaměřují na bohaté organizace (Kolouch, 2016).
- **Insider**: hrozby od zaměstnanců organizace, kteří mohou přispět k úniku dat úmyslně nebo neúmyslně z nedbalosti (Jirásek, 2015).
- **Man-in-the-Middle (MitM)**: útoky, při kterých se útočník dostane mezi dvě komunikující strany a odposlouchává je (např. telefonní hovor), čímž získá jejich osobní údaje (Jirásek, 2015).
- **Dialer**: program, který se instaluje do počítače nebo chytrého telefonu bez vědomí uživatele. Jeho cílem je připojit zařízení k internetu přes pomalé a drahé komutované připojení, obvykle provozované útočníkem. (Jirásek, 2015).

8 Dezinformace

Dezinformace jsou charakterizovány jako záměrně zavádějící informace s cílem manipulovat širokou škálou cílových skupin. (Grieve, 2023). Tyto informace mohou být šířeny prostřednictvím různých kanálů včetně sociálních médií, zpravodajských portálů nebo i osobních interakcí.

Jack Grieve také ve své knize klade důraz na to, že klíčem k porozumění problému dezinformací je porozumění jazyku dezinformací (Grieve, 2023). Falešné zprávy se nejčastěji objevují v textové podobě, ať už jde o článek v novinách, reportáž v rozhlase, příspěvek na sociálních sítích nebo televizní rozhovor. To činí analýzu jazyka falešných zpráv zásadní pro identifikaci a boj proti šíření dezinformací.

8.1 Rysy dezinformací

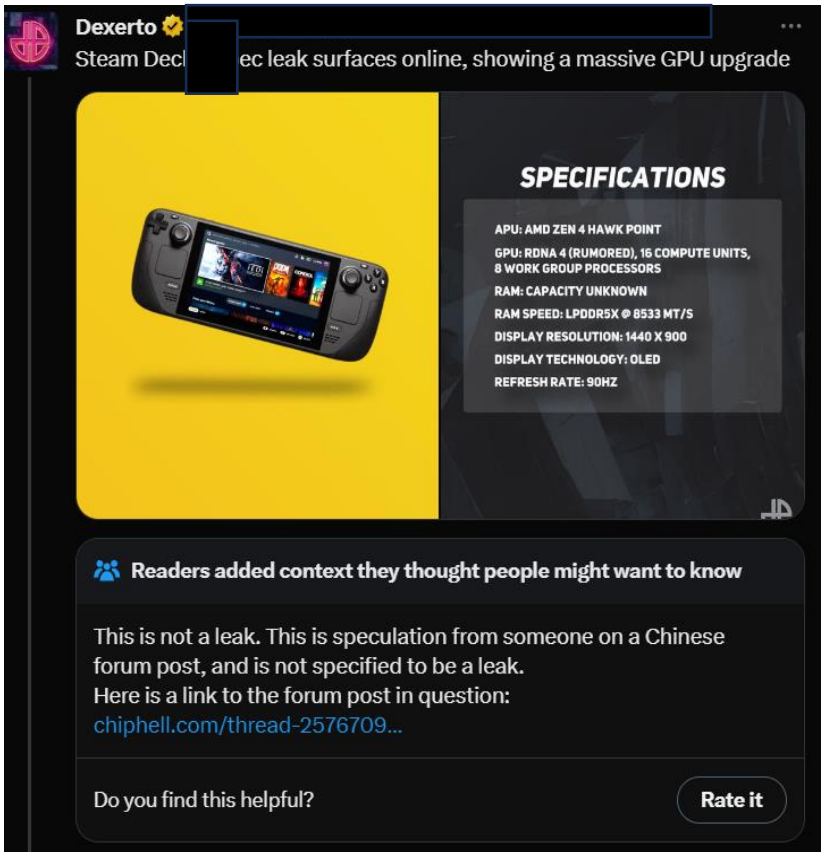
V průzkumu dezinformací lze vypozorovat několik rysů, které se neustále opakují. Dají se rozdělit do několika oblastí:

- přesnost dezinformace většinou obsahují informace nepřesné a zkreslené;
- emocionální apely – dezinformace používají často emocionální jazyk k manipulaci emocí čtenářů;
- osobní útoky – osobní útoky na jednotlivce nebo skupiny, aby zdiskreditovaly jejich důvěryhodnost a podkopaly jejich argumenty (příkladem by mohl být deepfake nějakého známého politika);
- gramatika – u dezinformací jsou časté gramatické chyby;
- obecný jazyk – dezinformace často používají neformální jazyk či slang;
- zdroje – dezinformace často neodkazují na žádné důvěryhodné zdroje;

Analýzou jazykových rysů je možné identifikovat potenciální dezinformace a zvýšit povědomí mezi čtenáři, aby byli kritičtější k informacím, se kterými se setkávají online a v médiích.

Na obrázku 3 ze sítě X si můžeme ukázat několik rysů, proč je zrovna tento článek dezinformací:

1. sociální síť X poskytuje dodatečný text o tom, že informace v tomto příspěvku nejsou ověřené a jedná se pouze o spekulaci;
2. žádná citace: autor neuvedl žádný zdroj;
3. slovo leak (únik informací) může často značit dezinformaci, protože uniklé informace mohou být neúplné nebo zavádějící. Většinou takové informace existují z důvodu získání více prokliků.



Obrázek 4: Fake news https://twitter.com/Dexerto

8.2 Dezinformace jako hrozba pro demokracii

- Narušují důvěru ve veřejné instituce. Dezinformace mohou zkreslovat obraz o veřejných institucích, což může vést k tomu, že občané nebudou důvěřovat vládě, médiím nebo dalším institucím.
- Dezinformace mohou být použity k podkopání legitimity demokratických procesů, kterými jsou například volby nebo referenda. To může vést k tomu, že občané nebudou považovat výsledky těchto procesů za platné.
- Dezinformace mohou být použity k podněcování násilí a extremismu. To může vést k tomu, že občané budou více náchylní k násilným činům nebo k podpoře extremistických skupin.

Vzhledem k tomu jsou důležité následující kroky:

- Měla by se posílit mediální gramotnost. Občané by měli být schopni kriticky hodnotit informace.
- Šířit povědomí a vzdělávat o dezinformacích.
- Bojovat za lepší regulaci příspěvků na sociálních sítích.

9 AI

Umělá inteligence (Artificial Inteligence) je schopnost strojů napodobovat lidské funkce, jako je uvažování, učení se, plánování nebo kreativita. Je to rychle se rozvíjející technologie, a proto je v oblasti kyberkriminality velmi nebezpečná. Zkoumání „Proceedings of the International Conference on Cybersecurity and Cybercrime“ (Lozonschi, 2023), které analyzuje AI jako hrozbu pro naši kyberbezpečnost, byly vypozorovány tyto závěry:

- AI v oblasti kyberkriminality zahrnuje vytváření deepfake, zdokonalování algoritmů pro hádání hesel a pro krádež identity
- s vývojem AI se vyvíjí i schopnost zločinců zaměřených na kyberkriminalitu vyhnout se její detekci a tím pádem i jejich dopadení

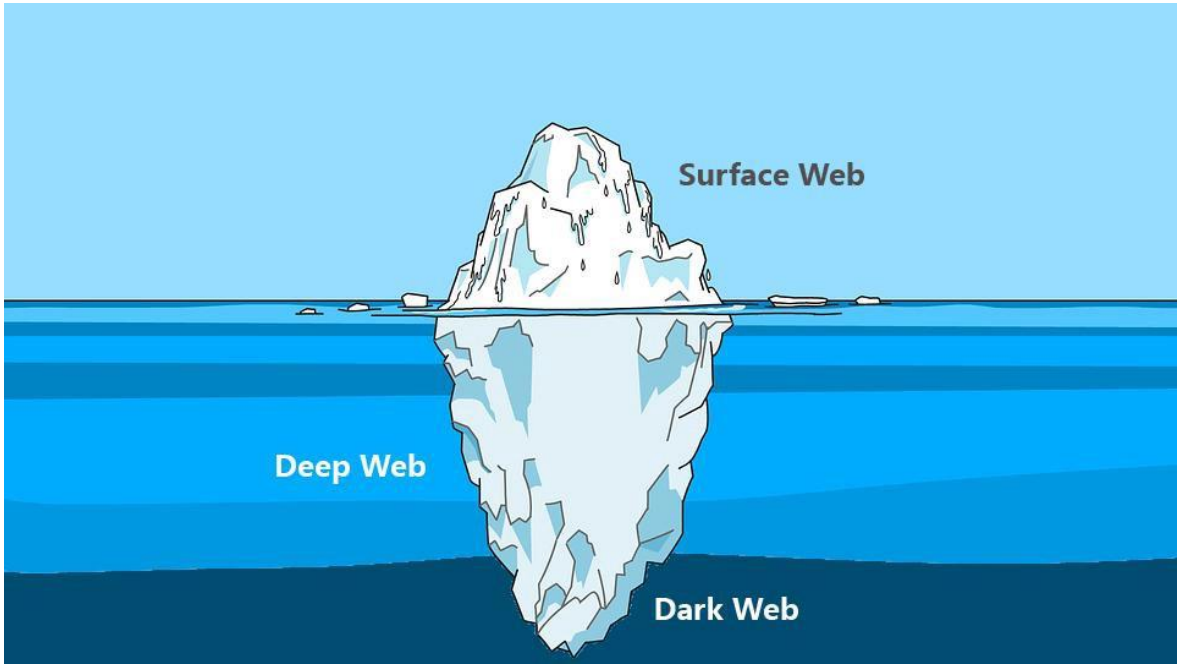
Závěry ohledně kyberbezpečnosti:

- AI se využívá v rámci obrany k automatickému prohledávání sítí a odrážení útoků. To zahrnuje její používaní k detekci anomálií v síťovém provozu, identifikaci phishingových e-mailů a blokování škodlivých webových stránek
- AI je v kontextu kybernetické kriminality dvojsečnou zbraní

10 Dark Web

Web je rozdělený do tří částí: **Surface Web, Deep Web a Dark Web,** které se dělí podle toho, zda jsou indexovány běžnými vyhledávači**.** Surface web je nejvyšší vrchol pomyslného ledovce, což znamená, že na tento druh webu nás dostanou klasické vyhledávače jako jsou Bing nebo Google. Toho dosáhnou tím, že každá stránka je v takzvaném indexu, což je seznam webových stránek, které jsou uspořádány podle klíčových slov. Vyhledávače indexují webové stránky, aby je mohly uživatelům najít. Většina webu však není indexována, protože je příliš rozsáhlá a neobsahuje žádné hypertextové odkazy (Alaidi, 2022).

To znamená, že ostatní webové stránky nemohou tuto část webu odkazovat. Naproti tomu Deep Web je tou částí webu, kterou vyhledávače nevidí, a obsahuje Dark Web, což je jeho hlubší součást.



Obrázek 5: Rozdělení webu https://shorturl.at/tvG37

Hlavní rozdíl mezi Deep Web a Dark Web je ten, že Dark Web je přístupný pouze za použití speciálního software nebo proxy serveru a je charakteristický svou anonymitou, která umožnuje uživatelům provozovat nelegální aktivity jako je prodej drog, zbraní, dětské pornografie či obchod s lidmi. Často jsou přítomny finanční podvody nebo pirátský obsah. Je ale důležité upozornit na to, že Dark Web může být taky použit pro legální účely, jako je například ochrana soukromí novinářů. Deep Web nemusí být přímo nelegální, většinou zahrnuje soukromé weby jako jsou vnitřní firemní sítě, vědecké databáze a různé archívy. Například **intranet** je firemní síť, která není dostupná veřejnosti a tím tvoří částečně Deep Web (Kolouch, 2016).

11 Napadání osobních údajů

Na internetu existuje mnoho hrozeb a jednou z nich je krádež osobních údajů. Ty musí lidé chránit, jestliže, nechtějí, aby někdo měl jejich osobní údaje, kterými by mohl zasahovat do jejich soukromí a osobní svobody nebo jim jejich identitu ukrást. Nejdůležitějším způsobem, jak ochránit své soukromí a osobní údaje je prevence: používat dostatečně silná hesla, dvoufázový autentifikátor, mít aktualizovaný software, používat VPN (služba, která šifruje vaše internetové připojení), navštěvovat pouze důvěryhodné stránky a hlavně mít selský rozum.

11.1 Cookies

„*Informace (které se typicky nabalují na cookies aj.) uložené v uživatelově místním úložišti se mohou stát i zajímavým cílem pro útočníka, neboť právě z těchto informací je možné zjistit např. vzorce chování uživatele.“* (Kolouch, 2016, str. 149)

Cookies jsou malé textové soubory, které se ukládají do zařízení uživatelů, jako jsou notebooky nebo chytré telefony, aby usnadnily fungování webových stránek (funkční soubory cookie) nebo ke shromažďování profilových informací, které umožňují například cílenou reklamu (Strycharz, 2021).
Rozdělují se na dva typy: cookies prvních stran a cookies třetích stran.
Cookies prvních stran jsou pouze na stránce, na které aktuálně jste. Jsou důležité k tomu, aby stránka fungovala jako celek, proto se nedoporučuje je blokovat. Obvykle se používají pro legitimní účely, jako je zapamatování přihlášení, předvoleb nebo položek v nákupním košíku (Munir, 2023).
„Internetové stránky mohou využívat externích služeb, které ukládají vlastní soubory cookies – tzv. cookies třetích stran.“ (Evropská komise, 2024, str. 1) Cookies třetích stran jsou používány k cílení reklamy nebo k analýze chování. To je známý fenomén toho, kdy si uživatel chce ráno koupit sekačku a večer, když projíždí web, dostane reklamu, která ke koupi sekačky vybízí.

11.2 E-Privacy Directive

E-Privacy Directive je zákon, který se snaží omezit sběr osobních dat a chránit tak soukromí uživatelů. V zákonu stojí, že ukládání cookies je povoleno pouze pokud uživatel dá výslovný souhlas. To znamená, že klikne na *„povolit vše“*. V zákonu se také píše, že uživatel musí mít vždy možnost cookies odmítnout. Vývojáři stránek proto musí zajistit, aby uživatel dostal všechny podrobnosti ohledně cookies a aby je mohl jak přijmout, tak odmítnout. Někteří vývojáři však dělají odmítnutí cookies těžší, než by muselo být. Buď skryjí tlačítko na odmítnutí, nebo donutí uživatele rozkliknout podrobnosti a každý cookie po jednom vypnout. To většinou uživatele donutí cookies jednoduše přijmout a dále je neřešit, čímž uživatel riskuje krádež svých osobních dat (Bond, 2021).

Obrázek 6: Cookies pop-up https://shorturl.at/rSW25

12 Deepfake

Deepfake (DF) je označení pro realistickou úpravu videa nebo snímku za použití umělé inteligence. To se vypracuje tak, že obličej jedné osoby se vymění za obličej osoby druhé. DF se dá využít i pozitivně, a to k vytvoření zábavného kontentu, ale bohužel se často v dnešní době používá k propagandě, manipulaci široké veřejnosti či k výrobě pornografie.

Označení „Deepfake“ je odvozeno od „Deep Learning (DL)“ a „Fake“ a charakterizuje konkrétní fotorealistické video, zvukovou nahrávku nebo snímky vytvořené s podporou DL. Deep learning je podmnožina metod strojového učení, která se opírá o umělé neuronové sítě s reprezentativním učením. Přídavné jméno „deep“ odkazuje na použití více vrstev v síti. Studie *„Deepfake Detection: A Systematic Literature Review“* (Rana, 2022), která shrnuje metody pro detekci DF, došla k těmto závěrům:

- metody založené na DL jsou široce používány k detekci Deepfake
- v experimentech dataset FF++ (FaceForensics++) zaujímá největší podíl. Tento dataset obsahuje více než 500 000 falešných videozáznamů, které jsou rozděleny do různých kategorií, jako je politika, sport nebo celebrity.
- „detekční přesnost“ je nejběžněji používaným metrickým ukazatelem pro měření účinnosti metod detekce DF. Detekční přesnost je procento falešných videozáznamů, která jsou rozpoznána jako falešná.

12.1 Rozpoznání Deepfake

V rámci zkoumání metod rozpoznávání DF byla identifikována následující pravidla:

- při sledování úst je třeba dávat pozor na jejich rozmazání a nepřirozený pohyb
- nepřirozený pohyb může být patrný i u jiných částí těla, například při pohybu rukou nebo hlavy, protože algoritmus umělé inteligence zatím **ještě** není dokonalý
- zvuk může znít roboticky nebo jinak uměle
- zblízka mohou obličeje vypadat jako statické obrázky
- trénink na rozpoznávání DF může pomoci zlepšit schopnost člověka tato videa a zvuky identifikovat. Čím více se člověk s DF setká, tím lépe bude schopen identifikovat jejich charakteristické znaky

Nyní DF rozpoznáme většinou z toho důvodu, že technologie na tvorbu DF ještě není tak dokonalá. V budoucnu se bude AI stále rozvíjet a je dost pravděpodobné, že nebude již možné rozeznat DF jen „*od oka*“.

12.2 Možnosti řešení problémů s rozpoznáváním DF

- vývoj nových metod rozpoznávání DF pro lepší detekci
- vzdělávání veřejnosti. Lidé by měli být informováni o tom, jak rozpoznat DF, aby mohli lépe chránit sebe a ostatní před dezinformacemi.
- regulace tvorby tím, že s tvorbou DF, pakliže u ní bude prokázána snaha záměrně někomu uškodit, bude zacházeno jako s trestným činem.

12.3 Technologie tvorby deepfake

12.3.1 Webová aplikace

Jednou z webových aplikací je i HeyGen, který je známý pro své snadné použití bez technických znalostí. Tato aplikace umožňuje vytvořit avatara jakéhokoliv člověka a jeho hlasu a napsat skript, podle něhož program vytvoří video, kde avatar mluví a hýbe se.

Výhody:

- snadné použití, nevyžaduje technické znalosti
- zdarma a dostupné online
- rychlé a jednoduché výsledky

Nevýhody:

- vodoznaky v bezplatné verzi

Webová stránka HeyGen: https://app.heygen.com/

12.3.2 Mobilní aplikace

Aplikace na tvorbu deepfake, která se dočkala velké popularity je například FaceApp (https://www.faceapp.com). Tato slouží k úpravě fotografií a videí, přičemž používá funkce deepfake, jako je stárnutí nebo změna pohlaví.

Výhody:

- snadné použití a zábavná forma
- dostupnost na mobilních zařízeních

Nevýhody:

- omezené funkce a možnosti
- nižší kvalita výsledků

Obrázek 7: Výsledek FaceApp https://www.faceapp.com

12.3.3 PC program

- Mezi PC programy patří DeepFaceLab. Je to snadno použitelný program s intuitivním rozhraním, který nabízí základní funkce deepfake, jako je výměna tváří a morphing (technika úpravy obrázků, kdy se dvě fotografie obličejů prolnou dohromady, aby vznikl obličejů. Funguje to tak, že se vyberou dvě videa, z nichž jedno je source (video obličeje, který chci použít) a druhé destination (video s obličejem, kterým chci source nahradit). Následně program rozstříhá obě videa po jednom snímku, aby mohl udělat model pro trénování.

Obrázek 8: Preview procesu tréninku deepfake modelu https://www.deepfakevfx.com

- Webová stránka Deepfacelab: https://www.deepfakevfx.com

Výhody:

- pokročilé funkce a možnosti
- vyšší kvalita výsledků
- zdarma

Nevýhody:

- náročnější na instalaci a použití
- vyžaduje technické znalosti
- vyžaduje silné GPU a CPU
- časová náročnost

Obrázek 9: Výsledek programu DeepFaceLab

12.4 Kriminální využití deepfake

Deepfake se může použít v počítačové kriminalitě k:

šíření dezinformací:

- vytváření falešných zpráv a videí, které mohou být použity k ovlivňování veřejného mínění

podvodu:

- vytváření falešných identit a podvádění lidí. Například vytvoření falešné reklamy s cílem z obětí získat osobní údaje nebo peníze

vydírání:

- vytváření kompromitujících materiálů. Například vytvoření falešného videa, na kterém je někdo zachycen při nezákonné nebo neetické činnosti

12.5 Pozitivní využití deepfake

Deepfake však může být využit i kladně, a to v následujících oblastech:

vzdělávání a zpřístupnění informací:

- tvorba interaktivních učebních materiálů - oživení historické postavy nebo události, čímž se zpřístupňuje zprostředkovávání vzdělávacího obsahu poutavějším způsobem.

zábava:

- konceptualizace a implementace inovativních forem zábavy

věda a výzkum:

- simulace a modelování komplexních systémů a jevů
- zdokonalování lékařské péče. AI deepfake terapeut může lidem s psychickými problémy pomoct s úzkostmi, depresemi a dalšími potížemi.

13 Vlastní práce – dotazník

Hlavním cílem dotazníku je porozumět tomu, jak veřejnost vnímá kyberkriminalitu a jaká preventivní opatření používá, jakou má důvěru v online technologie a služby, a jak umí rozeznat „fake“ od reality.

Dílčí cíle:

- zmapovat znalosti a postoje respondentů k dezinformacím, deepfake, malware a online podvodům
- zhodnotit preventivní opatření, která respondenti používají k ochraně před kyberkriminalitou
- identifikovat případné rozdíly ve vnímání kyberkriminality v závislosti na demografických faktorech (věk, pohlaví, vzdělání atd.)

13.1 Demografické údaje

Počet respondentů: 76

Věk:

- 15-19 let: 36 respondentů (48 %)
- 20-29 let: 21 respondentů (28 %)
- 30-50 let: 10 respondentů (13,3 %)
- 51-80+ let: 8 respondentů (10,7 %)

Pohlaví:

- Muži: 41 respondentů (55,4 %)
- Ženy: 31 respondentů (41,9 %)
- Jiné/neuvedeno: 2 respondenti (2,7 %)

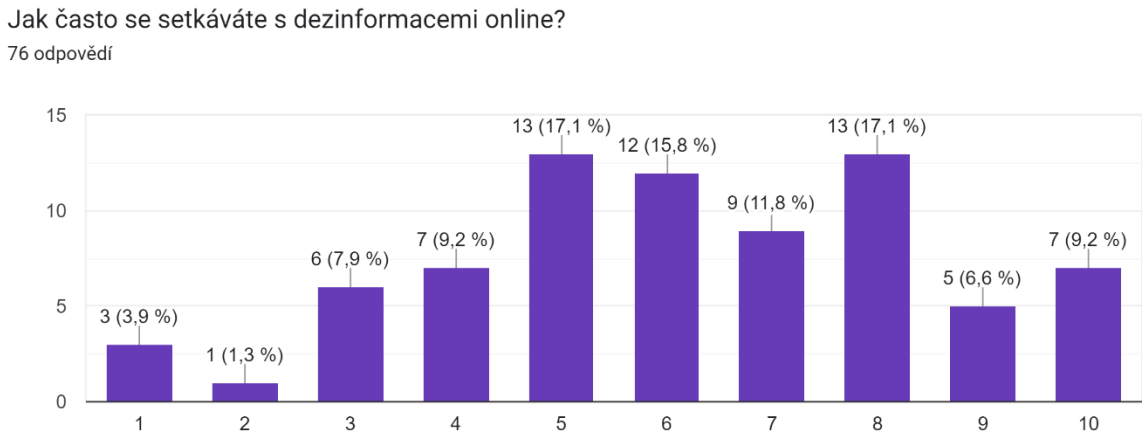
Dokončené vzdělání:

- Základní: 13 respondentů
- Učiliště bez maturity: 5 respondentů
- Středoškolské s maturitou: 29 respondentů
- Vysokoškolské nedokončené: 4 respondenti
- Vysokoškolské: 8 respondentů
- Stále studuji: 33 respondentů

Pozn.: respondenti mohli zaškrtnout své aktuální vzdělání a zároveň i to, že stále studují, proto nejsou uvedena procenta.

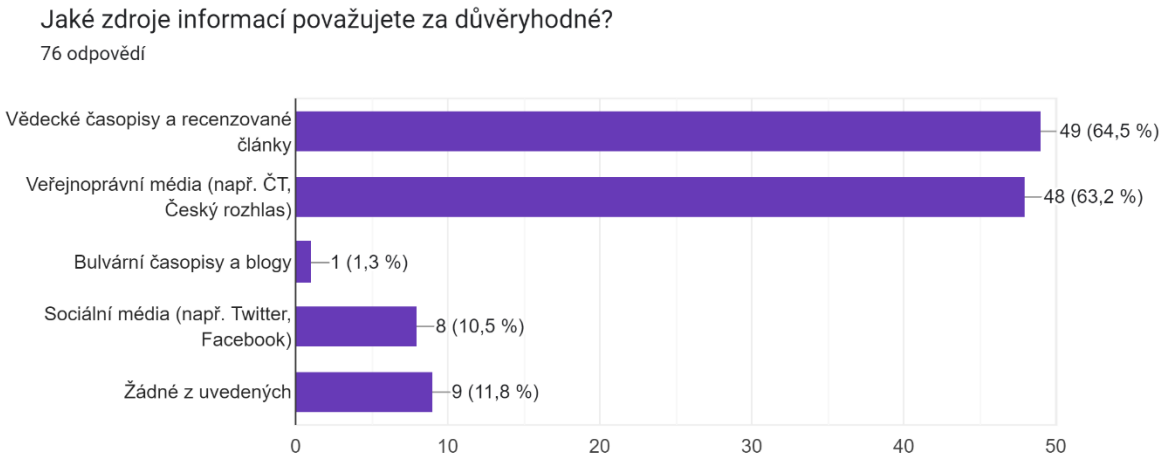
13.2 Dezinformace

Dotazníkové šetření ukázalo, že se s dezinformacemi online respondenti setkávají poměrně často (průměrná hodnota 6,3, přičemž 10 znamená potýkám se s nimi neustále). To zdůrazňuje důležitost boje proti šíření dezinformací a zvyšování mediální gramotnosti.



Tabulka 1: Vlastní šetření: dezinformace obecně

Výsledky dotazníkového šetření ukazují, že vnímání důvěryhodnosti informací se liší v závislosti na typu zdroje. Většina lidí věří ověřeným zdrojům, jako jsou vědecké časopisy či veřejnoprávní média, zatímco bulvární časopisy a sociální média vnímají jako méně důvěryhodné. To je vnímáno jako pozitivní výsledek.

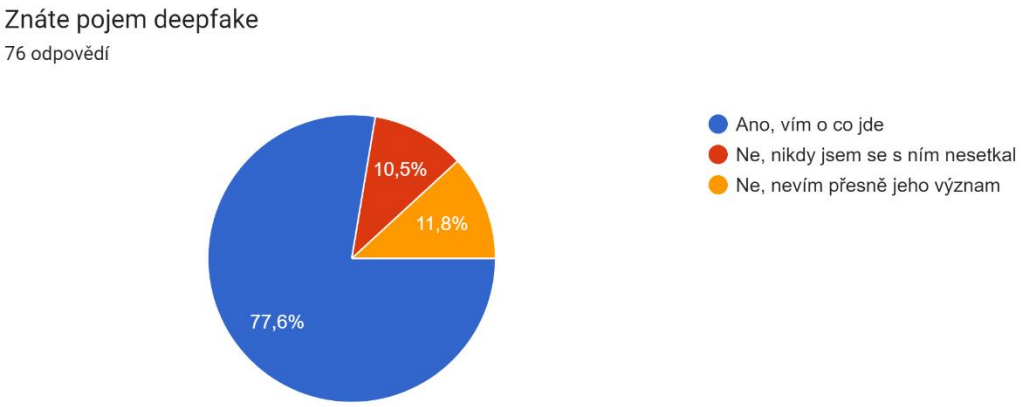


Tabulka 2: Vlastní šetření: důvěryhodné zdroje

Ověřování informací je nezbytné pro efektivní a zodpovědné používání internetu. Bez ověřování informací se vystavujeme riziku šíření dezinformací, manipulací a zavádějících tvrzení. Z dotazníku bylo zjištěno:

- 44,7 % ověřuje zdroj
- 50 % používá kritické myšlení
- 77,6 % ověřuje informace z více zdrojů
- 5,3 % neověřuje žádné informace

13.3 Deepfake



Tabulka 3: Vlastní šetření: pojem deepfake

Z grafu je patrné, že ačkoliv povědomí o deepfake roste, stále existuje značná skupina lidí, kteří o technologii nevědí nebo o ní slyšeli jen okrajově.
Dotazník obsahoval deepfake video, o kterém měli respondenti rozhodnout, zda se jedná o skutečné video nebo ne.

- 52 % respondentů si byli **100 % jistí**, že se jedná o deepfake.
- 22 % respondentů si byli **hodně jistí**, ale ne na 100 %.
- 11 % respondentů si **spíše mysleli**, že se jedná o skutečné video.
- 4 % respondentů **věřili**, že se jedná o skutečné video.

Výsledky ukazují, že ačkoliv se povědomí o technologii deepfake šíří, stále existuje značná skupina lidí, kteří s ní nejsou obeznámeni nebo ji nedokáží správně rozpoznat.

Koncept deepfake vyvolává otázky ohledně jeho morálního statusu. Může být vnímán jako nástroj pro manipulaci a klamání, čímž by se zařadil do kategorie neetických praktik. Na druhou stranu existují i potenciální legitimní využití deepfake, například v oblasti vzdělávání, umění nebo zábavy.

- 40,8 % respondentů si myslí, že je **nemorální**
- 34,2 % respondentů si myslí, že je **spíše nemorální**
- 15,8 % respondentů zaujalo **neutrální postoj** k morálnosti deepfake
- 9,1 % respondentů si myslí, že je **spíše morální**
- **Žádný respondent nevnímá deepfake jako čistě morální**

Zdá se, že existuje silný konsenzus ohledně nemorálnosti deepfake. Většina respondentů ho vnímá jako neetický a zavrženíhodný.

13.4 Malware

Na otázku „Víte, jak se bránit proti malware? Máte nainstalovaný na svém počítači/notebooku nějaký antivirus?“ bylo zodpovězeno následovně:

- většina respondentů (76 %) deklaruje, že ví, jak se bránit proti malware;
- z nich 44,7 % spoléhá na základní ochranu Windows Defender /Apple XProtect a 31,6 % používá antiviry třetí strany;
- 10,5 % respondentů neví, jak se bránit proti malware, ale má nainstalovaný antivirus;
- 5,3 % respondentů neví, jak se bránit proti malware a nemá nainstalovaný žádný antivirus;
- 7,9 % respondentů nemá počítač/notebook.

Z dotazníkového šetření vyplývá, že ačkoliv je povědomí o prevenci malware poměrně vysoké, stále existuje značné množství uživatelů, kteří nevědí, jak se adekvátně bránit, čímž se vystavují bezpečnostním rizikům.

Z dotazníkového šetření vyplývá, že 64 % respondentů se setkalo s malware ve svých PC, v 50,7 % případů antivirus dokázal malware odstranit bez ztráty dat. Ztráty dat utrpělo 13,3 % respondentů, kteří se s malware setkali.

Vzhledem ke zjištěním z dotazníkového šetření je nezbytné dodržovat následující doporučení pro minimalizaci dopadů malware útoků:

- pravidelně zálohovat důležitá data na externí médium nebo do cloudu;
- udržovat software a antivirus aktualizovaný;
- být opatrní při otevírání příloh e-mailů, klikání na odkazy a stahování souborů z neznámých zdrojů;
- v případě podezření na malware provést scan počítače antivirem.

13.5 SCAM

Z dotazníkového šetření vyplývá, že **77,6 % respondentů se setkalo s online podvodem**. **67,1 %** se mu dokázalo vyhnout, zatímco **10,5 %** se stalo obětí podvodu. To ukazuje, že online podvody jsou poměrně běžné a že většina se jim dokáže efektivně ubránit vyhnout. Pro prevenci online podvodů je důležité být ostražitý, používat selský rozum a informovat se o různých typech podvodů.

Dotazníkové šetření ukázalo, že:

- **phishing** zná 68,5 % respondentů
- **podvodné e-shopy a inzeráty** 90,4 % respondentů
- **investice a kryptoměny** 71,2 % respondentů
- **podvodné charity** 75,3 % respondentů
- **podvody láskou** 63 % respondentů
- **ransomware** 43,8 % respondentů
- **smishing a vishing** 12,3 % respondentů

Výsledky ukazují vysokou úroveň povědomí o online podvodech, stále ale existuje prostor pro zlepšení. I když 100% znalost o online podvodech je utopie, s aktivním přístupem a společným úsilím lze minimalizovat jejich dopad a chránit jak jednotlivce, tak i společnost jako celek.

14 Demografické rozdíly

Analýza demografických faktorů a jejich vlivu na vnímání kyberkriminality. Cílem je zjistit, zda existují statisticky významné rozdíly v odpovědích respondentů v závislosti na jejich věku, pohlaví a vzdělání.

14.1 Dle věku

Méně starších respondentů (51-80+) uvedlo, že se setkávají s dezinformacemi, na rozdíl od mladších lidí (15-50).
Lidé ve věku 30-50 let nejlépe rozpoznávají deepfake.
Lidé ve věku 20-29 let považují deepfake za nejméně morbidní.

14.2 Dle pohlaví

Muži se setkávají s dezinformacemi o něco častěji než ženy.
Ženy jsou o něco lepší v rozpoznávání deepfake než muži.
Ženy vnímají deepfake jako více morbidní než muži.

14.3 Dle vzdělání

Lidé s vyšším vzděláním se setkávají s dezinformacemi nejčastěji.
Lidé s vyšším vzděláním lépe rozpoznávají deepfake než lidé s nižším vzděláním.
Lidé s nižším vzděláním vnímají deepfake jako více morbidní než lidé s vyšším vzděláním.

Věk:	Setkání s dezinformacemi:	Rozpoznání DF	Morbidnost deepfake (0 = morbidní)
15-19	5,5/10	8,3/10	2,667/10
20-29	7,4/10	8,625/10	3,17/10
30-50	6,667/10	9/10	2,667/10
51-80+	5/10	7,4/10	2,75/10
Pohlaví:			
můž	6,68/10	8,5/10	3,317/10
žena	5,9/10	9/10	2,225/10
Vzdělání:			
Vysoké	7,5/10	9,4/10	3/10
Střední	6,07/10	9/10	1,85/10
Základní	5,35/10	9,28/10	2,35/10

Tabulka 4: Vlastní šetření: demografické výsledky

15 Dopady počítačové kriminality

Vnímání kybernetických hrozeb:

- průzkum ukazuje, že respondenti si uvědomují hrozby vycházející z dezinformací, deepfake, malware a online podvodů. To však neznamená, že by se o nich i nadále nemělo rozšiřovat povědomí. Naopak to ukazuje, že boj s nimi je efektivní.

Dopady na ekonomiku:

- data říkají, že počítačová kriminalita má dopady na společnost, včetně finančních ztrát, krádeží osobních údajů a poškození reputace. Tyto informace zdůrazňují závažnost ekonomických důsledků kyberkriminality

Prevence proti malware:

- průzkum zjistil, jaké nástroje veřejnost používá k obraně proti malware a jaké povědomí o ochraně proti malware mají

Demografické faktory:

- analýza demografických dat ukazuje, že vnímání kyberkriminality a jejích dopadů se liší v závislosti na věku, pohlaví a vzdělání

16 Závěr

Bakalářská práce se zabývá tématem kyberkriminality a jejím vlivem na společnost. Práce analyzuje různé typy kyberkriminality, jako jsou dezinformace, deepfake, malware, online podvody, deepweb a darkweb. Práce také zkoumá dopady kyberkriminality na jednotlivce, firmy a společnost jako celek.

Z výzkumu vyplynulo, že kyberkriminalita je i v dnešní době, kdy existuje mnoho veřejně přístupných prostředků k ověřování informací problémem, který negativně postihuje každého člověka nehledě na pohlaví a věk. Přestože se před ní lidé umí lépe bránit, tak stále mnohým způsobuje finanční ztráty, krádeže osobních údajů, poškození reputace a narušení důvěry v online a veřejné sociální prostředí. Je tedy nutné se vůči ní vymezit, šířit o ní povědomí a bojovat proti ní dál.

Práce zdůrazňuje důležitost prevence kyberkriminality. K té je nutné zvýšit povědomí o jejích rizicích a vzdělávat nejen počítačové uživatele o tom, jak se chránit. Je také důležité, aby firmy a instituce investovaly do kybernetické bezpečnosti a implementovaly adekvátní ochranná opatření.

Boj s kyberkriminalitou je komplexní úkol, který vyžaduje spolupráci všech aktérů – jednotlivců, firem, institucí a především států.

Citovaná literatura

al., A. e. (2020). *Systematic Literature Review on IoT-Based Botnet Attack.* IEEE.

Alaidi, A. H. (2022). Dark Web Illegal Activities Crawling and Classifying. V *Interactive Mobile Technologies* (stránky 122-139). Wasit: College of Computer Science and Information Technology.

Avast Academy. (2024). How to create a botnet.

Bentham Science Publishers and BioMed Central. (26. 3 2020). *Online Romance Scams: Relational Dynamics and Psychological Characteristics of the Victims and Scammers. A Scoping Review.* Načteno z PubMed Central: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7254823/

Bluevoyant. (2022). *Cybercrime: History, Global Impact & Protective Measures [2022]*. BlueVoyant.

Bond, R. (2021). *The EU E-Privacy Directive and Consent to Cookies.* Načteno z Heinonline: https://heinonline.org/HOL/LandingPage?handle=hein.journals/busl68&div=17&id=&page=

Button, C. C. (2017). *Cyber Frauds, Scams and their Victims.*

Coveillance.org/cookie. (2. 1 2021). Načteno z Wikibooks: https://en.wikibooks.org/wiki/Coveillance.org/cookie

Dlubalová. (2023). *Na nebezpečí kyberkriminality upozorní Den bezpečnějšího internetu*. Načteno z Ministerstvo vnitra České republiky: https://www.mvcr.cz/clanek/na-nebezpeci-kyberkriminality-upozorni-den-bezpecnejsiho-internetu.aspx#:~:text=února%202023%20spolupořádá.,%25%20(94%2C9%20%25).

Evropská komise. (2024). *Evropská komise*. Načteno z Používání cookies.

FEDERAL TRADE COMMISION. (23. Únor 2023). *FTC.* Načteno z FTC: https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022

Grieve, H. W. (2023). *The Language of Fake News.* Cambridge Elements.

Hinds, E. J. (Listopad 2020). *"It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal,*. Načteno z sciencedirect: https://www.sciencedirect.com/science/article/abs/pii/S1071581920301002

Israel, D. U. (2015). Declaring War on the Movies:. *A (Legal) Review of North Korea, Sony, and The Interview*, 2.

Jirásek, N. P. (2015). *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie ČR v Praze.

Kieffer, G. R. (2017). Understanding and Combating Investment Fraud. V P. B. Olivia S. Mitchell, *Financial Decision Making and Retirement Security in an Aging World* (stránky 186-189). Oxford: OXFORD.

Kolouch, J. (2016). *CyberCrime.* Praha: CZ.NIC, z. s. p. o.

Li, A. (. (2021). *An Analysis of the Recent Ransomware Families.* Indianapolis: Purdue Univesity.

Lozonschi, I. B. (2023). Proceedings of the International Conference on Cybersecurity and Cybercrime - 2023. V I. B. Carla LOZONSCHI, *Artificial Intelligence and its Impact on Cybercrime* (stránky 120-126). The Central and Eastern European Online Library.

Maniriho, A. N. (2022). *A study on malicious software behaviour analysis and detection techniques: Taxonomy, current trends and challenges.* ScienceDirect.

Ministerstvo vnitra. (2024). *mvcr.* Načteno z Kybernetický terorismus, kyberterorismus: https://www.mvcr.cz/clanek/kyberneticky-terorismus-kyberterorismus.aspx
Munir, S. I. (1. Únor 2023). *National Science Foundation.* Načteno z CookieGraph: Understanding and Detecting First-Party Tracking Cookies: https://par.nsf.gov/servlets/purl/10421525
Phillips, K. (2022). *Conceptualizing Cybercrime: Definitions, Typologies.* Basel: forensic sciences.
Ramun, S. K. (26. 6 2023). *Diablo 4 DDoS Attack Explained*. Načteno z afkgaming: https://afkgaming.com/gaming/diablo-4/diablo-4-ddos-attack-explained
Rana, M. N. (2022). Deepfake Detection: A Systematic Literature Review. V M. N. Md Shohel Rana, *IEEE Access* (stránky 25494 - 25513). IEEE.
Strycharz, S. H. (Červenec 2021). *Sciencedirect.* Načteno z Computers in Human Behavior.
Tapia, J. (2022). *The Budapest Convention on Cybercrime.*
US Department of Commerce. (2002). *Export Administration Regulations (EAR).* Načteno z https://www.bis.doc.gov/: https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear

Seznam obrázků, tabulek, grafů a zkratek

Seznam obrázků

Seznam tabulek

Odkaz na výsledky dotazníku

https://docs.google.com/spreadsheets/d/1UdTRDVY9Ee2tuiI5bUvI8DWKNXoJjQwmlQwrR7OltN0/edit?usp=sharing

Seznam grafů

Seznam použitých zkratek

AI - Artificial Inteligence

DF - Deepfake

DoS - Denial-of-Service útok

DDoS - Distribuovaný DoS útok

RaaS - Ransomware-as-a-Service

FTC - Federální obchodní komise

IEEE - Institute of Electrical and Electronics Engineers

C&C - Command and Control

P2P - Peer-to-peer

IRC - Internet Relay Chat

HTTP - Hypertext Transfer Protocol

URL - Uniform Resource Locator

APTs - Advanced Persistent Threats

MitM - Man-in-the-Middle útok

FF++ - FaceForentics++

VPN - Virtual Private Network

SCAM - Podvod

CEO - Chief executive officer

Přílohy

Dotazníkové šetření o vnímání kyberkriminality veřejností

Cílem tohoto šetření je lépe porozumět tomu, jak veřejnost vnímá kyberkriminalitu a jaká preventivní opatření používají, jakou mají důvěru v online technologie a služby, a jak umí rozeznat faleš od reality.

Údaje budou použity pouze pro výzkumné účely a budou anonymizovány. To znamená, že vaše odpovědi nebudou spojeny s vaším jménem ani s žádnými jinými identifikačními údaji.

Děkujeme za váš čas a za vaši ochotu.

Věk

- 15 - 19
- 20 - 29
- 30 - 50
- 51 - 80+

Pohlaví

- Muž
- Žena
- Jiné/Nechci uvádět

Vzdělání

- Základní
- Učiliště bez maturity
- Střední s maturitou
- Vysoké
- Vysoké nedokončené
- Stále studuji

Dezinformace

- Zavádějící informace šířené online, úmyslně nebo neúmyslně.

Jak často se setkáváte s dezinformacemi online?

- Nesetkávám/Nezaznamenávám
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- Pořád

Jaké zdroje informací považujete za důvěryhodné?

- Vědecké časopisy a recenzované články
- Veřejnoprávní média (např. ČT, Český rozhlas)
- Bulvární časopisy a blogy
- Sociální média (např. Twitter, Facebook)
- Žádné z uvedených

Jak si ověříte, že informace na internetu je ověřená?

- Ověřím zdroj
- Použiji kritické myšlení
- Ověřím informace z více zdrojů
- Informace nikdy neověřuju

Deepfake

- Technologie, která umožňuje manipulovat s videem a zvukem tak, aby se zdálo, že někdo říká nebo dělá něco, co ve skutečnosti neřekl ani nedělal.

Znáte pojem deepfake

- Ano, vím, o co jde
- Ne, nikdy jsem se s ním nesetkal
- Ne, nevím přesně jeho význam

Jak moc věříte v pravdivost videa níže? (video)

- Není deepfake
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- Je deepfake

Jak moc vám přijde deepfake morální?

- Nemorální
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- Morální

Malware

- Škodlivý software, který se může šířit z počítače na počítač a poškodit data.

Víte, jak se bránit proti malware? Máte nainstalovaný na svém počítači/notebooku nějaký antivirus?

- Ano, vím, jak se bránit proti virům - používám základní ochranu Windows Defender (Apple XProtect)
- Ano, vím, jak se bránit proti virům - používám antivirus třetí strany (Avast, Eset, Kaspersky...)
- Ne, nevím, jak se bránit proti virům, ale nějaký antivirus mám
- Ne, nevím, jak se bránit proti virům a o žádném antiviru nevím
- Nemám PC/NTB

Měl jste někdy v PC virus? Pokud ano, utrpěl jste někdy nějakou ztrátu?

- Ano, měl, ztrátu jsem neutrpěl, antivirus mi malware odstranil
- Ano, měl, ztrátu jsem utrpěl...
- Ne

Scam

Podvodná technika s účelem získání peněz nebo osobních údajů online

Setkali jste se někdy s online podvodem?

- Ano, ale vyhnul jsem se mu
- Ano, byl jsem obětí
- Ne

Jaké znáte formy podvodů?

- Phishing
- Smishing
- Vishing
- Podvodné e-shopy a inzeráty
- Ransomware
- Investice a kryptoměny
- Podvody láskou (romance scams)
- Podvodné charity