Digitální stopa fyzické osoby v prostředí internetu

Bc. Jaroslav Liška

Diplomová práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Jaroslav Liška**
Osobní číslo:	**A21468**
Studijní program:	**N1032A020003 Bezpečnostní technologie, systémy a management**
Specializace:	**Bezpečnostní management**
Forma studia:	**Kombinovaná**
Téma práce:	**Digitální stopa fyzické osoby v prostředí internetu**
Téma práce anglicky:	**Digital Footprint of a Natural Person in the Internet Environment**

Zásady pro vypracování

1. Proveďte literární rešerši tématu zadání práce.
2. Navrhněte legislativní rámec řešení tématu práce.
3. Zvolte způsob vyhodnocení chování uživatele v kybernetickém prostoru s ohledem na možnost zachycení digitální stopy.
4. Ověřte návrh svého řešení.
5. Vyhodnoťte výstupy práce a diskutujte její slabá místa.

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

Seznam doporučené literatury:

1. CYBERCRIME, JUDr. Jan Kolouch, Ph.D., Vydavatel: CZ.NIC, z. s. p. o., 1. vydaní, Praha 2016, kniha vyšla jako 14. publikace v Edici CZ.NIC. ISBN 978-80-88168-18-8.
2. CYBERSECURITY, doc. JUDr. Jan Kolouch, Ph.D., Bc. Pavel Bašta, Andrea Kropáčová, Bc. Martin Kunc1. vydání, Praha 2019, kniha vyšla jako 20. publikace v Edici CZ.NIC. ISBN 978-80-88168-34-8.
3. INTERNET JAKO OBJEKT PRÁVA: hledání rovnováhy autonomie a soukromí, MATEJKA, J.
4. Internet jako objekt práva: hledání rovnováhy autonomie a soukromí. 1. vydání, Praha 2013, kniha vyšla jako 6. publikace v Edici CZ.NIC. ISBN 978-80-904248-7-6.
5. ZODPOVEDNOSŤ NA INTERNETE podľa českého a slovenského práva, Martin Husovec, Vydavatel: 1. vydání, Praha 2014, kniha vyšla jako 8. publikace v Edici CZ.NIC. ISBN 978-80-904248-8-3.
6. Buď pánem svého prostoru, přeloženo z anglického originálu knihy Own your space. 1.vydání, 2010, vydáno nakladatelstvím 100 Page Press, Inc, CA. Online verze je dostupná na ownyourspace.net.
7. BÁJEČNÝ SVĚT ELEKTRONICKÉHO PODPISU, Jiří Peterka, vydavatel: CZ.NIC, z. s. p. o., Americká 23, 120 00 Praha 2, Edice CZ.NIC,www.nic.cz.
8. KRYPTOGRAFIE OKOLO NÁS, Karel Burda, vydavatel: CZ.NIC, z. s. p. o. Milešovská 5, 130 00 Praha 3, Edice CZ.NIC, www.nic.cz, 1. vydání, Praha 2019. Kniha vyšla jako 24. publikace v Edici CZ.NIC. ISBN 978-80-88168-52-2.

Vedoucí diplomové práce: **prof. Mgr. Roman Jašek, Ph.D., DBA**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **2. prosince 2022**
Termín odevzdání diplomové práce: **1. června 2023**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 8. prosince 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou 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;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové 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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 29. 5. 2023

Bc. Jaroslav Liška v.r.
podpis studenta

ABSTRAKT

Diplomová práce si klade za úkol přiblížit jednotlivci, co vše se ukrývá pod výrazem „digitální stopa“. Nastiňuje možnosti vlastní informační bezpečnosti a anonymity v prostředí internetu. Popisuje bezpečnostní rizika, která toto prostředí představuje a vhodné způsoby obrany. Cílem práce je na základě analýzy chování uživatele v kyber prostoru nalézt jeho digitální stopu, tuto dále popsat a vhodnou formou i s ohledem na právní rámec legislativy vyhodnotit.

Klíčová slova: digitální stopa, informační bezpečnost, anonymita, kyberprostor, bezpečnost.

ABSTRACT

The diploma thesis aims to make clear what the term "digital footprint" means. It outlines possibilities of information security and anonymity of an individual in the Internet environment. It describes security risks existing in this environment and appropriate means of defence. The aim of the thesis is to follow a user´s digital footprint based on the analyses of their behaviour in the cyberspace and, further, describe the footprint and evaluate it concerning the applicable legal framework.

Keywords: digital footprint, information security, anonymity, cyberspace, safety.

Mé poděkování patří prof. Mgr. Romanu Jaškovi, Ph.D., DBA za odborné vedení, trpělivost a ochotu, kterou mi v průběhu zpracování diplomové práce věnoval. Zároveň bych chtěl poděkovat svým kolegům za podporu, kterou mi poskytly při studiu.

Motto:

> „Přijměte odpovědnost za Váš život. Vězte, že jste to Vy, kdo Vás dostane tam, kam chcete, nikdo jiný to neudělá.“ – Les Brown

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

OBSAH

ÚVOD

Informace byly v průběhu vývoje civilizace vždy velmi cenným aktivem, které bylo potřeba chránit. Znalost informací v různých oblastech dávalo výhodu nad těmi, kteří informace neměli. Nemusí jít přímo o válečné konflikty, ale i o know-how a znalosti potřebné k technologickému náskoku a rozvoji. Informační bezpečnost vznikla současně s informacemi, které je nutné chránit. Před příchodem informačních technologií se informační bezpečnost zajišťovala především fyzickou bezpečností, různými druhy šifrovacích mechanismů (např. Caesarova šifra) a technickými prostředky (např. Enigma) pro jejich aplikaci.

Současná moderní doba, která přináší potřebu celosvětové komunikace, výměny informací a propojování uživatelů generuje a sdílí velké množství citlivých dat a informací, které je potřeba chránit.

Prostředí a zdánlivá anonymita internetu nabízí výrazně snazší možnosti informace zcizit, poškodit, nebo zneužít. Nápad počítačové kriminality (zneužití informačních technologií, zcizení identity, vydírání, útok na finanční toky a soukromí, ztrátu důvěrných informací apod.) je na vzestupu a jednotlivec oproti firemnímu prostředí nemá většinou možnost platit si osobu, nebo firmu na zajištění vlastní informační bezpečnosti. Právě jednotlivec se tak stává nejslabším článkem informační bezpečnosti.

V teoretické části je uvedeno, co je myšleno informační bezpečností a digitální stopou. Jednotlivé části popisují druhy informací, formy bezpečnosti, typy digitálních stop a fragmentů zanechaných uživatelem v prostředí internetu, na zařízeních, které používá a legislativní rámec této problematiky. Nedílnou součástí je oddíl o kybernetické bezpečnosti.

V praktické části bude využito poznatků z teoretické části k analýze chování uživatele v internetovém a kyber prostředí. Cílem je nalézt jeho digitální stopy, popsat rizikovost jeho chování a toto chování vyhodnotit. Tento oddíl zahrnuje praktickou ukázku analýzy datových nosičů, které byly podrobeny různým metodám omezení digitální stopy, kterou obsahují. Chování uživatele bylo vyhodnoceno na základě dotazníkového šetření se zaměřením na jeho informační bezpečnost. Závěr praktické části je pak věnován analýze rizik v prostředí kyber prostoru. Koncepce práce a její teoretická i praktická část je navržena tak, aby odrážela a naplnila všechny body jejího zadání.

I. TEORETICKÁ ČÁST

1 INFORMAČNÍ BEZPEČNOST

Informační bezpečnost (Information Security) je samostatným oborem, který se zabývá bezpečností uložených a zpracovávaných dat prostřednictvím informačních technologií. Počátky informační bezpečnosti sahají do první poloviny osmdesátých let dvacátého století, souvisejí s rozvojem výpočetní techniky a přesunem zpracování dat z klasické papírové podoby do elektronické.

1.1 Obecné pojmy

Pro pochopení navazujících částí je potřeba znát a uvést definice základních pojmů z této oblasti.

1.1.1 Informace

Informace (z latinského in–formatio, utváření, ztvárnění). V přenesené formě jde o utváření formy myšlenky a její zhmotnění do komunikovatelné podoby s cílem tuto myšlenku přenášet. V oblasti informačních technologií se informace považuje za kvantitativní vyjádření obsahu zprávy. Její měrnou jednotkou je bit, který reprezentuje stav 1, nebo 0. S pojmem informace dále souvisí:

- Data – vyjadřují formalizované řetězce znaků, které je potřeba nejdříve vhodnou formou zpracovat, než se stanou informací.
- Znalost – data uvedená do kontextu již existujících znalostí a interpretovaná do hierarchicky uspořádaných znalostních struktur v rámci informačního systému, nebo paměti příjemce.

1.1.2 Kyberprostor

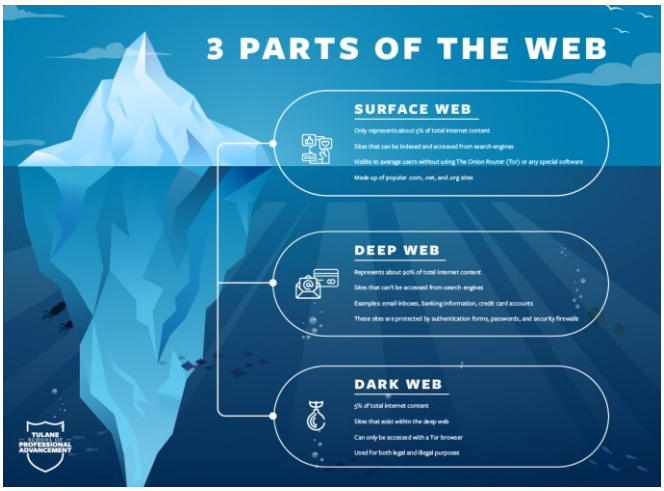
Výkladový slovník kybernetické bezpečnosti definuje kyberprostor (Cyberspace) jako:

- digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací. [1]

Po technické stránce lze kyberprostor popsat jako souhrn informačních a komunikačních technologií, vzájemně propojených prostřednictvím protokolu TCP/IP do globální celosvětové počítačové sítě.

Kyberprostor bývá velmi často prezentován formou pomyslného ledovce, rozděleného na tři části:

- **dostupný web** (surface web) – internetové stránky a obsah dostupný prostřednictvím internetového prohlížeče a přístupný pro indexovací roboty. Reprezentuje cca 5 % celkového obsahu internetu,
- **hluboký web** (deep web) – internetové stránky a obsah, který je chráněn prostřednictvím autentizace a autorizace (přihlašovací formuláře s heslem, hw klíče apod.). Např.: e-mailové schránky, bankovní účty, placené služby apod. Reprezentuje cca 90 % internetového obsahu,
- **temný web** (dark web) – obsah není indexován vyhledávači a je dostupný prostřednictvím prohlížeče Tor[1], který zajišťuje anonymizaci uživatele a jeho síťových aktivit před sledováním a analýzou aktivit při pohybu na internetu. Internetový obsah je dostupný pomocí speciálních „onion“ adres. Např.: http://3g2upl4pq6kufc4m.onion/ (vyhledávač DuckDuckGo). Dark web reprezentuje cca 5 % internetového obsahu.



Obrázek 1. Reprezentace kyberprostoru[2]

[1] Internetový prohlížeč postavený na jádře prohlížeče Mozilla Firefox. Dostupný z internetu: https://www.torproject.org/download/

[2] Zdroj dostupný z internetu: https://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web

1.1.3 Terminál

Za terminál považujme prostředek, za jehož užití vstoupíme do prostředí kyberprostoru. Terminálem může být jakékoliv zařízení s konektivitou do globální sítě internet, či jiné sítě. Zpravidla se jedná o osobní počítač, notebook, mobilní telefon, infotaiment automobilu, nositelnou techniku („chytré hodinky“), zdravotnické přístroje a další prostředky označované jako „Internet of Things“ (zratka IoT).

1.1.4 Informační systém

Informační systém je soubor lidí, technických prostředků a metod (programů), zabezpečujících sběr, přenos, zpracování, uchování dat, za účelem prezentace informací pro potřeby uživatelů činných v systémech řízení.[3][2]

1.1.5 Bezpečnost

Bezpečnost je definována jako stav, kdy jsou hrozby vůči referenčnímu objektu sníženy na nejnižší akceptovatelnou úroveň. S pojmem bezpečnost jsou zároveň spojeny výrazy:

- **hrozba** – škodlivý přírodní, nebo člověkem způsobený jev, který může mít škodlivý účinek vzhledem k životu a zdraví člověka, nebo majetku,
- **riziko** – pravděpodobnost, že nastane událost, kterou hrozba představuje,
- **zranitelnost** – pojem pro označení slabiny, nebo nedostatku referenčního objektu, která umožňuje uplatnění hrozby (např. chyba ve zdrojovém kódu aplikace).

1.1.6 Ochrana informací

Na bezpečnost a ochranu informací v prostředí kyberprostoru lze pohlížet těmito směry:

- **právní ochrana** – legislativní úpravy vzhledem ke vzniku, způsobu nakládání, uchování a celému životnímu cyklu informace (formou zákonů, norem a nařízení např.: známé GDPR[4]),

[3] Zdroj: MOLNÁR, Zdeněk. Podnikové informační systémy. Praha: ČVUT, 2009. 195 s. S. 13.
[4] General Data Protection Regulation, (obecné nařízení o ochraně osobních údajů, zkráceně ONOOÚ).

- **fyzická ochrana** – s ohledem na virtuálním prostředí kyberprostoru a nehmotné povaze informace je tato ochrana chápána nejenom jako fyzická (fyzické médium v trezoru), ale i softwarová ochrana (šifrování, zálohování).

Základní model bezpečnosti a ochrany informací je postaven na tzv. CIA (dále jen CIA) triádě, která definuje tyto základní atributy:

- **důvěrnost** (confidentiality) – zajištění přístupu k informacím a systémům pouze tomu, kdo je autorizován k nim přistupovat,
- **integrita** (integrity) – zajištění systému a konzistence dat proti neautorizovaným změnám,
- **dostupnost** (availability) – zachování dostupnosti informačního systému, služeb a přístupu k chráněným informacím a datům.

Legislativní rámec pro systémy řízení bezpečnosti informací (ISMS[5]) poskytuje norma ISO 27001. Ta je sice primárně určena pro firemní prostředí, IT systémy a zaměstnance, ale lze ji aplikovat i pro zajištění osobní bezpečnosti. Splněním těchto atributů se docílí výrazného posílení informační bezpečnosti.

1.1.7 Kybernetický útok

Za kybernetický útok můžeme považovat jakékoliv protiprávní jednání útočníka, nebo automatizovaného systému proti zájmům jiné osoby. Zpravidla se jedná o narušení některého, nebo všech atributů CIA triády. Útoky jsou vedeny těmito způsoby:

- útoky z vnějšku prostřednictvím globální počítačové sítě (využití zranitelností operačních systémů, internetového prohlížeče),
- vnitřní útok vedený někým, kdo má přístup do informačního systému, počítačové sítě, nebo ke koncovým zařízením (vynášení dat pomocí přidělených přístupových údajů, sdílená zařízení),
- aktivní útok s cílem pozměnit, nebo zničit informace, využití napadeného systému k zakrývání identity útočníka, nebo systémových prostředků pro těžbu kryptoměn a k útokům typu DoS a DDos[6],

[5] Information Security Management Systém.
[6] DoS - Denial of Service, odepření služby, DDos - Distributed Denial of Service, distribuované odepření služby.

- pasivní forma útoku je zacílena na sběr citlivých dat typu hesla, kontakty, případně na zajištění perzistence v napadeném systému pro pozdější využití.

1.2 Druhy hrozeb v kyberprostoru

Statistiky řešených incidentů CSIRT.cz[7] (otevřené i zavřené, omezena na posledních pět let a začátek roku 2023) uvádí, že nejčastějšími typy útoků jsou Phishing, SPAM a Malware.

Tabulka 1. Druhy incidentů CSIRT.cz[8]

	2018	2019	2020	2021	2022	2023	Celkem
Phishing	518	483	738	1277	1485	447	4948
Spam	144	128	216	163	220	65	936
Malware	135	85	109	141	224	40	734
Ostatní[9]	58	85	86	58	63	46	396
Probe	171	141	68	67	69	8	524
Trojan	0	0	0	0	0	0	0
DOS	7	16	16	11	0	0	50
Botnet	20	4	2	1	4	0	31
Virus	0	0	0	0	0	0	0
Portscan	16	3	29	7	2	0	57
Pharming	10	9	3	0	0	0	22
Celkem	1079	954	1267	1725	2067	606	7698

[7] CSIRT.cz (z anglického Computer Security Incident Response Team) „Skupina pro reakci na počítačové bezpečnostní události“), česká obdoba bezpečnostní ho uskupení CSIRT.
[8] Zdroj dostupný z internetu: https://csirt.cz/cs/o-nas/statistiky/
[9] Incidenty, které nelze jednoduše zařadit do jiných skupin. Jde převážně o typy incidentů s ojedinělým výskytem.

1.2.1 Kyber hrozby

Kybernetické hrozby nelze vztahovat pouze do prostředí Internetu, neboť mají přesah až do koncové techniky uživatelů. Prostředí Internetu je především vektor útoku, odkud hrozba směřuje a do kterého může za určitých okolností i směřovat (např.: DDoS útoky).

Následující přehled uvádí typy bezpečnostních hrozeb:

- **Phishing** – podvodná technika, která se pomocí sociálního inženýrství snaží vylákat citlivé údaje (hesla, čísla kreditních karet apod.), útok probíhá zpravidla formou elektronické komunikace, nebo SPAMu.
- **SPAM** – nevyžádaná elektronická pošta (analogie k „reklamním letákům“ ve schránkách). Typickým obsahem je nabídka levného zboží, suplementů, léků a pornografie.
- **Malware**[10] – obecné označení pro širší skupinu škodlivého softwaru, který bez vědomí uživatele provádí škodlivé činnosti. Malware se liší svým chováním a průnikem do systému (viry, červy, falešné antiviry, spyware, ad-ware, trojské koně, keyloggery, ransomware a minnery).
- **Ransomware** – složeno z anglického „Ransom“ (výkupné) a software, jedná se o tzv. „vyděračský software“, který po průniku do systému zašifruje obsah disku, nebo část uživatelských dat. Následně požaduje za dešifrování výkupné, většinou platbu v některé z kryptoměn (např.: WannaCry[11]).
- **DoS**, **DDoS** – odepření služeb, distribuované odepření služeb[12]. Typ útoku na internetové stránky a služby dostupné z internetu. Služba, nebo stránka je zahlcena velkým množstvím požadavků, které nedokáže zpracovat, a regulérní požadavky uživatele nejsou vyřízeny.
- **Pharming** – útok na citlivé údaje uživatelů (hesla, informace z platebních karet, přihlašovací údaje k internetovému bankovnictví pod.), který je založen napadení

[10] Složenina z anglického malicious (zlomyslný) software.
[11] Zdroj dostupný z internetu: https://www.avast.com/cs-cz/c-wannacry
[12] DoS – Denial of Services, DDoS - Distributed Denial of Service.

DNS[13] záznamů a přepis IP adresy na podvržené stránky se shodným designem. Uživatel je uveden v omyl a v domnění legitimního webu zadá dobrovolně své údaje.

Všechny tyto nežádoucí činnosti vedené vůči uživateli mají jako cíl především finanční profit. Jakoukoliv formou získat osobní informace, či jiné informační aktivum, které je následně možné převést na finanční prostředky. Druhotným účelem je cílené poškození uživatele, nebo získání pozornosti a slávy.

1.2.2 Sociální inženýrství

Neméně důležitou technikou útoků na uživatele a jeho identitu je tzv. „Sociální inženýrství“. Nejslabším článkem bezpečnostního řetězce je člověk. Výchozí předpoklad je, že je snazší získat osobní informace a přístupové údaje přímo od něj, než se pokusit obejít zabezpečení jeho výpočetní a komunikační techniky.

Jde o manipulační techniky působící na chamtivost, strach, závist, časový tlak a další lidské vlastnosti, které ovlivňují jeho psychiku. Promyšlenou technikou se uvede uživatel do stavu, kdy sám sdělí informace, které by za normálních okolností nesdělil.

Příkladem jsou například podvodné zprávy, e-maily, nebo volání z bank s údajným narušením bezpečnosti účtu a žádostí o sdělení přístupů, případně o výběr a převedení prostředků na bezpečný účet (např. vkladovým bankomatem s převodem na kryptoměnu na účet útočníka) apod.

Tímto uměním (sociální inženýrství) vynikal a popisuje ho ve své knize „Umění klamu“ [3] i známý a usvědčený hacker Kevin Mitnick, který více než znalostmi pronikal do počítačových systémů těmito technikami.

[13] DNS - Domain Name Systém, systém zajišťující překlad doménových názvů na cílové adresy za účelem jednoduchého procházení internetu (např. www.seznam.cz se překládá na IP adresu 77.75.77.222).

2 LEGISLATIVA

Legislativní úpravu kybernetické bezpečnosti v české republice lze rozdělit do dvou oblastí. První oblastí je „národní prostředí“, kterou zajišťuje především NÚKIB[14]. Druhá oblast, která by řešila jednotlivce, není zcela, nebo dostatečně upravena. Vztahuje se na ní však částečně současná legislativa pro reálný prostor.

2.1 Národní kybernetická bezpečnost

Na zajištění národní kybernetické a informační bezpečnosti (zahrnuje kritickou infrastrukturu a významné informační systémy a ochranu utajovaných informací) se podílí především tyto orgány, sdružení a organizace:

2.1.1 NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku veřejně regulované služby v rámci družicového systému Galileo. Vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).[15]

2.1.2 CERT

CERT[16] (Computer Emergency Response Team), skupina, která se věnuje bezpečnostním událostem, incidentům a zranitelnostem. Poskytuje služby a podporu těm, které se dostaly do problémů s narušením počítačové bezpečnosti.[17]

[14] Národní úřad pro kybernetickou a informační bezpečnost.
[15] Zdroj dostupný z internetu: https://www.nukib.cz/cs/o-nukib/
[16] Z anglického Computer Emergency Response Team – „Skupina pro řešení bezpečnostních problémů“.
[17] www stránky dostupné z http://www.cert.org

2.1.3 CSIRT ČR

Národní CSIRT ČR (Computer Security Incident Response Team)[18] je vykonávaný dle veřejnoprávní smlouvy uzavřené s Národním bezpečnostním úřadem. Ten se stal gestorem problematiky kybernetické bezpečnosti v říjnu 2011. Tým CSIRT.CZ[19] plní úlohu národního CERT České republiky podle Zákona o kybernetické bezpečnosti. Národní CERT tým zaštiťuje sdružení CZ.NIC[20].

2.1.4 CZ.NIC

Zájmové sdružení právnických CZ.NIC je národním správcem a provozovatelem registru doménových jmen „.cz“. Sdružení stojí rovněž za rozšiřování technologie DNSSEC[21], ale také za projekty „Turis“ (vysoce výkonný open source router), nebo službou „moje ID“ (bezpečné prokazování totožnosti a způsob přihlašování k službám soukromého sektoru i veřejné správy) v prostředí internetu. V neposlední řadě stojí i za edičním programem zaměřeným na vydávání odborných a naučných publikací spojených s internetem a technologiemi[22].

2.2 Legislativa ve vztahu k „národnímu prostředí“

Tabulka 2. Legislativa ve vztahu k „národnímu prostředí“

Zákon č. 181/2014 Sb.	Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
Vyhláška č. 82/2018 Sb.	Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

[18] CSIRT z anglického Computer Security Incident Response Team – „Skupina pro reakci na počítačové bezpečnostní události“).
[19] www stránky CSIRT ČR: https://csirt.cz/cs/o-nas/
[20] www stránky sdružení CD.NIC: https://www.nic.cz/
[21] Domain Name System Security Extensions, sada specifikací určená k rozšíření bezpečnosti systému DNS v IP sítích.
[22] Edice CZ.NIC, dostupná z internetu: https://knihy.nic.cz/

Zákon č. 148/1998 Sb.	Zákon o ochraně utajovaných skutečností a o změně některých zákonů.
Zákon č. 412/2005 Sb.	Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti.
Zákon č. 127/2005 Sb.	Zákon o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). Ve znění pozdějších předpisů.
Vyhláška č. 317/2014 Sb.	Vyhláška o významných informačních systémech a jejich určujících kritériích.
Nařízení vlády č. 432/2010 Sb.	Nařízení vlády o kritériích pro určení prvku kritické infrastruktury.
Vyhláška č. 437/2017 Sb.	Vyhláška o kritériích pro určení provozovatele základní služby.
Vyhláška č. 315/2021 Sb.	Vyhláška o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.
Vyhláška č. 316/2021 Sb.	Vyhláška o některých požadavcích pro zápis do katalogu cloud computingu.
Zákon č. 111/2009 Sb.	Zákon o základních registrech.

2.3 Legislativa ve vztahu k jednotlivci

Tabulka 3. Legislativa ve vztahu k jednotlivci

Zákon č. 40/2009 Sb.	Zákon trestní zákoník (v platném znění).
Zákon č. 141/1961 Sb.	Zákon o trestním řízení soudním (trestní řád).
Zákon č. 89/2012 Sb.	Zákon občanský zákoník (nový).
Nařízení (EU) 2016/679[23]	o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů. Obecné nařízení o ochraně údajů (GDPR).

2.3.1 Zákon 40/2009 Sb., ustanovení §230 - §232

Ve vztahu k trestným činům v oblasti počítačové kriminality jsou rozlišovány tyto oblasti a směry:

- Výpočetní technika využitá jako **nástroj** pro páchání trestné činnosti – ICT technika je využita páchání trestných činů v reálném světě. Jde tedy o činy, které jsou dostatečně popsány trestním zákoníkem. Například: Podvody (§ 203 TZ), vydírání (§ 175 TZ), poškození cizích práv (§ 181 TZ), provozování nepoctivých her a sázek (§ 213 TZ), ale i výroba a jiné nakládání s dětskou pornografií (§ 192 TZ).
- Druhým směrem jsou **ryze počítačové trestné činy**, které jsou uvedeny v těchto ustanoveních TZ:
    - § 230 – Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací.
    - § 231 – Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat.
    - § 232 – Neoprávněný zásah do počítačového systému nebo nosiče informací z nedbalosti.

Statistiky Policie České republiky (MV ČR) příliš nerozlišují trestné činy v oblasti kybernetické kriminality a jsou zúženy do ustanovení v níže uvedené tabulce. Není v nich

[23] Zdroj dostupný z internetu: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=LEGISSUM:310401_2

uvedeno druhotné rozlišení, zda trestné činy reálného světa byly provedeny prostřednictvím výpočetní techniky, či nikoliv. Například kyber šikana prostřednictvím sociálních sítí a následná sebevražda oběti šikany.

Tabulka 4. Statistika ve vztahu k ryze počítačovým trestným činům

Ust. tr. zák.	**Skutková podstata trestného činu**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**
§ 180	Neoprávněné nakládání s osobními údaji.	3	11	3	27	1	20
§ 182	Porušení tajemství dopravovaných zpráv.	28	41	35	49	22	32
§ 230 - § 232	Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací.	635	784	893	1092	1287	1866
§ 270 - § 271	Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi.	259	238	538	316	210	361

Zdroj (převzato): SMEJKAL, Vladimír. Kybernetická kriminalita.[4]

2.3.2 Data retention

Pojmem „data retention“ se označuje v České republice povinnost uchovávání provozních, lokalizačních údajů a dalších dat elektronických služeb. Tyto údaje zahrnují například číslo volaného, datum a čas hovoru nebo internetovou IP adresu uživatele v rozsahu minimálně 6 měsíců a maximálně 2 roky. Tato povinnost uchovávat provozní a lokalizační data svých zákazníků je upravena v § 97 odst. 3 zákona č. 127/2005 Sb. o elektronických komunikacích a vyžadují je zejména orgány činné v trestním řízení (OČTŘ) a bezpečnostní složky státu za účelem prevence, odhalování a vyšetřování trestných činů.

3 DIGITÁLNÍ STOPA V KYBERPROSTORU

Digitální stopa je informace zanechaná uživatelem v prostředí internetu nebo jako součást souborů.[5] Tyto stopy nejsou vždy soukromé a lze je za určitých podmínek odposlouchávat. Digitální stopy lze rozdělit na základě jejich vzniku:

- **vědomé** (aktivní), které vznikají přímou aktivitou a chováním uživatele v prostředí internetu. Může se jednat o příspěvky v internetových diskuzích, v profilech na sociálních sítích a povinně zveřejňované údaje správních orgánů.
- **nevědomé** (pasivní) stopy vznikají nezávisle na vědomí uživatele interakcí v online prostředí. Zpravidla jde o informace uchovávané poskytovatelem telekomunikačních služeb (IP adresy, logy serverů apod.) a sociálních sítí, nebo o geolokační údaje, soubory cookie a analytické funkce využitelné pro statistiky návštěvnosti a cílenou reklamu.

Základním uvědoměním a premisou uživatele by mělo být, že jakýkoliv obsah (především nevhodný, nebo citlivý) zveřejněný na internetu v tomto prostředí zůstává

navždy.

Ačkoliv nám Obecné nařízení o ochraně osobních údajů (GDPR) nabízí v článku 17. právo na výmaz („právo být zapomenut“), není zaručeno, že informace se již nekontrolovaně, nezávisle na správci těchto údajů nešíří dál (myšleno především v kontextu sociálních sítí). Nevěnování pozornosti této myšlence, může do budoucna způsobit uživateli závažnou reputační újmu nejen v osobním, ale i pracovním životě.

3.1 Digitální stopa

Digitální stopa je informace ve vztahu ke konkrétnímu referenčnímu objektu, která je svou formou nehmotné aktivum. Zároveň platí, že informace musí být v důsledku zhmotněna a uložena na fyzické médium. Ačkoliv jsou Internet, popřípadě cloudové služby považovány za virtuální prostředí, je nutné si uvědomit, že i za nimi stojí množství hardware (servery, aktivní prvky, vzájemně propojené sítě) a datových úložišť reprezentovaných fyzickými médii pro uchování dat.

Digitální stopa o chování uživatele tedy není zachovávána pouze v prostředí internetu. Zásadní a největší kolekce fragmentů chování uživatele ve formě digitálních stop je uložena přímo v technice, kterou pro přístup do online prostředí uživatel využívá. Zejména se jedná

o výpočetní techniku a mobilní techniku (počítače, notebooky a chytré telefony, smart a IoT zařízení). Příkladem mohou být především prohlížeče internetových stránek, jejich historie a další soubory (cache, cookie), které si prohlížeč uchovává za účelem lepší uživatelské přívětivosti a rychlosti načítání již zobrazených www stránek.

3.1.1 Zneužití digitální stopy

S ohledem na negativní využití digitálních stop je důležité zmínit především jevy související s útokem na osobní údaje, informace, identitu jednotlivce a útok proti jeho osobě a právům především těmi to způsoby:

- krádež osobních informací (e-mailová adresa, rodné číslo, bankovní údaje a údaje z platebních karet),
- zcizení celé digitální (internetové) identity (např.: herní účty), nebo její duplikace (falešné tzv. „fake“ účty známých osobností),
- kyberšikana (cyberlulling) – zneužití informačních technologií a elektronických médií k poškození oběti agresivní formou (např. mezi studenty, vůči učiteli apod.),
- kyberstalking – přenesení nebezpečného, opakovaného, stupňovaného pronásledování a obtěžování oběti do prostředí online světa prostřednictvím informačních technologií,
- reputační hrozby, které by se dali vyjádřit rčením „historie tě dostihne“. Důležitým faktem je, že tyto zveřejněné informace mohou osobní, nebo pracovní kariéru ovlivnit v neomezeném časovém horizontu. Příkladem může být nevhodná fotografie z večírku, podobně jako u prince Harryho z královské rodiny v nacistickém kostýmu roku 2005[24].

3.1.2 Využití digitální stopy

Pozitivní využití digitální stopy jednotlivce v prostředí internetu si lze představit jako užitnou hodnotu pro další uživatele, nebo systémy v tomto prostředí:

- internetové vyhledávače a indexační roboti – snaží se poskytovat co nejrelevantnější informace na základě uživatelských dotazů,

[24] Zdroj dostupný z internetu: https://www.timesofisrael.com/in-memoir-prince-harry-said-to-claim-infamous-nazi-costume-was-williams-idea/

- zcela jistě se každý personalista, který bude posuzovat životopis uchazeče o pracovní pozici, se pokusí informace v něm obsažené z části dohledat „na internetu“, případně porovnat s profesní sociální sítí typu LinkedIn[25].
- pasivní sledování – digitální stopa chování uživatelů (např. vyhledávání) na internetu je z velké části využívána také pro analýzu a sledování návštěvnosti www stránek, popřípadě pro kolekci dat informací o uživatelích za účelem dalšího využití. V tomto směru jsou nejznámější služby konglomerátu Alphabet Inc. (Google). Služba Google Analytics[26] a Google Adwords[27].

Digitální stopa má stejně jako fyzické kriminalistické stopy nezastupitelnou hodnotu nejen při rozkrývání trestné činnosti, ale i v průběhu jejího dokazování. Nemusí se přitom jednat striktně o stopy ve vztahu k digitální kriminalitě, ale i o stopy uchované v digitální technice, které prokazují páchání trestné činnosti mimo prostor internetu.

Zpravidla se jedná o telekomunikační techniku, která je zajišťována orgány činnými v trestním řízení v rámci přípravného řízení. Konkrétně jde o předběžná opatření a zajištění osob a věcí důležitých pro trestní řízení[28] (§67 – 88o). Přesněji ustanovení §78 a §79 (zajištění věcí důležitých pro trestní řízení) a §82 - §85c (Domovní a osobní prohlídka, prohlídka jiných prostor a pozemků, vstup do obydlí, jiných prostor a pozemků).

3.1.3 Omezení digitální stopy

Na základě výše uvedeného se nabízí otázka, jakým způsobem lze vlastní digitální stopu, ať už v prostředí internetu, nebo na technice, kterou jednotlivec využívá omezit, nebo zcela zabránit jejímu vzniku.

Úvahou z předchozího textu lze vyvodit, že samotnému vzniku digitální stopy nelze zcela zabránit, a to už z principu, že tato stopa je v prostředí kyberprostoru částečně vytvářena nezávisle na vědomí, nebo interakci uživatele. Největší možnost ovlivnit, nebo omezit svou

[25] www stránka: https://www.linkedin.com/
[26] www stránka: https://analytics.google.com/analytics/web/ (služba shromažďující informace o uživatelích navštěvujících www stránky pro vývojáře).
[27] www stránka: https://ads.google.com (online reklamní služba pro inzerenty, kteří chtějí oslovit reklamou potenciální zákazníky)
[28] Zákon č. 141/1996 Sb. – Trestní řád.

digitální stopu má tedy uživatel právě svým chováním v kyberprostoru a použitím technických prostředků k jejich omezení. Způsoby ovlivnění digitální stopy:

- **Netiketa** – všeobecný souhrn pravidel slušného chování na internetu. Netiketa byla definována S. Hambridge ze společnosti Intel, následně přijata jako standard RFC 1855 [6]. Právě způsob vyjadřování v prostředí internetu, diskuzích, sociálních sítích a médiích utváří digitální identitu jednotlivce. Rychlé sdílení nevhodných informací může mít nedozírné důsledky na reputaci.
- **Rozsah a důvěrnost informací** – informace se zveřejněním v kyberprostoru stává svobodnou a nelze zcela jistě zabránit dalšímu šíření. Je proto velice důležité zvážit její rozsah, citlivost a místo, kde je zveřejněna.
- **Technické prostředky** – softwarové a hardwarové prostředky k ochraně informací (šifrování, autentizace, autorizace) a korekci digitální stopy (anonymní přístup např.: VPN[29]).
- **Legislativa** – právní ochrana, nastavuje pravidla pro nakládání s informacemi a zveřejněnými údaji po celou dobu jejich životního cyklu (od vzniku po jejich likvidaci).

3.1.4 Odstranění digitální stopy

Digitální stopa může vzniknout již před narozením jednotlivce (záznamy elektronické zdravotní dokumentace o průběhu těhotenství), ale nemusí zaniknout s jeho smrtí (e-mailové schránky, účty a příspěvky na sociálních sítích, záznamy v digitálních matričních knihách).

Odstranění digitální stopy jednotlivce z kyberprostoru, či prostředí internetu je nemožné. Proto je důležité, aby jednotlivec průběžně vědomě tuto stopu ovlivňoval a omezoval. Tato myšlenka se zároveň dotýká tématu, jak má být nakládáno s jeho digitální identitou a stopou po jeho smrti – tzv. „digitální smrt a dědictví“).

[29] Virtuální privátní síť (virtual private network). Prostředek k propojení několika počítačových systémů prostřednictvím nedůvěryhodné počítačové sítě.

3.2 Uchování digitální stopy

Z pohledu uchování digitální stopy je zřetelná podoba dvou směrů, kde se informace o uživatelské interakci s komunikačními systémy a jeho osobní údaje nacházejí.

- prostředí internetu (kyberprostoru) – silně decentralizované prostředí s velkým množstvím nezávislých systémů pracujících izolovaně, nebo propojených do celosvětové sítě.
- fyzická média – zhmotněná myšlenka do formy informace na datové médium.

Na základě těchto směrů se pak liší způsob, jakým lze tyto informace je lze získat. Důležitým faktem, který je nutné zopakovat je, že tato data se vždy nachází na některém z druhů fyzických datových nosičů.

3.2.1 V prostředí internetu

K ověření existence vlastní digitální stopy v prostředí internetu je jako nejsnazší cesta zadání vlastního jména a příjmení, nebo přezdívky do internetového vyhledávače (např.: „František Novák“). Výsledky lze dále upřesňovat na základě dalších znalostí údajů, které se vztahují k hledané identitě (např. město: Zlín), anebo z již nalezených fragmentů digitální stopy. Postupným skládáním těchto fragmentů se utváří přehled o komplexní digitální identitě jednotlivce a jeho vazbách na další entity. Celá problematika vyhledávání informací zasahuje do oborů konkurenčního zpravodajství a vyhledávání z otevřených zdrojů[30]. Následující výčet uvádí, kde mohou být uchovávány digitální stopy v prostředí internetu.

3.2.1.1 Vyhledávače

Internetové vyhledávače pracují na principu indexačního robota. Automatizovaný systém systematicky prochází internetový obsah za účelem vytváření a aktualizace globálního vyhledávacího katalogu. Na základě různých atributů a parametrů procházení stránek s obsahem je jim přiřazena váha, která udává kvalitu obsahu a ve výsledku se projeví relevancí vrácených výsledků. Tyto vyhledávací katalogy dosahují kapacit v řádech PB

[30] Competitive Intelligence a Open Source Intelligence (OSINT). K vyhledávání se používá například open-source software Maltego, dostupný z internetu: https://www.maltego.com/

(petabyte)[31]. Vyhledávací systém se pak uživateli snaží nabízet co nejrelevantnější výsledky na zadaný dotaz.

Negativním důsledkem indexace je poměrně často stav, kdy jsou zaindexována a následně i ve výsledcích zobrazena citlivá data nebo informace, které nemají být veřejné (chyby vývojářů, špatně nastavené servery apod.). Tohoto stavu využívá technika „Google hacking“[32], která vhodně upraveným dotazem do vyhledávače hledá známé zranitelnosti webových serverů, výpisy nastavení, souborů, zálohy databází včetně uložených přístupových údajů a jiná citlivá data.

3.2.1.2 Provozní a telekomunikační údaje

Povinnost uchovávat po dobu 6 měsíců provozní a lokalizační údaje pro fyzické a právnické osoby zajišťující veřejnou komunikační síť, nebo veřejně dostupnou službu elektronických komunikací je zakotvena v zákoně č. 127/2005 Sb. Zákon o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). Tato stopa vzniká a je uchovávána nezávisle na vůli uživatele. Tyto údaje mohou být za splnění zákonných podmínek zpřístupněny orgánům činným v trestním řízení. Provozní údaje však bývají uchovány u provozovatele mnohem delší dobu z důvodu reklamací, nebo prosté lenosti. Zcizení takových dat znamená zásadní prolomení ochrany osobních údajů.

3.2.1.3 Servery a databáze

Veškerý obsah generovaný a uložený v prostředí internetu je uložen serverech a v databázích provozovatelů hostingových služeb, firemních serverech a koncových zařízeních jednotlivců. Každý z těchto systémů je složen z hardware a software (operační, serverový, databázový systém) s konektivitou do online světa. Softwarové produkty velmi často obsahují chyby a zranitelnosti, které jsou využitelné k excitaci uloženého obsahu.

Zároveň tyto systémy obsahují a uchovávají své vlastní provozní údaje a dodatečné informace k uživatelskému obsahu (IP adresy, data a časy vzniku a změny

[31] Petabyte (petabajt) 10^{15} bajtů.
[32] Katalog vyhledávacích dotazů: https://www.exploit-db.com/google-hacking-database

obsahu – metadata[33]), ty následně mohou být využity pro forenzní analýzu vektoru útoku na systém, nebo zajištění digitální stopy vedoucí k identitě jednotlivce.

3.2.1.4 Internetové stránky, fóra, blogy

Jsou dalšími ze zdrojů cenných informací ve vztahu k digitální stopě. Obsah a myšlenky uživatele, které prezentuje v prostředí sociálních služeb a sítí, dotvářejí charakter jeho identity. Tyto informace podobně jako informace ze sociálních sítí pak mohou být základem pro cílený útok na identitu uživatele některou z forem sociálního inženýrství. Osobní www stránky, nebo obsahové stránky založené na CMS systémech[34] jsou vhledem k celosvětové rozšířenosti velmi oblíbeným terčem útoku na jejich známé zranitelnosti. Samotný fakt, že www stránka je smazána z prostředí internetu neznamená, že není již dohledatelná. Služba Archive.org je digitální knihovnou, která uchovává částečný přístup k některým digitálním materiálům, médiím a internetovému obsahu (např.: náhled stránky www. seznam.cz z roku 2004) [35].

3.2.1.5 Sociální sítě

Mezi nejznámější sociální, nebo oborové sítě patří například Facebook, Instagram, Twitter, LinkedIn a Vkontakte[36]. Jsou nejsilnější zdroj osobních informací a sociálních vazeb, které jednotlivec i jeho přátelé o sobě a navzájem zveřejňují zcela dobrovolně. Ani takto velkým společnostem se však nevyhýbají úniky dat. Nemusí jít přímo o útok na sítě jako takové, ale například podobně jako to bylo u Facebooku, o carving uživatelských dat prostřednictvím API, které nebylo ošetřeno vůči strojovému zpracování. Následně byla data o více než 533 milionech uživatelů zveřejněna na internetu[37].

---

[33] Metadata, data o jiných datech.
[34] CMS (z anglického content management system) systémy na správu internetového obsahu (blogy, diskuze), označované také výrazem „redakční systémy“ (např.: Wordpress, Joomla).
[35] Zdroj dostupný z internetu: https://web.archive.org/web/20040101143128/http://seznam.cz/ (Archivní náhled stránky www.seznam.cz z 1. 1. 2004).
[36] Obdoba amerického Facebooku, oblíbená především v Rusku, Bělorusku, Moldavsku a Kazachstánu.
[37] Zdroj, dostupný z internetu: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4

3.2.1.6 Cloudové služby

Jsou služby založené na principu využití počítačových technologií, které jsou přístupné prostřednictvím internetu. Založeny jsou na některém z distribučních modelů (SaaS, PaaS, IaaS)[38] v závislosti na tom, co je nabízeno (HW, SW, jejich kombinace). Mezi nejznámější cloudové služby, které využíváme, aniž bychom si to mnohdy uvědomovali, patří služby tří nejvýznamnějších technologických společností na světě, na které jsou navázány jejich služby a ekosystém.

- **Apple** – Apple ID, online účet ke službám iCloud, iTunes, AppStore, Apple music a dalším.
- **Google** – online účet ke službám Gmail, Google play, Disk Google, Adwords, Adsense, Obrázky Google a další.
- **Microsoft** – online učet k službám Outlook.com, OneDrive, Bing, Microsoft Store a zařízením s operačním systémem Microsoft Windows.

Únikem přihlašovacích údajů, nebo jiným neoprávněným přístupem k uloženým datům v těchto službách se dostává do rukou útočníkovi doslova téměř celý digitální život jednotlivce, kterému patří.

Disk Goole, OneDrive, iCloud, Mega[39], nebo česká služba Uloz.to[40], patří do kategorie cloudových služeb pro sdílení dat prostřednictvím internetu. Ukázkou, jak nebezpečně dokážou uživatelé nakládat je svými osobními je, že touto službou s veřejným vyhledáváním přenášejí i tak citlivé soubory, jako jsou certifikáty se soukromým klíčem[41].

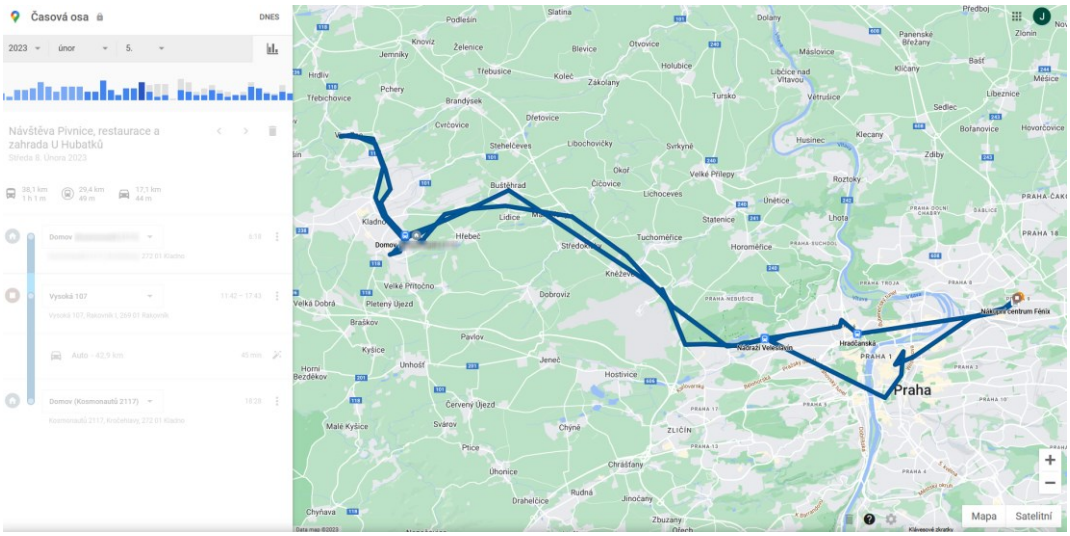
Příkladem, jaká data o chování a způsobu využívání služeb uchovává například za účelem poskytování přizpůsobených služeb, jako je rychlejší vyhledávání a užitečnější doporučení aplikací a obsahu jsou služby Google moje aktivita[42], nebo přehled soukromí od Microsoftu[43].

---

[38] Anglické zkratky: Software as a Service, Platform as a Service, Infrastructure as a Service.
[39] Zdroj: https://mega.io/desktop
[40] Zdroj: https://uloz.to/
[41] Dotaz dostupný z internetu: https://gozofinder.com/cse/ulozto/cz?query=PFX , zobrazí soubory PFX, které jsou soukromou částí certifikátu.
[42] www stránka Google moje aktivita, dostupná z internetu: https://myactivity.google.com/
[43] www stránka Osobní údaje pod kontrolou, dostupná z internetu: https://account.microsoft.com/account/privacy?view=usage

3.2.1.7 Geolokační služby

Geolokační služby povolené na zařízeních, která používáme, doplňují digitální stopu, nebo vytvořené soubory o atribut polohy uživatele, kde se pohyboval v době jejího vzniku. Míra její přesnosti je daná způsobem, jakým zdrojem je vytvářena od nejpřesnější, dané GPS souřadnicemi, méně přesnou danou například pokrytím mobilních stanic telekomunikačních operátorů[44], až po polohu danou poskytovatelem internetového připojení. Příkladem může být ukládání metadat (např.: místo pořízení fotografie) do EXIF údajů obrazových souborů, nebo časové osy od společnosti Google. Ta zobrazuje místa, která byla navštívena na základě historie polohy. Tato stopa je částečně ovlivnitelná prostřednictvím aplikací typu „Fake GPS location“, nebo prostřednictvím VPN připojení.



Obrázek 2. Google – časová osa[45]

3.2.1.8 IoT zařízení

IoT (Internet of Things) – internet věcí je koncept a myšlenka ekosystému propojených jednoduchých elektronických zařízení a věcí prostřednictvím internetové konektivity bez asistence člověka. Digitální transformací hloupých zařízení do „smart“ světa lze docílit zjednodušení automatizaci procesů běžného života. Příkladem může být lednice, která si pohlídá trvanlivost potravin, nebo integrovaný bezpečnostní systém, kde je základní funkce rozšířena například o automatizaci vytápění, hlídání zaplavení sklepu apod. Jedním

[44] BTS - Base Transmitting Station
[45] Služba Google – časová osa, zdroj dostupný z internetu: https://www.google.com/maps/timeline

z konceptů sjednocení více samostatných systémů prostřednictvím jednoho místa je chytrá domácnost. Cílem je ovládání všech zařízení domácnosti prostřednictvím jediné aplikace. Data zařízení jsou uložena částečně lokálně, ale především v cloudu.

3.2.1.9 E-mailové účty

E-mailové služby, ačkoliv se to nemusí na první pohled zdát, jsou také formou cloudové služby. Ta je velmi úzce spojena nejenom s osobní identitou v kyberprostoru, ale také v reálném životě. Ztráta kontroly nad e-mailovým účtem téměř jistě může znamenat částečnou, nebo úplnou ztrátu digitální identity.

V prostředí internetu se na e-mailový účet váže většina služeb, které uživatel používá. Ty zpravidla využívají e-mail nejenom jako uživatelské jméno pro přihlášení do služby, ale především jako kontaktní místo, kam zaslat, nebo vygenerovat nové přístupové údaje v případě jejich ztráty. Způsob útoku na e-mailový účet pak může být veden využitím znalosti přístupových údajů[46], následnou změnou hesla, kontaktních údajů, alternativních způsobů obnovy a přihlášení do účtu.

Z tohoto důvodu je velmi důležité používat služby, které umožňují více faktorové ověřování k přihlašování do služby. Zejména u e-mailového účtu platí důležité pravidlo použití unikátního silného hesla.

3.2.2 Fyzické uložení digitální stopy

V úvodu kapitoly „Digitální stopa“ byla předložena myšlenka, že ať už je prostředí internetu jakkoliv virtuální, z principu své povahy je informace v konečném důsledku myšlenka zhmotněná na některý z druhů fyzických nosičů ve formě datových souborů, nebo obsazeného paměťového prostoru. Tato informace je uložena (aktivně, pasivně) a interpretována programovým vybavením (operační systém, prohlížeč www stránek, firmware) zařízení, které uživatel využívá. Následující přehled předkládá místa, kde mohou být stopy uloženy.

[46] Např. využitím databází uniklých přístupových údajů služeb, nebo některou z technik jako jsou session hijacking (odcizení cookie s přihlášením), MiM (Men in the Middle).

3.2.2.1 Fyzická média

Pevné disky (HDD, SSD, NVMe, SAS, SCSI) a přenositelná média (USB flash disky, paměťové karty SD, micro SDHC, XD Picture, apod.) jsou základní fyzická úložiště, na která se ukládají informace. Mohou být v organizované struktuře v některém ze souborových systémů, zpravidla ve formě datových souborů, ale také jako surová data (RAW) s fyzickou adresací paměti (např.: paměťové čipy IoT zařízení apod.).

3.2.2.2 Souborové systémy

Souborový systém v oblasti výpočetní techniky je způsob, jakým jsou informace organizovány na fyzickém nosiči dat. Organizace spočívá v hierarchickém uložení jednotlivých souborů v adresářové struktuře. Nejde při tom jenom o uchování informace o fyzickém uložení, ale v závislosti na daném souborovém systému i doplňkové informace ve vztahu k těmto datům. Moderní souborové systémy udržují informace o vlastnictví a přístupových právech k datům. Díky možnostem souborových systémů je možné rozdělit jedno fyzické médium na více samostatných logických oddílů s různým typem souborového systému. Mezi artefakty digitální stopy ve vztahu k fyzickým médiím patří:

- Časové značky (vznik, editace a poslední přístup k souboru),
- Metadata – doplňková „data o datech“ (autor, autor poslední změny, společnost, komentáře, celková doba úpravy, apod.).
- Smazané soubory – běžné odstranění souboru a dat nedává jistotu trvalého zničení stopy. V souborovém systému se pouze odstraňuje informace o existenci souboru. Pokud nedojde k přepsání původního paměťového prostoru, kde byla data fyzicky uložena, stále existuje možnost jejich částečné, nebo úplné obnovy.
- Slack – souborový systém rozděluje prostor na jednotlivé sektory, které jsou obsazovány soubory. Pokud nedojde k úplnému obsazení sektoru nově uloženým souborem, zbývající neobsazená část sektoru obsahuje volné místo, nebo části souboru, který zde byl uložen v minulosti.

3.2.2.3 Výpočetní technika

Ve smyslu počítačů, notebooků, záznamníků, kompaktních fotoaparátů, kamerových systémů, tiskáren a gatgetů[47] apod. obsahuje různorodé množství interních a externích paměťových nosičů. Ze všech těchto médií v závislosti na jejich zabezpečení lze forenzními nástroji získat jak systémové informace, tak uživatelské soubory a data, která jsou na nich vytvářena a zpracovávána. Proto by měl být kladen velký důraz na jejich softwarové i hardwarové zabezpečení.

3.2.2.4 Mobilní telefony

Mobilní a chytré telefony se staly každodenní součástí našeho pracovního i soukromého života. Právě tato zařízení považuji za největší zdroj osobních informací co do komplexity. Mnoho uživatelů je využívá stále častěji jako primární zařízení pro přístup k internetu a to v rozsahu celého dne, bez ohledu na účel (soukromí, zábava a práce). Svou povahou mobility je tak ještě důležitější tyto zařízení zabezpečit proti úniku informací v důsledku ztráty, nebo krádeže.

3.2.2.5 Operační systémy

Pro oživení jednoduchých malých hardwarových systémů se vyžívá firmware[48], u větších komplexnějších systémů a zařízení se jako střední vrstva mezi fyzickým HW (počítače, notebooky, chytré telefony) a dalším programovým vybavením používají operační systémy[49]. Pro forenzní analýzu jsou operační systémy cenných zdrojem dat. Operační systémy zaznamenávají provozní údaje a nastavení. Ty jsou uchovávány za účelem jejich provozu, nebo pro diagnostiku problémů. Některé z uchovávaných informací jsou:

- Soubory nastavení (registry Windows, ini soubory, plist soubory u zařízení Apple), seznamy nainstalovaných aplikací.
- Dočasné soubory generované operačním systémem, nebo aplikacemi používanými uživatelem.

---

[47] Jednoúčelové zařízení, většinou technického rázu se specifickou a často populární funkcí.

[48] programové vybavení, které slouží k ovládání jednoduchých a embedded zařízení (např. kalkulačka, záznamník, některé počítačové komponenty).

[49] Nejznámější operační systémy: Microsoft Windows, Apple macOS, iOS, Android, Debian (jedna z mnoha distribucí otevřeného operačního systému založeného na jádře Linuxu).

- Logy událostí (systémové chyby, časy přihlášení / odhlášení uživatele, připojená zařízení k systému, auditování přístupu k souborovému systému).
- Nastavení sítě (seznam, nastavení zabezpečení wi-fi, připojené síťové jednotky).
- Hash[50] hodnoty uložených hesel a jiných přístupových údajů.

3.2.2.6 Programové vybavení

Programové vybavení (programy, mobilní aplikace a kancelářské balíky) je poslední softwarová vrstva rozšiřující základní vybavení operačního systému. Stejně jako vývojáři operačních systémů tak i autoři aplikací uchovávají konfigurační a některé provozní údaje v souborech a registrech systému, na kterých jsou provozovány. Nejvíce informací ve vztahu k digitální identitě jednotlivce vytváří a ukládají:

- **prohlížeče internetových stránek**[51] – udržují informace o historii navštívených stránek, záložky oblíbených stránek, automatické doplňování formulářů a uložené autentizační údaje. Dále ukládají velké množství dočasných souborů (cache) procházených www stránek za účelem rychlejšího načítání při jejich dalším zobrazení.
- **e-mailový klienti** – jeden ze způsobů prohlížení obsahu e-mailové schránky. E-mailový klient je nakonfigurován a v závislosti na použitém komunikačním protokolu[52] stahuje celou, nebo jen část obsahu schránky na lokální zařízení do datových souborů. Dalším způsobem je přímé procházení schránky prostřednictvím prohlížeče www stránek.

3.2.2.7 Datové soubory

V části „souborové systémy“ byla nastíněna forma ukládání informací do souborů a jejich doplňující informace – **metadata**. Aplikace, které uživatel používá a vytváří v nich obsah, ho ukládají na datové médium ve speciální struktuře (formátu). K odlišení tohoto formátu se používá přípona (extension), dle které operační systém volí výchozí aplikaci pro otevření souboru. Mezi nejčastější soubory, které uživatel vytváří, jsou soubory:

---

[50] Hash – výsledek jednosměrné kryptografické funkce, využití k ověření integrity souborů a zabezpečení hesel.
[51] Např.: Google Chrome, Microsoft Bing, Microsoft Internet Explorer, Mozilla Firefox, Opera.
[52] Např.: POP3, nebo IMAP.

- kancelářských balíků typu Microsoft Office, OpenOffice (texty, tabulky, prezentace, databáze, publikace a poznámky) apod.
- PDF (portable document format) – formát souboru určený k přenosu a prezentaci nezávisle na hardware a software prostředí, na kterém se prezentuje. PDF je výměnný formát, který má možnost nést v rámci obsahu i digitální podpis autora.
- Audiovizuální obsah ve formě hudby a videí (např.: Mp3, Mp4, AVI, MPEG-4).
- Grafické soubory a formáty obrázků (BMP, PCX, GIF, JPG).

Metadata uchovávají informace o autorovi, čas strávený úpravami, verzi aplikace v které byly vytvořeny a způsob kódování dat.

Zejména u některých grafických formátů (JPG, TIFF, RIFF, PNG a JPG) je uložen speciální formát metadat – Exif[53] data. Exif data jsou vkládány do souborů při jejich vytvoření, nebo editaci. Ukládají se do nich informace o použitém HW a SW, ve kterém byly zpracovány. Ukládané informace jsou poměrně rozsáhlé a mohou obsahovat forenzně relevantní údaje:

- Výrobce a model zařízení, verze software, rozlišení.
- Čas a program expozice, barevný prostor, clona a ohnisková vzdálenost.
- V případě, že to zařízení podporuje, tak především i geolokační údaje.

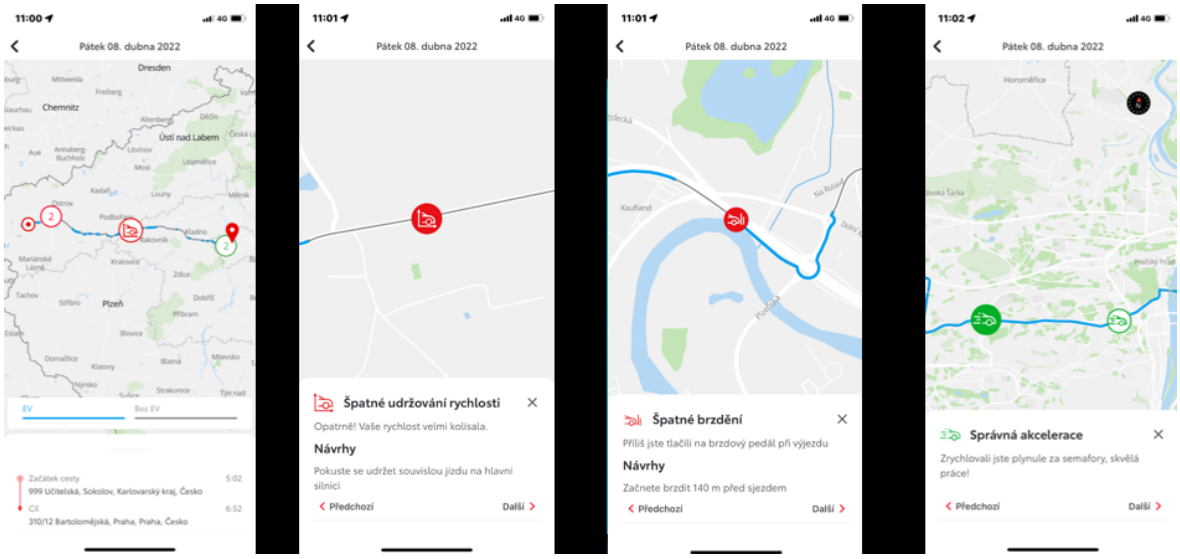
3.2.2.8 Nositelná technika

Nositelná technika je kategorie produktů, které jsou svým vzhledem a charakteristikou uzpůsobené k připevnění, nebo nošení na těle uživatele. Tato technika může obsahovat senzory, které mají za úkol zpracovávat faktory lidského života (srdeční tep, počet kroků, saturace nasycení krve kyslíkem, akcelerometr, gyroskop apod.). Mimo tuto oblast z velké části slouží především k zábavě. Nejznámějším zástupcem jsou „chytré hodinky“, nebo fitness náramky, ale může se jednat i o outdoorové a špionážní kamery, brýle pro rozšířenou realitu (např. Google Glass, PlayStation VR V2), nebo zdravotnické pomůcky, jako jsou inzulínové pumpy. Z některých z uvedených zařízení lze získat poměrně široký rozsah informací o fyzickém chování a stavu jejich nositele. Důkazem využití těchto dat je například i usvědčení pachatele z trestného činu vraždy[54].

[53] Exif – z anglického Exchangeable image file format.
[54] Zdroj dostupný z internetu: https://9to5mac.com/2021/06/18/smartphone-and-smartwatch-data-murder/

3.2.2.9 Vozidla

Řídící jednotky a infotaimenty[55] moderních motorových vozidel v sobě uchovávají velké množství provozních, diagnostických a geolokačních dat. Ve vztahu k vozidlu jde o „operační systém, který prezentuje diagnostické informace, ovládá multimédia a zajišťuje propojení s jinými zařízeními a internetem“.



Obrázek 3. Aplikace „MY T“[56]

3.2.2.10 Ostatní zařízení

Uvedený výčet médií a zařízení není zcela kompletní, nebo jsou v něm zahrnuty jen částečně svým principem (např. minipočítače, platformy a zařízení založená Raspberry Pi[57], drony a jiné gadgety). Obecně lze vyslovit tvrzení, že jakékoliv zařízení s konektivitou do prostředí internetu s vlastním firmware, nebo operačním systémem obsahuje paměťový prostor se systémovými a uživatelskými daty. Tento prostor lze forenzními nástroji, nebo v laboratorních podmínkách extrahovat.

[55] (z anglického information + entertaiment) spojení slov informace a zábava.
[56] Náhled z aplikace „My T“ o způsobu a stylu jízdy řidiče z infotaimentu vozidla Toyota. Aplikace dostupná z internetu: https://www.toyota.cz/majitele/myt-online-sluzby/myt
[57] Rapsberry Pi Foundation, charitativní společnost založená pro podporu výuku informačních věd a výrobce jednodeskových počítačů. Dostupné z internetu: https://www.raspberrypi.org/

4 KYBERNETICKÁ BEZPEČNOST

Kybernetická bezpečnost nejenom čistě v kontextu digitální je komplexní záležitost, skládá se z více jednotlivých částí, utvářející celek, který zvyšuje odolnost celého systému (referenčního objektu) vůči zranitelnostem. Systém kybernetické bezpečnosti je postaven na zajištění CIA triády (důvěrnost, integrita a dostupnost), a měl by zahrnovat tyto oblasti, které možnosti narušení CIA pomohou snížit na akceptovatelnou úroveň:

- **Softwarová ochrana** – aktualizace operačních systémů, ovladačů zařízení a aplikací, antivir, firewall, šifrování.
- **Hardwarová ochrana** – ochrana proti selhání hardware (např. RAID, zálohování dat), záložní zdroje, redundantní zdroje a hw šifrování.
- **Ochrana dat a identity** – zabezpečení uživatelských účtů prostřednictvím autentizace a autorizace, zabezpečení dvou a více faktorovou autentizací, zabezpečení uživatelských účtu online služeb.
- **Fyzická bezpečnost** – zajištění ochrany proti neoprávněné manipulaci s prostředky výpočetní techniky a možnosti její zcizení.
- **Chování uživatele** – edukace a rozšiřování bezpečnostního povědomí a znalostí uživatele a neposlední řadě použití „zdravého selského rozumu“, neboť právě koncový uživatel je nejslabším článkem kyber bezpečnosti.

4.1 Zabezpečení komunikační techniky

V soukromé a podnikové sféře je oblast bezpečnosti výpočetní a komunikační techniky zpravidla přenesena na oddělení informatiky, správce sítě nebo řešena formou outsourcingu. Jednotlivec nemá tolik možností, finančních prostředků, nebo znalostí a oblast bezpečnosti zůstává na jeho osobě.

Navzdory tomu může komunikační techniku (výpočetní i mobilní zařízení a telefony) zabezpečit vlastní silou, za využití obecně známých a zveřejněných „best practice“[58] i běžný uživatel. Zde se nabízí velký prostor pro edukaci a zvyšování bezpečnostního povědomí již na základních školách v rámci hodin informatiky, protože věk uživatelů komunikační

[58] Z angličtiny: „nejlepší postup“. Postupy a techniky, které jsou obecně přijímané jako lepší, než známé alternativy a dosahují nejlepší výsledky. Např.: „Desatero internetového zabezpečení“. Dostupné z internetu: https://blog.avast.com/cs/2014/06/05/desatero-internetoveho-zabezpeceni/

techniky se mnohdy posunul i do předškolního věku. Obecně lze bezpečnost informačních technologií rozčlenit do těchto kategorií:

4.1.1 Softwarová bezpečnost

Softwarová (programová) bezpečnost zahrnuje ochranu počítačových systémů před útoky z internetu, nebo z vnitřního prostředí.

4.1.1.1 Aktualizace

Aktualizace jsou opravný programový kód pro OS, nebo jiné programové vybavení. Důvodem vydávání je fakt, že každá aplikace napsaná člověkem může obsahovat chyby, které budou využity jako zranitelnost k napadení systému a páchání škodlivé činnosti. K zajištění bezpečnosti je nutné aplikovat aktualizace, nebo zajistit jejich automatickou instalaci.

Jedná se především o aktualizace operačních systémů, programového vybavení a aplikací třetích stran (s důrazem na internetové prohlížeče a jejich doplňky). Neméně důležité je však aktualizovat i zařízení a aktivní prvky, které zajišťují (router, WiFi anténa, switch), nebo mají přímý přístup do prostředí internetu (NAS, IoT, tiskárny, atd.).

4.1.1.2 Antivir

Software, který slouží k detekci, blokování a odstraňování škodlivého softwaru (malware), jako jsou viry, trojské koně, spyware, adware a další formy škodlivého softwaru. Pracuje na základě definicí známých virů (detekuje již známý škodlivý SW), nebo na základě heuristické analýzy, která dokáže detekovat závadné chování aplikací, nebo chování specifické pro škodlivý SW. Základní antivir může být součástí OS, nebo také jako samostatný komerční produkt s rozšířenými funkcemi[59]. Uživatel by neměl vypínat, nebo jakkoliv jinak snižovat funkčnost Antiviru.

4.1.1.3 Firewall

Bezpečnostní mechanismus, který slouží k ochraně počítačové sítě před neautorizovaným přístupem a útoky z internetu, nebo vnitřní sítě. Firewall funguje jako filtr, který kontroluje

[59] Součástí antiviru, nebo bezpečnostního SW, může být i firewall, SPAM filtr, ochrana identity, správce hesel.

veškerý síťový provoz a rozhoduje, zda ho povolí nebo zablokuje na základě nastavených pravidel. Firewally mohou být hardwarové, zabudované přímo v síťovém zařízení (např. v routeru), nebo softwarové aplikace, které běží na počítači.

4.1.2 Hardwarová bezpečnost

Hardwarovou bezpečnost lze brát jako ochranu dat proti selhání fyzického HW. Zpravidla bývá využíváno zálohování na externí média, uložení dat v „cloudu“, nebo pomocí systému RAID[60] (data jsou rozložena vhodným způsobem na více disků, podle typu RAID je systém odolný proti výpadku jednoho, nebo více disků).

Dalším pohledem mohou být různé útoky na USB rozhraní. Může jít o různé USB HW gadgety, či jiné legitimní zařízení na pozadí pracující se škodlivým účinkem (keyloggery, Bash Bunny[61]). Popřípadě útok cílený na zvědavost uživatele. Například formou, „co se nachází na nalezeném flash disku?“ (záměrně ztraceném útočníkem v okolí firem apod.), kdy může jít například o USBKill[62]

4.1.3 Informační bezpečnost

Základním prvkem informační bezpečnosti by mělo být šifrování důležitých informací a externích médií, proti ztrátě, zcizení, nebo neautorizovanému přístupu (např.: podplacení pracovníci úklidových služeb v kancelářích firem apod.). Důležité je používání unikátních, dostatečně silných hesel k šifrovacímu certifikátu a uživatelskému účtu v operačním systému. Základní způsoby rozdělení šifrovacích principů:

- FBE (File base encription) – šifrování na úrovni jednotlivých souborů, nebo složek. Například EFS[63] - nativní šifrování v OS Microsoft Windows, nebo populární multiplatformní PGP (Pretty Good Privacy), které bylo přijato jako internetový standard pod názvem OpenPGP[64].
- FDE (Full disk encryption) – šifrování na úrovni celých oddílů a disků. Například BitLocker společnosti Microsoft v operačních systémech Windows, nebo FileVault

[60] RAID (anglicky Redundant Array of Independent Disks – vícenásobné pole nezávislých levných disků).
[61] Dostupné z internetu: https://shop.hak5.org/products/bash-bunny
[62] Dostupné z internetu: https://usbkill.com/
[63] Encrypting File System (EFS) je šifrovaný souborový systém v Microsoft Windows 2000 a novějších.
[64] Dostupné z internetu: https://www.openpgp.org/

využívané v zařízeních společnosti Apple. Mezi šifrovací produkty třetích stran lze zařadit například TrueCrypt, resp. jeho nástupce VeraCrypt[65].

- Dalším způsobem „znečitelnění“ dat může být steganografie, která není přímo šifrováním, ale pouze skrytím dat v jiném obsahu.

Při využívání jakéhokoliv způsobu šifrování je důležité vlastnit bezpečně uloženou zálohu šifrovacího certifikátu, obnovovacích klíčů, nebo nastavení alternativního způsobu obnovy k dešifrování dat.

4.1.4 Fyzická bezpečnost

Fyzická bezpečnost částečně zasahuje i do bezpečnosti hardwarové. Pro útočníka může být mnohem výhodnější a snazší získat přístup k informacím a datům uživatele tím, že zařízení zcizí. Následně využije přímý přístup k zařízení, nebo nosiči informací. Nemusí se však jednat přímo o cílený útok, ale i jen o prostou ztrátu zařízení, flash disku, nebo externích médií. Je pak k zamyšlení, jakou hodnotu mají tato zařízení v případě jejich ztráty, nebo zveřejnění jejich obsahu. V obou případech by měla zafungovat další vrstva zabezpečení např. šifrování zařízení a ochrana heslem, nebo více faktorovou autentizací, aby se tato média stala neupotřebitelnými.

4.1.5 Ochrana identity

Jako základní ochrana identity a osobních dat je nejčastěji využívaná ochrana heslem. V souvislosti se zabezpečením se uvádí výrazy, které se často zaměňují.

- autentizace – proces ověření identity („kdo jsem“), zpravidla uživatelským jménem a heslem.
- autorizace – určuje, kam má autentizovaný uživatel přístup na základě uživatelských práv a rolí („kam mohu“).

Nedílnou součástí ochrany identity je rovněž to, co a kde o sobě konkrétní uživatel zveřejňuje v prostředí kyberprostoru. Cokoliv se v prostředí internetu zveřejní ve vztahu k uživateli zpravidla nelze odstranit, nebo s velkými obtížemi. Z jednotlivých částí informací lze poskládat profil uživatele, který by šlo využít k některému útoku formou

[65] Dostupné z internetu: https://www.veracrypt.fr/en/Home.html

sociálního inženýrství, nebo může být do budoucna vážnou reputační hrozbou v kariérním životě.

Velmi důležité je využívat vlastní telekomunikační, výpočetní techniku a připojení k internetu. Resp. na důležité operace (mobilní bankovnictví, použití e-mailu apod.) nevyužívat veřejně dostupná zařízeni, „free“, otevřené a neznámé hotspoty, které mohou být podvržené s odposlechem komunikace.

4.1.5.1 Uživatelská hesla

Teorií na tvorbu bezpečných a unikátních hesel bylo napsáno mnoho. Důležitým faktem je:

„**bezpečnost uživatele je vykoupena jeho pohodlím**“.

Uživatel s rostoucím množstvím využívaných služeb, začne používat jednoduchá (zapamatovatelná) hesla, mnohdy se zcela pro něj specifickým vzorem. Pokud využije strojově generované silné heslo, má problém si je zapamatovat a často si je někam zapíše. Problémem jsou databáze uniklých hesel, které jsou veřejně dostupné na internetu a obsahují kompromitované uživatelské účty a hesla různých služeb. Kompromitaci si může uživatel ověřit například na stránkách „HaveBeenPwned“[66]. V rámci zvýšení bezpečnosti by měl využívat aplikace na správu hesel (např.: KeePass), která generuje bezpečná hesla a chrání je jediným hlavním heslem a silným šifrováním.

4.1.5.2 Více faktorové ověření

Postupem času se ukázalo zabezpečení heslem jako nedostatečné a jsou nasazovány systémy dvou (2FA) a více faktorové autentizace. Ta spočívá v ověření uživatele na základě více faktorů:

- „Tím co ví“ – uživatelské jméno a heslo,
- „Tím co má“ – druhý a další faktor, potvrzení na mobilním telefonu, zadání bezpečnostního kódu z aplikace např. Google Authenticator, otisk prstu, snímání obličeje, sítnice oka, hlasu, apod.

Ani tento způsob zabezpečení nemusí být vždy bezpečný a odolný například vůči útokům typu „Session Stealing“ (zcizení relace), nebo „Session Hijacking“. V současné době se jeví

[66] Služba na ověření kompromitace uživatelských účtů, dostupné z internetu: https://haveibeenpwned.com/

jako vhodný způsob ověřování hardwarové „password less“ (bez heslové) řešení typu Yubikey[67].

4.2 Anonymita

Anonymita v prostředí internetu je jen zdánlivá, nicméně za využití některých prostředků a způsobů chování se dá nastavit její poměrně dobrá úroveň.

4.2.1 Virtual private network (VPN)

VPN (virtuální privátní síť) je služba, která umožňuje vytvořit bezpečné šifrované spojení mezi zařízeními prostřednictvím internetu[68]. VPN maskuje skutečné IP adresy za adresy VPN serverů, které tuto službu zajišťují. Umožňuje tak zakrýt vaši skutečnou polohu a online aktivity. Často je služba využívána k připojení „home office“ zařízení do firemní sítě, nebo také ke změně lokality za účelem sledování online streamovacích služeb nedostupných v naší lokalitě.

Tyto služby mají vliv na rychlost konektivy do internetu a jejím využíváním se zpomalují. Dalším ohledem je to, jaké jurisdikci se nachází poskytovatel (servery apod.) VPN a jakým způsobem se staví k požadavkům orgánů činných v trestním řízení o vydání provozních a telekomunikačních dat.

4.2.2 The Onion Router (TOR)

Systém zajišťuje anonymizované šifrované spojení pomocí upraveného prohlížeče www stránek. Upravený prohlížeč je postavený na jádře Mozilla Firefox[69]. Komunikace probíhá přes několik uzlů (nodů), kdy nejsou současně čitelné zdrojové a cílové adresy v žádném kroku cesty. V průběhu komunikace je známá tedy pouze adresa předchozího z nodů. Podobně jako u VPN tento způsob komunikace má vliv na rychlost procházení internetového obsahu. Bezpečnost je dána velkým množstvím nodů. Nezodpovězenou otázkou zůstává, zda některý z těchto nodů není pod správou některých národních složek zabývajících se kyber kriminalitou.

---

[67] Hardwarové produkty více faktorového ověření firmy Yubico, dostupné na internetu: https://www.yubico.com/products/
[68] Například OpenVPN, dostupné z internetu: https://openvpn.net/
[69] Dostupný z internetu: https://www.torproject.org/download/

4.2.3 E-mailová komunikace

V rámci e-mailové komunikace by měl uživatel využívat více e-mailových účtů s konkrétním účelem (soukromý, zábava, registrace, na neznámé služby apod.), a to jak z hlediska bezpečnosti, tak z důvodu přehlednosti komunikace. Další možností je využití některého z poskytovatelů anonymních a na bezpečnost zaměřených e-mailů[70].

4.2.4 Omezení digitální stopy

Omezení vzniku digitální stopy ve vztahu ke kyberprostoru, anonymitě (mimo použití VPN, TOR) a bezpečnosti na koncové technice uživatele lze docílit především používáním anonymních oken internetových prohlížečů, „sandbox“[71] prohlížečem, nebo „life distribucí“ operačních systémů založených na jádře Linuxu[72]. K omezení stávající digitální stopy na technice je možné použití software pro údržbu počítače.

[70] Dostupný z internetu: https://proton.me/
[71] Virtualizační nástroj, který umožňuje prohlížet www stránky, nebo spouštět aplikace v bezpečném virtuálním prostředí, které je zcela izolováno od zbytku počítačového systému. Např. sandbox od společnosti Avast, dostupný vrámci produktu Premium Security.
[72] Například Debian, dostupný z internetu: https://www.debian.org/

PRAKTICKÁ ČÁST

5 ANALÝZA DATOVÝCH NOSIČŮ

V úvodu kapitoly „Digitální stopa“ a části „Fyzické uložení digitální stopy“ byla vyslovena teze, že informace je v konečném důsledku myšlenka zhmotněná na některý z druhů fyzických nosičů ve formě datových souborů, nebo obsazeného paměťového prostoru. Za účelem zpracování praktické části byly využity nakoupené, darované, staré, nebo vlastní disky a paměťová média. Praktická část bude prezentovat, jaké artefakty, fragmenty souborů, popřípadě metada jsou zjistitelná na pevných discích a paměťových médiích prostřednictvím forenzních nástrojů, nebo běžně dostupných softwarových nástrojů. Především na zakoupených a darovaných discích je záměr pokusit se o obnovu dat po předchozím majiteli a demonstrovat, jakým způsobem se změní počet artefaktů po určitých systémových akcích.

5.1 Předpoklady, vybavení

K analýze a demonstraci pokusů s paměťovými médii (pevné disky, flash disky apod.) byl využit počítač (referenční sestava) v konfiguraci: Intel i7-3770K, 32GB RAM, 1TB SSD, 3TB HDD, 6TB HDD s operačním systémem Windows 10 Pro 64bit.

- Pro účely testování omezení digitální stopy byl záměrně využit běžně dostupný program CCleaner (free verze 6.11.10455, 64bit).
- pro následnou analýzu byl použit forenzní nástroj Magnet Axiom (verze 6.11.0.34807) s povolenou možností analýzy smazaných souborů (carving).
- Jako doplňkové programové vybavení je využito programů WinHex, FTK Imager a „life“ Linuxová distribuce Kali[73].

5.1.1 Předpoklady, příprava vzorků

Z předložených paměťových médií (HDD, SSD, flash disky apod., dále jen „vzorky“) budou vytvořeny zálohy formou bitové kopie za účelem zachování původního stavu před provedenými akcemi.

[73] Kali Linux je open-source linuxová distribuce založená na Debianu zaměřená na různé úkoly v oblasti informační bezpečnosti, jako je penetrační testování, bezpečnostní výzkum, počítačová forenzní analýza a reverzní inženýrství.

Následně bude provedena:

- Analýza výchozí bitové kopie na vyhledání fragmentů souborového systému a artefaktů operačního systému.
- Systémovými nástroji operačního systému, nebo aplikacemi bude provedeno omezení, nebo zničení digitálních stop a dat na vzorcích.
- Dále bude provedena bitová kopie pro účely zaznamenání stavu a analýzu změn po předchozích úpravách prostřednictvím forenzního nástroje.
- Následně bude paměťové médium (vzorek) obnoven do původního stavu, aby bylo možné provést další pokusy jinými metodami.

5.1.2 Použité metody

V tabulkách s uvedenými výsledky analýz a testů jsou uvedeny zkratky metod a pokusů s tímto významem:

- **Původní** (**ORG**) – analýza disku byla provedena nad původními daty bez jakékoliv úpravy.
- **SmSV** – analýza dat byla provedena po prostém smazání logického oddílu (svazku) standartními prostředky operačního systému Windows (správa disků).
- **RyFo** – analýza dat byla provedena po provedení „Rychlého formátu“ standartními prostředky operačního systému Windows.
- **UpFo** – analýza dat byla provedena po provedení úplného formátu standartními prostředky operačního systému Windows.
- **CC** – analýza dat byla provedena po použití funkce „pokročilé vyčištění“ programem CCleaner se zaškrtnutím možností všech artefaktů v části „Windows“ a „Aplikace“ (běžné smazání).
- **FrSP** – analýza dat byla provedena po použití funkce „čištění disku“ (volné místo) aplikací CCleaner.
- **Wipe** – analýza dat byla provedena po přepsání celé datové oblasti hodnotou 0 „nula“ prostřednictví programu CCleaner.

5.1.3 Pojmy

Aplikací metod a následnou analýzou bude zkoumána jejich účinnost na omezení, nebo zničené digitálních dat na vybraných vzorcích. Ve vztahu k uvedeným metodám je potřeba osvětlit tyto pojmy:

- **Bitová kopie** – je soubor, ve které, je uložen přesný obraz veškerých dat (po jednotlivých bitech) paměťového média. Bitová kopie uchovává přesné rozložení logických oddílů souborového systému včetně smazaných souborů. V případě selhání paměťového média (pevný disk apod.) lze prostřednictvím bitové kopie obnovit data na jiné médium v původní podobě k danému datu zálohy.
- **Hash** - výsledek jednosměrné kryptografické funkce, která z posloupnosti neurčitého počtu znaků vytvoří unikátní řetězec o pevné délce (často používané hashovací funkce: MD5, SHA1, SHA256). Využívá se k ověření integrity souborů, bitových kopií, zabezpečení hesel v databázích a kryptografii (např. digitální podpis).
- **Carving** – metoda, při které probíhá pokus o zpětnou rekonstrukci datových souborů z jejich fragmentů bez dostupnosti meta dat, nebo informací ze souborového systému. Vlastnosti a typ souboru není definován jeho příponou v souborovém systému, ale tzv. „magic numbers“ (signatura) v hexadecimální podobě na začátku, nebo konci dat definujících soubor. Touto metodou (carvingem) lze tedy rozpoznat typ souboru s chybnou, nebo chybějící příponou definující typ souboru.

5.2 Analýza vzorků

Nad vybranými vzorky byly provedeny uvedenými metodami pokusy o ovlivnění, nebo zničení digitální stopy. Využito bylo standartních prostředků operačního systému Windows, popřípadě běžně dostupného programového nástroje CCleaner. Následnou analýzou byla zjišťována změna počtů nalezených fragmentů.

5.2.1 Analýza systémových disků

Analýza slouží k ukázce množství artefaktů digitální stopy na discích s operačním systémem Microsoft Windows. K analýze a zobrazení výsledků po omezení digitální stopy v operačním systému byly využity následující vzorky:

- Vzorek #01 - Samsung SSD 860 EVO 250GB, sériové číslo: S4CJNF0NC56184X, deklarovaná kapacita 250GB. Pevný disk byl vyžívaný jako systémový v domácím počítači sdíleným více uživateli. Operace změn proběhly pod uživatelem s omezenými právy.
- Vzorek #02 - Samsung SSD 840 EVO 250GB, sériové číslo: S1DBNSBF880487Y, deklarovaná kapacita 250GB. Pevný disk byl využívaný jako systémový

v notebooku, který sloužil na domácí i pracovní využití. Operace změn proběhly pod uživatelem s právy správce.

Vzhledem k rozsahu artefaktů získaných analýzou, byly tabulky s výsledky přesunuty do PŘÍLOHY P I: ANALÝZA SYSTÉMOVÝCH DISKŮ.

Tabulka 5. Výsledky analýzy systémových disků (vzorky #01, #02)

	Počet nalezených artefaktů			**% Změna**	
	Původní	CC	FrSp	CC	FrSP
Vzorek #01	339813	327920	279234	-3,50 %	-17,83 %
Vzorek #02	2916760	1920747	1882610	-34,15 %	-35,46 %
			Průměr	-15,33 %	-26,65 %

Výsledky u těchto vzorků odráží rozdílnost mezi možnosti omezení digitální stopy, pokud probíhají (u metody CC) pod různými uživatelskými právy u uživatelského účtu.

U vzorku #01, které proběhlo pod omezenými právy, se vztahuje především na oblasti, které jsou uživateli s těmito právy přístupné (historie prohlížení www stránek, dočasné soubory, poslední otevřené soubory apod. – vše pouze v jeho uživatelském profilu).

Vzorek #02 byl metodou „CC“ proveden pod právy správce operačního systému a má tedy možnost odstranit artefakty i v místech, kam běžný uživatel nemůže (především forenzně zajímavé systémové a aplikační logy operačního systému).

U obou vzorků byl rovněž proveden pokus s omezením obnovitelných artefaktů metodou „FrSp“ (vyčištění volného místa). Výsledky jsou uvedeny v tabulce č. 5 „Výsledky analýzy systémových disků“. Podrobnější výsledky o způsobech a účinnosti mazání pevných disků jsou uvedeny v následující kapitole.

5.2.2 Analýza způsobů mazání disků

Operace změn byly provedeny na referenční sestavě přes externí SATA USB box, ve kterém byly disky připojeny. K analýze a zobrazení výsledků dle jednotlivých způsobů mazání dat na pevných discích byly použity následující vzorky:

- Vzorek #04 – Western Digital (WD2500JS), sériové číslo: WCANKL741236, deklarovaná kapacita 250GB. Pevný disk byl využíván jako datový disk (nesystémový) v běžném kancelářském počítači.
- Vzorek #05 – Western Digital (WD7500AALX), sériové číslo: WCATR6774818, deklarovaná kapacita 750GB. Pevný disk byl využíván jako datový disk (nesystémový) v domácím stolním počítači.
- Vzorek #06 – externí box značky ICY BOX s vloženým HDD značky Hitachi, sériové číslo: 120921TE85113Q0HNYJR, deklarovaná kapacita 500GB. Po připojení k operačnímu systému se souborový systém jevil jako prázdný.

Vzhledem k rozsahu získaných artefaktů analýzou, byla tabulka s výsledky přesunuta do PŘÍLOHY P II: ANALÝZA DATOVÝCH DISKŮ.

U jednotlivých vzorků, byly provedeny pomocí metod a postupů uvedených v částech „Předpoklady, příprava vzorků“ a „Použité metody“ různé postupy mazání obsahu na disku. Výsledky jsou prezentovány v následujících tabulkách.

Tabulka 6. Výsledky analýzy datových disků, fragmenty (vzorky #04, #05, #06)

	Počet nalezených artefaktů				
	Původní	SmSv	RyFo	UpFo	Wipe
Vzorek #04	17585	9756	9517	4	1
Vzorek #05	14738	9517	1	2	1
Vzorek #06	9534	17479	9534	13	10

Tabulka 7. Výsledky analýzy datových disků, % změny (vzorky #04, #05, #06)

	% Změna počtu nalezených artefaktů			
	SmSv	RyFo	UpFo	Wipe
Vzorek #04	-44,52 %	-45,88 %	-99,98 %	-99,99 %
Vzorek #05	-31,40 %	-99,99 %	-99,99 %	-99,99 %
Vzorek #06	83,33 %	0 %	-99,86 %	-99,90 %
Průměr	-53,08 %	-48,62 %	-99,94 %	-99,96 %

U vzorku #06 bylo po pouhém smazání logického svazu (SmSv) nalezeno o cca 83 % více fragmentů, než ve výchozím stavu (Původní). Toto bylo zapříčiněno způsobem obnovení smazaných dat. Část dat byla obnovena na základě obnovené tabulky smazaného souborového systému. Druhá část dat byla obnovena „carvingem“, kdy forenzní nástroj obnovil data na základě čtení paměťového prostoru daného média po bitech a analýze hlaviček souborů. Jedná se tedy z velké části o duplicitní fragmenty.

Po provedení „rychlého formátu“ (RyFo) u stejného vzorku forenzní nástroj obnovil stejný počet artefaktů, jako u výchozího stavu před mazáním.

U metod „úplný formát“ (UpFo) a „wipe“ (Wipe) jsou výsledky u všech vzorků srovnatelné. Nicméně u vzorku #06 bylo nalezeno 10 artefaktů i po metodě „wipe“. Podrobnou analýzou bylo zjištěno, že se jedná o fragmenty video souborů s velmi malým rozlišením a velikostí v řádu několika Bytů. Lze tedy usoudit, že se jedná o fragmenty typu „slack“.

Z uvedených pokusů a analýzy plyne, že metody smazání svazku (SmSv) a rychlé formátování (RyFo) se k odstranění obsahu disků nehodí vůbec. Metoda úplného formátu (UpFo) se jeví dle výsledků jako dostatečná, ale vzhledem k nejlepším výsledkům i zažitým forenzním postupům doporučuji metodu „wipe“ (přepsání celého paměťového prostoru jiným obsahem).

5.2.3 Analýza flash disků

Operace změn byly provedeny na referenční sestavě formou vyčištění prázdného (nevyužitého) místa a porovnáním s původním stavem. K analýze byly využity běžné „flash disky“, které uživatelé zpravidla využívají k přenosu dat mezi jednotlivými zařízeními a záloze. K analýze a zobrazení výsledků nalezených artefaktů po změnách byly použity následující vzorky:

- Vzorek #14 – flash disk Verbatim DTSE3, deklarovaná kapacita 8GB.
- Vzorek #15 – flash disk ADATA UV150, deklarovaná kapacita 64GB.
- Vzorek #16 – flash disk Kingston DTSE, deklarovaná kapacita 16GB.
- Vzorek #17 – flash disk Verbatim Store N Go, deklarovaná kapacita 16GB.
- Vzorek #18 – flash disk Kingston DTSE, deklarovaná kapacita 16GB.
- Vzorek #19 – flash disk ADATA, deklarovaná kapacita 8GB.
- Vzorek #20 – flash disk Kingston DataTraveler, deklarovaná kapacita 16GB.

- Vzorek #21 – flash disk Kingston HyperX, deklarovaná kapacita 256GB.

Vzhledem k rozsahu získaných artefaktů analýzou, byly tabulky s výsledky přesunuty do PŘÍLOHY P III: ANALÝZA FLASH DISKŮ.

Tabulka 8. Výsledky analýzy flash disků (vzorek #14 - #21)

	Původní	**FrSp**	**% Změna**
Vzorek #14	1837	1317	-28,31 %
Vzorek #15	30	19	-36,67 %
Vzorek #16	31063	3135	-89,91 %
Vzorek #17	3581	416	-88,38 %
Vzorek #18	164155	832	-99,49 %
Vzorek #19	3002	2867	-4,50 %
Vzorek #20	19612	19008	-3,08 %
Vzorek #21	113830	9419	-91,73 %
		Průměr	-55,26 %

U vybraných vzorků bylo provedeno vyčistění volného (nevyužitého) místa na paměťovém médiu uvedenou metodou „FrSp“ (přepsání jiným obsahem, zpravidla hodnotou nula „0“ na bitové úrovni), aby bylo zamezeno obnově smazaného obsahu. Následně bylo analýzou (včetně carvingu) provedeno porovnání počtu nalezených artefaktů oproti původnímu stavu.

Zejména u vzorků #16, #21 a #18 lze pozorovat výrazné snížení možnosti obnovy artefaktů smazaných v minulosti. Tímto způsobem tedy lze smazaná data trvale odstranit, až na úroveň pouze aktuálního obsahu na datovém nosiči. Zejména u externích médií, která jsou sdílena s více uživateli, nebo u kterých je vyšší pravděpodobnost ztráty, nebo zcizení je vhodné dle uvážení tuto operaci provádět pravidelně.

V souvislosti s touto metodu je důležité upozornit na rozdíl mezi médii založenými na magnetickém záznamu (HDD) a médii založených na polovodičových čipech („flash“ a „nand“). U druhé technologie je životnost paměťových buněk (omezený počet zápisů) polovodičového čipu řízena vnitřním firmwarem a data jsou ukládána rovnoměrně dle míry

opotřebení buněk. Pravidelná operace mazání (přepisem volného místa) tak může mít vliv na životnost média.

Z tohoto důvodu je vhodné u externích médií preferovat jejich šifrované varianty (HW, SW), nebo využít možnosti operačních systémů a aplikací třetích stran.

5.2.4 Analýza paměťových SD karet

Operace změn byly provedeny na referenční sestavě formou vyčištění prázdného (nevyužitého) místa a porovnáním s původním stavem. K analýze byly využity běžné paměťové SDHC karty. K analýze a zobrazení výsledků nalezených artefaktů po změnách byly použity následující vzorky:

- Vzorek #10 – SDHC karta, deklarovaná kapacita 4GB. Paměťová karta byla využívána v kompaktním fotoaparátu.
- Vzorek #11 – micro SDHC karta, deklarovaná kapacita 8GB.
- Vzorek #13 – micro SDHC karta, deklarovaná kapacita 8GB. Paměťová karta byla vložena ve slotu notebooku prostřednictvím SDHC redukce.
- Vzorek #22 – micro SDHC karta, deklarovaná kapacita 16GB. Paměťová karta sloužila jako datové médium na uložení hudebních souborů ve FM transmitteru.
- Vzorek #23 – SDHC karta, deklarovaná kapacita 32GB. Paměťová karta byla vložena v zařízení „fotopast“ (v operačním systému se jevila jako „prázdná“).
- Vzorek #24 – SDXC karta, deklarovaná kapacita 64GB. Paměťová karta byla využívána jako médium sdílené více uživateli ve fotoaparátu Canon.

Vzhledem k rozsahu získaných artefaktů analýzou, byly tabulky s výsledky přesunuty do PŘÍLOHY P IV: ANALÝZA SD PAMĚŤOVÝCH KARET.

Tabulka 9. Výsledky analýzy SD paměťových karet

	Původní	**FrSp**	**% Změna**
Vzorek #10	1770	5	-99,70 %
Vzorek #11	7462	1	-99,99 %
Vzorek #13	167	101	-39,52 %
Vzorek #22	2253	966	-57,12 %
Vzorek #23	370088	3	-99,99 %
Vzorek #24	10321	93	-99,10 %
		Průměr	**-82,57 %**

U vybraných vzorků bylo provedeno vyčistění volného (nevyužitého) místa na paměťovém médiu uvedenou metodou „FrSp“ (přepsání jiným obsahem, zpravidla hodnotou nula „0“ na bitové úrovni), aby bylo zamezeno obnově smazaného obsahu. Následně bylo analýzou (včetně carvingu) provedeno porovnání počtu nalezených artefaktů oproti původnímu stavu.

U uvedených vzorů je patrné, že ačkoliv byla v minulosti data smazána, nebo přesunuta (např. po vyfotografování a přesunu do počítače, nebo notebooku) je jejich velká část, podobně jako u analýzy flash disků, obnovitelná.

5.3 Dotazníkové šetření

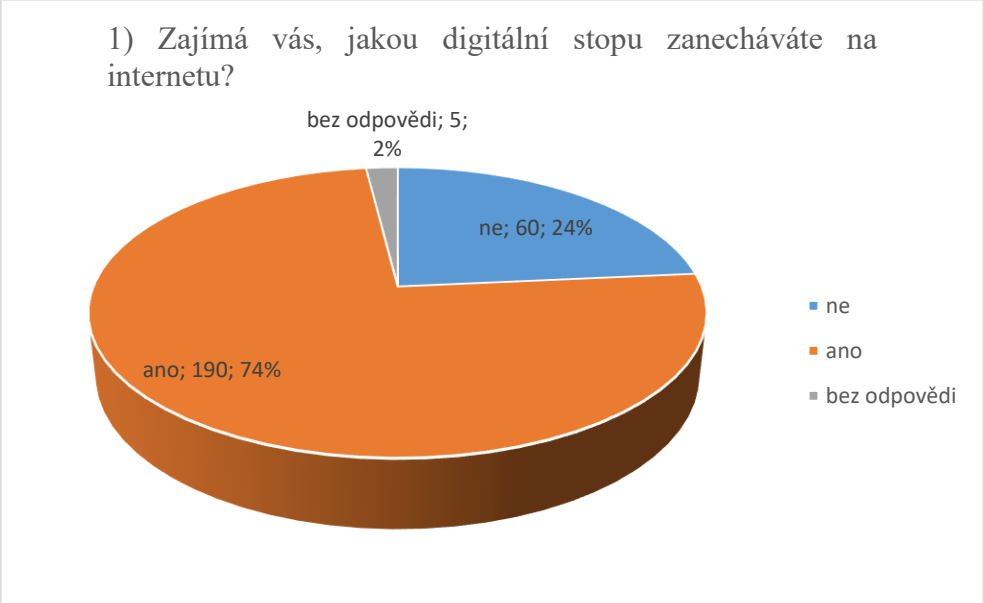
Za účelem zjištění, jak se uživatelé výpočetní techniky staví ke své bezpečnosti v kyberprostoru a ve vztahu k digitální stopě, jakou za sebou za sebou zanechávají, byl vytvořen dotazník, který byl vystaven na platformě „Vyplň to“[74].

Dotazníkové šetření bylo zpřístupněno v období 21. 04. 2023 – 05. 05. 2023, bez uvedení kategorie (např. IT), aby výsledky nebyly ovlivněny uživateli zajímajícími o tuto oblast. Otázky byly zvoleny uzavřené z důvodu snazšího zpracování a vyšší návratnosti.

Otázky byly rozloženy do oblastí bezpečnosti zařízení, operačního systému a informační bezpečnosti ve vztahu na chování uživatele v prostředí internetu. Celkově odpovědělo 255 respondentů z 319 (návratnost dotazníků cca 80 %).

5.3.1 Výsledky dotazníkového šetření

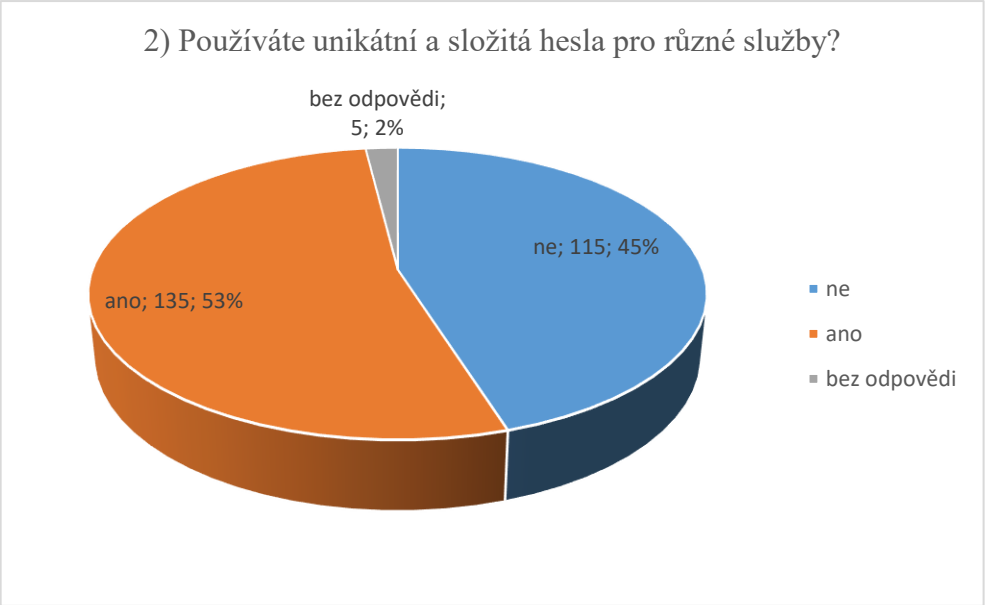
Graf 1: Výsledky otázky č. 1



Výsledky zobrazují, že téměř třem čtvrtím dotázaných respondentů není lhostejné, jakou digitální stopu za sebou zanechávají.

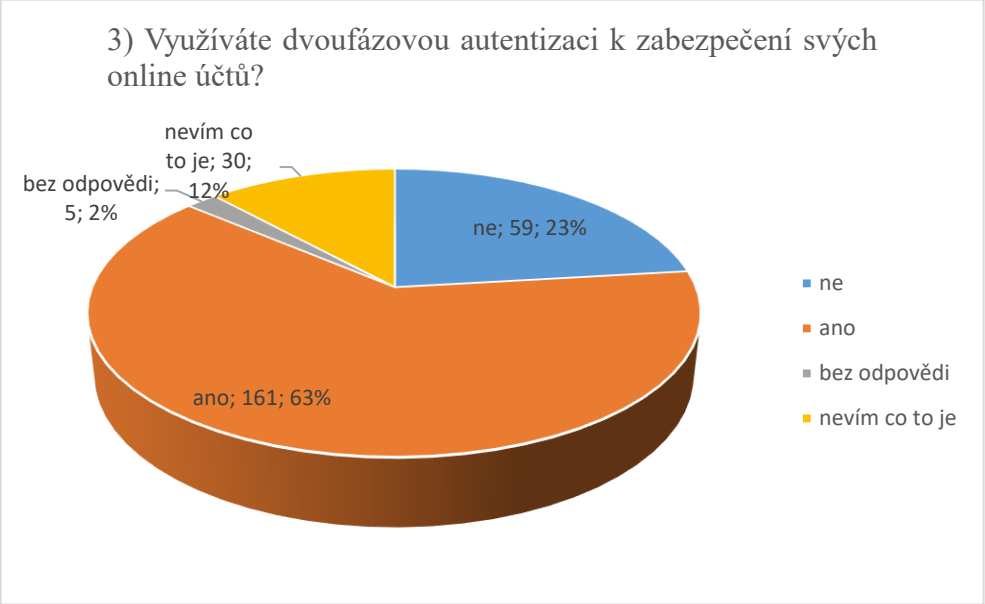
[74] Služba dostupná z internetu: https://www.vyplnto.cz

Graf 2: Výsledky otázky č. 2



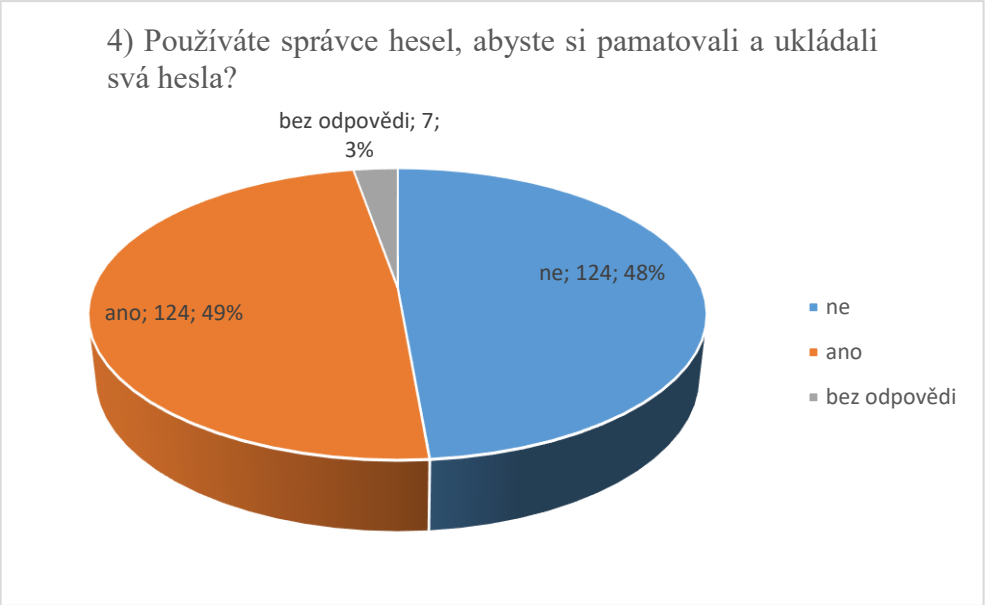
V odpovědi u dotazu na unikátnost a složitost hesel pro různé typy služeb se uživatelé dělí přibližně na polovinu, což není zcela uspokojivý výsledek. Velmi častým útokem na služby bývá právě s využitím databází uniklých hesel. Pokud využívá uživatel stejná hesla, zvyšuje útočníkovi šance na úspěch u více služeb. Zde vnímám prostor pro zlepšení.

Graf 3: Výsledky otázky č. 3



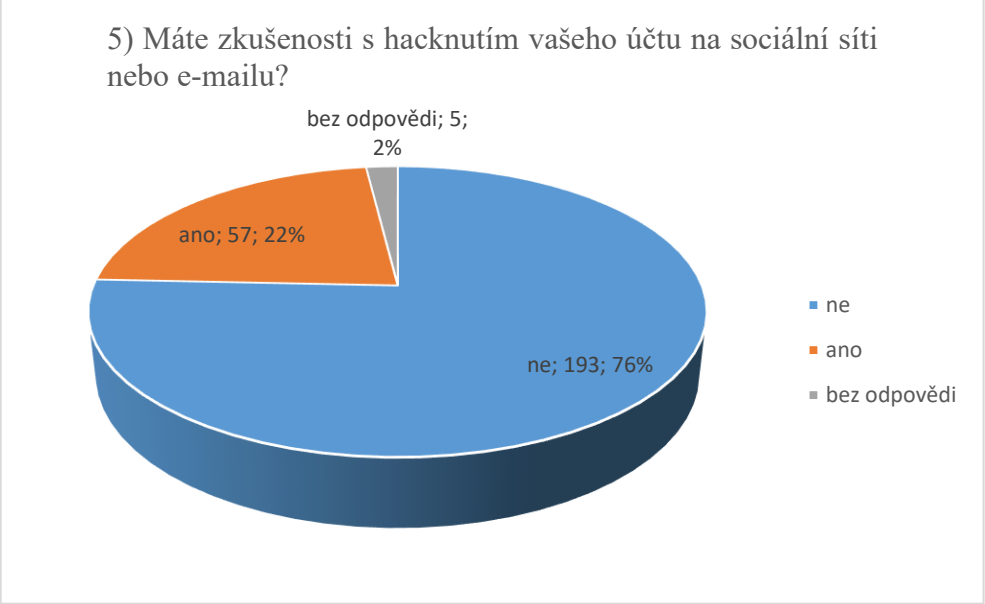
Využití dvoufázové autentifikace uvádí 63 % dotázaných uživatelů. Nicméně je možné, že k tomuto číslu patří i část uživatelů, kteří odpověděli „nevím co to je“, protože tuto autentifikaci používají, aniž by věděly, jak je odborně nazývána.

Graf 4: Výsledky otázky č. 4



Podobně jako u odpovědí na otázku č. 2 se uživatelé, kteří používají aplikace na správu hesel a kteří ne, rozdělují téměř na polovinu. Analýzou výsledků bylo zjištěno, že ti kteří používají unikátní a silná hesla (135 respondentů) využívají správce hesel rovněž jen z poloviny (67 využívá / 68 nevyužívá). Podobných výsledků bylo i u uživatelů bez silných unikátních a silných hesel (57 využívá / 56 nevyužívá).

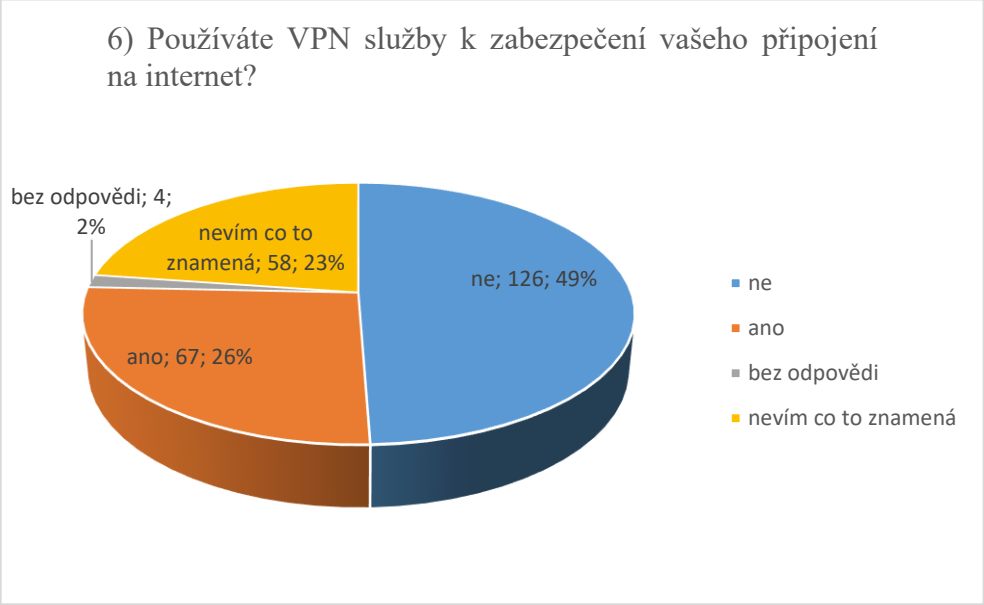
Graf 5: Výsledky otázky č. 5



Více jak tři čtvrtiny dotázaných uvádí, že nemají zkušenost s napadením účtu na sociální síti. Jde o pozitivní výsledek, který je zcela jistě dán „vnucováním“ bezpečnosti (dvou a více

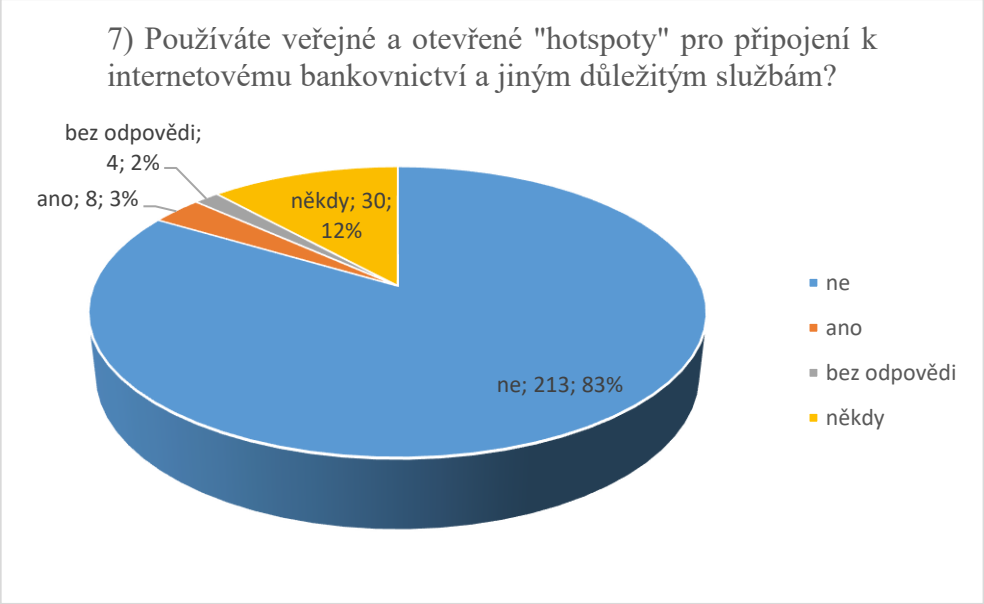
faktorová autentizace) uživatelům ze strany provozovatelů těchto sítí. Z 57 poškozených 24 nepoužívá silná a unikátní hesla a 12 nepoužívá dvou a více faktorovou autentizaci.

Graf 6: Výsledky otázky č. 6



Necelá čtvrtina z dotázaných neví, co služba VPN znamená a jaké výhody přináší. Polovina z dotázaných tyto možnosti nevyužívá. Vzhledem k uzavřenosti otázky nelze u poslední části respondentů určit, zda využívají VPN k zabezpečení připojení k internetu, nebo jen například ke změně geolokace kvůli omezením streamovacích služeb.

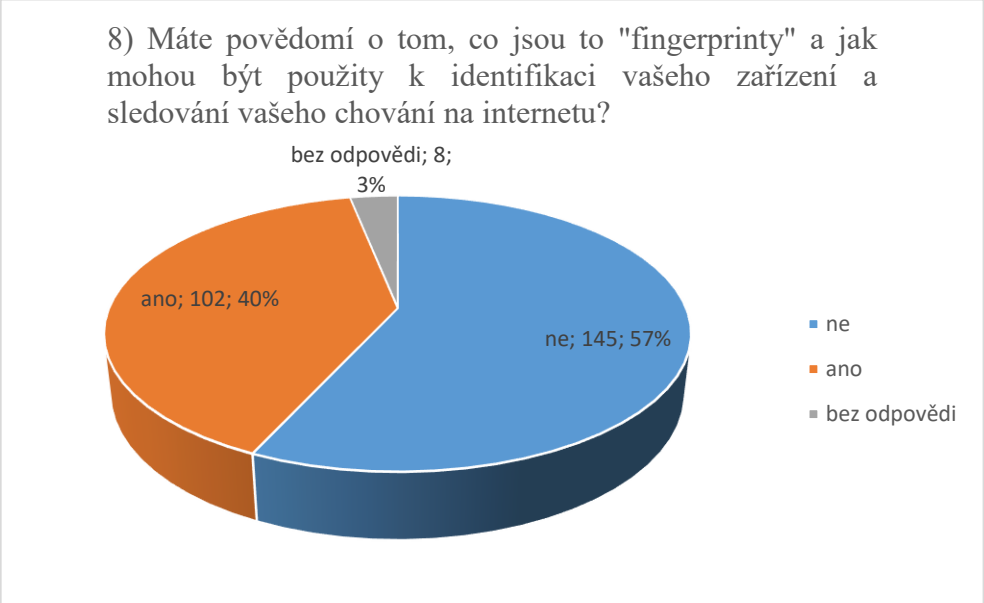
Graf 7: Výsledky otázky č. 7



Výsledky odpovědí vnímám jako velmi pozitivní z hlediska bezpečnosti, kdy lze poměrně snadno vytvořit otevřený „hotspot“ známých společností (Starbucks, McDonalds apod.) a

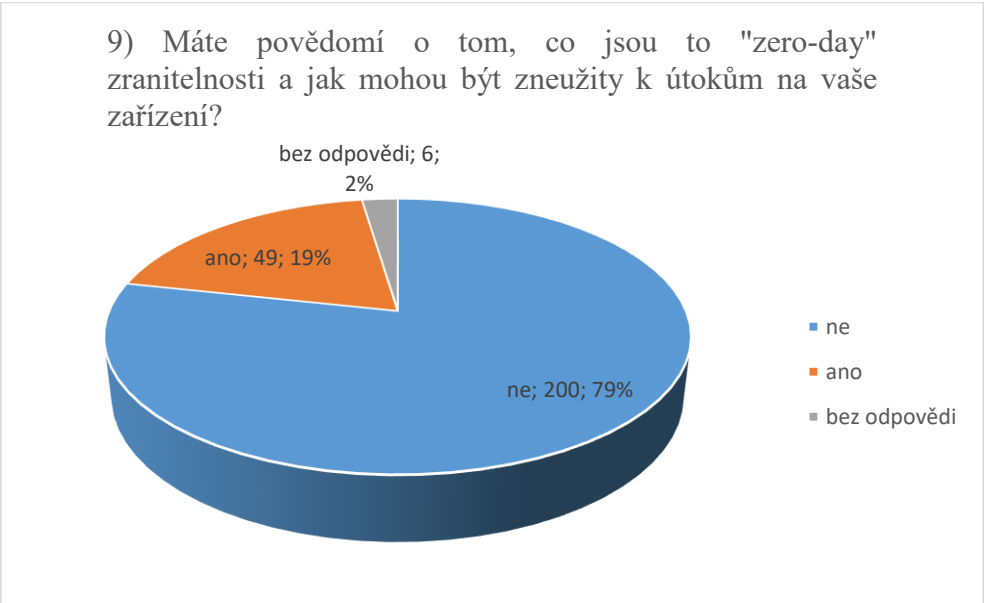
zachytávat provoz probíhající komunikace. Vzhledem k dobré dostupnosti datového pokrytí, tarifů a jejich cen není třeba využívat veřejné body k připojení k internetu.

Graf 8: Výsledky otázky č. 8



Ze 102 respondentů, kteří uvedli, že mají povědomí o „fingerprintu“ se jich 84 zajímá, o to jakou digitální stopu za sebou zanechávají. Lze to vnímat, jako dobré povědomí o bezpečnosti. Tito uživatelé rovněž užívají silná a unikátní hesla (61 odpovědí), více faktorovou autentizaci (62x) a správce hesel (45x).

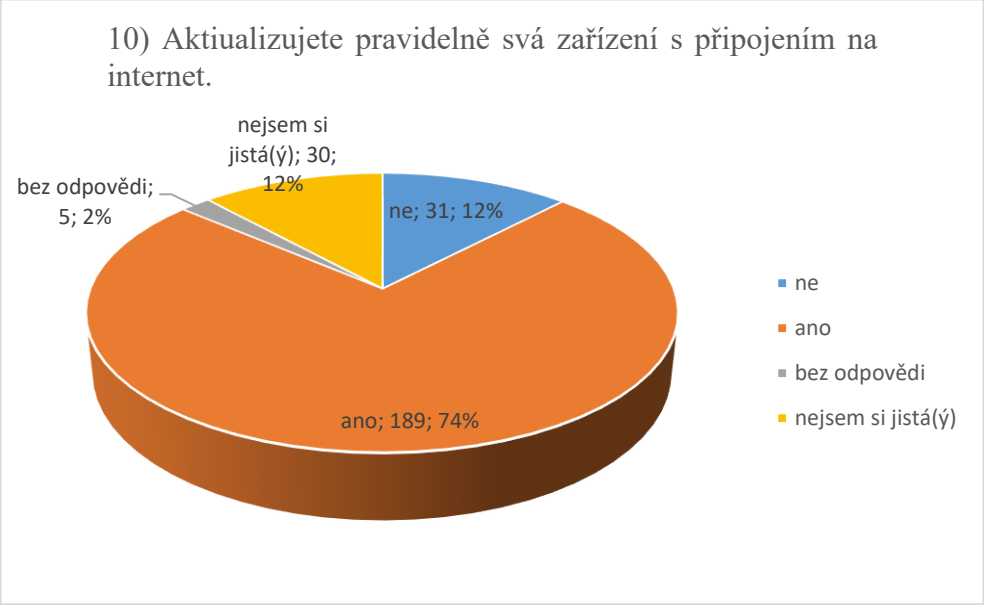
Graf 9: Výsledky otázky č. 9



Uvedená otázka patří mezi více technické s předpokladem, že většina respondentů s tímto termínem nebude obeznámena. Rozložení uživatelů se znalostí této problematiky dle

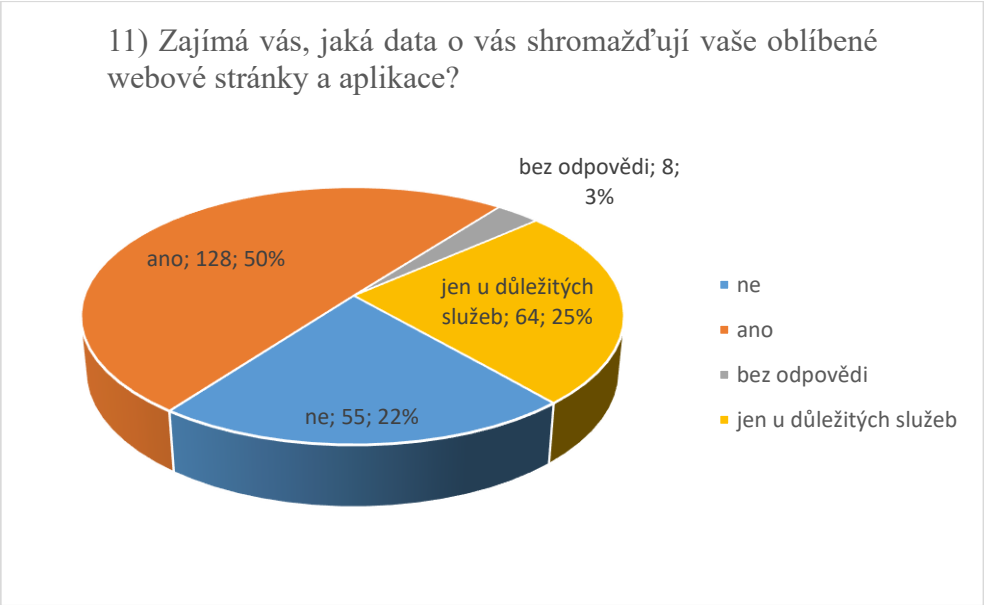
vzdělání je následující: vysokoškolské 31x, středoškolské 16x, neuvedeno 2x a základní vzdělání 1x.

Graf 10: Výsledky otázky č. 10



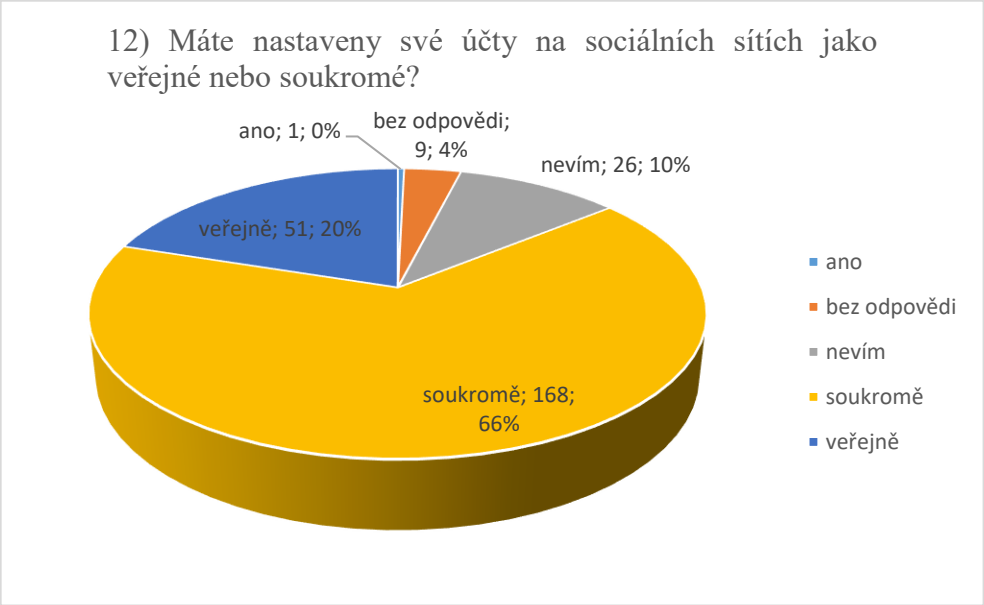
Výsledky odpovědí na tuto otázku jsou pozitivní, téměř tři čtvrtiny uživatelů tvrdí, že svá zařízení aktualizují. Velký podíl na výsledku bude především díky výrobcům operačních systémů (mobilní i PC platformy), kdy je uživatelům „vnucují“ bezpečnostní aktualizace formou automatických aktualizací. Toto by měl být standart i pro ostatní SW developery.

Graf 11: Výsledky otázky č. 11



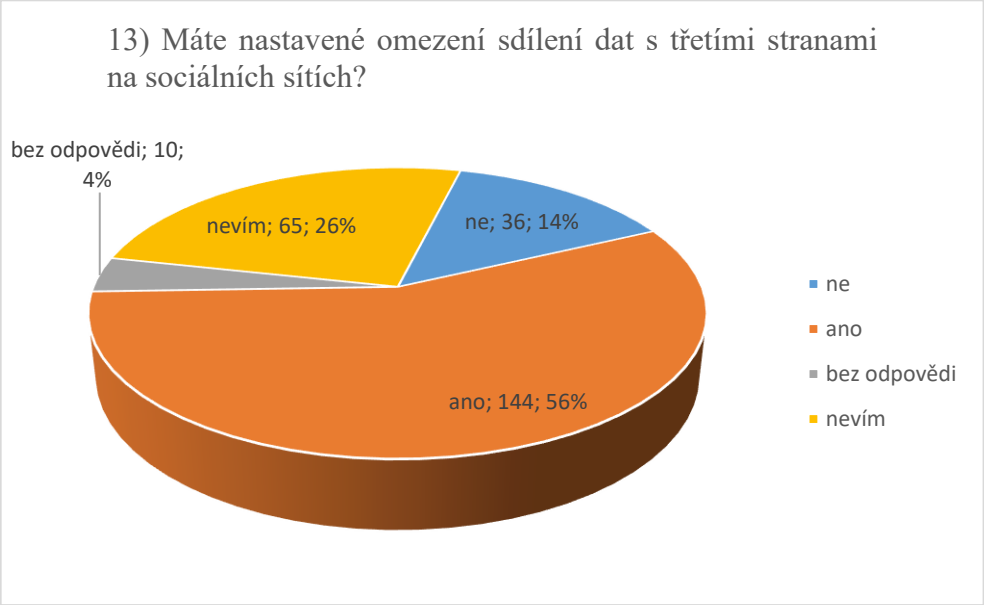
Z uvedených výsledků vyplývá, že polovina dotázaných má zájem o to, jakým způsobem se nakládá s jejími osobními daty. Čtvrtina uživatelů má tento zájem minimálně u služeb, které považuje za důležité.

Graf 12: Výsledky otázky č. 12



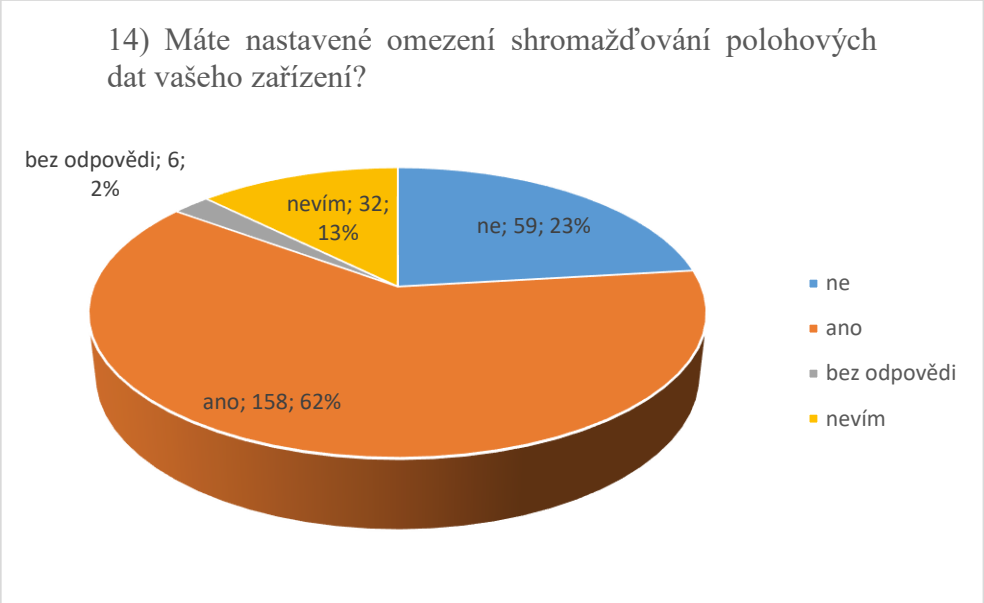
Výsledky ukazují, že dotazovaní jednotlivci jednoznačně dbají na své soukromí a své profily na sociálních sítích jako soukromé. Z 35 uživatelů s odpovědí „nevím“ a „bez odpovědi“ se jich 8 nezajímá o svou digitální stopu a 5 mají zkušenost s útokem na jejich uživatelský profil na sociálních sítích.

Graf 13: Výsledky otázky č. 13



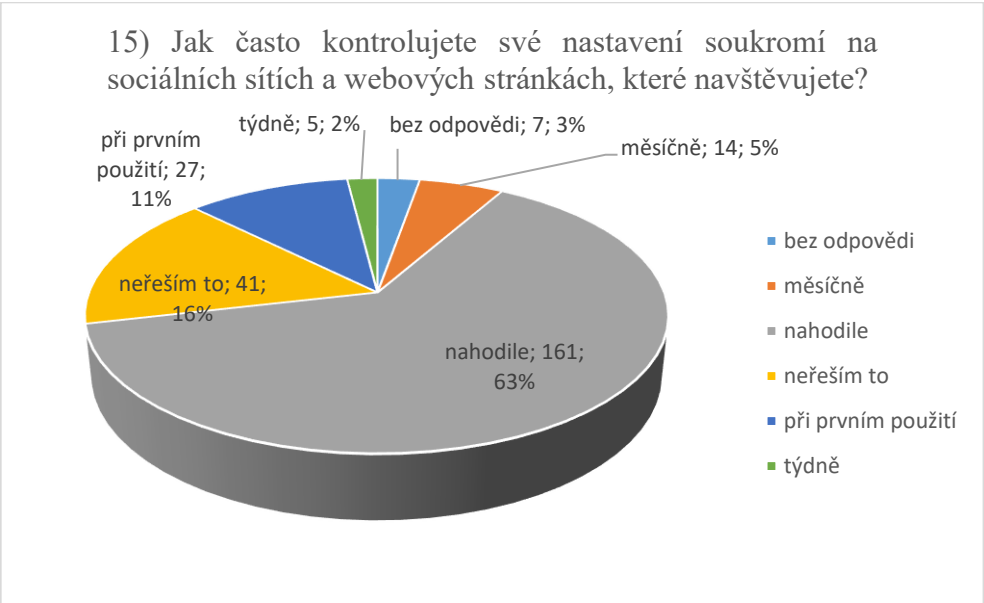
Více jak polovina uživatelů se snaží omezovat sdílení osobních údajů třetím stranám. Zbývající uživatelé buď nevědí, nebo si nejsou jisti, jak jsou souhlasy se sdílením údajů třetím stranám nastaveny. Zde se nachází prostor pro zdůraznění důležitosti čtení smluvních podmínek, nebo nastavování přijímání a ukládání souborů cookie.

Graf 14: Výsledky otázky č. 14



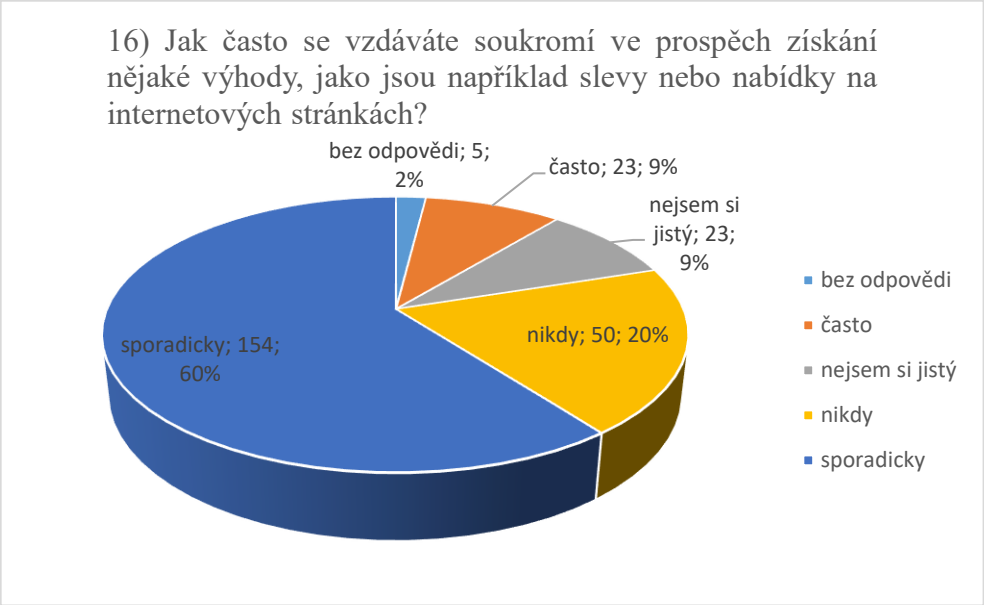
Minimum uživatelů (13 %) uvádí, že neví, zda je nějak omezeno shromažďování polohových dat v jejich zařízeních. Ve většině případů (62 %) dle výsledků uživatelé sběr geolokačních údajů omezují. Ostatní pak nastavení neomezují.

Graf 15: Výsledky otázky č. 15



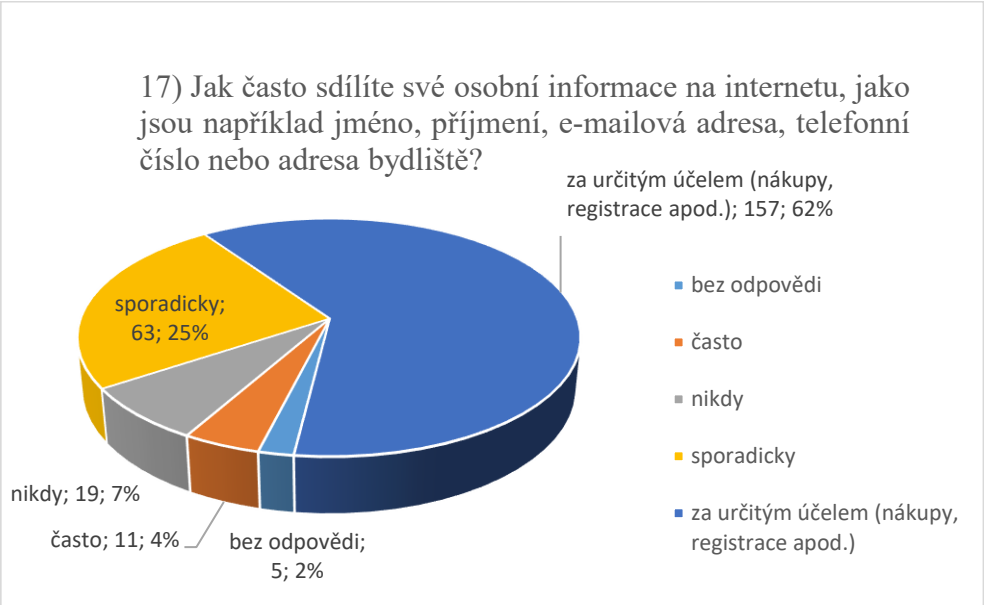
Z dotázaných respondentů jich 81% má zájem kontrolovat možnosti nastavení soukromí služeb, které využívají (11 % minimálně při prvním použití služeb), ostatní v určitém intervalu pravidelně. Téměř pětina však své soukromí a bezpečnost neřeší.

Graf 16: Výsledky otázky č. 16



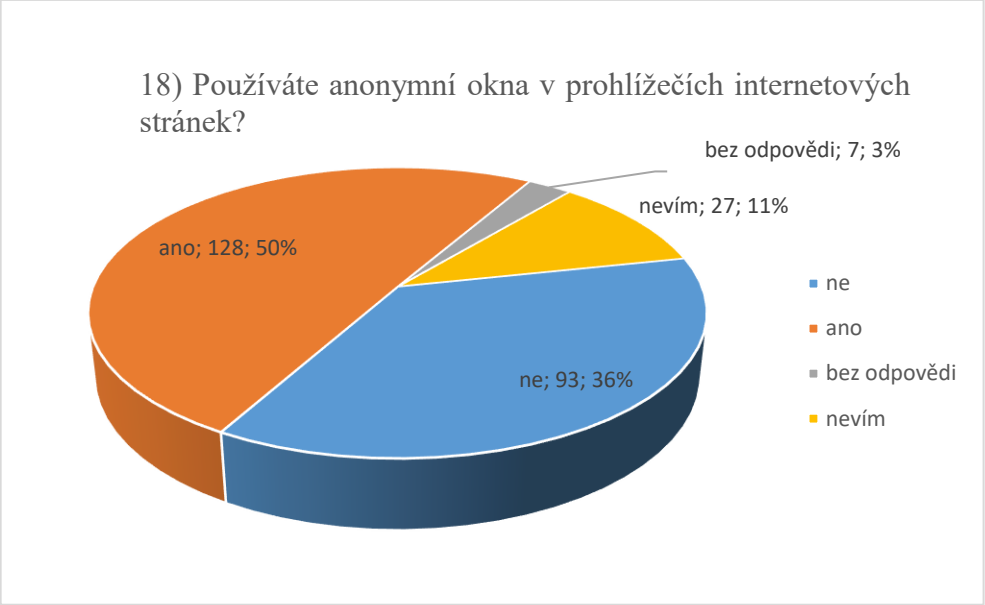
Na dotaz, jak často se uživatelé vyměňují své soukromí a osobní údaje za výhody například formou slev odpovědělo 20 % dotázaných, že nikdy, 60 % sporadicky, což považuji za dobrý výsledek. Nicméně téměř vždy jde mezi uživatelem a provozovatelem služeb formou registrace a souhlasem s obchodními podmínkami o obchod s osobními údaji, minimálně pro marketingové účely. Je tedy velmi důležité číst obchodní podmínky.

Graf 17: Výsledky otázky č. 17



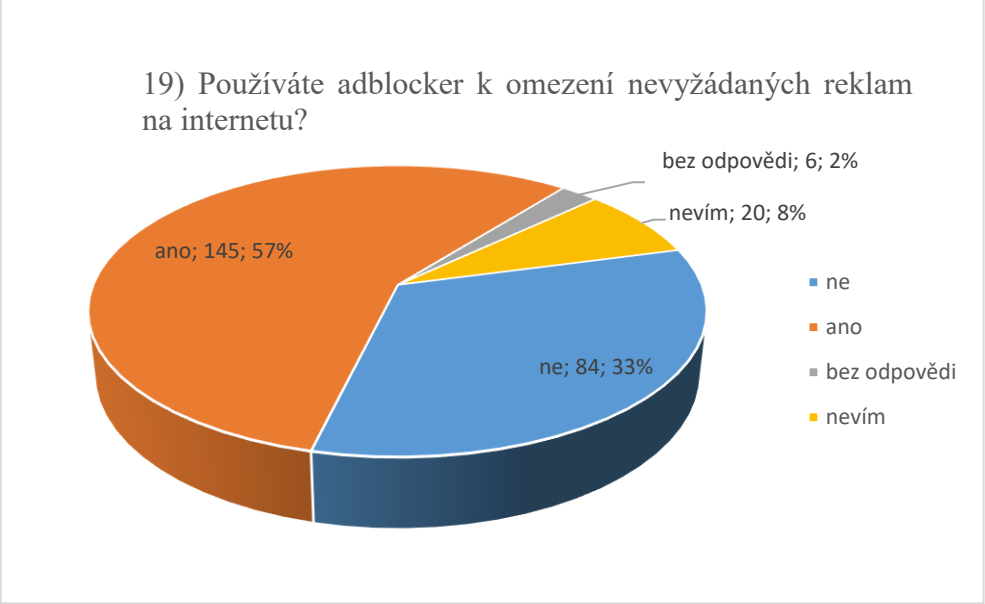
Podobně jako u předchozí otázky jsou uživatelé ve sdílení uvedených citlivých údajů na internetu zdrženliví a 62 % dotázaných uvádí, že je sdílí pouze za legitimním účelem. Především nákupů v e-shopech a registracích. Čtvrtina uvádí, že osobní údaje sdílí pouze sporadicky.

Graf 18: Výsledky otázky č. 18



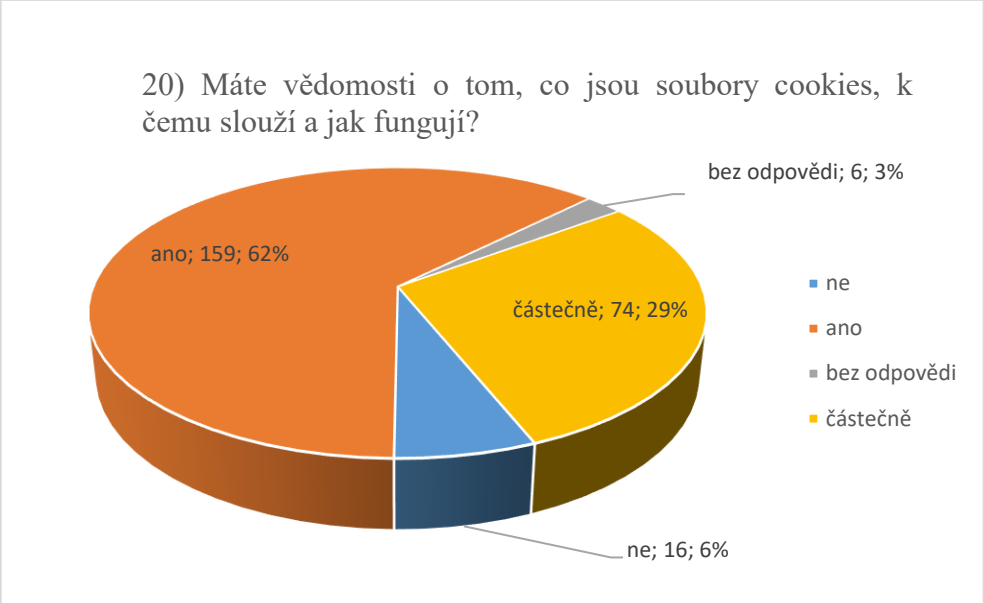
Z výsledků grafů vyplývá, že polovina uživatelů zná a využívá možnosti používání anonymních oken v internetových prohlížečích, které omezují digitální stopu uživatele (bez ukládání historie, souborů cookies a hesel). Nicméně je důležité zdůraznit, že částečně skrývá Vaší aktivitu na internetu, ale neučiní Vás neviditelnými.

Graf 19: Výsledky otázky č. 18



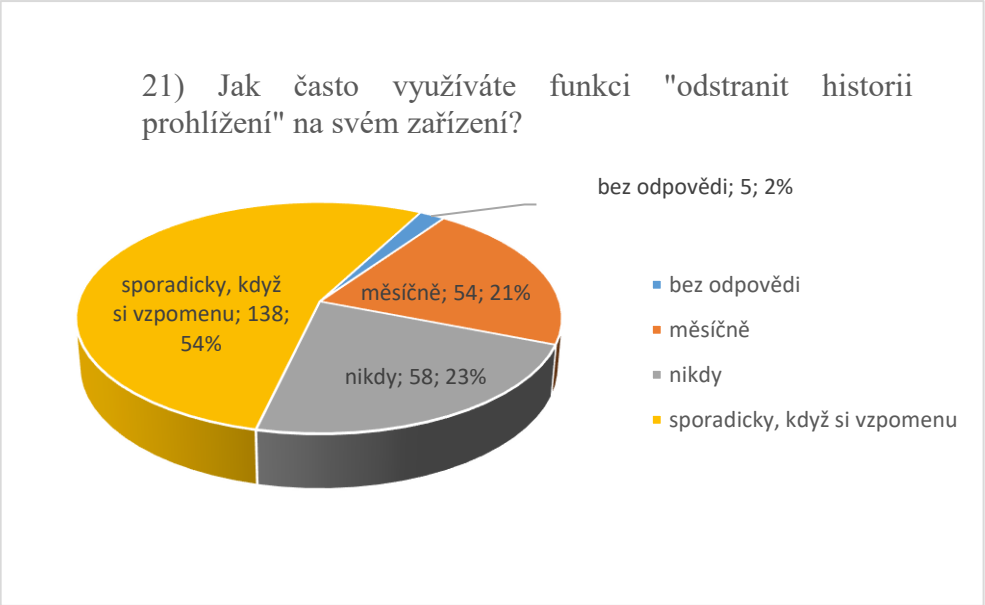
I z odpovědí na tuto otázku lze vyčíst, že uživatelé znají a vyžívají možnosti doplňků do internetových prohlížečů, které dokáží omezit a blokovat nežádoucí reklamy a soubory. Kladně odpovědělo 57 %, negativně 33 % uživatelů. Ostatní si nejsou jisti, ale je možné, že tyto doplňky v prohlížeči mají.

Graf 20: Výsledky otázky č. 19



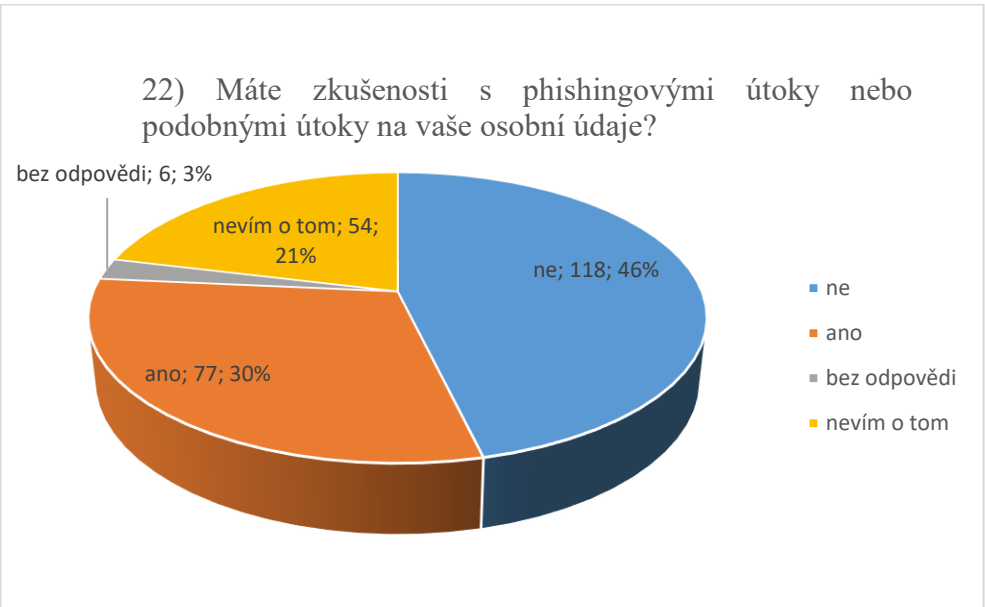
Většina dotázaných (zahrnuje odpověď „ano“ a „částečně“) ví, nebo má povědomí o souborech cookies a jejich významu. Tento převážně kladný stav přikládám tomu, že od 1. ledna 2022 nestačí, aby provozovatel www stránek pouze informoval, že cookies používá. Díky novele zákona č. 127/2005 Sb. má nyní uživatel právo se rozhodnout, zda web může cookies používat.

Graf 21: Výsledky otázky č. 21



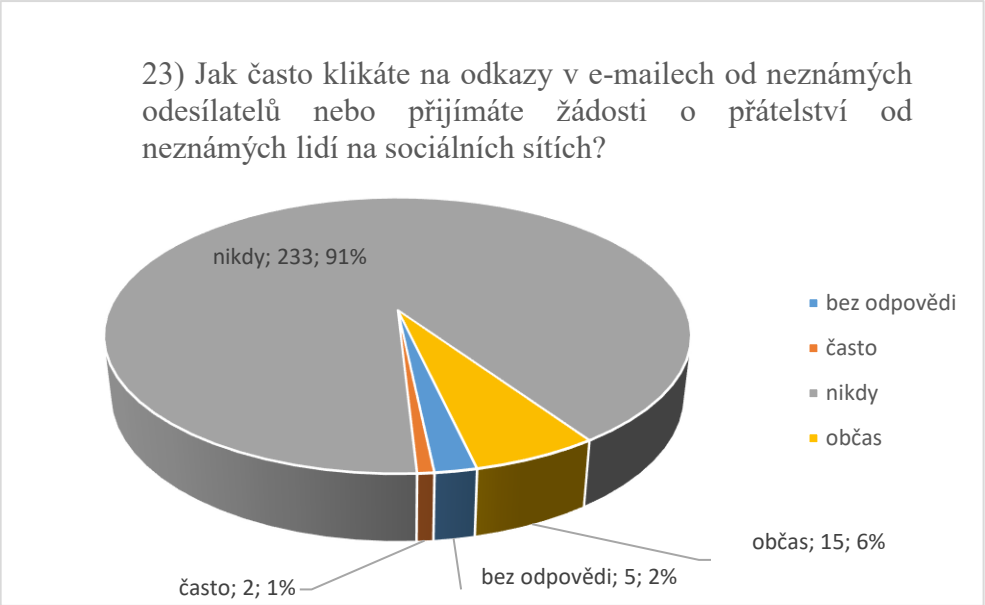
I v této navazující otázce na informační bezpečnost a využívání možností prohlížečů internetových stránek odpověděli uživatelé ze tří čtvrtin kladně (odpovědi „sporadicky“ a „měsíčně), že omezují historii prohlížení www stránek.

Graf 22: Výsledky otázky č. 22



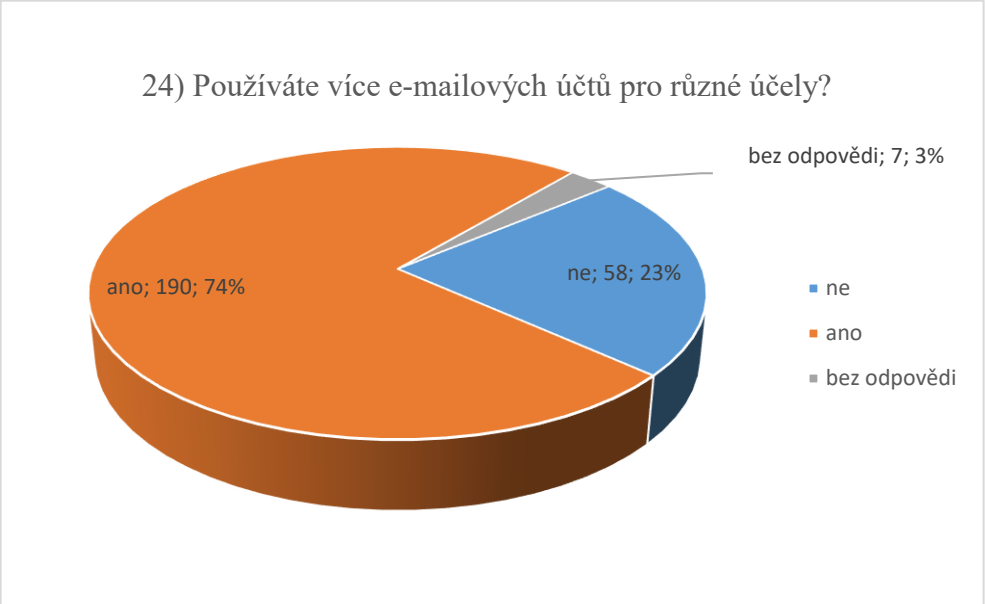
Ze sedmdesáti sedmi uživatelů (30 %), kteří uvádějí zkušenost s phishingovými útoky na jejich údaje se jich stalo dvacet dva obětí „hacknutí“ jejich účtu na sociální síti nebo e-mailu (otázka č. 5). Sedmnáct z těchto dvaadvaceti zároveň uvedlo, že využívají dvou faktorovou autentizaci.

Graf 23: Výsledky otázky č. 23



Na takto položený dotaz zodpovědělo více jak 90 % uživatelů striktně, že nikdy nepřijímají žádosti na přátelství od neznámých lidí ze sociálních sítí a neklikají na odkazy z cizích zdrojů. Tento výsledek hodnotím z osobní zkušenosti velmi kladně a vnímám velký posun v přístupu uživatelů směrem zvýšení vlastní bezpečnosti zodpovědným přístupem.

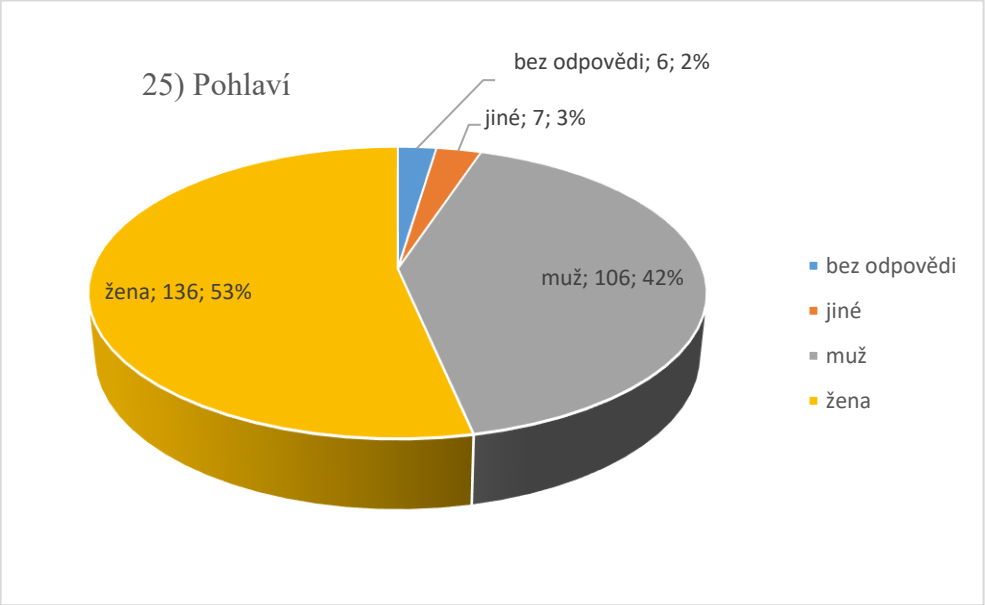
Graf 24: Výsledky otázky č. 24



Využívání více e-mailových účtu a uživatelských účtů (práce, soukromí, nákupy, pro „pochybné služby“ apod.) je z hlediska bezpečnosti důležité. Výsledek téměř tři čtvrtiny je důkazem, že se uživatelé chovají zodpovědně.

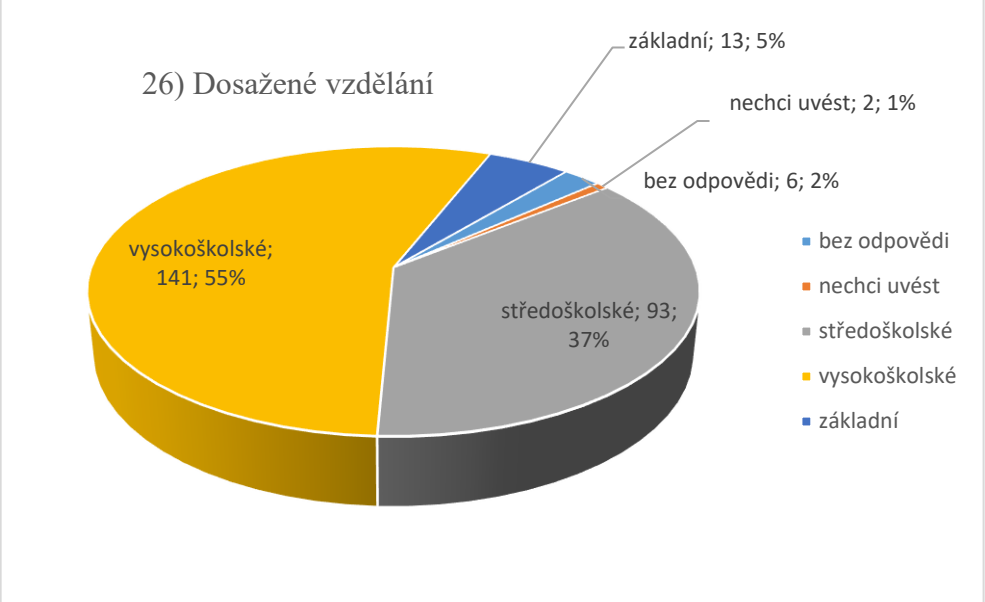
Následující grafy prezentují zastoupení respondentů, kteří se zúčastnili vyplnění průzkumu. Zobrazují rozložení dle jejich pohlaví, dosaženého vzdělání a věku:

Graf 25: Výsledky otázky č. 25



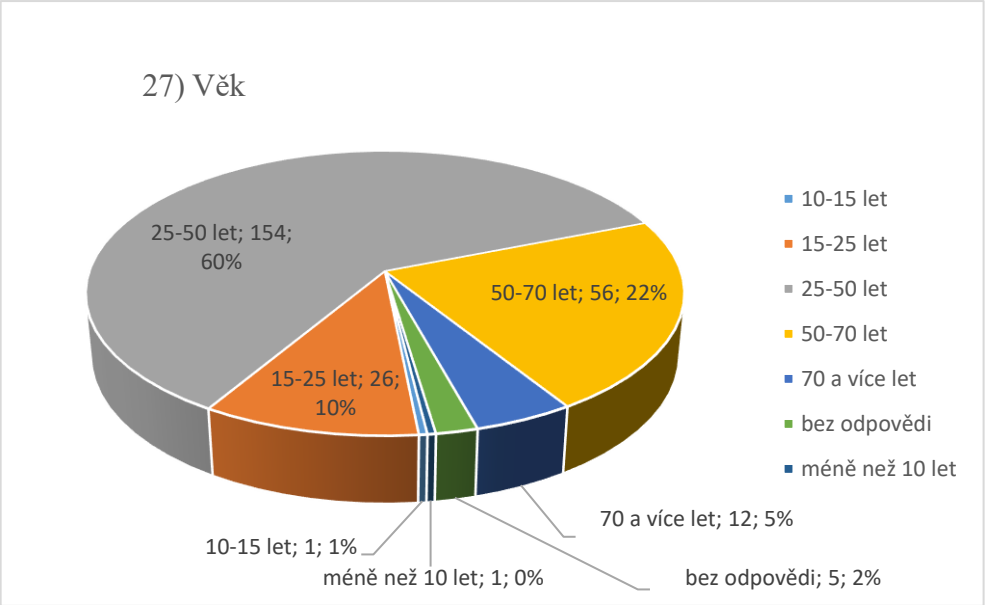
Z dotázaných respondentů lze pozorovat lehce převahu žen na úkor mužů a dalších odpovědí.

Graf 26: Výsledky otázky č. 26



Z dotázaných žen bylo 8 se základním vzděláním, 54 se středoškolským a 74 s vysokoškolským. Z dotázaných mužů a ostatních odpovědí 5 vzdělání neuvedlo, 8 se základním vzděláním, 39 se středoškolským a 67 s vysokoškolským.

Graf 27: Výsledky otázky č. 27



Nejvyšší podíl na odpovědích mají lidé ve věku 25 – 50 let. Dále lze pozorovat i vyšší podíl starší generace (50 – 70 let a 70 a více). Naopak cca 13 % respondentů spadá do kategorie pod 25 let (odpovědi „15 – 25 let“ a ostatní).

5.4 Analýza rizik hrozeb

Následující analýza rizik uvádí pravděpodobnost kybernetických hrozeb (způsoby útoků a rizika) a následky jejich negativního dopadu na určená aktiva. Nejdříve byla provedena identifikace aktiv, na kterou navazuje určení zdrojů hrozeb.

V dalších krocích jsou ohodnoceny pravděpodobnosti výskytu daných hrozeb a vektory útoků, vycházejících z potřebných sil (útočníci), prostředků k vykonání útoku a jejich četnosti. Dále je ohodnocen negativní dopad těchto útoků na zájmová aktiva. Hodnotící kritéria jsou určena expertním odhadem. Výsledkem je výpočet celkové míry rizika dle jejich závažnosti.

Tabulka 10. Vymezení chráněných aktiv.

Aktiva	**Upřesnění**
Život a zdraví	Účinek na zdraví a život uživatele vlivem útoku. Může se jednat například o účinek na psychické zdraví vlivem excitace citlivých údajů a fotografií, až po eskalaci v sebevraždu jako důsledek kyber šikany.
Majetek	Finanční zhmotnění výsledku kybernetického útoku. Například: krádeže údajů z platebních karet, podvodné vylákání finančních prostředků, využití zařízení k těžbě virtuálních měn a zničení hardware.
Informace	Útoky na informační aktiva a narušení důvěrnosti, integrity a dostupnosti těchto dat.

Tabulka 11. Vymezení a identifikace hrozeb.

Zdroj hrozby	**Upřesnění**
Vnější útoky	Veškeré útoky z vnějšího perimetru – útoky z prostředí internetu, ale i fyzického prostoru.
Technické chyby	Technické chyby (HW i SW), například selhání hardware a následná ztráta dat, nefunkční zálohování apod.).

5.4.1 Pravděpodobnost technické chyby

Určení pravděpodobnosti způsobu a vektoru daných útoků vychází ze součtu bodů těchto hodnotících kritérií:

- **Zdroj útoku,** technické chyby (selhání) a vektor provedení daného způsobu útoku. Škála od 7 do 1 bodu, kdy 7 bodů znamená zdroj útoku amatéra (uživatel, script kiddies), 1 bod je koordinovaný, dlouhodobě připravovaný útok jedné, nebo více osob.
- **Prostředky** k provedení daného způsobu útoku. Škála od 7 do 1 bodu, kdy 7 bodů značí, že útok je možný se základními prostředky, 1 bod představuje složitý útok, vyžadující sofistikované nástroje.
- **Výskyt**, nebo četnost daného útoku (hrozby, chyby). Škála od 7 do 1 bodu, kdy 7 bodů je velmi četný útok, 1 bod znamená, že útok, chyba, se nevyskytuje, nebo je jeho/její četnost minimální.

Tabulka 12. Pravděpodobnost způsobu útoku

	Pravděpodobnost			
Identifikace hrozících způsobů útoku a rizik	**Zdroj útoku**	**Prostře-dky**	**Výskyt**	**Součet (P)**
Ztráta nešifrovaného zařízení	7	7	4	18
Zneužití přístupu k zařízení s možností neautorizovaného přístupu.	6	7	5	18
Neaktualizovaný operační systém	5	7	6	18
Ztráta šifrovaného zařízení	7	7	4	18
Krádež nešifrovaného zařízení	6	6	5	17
Zavlečení škodlivého SW	4	7	6	17
Krádež šifrovaného zařízení	6	6	5	17
Únik citlivých dat	7	6	3	16
Útok phishing	5	3	7	15
Výpadek napájení	5	6	3	14

Krádež nebo prolomení hesla	4	3	6	13
SPAM	4	3	6	13
Fyzické zničení zařízení, nebo primárního datového aktiva	7	4	1	12
Kompromitace (prolomení účtu sociální sítě)	4	3	5	12
Útok sociálním inženýrstvím	4	3	5	12
Kompromitace (prolomení e-mailu)	5	3	3	11
Kompromitace (škodlivým software, ostatní)	5	2	4	11
Útok malware	3	3	5	11
Selhání hardware	4	5	2	11
Průnik z vnější sítě do vnitřní sítě	2	3	5	10
Selhání datových nosičů	3	5	2	10

Hodnotící kritéria jsou určena expertním odhadem. Výsledky ve sloupci „Součet (P)“ jsou dány součtem hodnot v jednotlivých sloupcích (Zdroj útoku, Prostředky, Výskyt). Tabulka je seřazena sestupně dle sloupce „Součet (P)“.

5.4.2 Určení negativního dopadu

Určení negativního dopadu vektoru daných útoků vychází ze součtu bodů hodnotících kategorií (dopad na život a zdraví, majetek, finance a informace).

- Dopad na **životy a zdraví**. Škála od 7 do 1 bodů, kdy 7 bodů je fatální újma (smrt jedné, či více osob apod.), 1 bod – drobná psychická újma.
- Dopad na **majetek**. Škála od 7 do 1 bodů, kdy 7 bodů je velká finanční újma, až po 1 bod – bez finančního dopadu.
- Dopad na **informace**. Škála od 7 do 1 bodů, kdy 7 bodů – excitace, nebo úplná ztráta dat, až po 1 bod – bez dopadu na data.

Tabulka 13. Určení negativního dopadu

	Negativní dopad			
Určení negativního dopadu útoku (hrozby)	**Zdraví a život**	**Maje-tek**	**Infor-mace**	**Součet (N)**
Zneužití přístupu k zařízení s možností neautorizovaného přístupu.	5	7	7	19
Ztráta nešifrovaného zařízení	4	6	6	16
Krádež nešifrovaného zařízení	4	6	6	16
Kompromitace (prolomení e-mailu)	5	6	5	16
Únik citlivých dat	2	6	7	15
Krádež nebo prolomení hesla	4	4	6	14
Selhání datových nosičů	5	2	7	14
Fyzické zničení zařízení, nebo primárního datového aktiva	3	4	6	13
Průnik z vnější sítě do vnitřní sítě	2	5	6	13
Útok phishing	4	5	3	12
Kompromitace (prolomení účtu sociální sítě)	4	4	4	12
Útok sociálním inženýrstvím	3	5	4	12
Ztráta šifrovaného zařízení	4	5	2	11
Krádež šifrovaného zařízení	4	5	2	11
Útok malware	3	4	3	10
Zavlečení škodlivého SW	2	3	3	8
SPAM	3	4	1	8
Kompromitace (škodlivým software, ostatní)	3	3	2	8
Neaktualizovaný operační systém	1	1	2	4
Selhání hardware	1	2	1	4

Výpadek napájení	1	1	1	3

Hodnotící kritéria jsou určena expertním odhadem. Výsledky ve sloupci „Součet (N)“ jsou dány součtem hodnot v jednotlivých sloupcích (Zdraví a život, majetek, informace). Tabulka je seřazena sestupně dle sloupce „Součet (N)“.

5.4.3 Celkové vyhodnocení míry ohroženosti

Celkové vyhodnocení je dáno **součinem** sečtených hodnot celkové pravděpodobnosti „Součet (P)“ a celkového negativního dopadu „Součet (N)“:

Celková míra ohrožení = (součet pravděpodobností) **x (s**oučet negativního dopadu).

Tabulka 14. Celkové vyhodnocení míry ohroženosti

Určení negativního dopadu útoku (hrozby)	**Součet (P)**	**Součet (N)**	**Celkem P x N**
Zneužití přístupu k zařízení s možností neautorizovaného přístupu.	26	45	342
Ztráta nešifrovaného zařízení	22	38	288
Krádež nešifrovaného zařízení	22	38	272
Únik citlivých dat	22	37	240
Ztráta šifrovaného zařízení	13	24	198
Krádež šifrovaného zařízení	13	24	187
Krádež nebo prolomení hesla	20	34	182
Útok phishing	15	27	180
Kompromitace (prolomení e-mailu)	21	37	176
Fyzické zničení zařízení, nebo primárního datového aktiva	19	32	156
Kompromitace (prolomení účtu sociální sítě)	16	28	144
Útok sociálním inženýrstvím	16	28	144
Selhání datových nosičů	21	35	140

Zavlečení škodlivého SW	11	19	136
Průnik z vnější sítě do vnitřní sítě	19	32	130
Útok malware	13	23	110
SPAM	9	17	104
Kompromitace (škodlivým software, ostatní)	10	18	88
Neaktualizovaný operační systém	6	10	72
Selhání hardware	5	9	44
Výpadek napájení	4	7	42

Výsledná tabulka je seřazena sestupně dle sloupce „Celkem“.

Z výsledku analýzy vyplývá, že vzhledem k definovaným aktivům se jako hrozba s nejvyšší relevancí jeví zneužití přístupu k nezabezpečenému zařízení (bez ochrany heslem apod.), případně ztráta nebo zcizení zařízení nezabezpečených šifrováním a úniky citlivých dat. Jako vhodné opatření se tedy jeví zabezpečení kryptografií, popřípadě u přenosných zařízení (notebook, projektor apod.) použití bezpečnostních zámků typu „Kensington lock“. Ztráta, nebo zcizení zašifrovaného zařízení s vhodným typem zálohování dat tak nese jen riziko materiální škody.

V druhé polovině výsledků analýzy nalezneme již hrozby a rizika spojené s kybernetickým prostředím, jako jsou útoky phishingu, škodlivého software a kompromitace e-mailových účtů a účtů na sociálních sítích. Mezi výsledky s nejnižší relevancí, avšak neméně důležité, patří rizika spojené s neaktuálním programovým vybavením, selháním hardware a výpadky napájení.

Na bezpečnost komunikačních systému, které uživatel využívá, se musí nahlížet komplexně. Stejně tak, jako že systém je silný, jako jeho nejslabší článek, vyplývá, že zvyšováním odolnosti jednotlivých subsystémů a částí snižujete zranitelnost celého systému.

ZÁVĚR

Diplomová práce byla zaměřena na digitální stopu jednotlivce v kyber prostou a prostředí internetu. Zdánlivá anonymita tohoto prostředí vybízí k trestné činnosti a rychlost sdílení a přenosu informací tomu ještě více napomáhá. Na rozdíl od reálného světa tak útočníci mohou přicházet z velké vzdálenosti, aniž by museli fyzicky opustit svou „kancelář“. Proto je velmi důležité klást důraz na informační bezpečnost a především bezpečnost jednotlivce, který nemá dostatek prostředků na její zajištění.

V teoretické části byly uvedeny základní pojmy v oblasti informační bezpečnosti a druhy hrozeb v kyber prostoru, včetně ochrany informací. Součástí této ochrany je i právní rámec, který se věnuje ochraně informací ve směrech národní bezpečnosti a ochrany jednotlivce. Právě legislativní úprava pro jednotlivce je řešena méně a zastupuje jí z velké části rámec pro trestné činy z reálného světa. Hlavní teoretickou částí je digitální stopa jednotlivce, ve které je uvedeno, co je myšleno digitální stopou, zda jí lze využít, zneužít, omezit, či celkově odstranit. Bylo vysvětleno, že fragmenty digitální stopy (důsledek interakce uživatele s informačními systémy) lze najít nejenom v prostředí internetu, ale vzhledem k povaze informace především na fyzické stopě – datovém médiu. Poslední teoretickou částí byla kybernetická bezpečnost a základy anonymity.

Praktická část vychází z teoretických základů a na základě pokusů s různými druhy paměťových médií ukazuje, jaké fragmenty digitální stopy lze z forenzního hlediska najít. Tato média byla podrobena různým metodám s cílem digitální stopu omezit běžně dostupným programovým vybavením. Druhou částí analýzy bylo vyhodnocení způsobu mazání pevných disků. Rizikovost chování uživatele byla vyhodnocena na základě dotazníkového šetření se zaměřením na informační bezpečnost a chování v internetovém a kyber prostředí. Poslední oddíl praktické části zahrnuje analýzu rizik v kyber prostoru na základě pravděpodobnosti způsobu útoku a určení negativního dopadu.

Celá práce, její teoretická i praktická část je navržena a zpracována tak, aby naplnila a odrážela všechny body jejího zadání. Věřím, že tohoto cíle se mi podařilo dosáhnout a práce bude přínosná.

SEZNAM POUŽITÉ LITERATURY

[1] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti. 3. aktualizované vydání. Praha: AFCEA, 2015, s. 37. Online. Dostupné z https://www.govcert.cz/download/slovnik/vykladovy_slovnik_KB_3_vydani.pdf

[2] MOLNÁR, Zdeněk. Podnikové informační systémy. Praha: ČVUT, 2009. 195s. s. 13.

[3] MITNICK, Kevin, SIMON, William. Umění klamu. 1. vyd. Gliwice: Helion, 2003. 345 s. ISBN 83-7361-210-6.

[4] SMEJKAL, Vladimír. Kybernetická kriminalita. 3. rozšířené a aktualizované vydání. Plzeň: Aleš Čeněk, s.r.o., 2022. 1166 s. ISBN: 978-80-7380-849, strana 650.

[5] BRECHLEROVÁ, Dagmar. Digitální stopy a jejich odstraňování. In: Computerworld [online]. 2016 [cit. 2018-05-06]. Dostupné z: https://computerworld.cz/securityworld/digitalni-stopy-a-jejich-odstranovani-53197

[6] Hambridge, S., "Netiquette Guidelines", FYI 28, RFC 1855, DOI 10.17487/RFC1855, October 1995, dostup-ný z internetu: https://www.rfc-editor.org/info/rfc1855

[7] Zákon č. 181/2014 Sb. - Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

[8] Vyhláška č. 82/2018 Sb. - Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

[9] Zákon č. 40/2009 Sb. - Zákon trestní zákoník.

[10] Zákon č. 141/1961 Sb. - Zákon o trestním řízení soudním (trestní řád).

[11] CYBERCRIME, JUDr. Jan Kolouch, Ph.D. Vydavatel: CZ.NIC, z. s. p. o., 1. vydaní, Praha 2016, kniha vyšla jako 14. publikace v Edici CZ.NIC. ISBN 978-80-88168-18-8

[12] CYBERSECURITY, doc. JUDr. Jan Kolouch, Ph.D., Bc. Pavel Bašta, Andrea Kropáčová, Bc. Martin Kunc, 1. vydání, Praha 2019, kniha vyšla jako 20. publikace v Edici CZ.NIC. ISBN 978-80-88168-34-8

[13] INTERNET JAKO OBJEKT PRÁVA: hledání rovnováhy autonomie a soukromí, MATEJKA, J. Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.

1. vydání, Praha 2013, kniha vyšla jako 6. publikace v Edici CZ.NIC. ISBN 978-80-904248-7-6

[14] ZODPOVEDNOSŤ NA INTERNETE podľa českého a slovenského práva, Martin Husovec,Vydavatel: 1. vydání, Praha 2014, kniha vyšla jako 8. publikace v Edici CZ.NIC. ISBN 978-80-904248-8-3

[15] Buď pánem svého prostoru, přeloženo z anglického originálu knihy Own your space. 1.vydání, 2010, vydáno nakladatelstvím 100 Page Press, Inc, CA. Online verze je dostupná na ownyourspace.net.

[16] BÁJEČNÝ SVĚT ELEKTRONICKÉHO PODPISU, Jiří Peterka, vydavatel: CZ.NIC, z. s. p. o., Americká 23, 120 00 Praha 2, Edice CZ.NIC,www.nic.cz

[17] KRYPTOGRAFIE OKOLO NÁS, Karel Burda, vydavatel: CZ.NIC, z. s. p. o. Milešovská 5, 130 00 Praha 3, Edice CZ.NIC, www.nic.cz, 1. vydání, Praha 2019. Kniha vyšla jako 24. publikace v Edici CZ.NIC. ISBN 978-80-88168-52-2

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

autentizace	Authentication (ověření a identifikace identity)
autorizace	Authorization (oprávnění pro přístup, nebo vykonání určité činnosti)
BTS	(BTS - Base Transmitting Station), základní vysílací stanice
CERT	Computer Emergency Response Team – „Skupina pro řešení bezpečnostních problémů“.
CIA	Confidentiality (důvěrnost), Integrity (integrita), Availability (dostupnost)
CMS	content management systém (systémy na správu obsahu)
Cookie	Cookie (sušenka), soubor uložený ve www prohlížeči klienta, ve kterém je uložené malé množství dat určených především k rozlišení uživatelů (přihlášená relace), uživatelské předvolby apod.
CSIRT	Z anglického Computer Security Incident Response Team („Skupina pro reakci na počítačové bezpečnostní události“)
cyberlulling	Kyberšikana
DDoS	Distributed Denial of Service, distribuované odepření služby
DNS	Domain Name System (systém doménových jmen)
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Service, odepření služby
Exif	Exchangeable image file format),
firmware	programové vybavení, které slouží k ovládání jednoduchých a embedded zařízení (např. kalkulačka, záznamník, některé počítačové komponenty)
GDPR	General Data Protection Regulation, (obecné nařízení o ochraně osobních údajů, zkráceně ONOOÚ)
HASH	výsledek jednosměrné kryptografické funkce, využití k ověření integrity souborů a zabezpečení hesel

IaaS	Infrastructure as a Service (infrastruktura jako služba)
infotaiment	(information + entertaiment) spojení slov informace a zábava.
IoT	Internet of things (internet věcí)
ISMS	Information Security Management System (systémy řízení bezpečnosti informací)
ISO	International Organization for Standardization (mezinárodní organizace zabývající se tvorbou norem)
Malware	malicious software
MiM	Men in the Middle (doslova Muž uprostřed), způsob útoku, ve kterém stojí útočník uprostřed komunikace mezi obětí a se službou s kterou komunikuje, tuto komunikaci odposlouchává.
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OČTŘ	orgány činé v trestním řízení
OS	Operating systém (operační systém)
OSINT	Open Source Intelligence (vyhledávání v otevřených zdrojích)
PaaS	Platform as a Service (platforma jako služba)
Ransomware	ransom software (výkupné +s oftware)
RFC dokument	request for comments (forma dokumentů specifikujících internetové protokoly a technologie pro rozvoj internetu)
SaaS	Software as a Service (software jako služba)
Session Hijacking	Útok, při kterém se útočník snaží zmocnit uživatelského SID (Session ID), které identifikuje jeho přihlášení
SPAM	nevyžádaná elektronická pošta
TCP/IP	Transmission Control Protocol / Internet Protocol (sada komunikačních protokolů používaných v počítačových sítích)
VPN	Virtual Private Network (virtuální privátní síť)

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: ANALÝZA SYSTÉMOVÝCH DISKŮ

Tabulka 15. Výsledky analýzy pevného disku (vzorek #01)

	250GB systémový disk (#01)		
Artefakty	Původní	CC	CC_wipe
Classifieds URLs	12	12	11
Cloud Services URLs	68	68	42
Facebook URLs	189	168	132
Google Analytics First Visit Cookies	18	0	0
Google Searches	48	46	0
Identifiers - Device	139	144	140
Identifiers - People	152	149	126
Loccaly Accessed Files and Folders	258	248	237
Parsed Search Queries	192	131	111
Passwords and Tokens	5	2	2
Pornography URLs	2	1	1
Rebuilt Desktops - Windows	1	1	1
Rebuilt Webpages	145	134	136
Social Media URLs	113	97	60
User Accounts	8	6	6
Web Char URLs	4	14	10
Chrome Extensions	41	41	41
Edge Chromium Autofill	10	0	0
Edge Chromium Bookmarks	1	1	1
Edge Chromium Cache Records	2106	1183	1183
Edge Chromium Cookies	328	93	93
Edge Chromium Downloads	11	5	5
Edge Chromium FavIcons	90	52	52
Edge Chromium Keyword Search Terms	8	5	5
Edge Chromium Login	3	0	0
Edge Chromium Shortcuts	44	4	4
Edge Chromium Web History	43	29	29
Edge Chromium Web Visit	51	31	31
Edge/Internet Explorer 10-11 Content	582	568	451
Edge/Internet Explorer 10-11 Cookies	36	21	21
Edge/Internet Explorer 10-11 Daily/Weekly History	233	229	213
Edge/Internet Explorer 10-11 Dependency Entries	4	4	5
Edge/Internet Explorer 10-11 Main History	176	164	156
Google Analytics First Visit Cookies Carved	5	5	5
Google Analytics URLs Carved	16	16	16
Internet Explorer Daily History	2	2	2
Internet Explorer Favorites	301	30	30

Internet Explorer Main History	1	1	1
Internet Explorer Typed URLs	4	3	3
Opera Autofil	1	1	1
Opera Cache Records	2076	2076	2076
Opera Cookies	233	233	233
Opera Downloads	3	3	3
Opera FavIcons	265	265	240
Opera Keyword Search Terms	3	3	3
Opera Web History	46	45	40
Opera Web Visits	72	72	70
Potential Browser Activity	65518	63458	50389
Safari History	2	2	1
WebKit Browser Seassion/Tabs (Carved)	67	67	67
WebKit Browser Web History (Carved)	197	191	131
KakaoTalk Shared Pictures - Windows	2	2	2
QQ	10	9	7
Audio	642	642	460
Carved Audio	976	963	788
Photoshop files	85	81	63
Pictures	86095	84471	69358
Potential Facebook Pictures	70	70	70
Thumbnail Pictures	2321	2042	2044
Videos	676	672	557
VLC Recently Played Files	6	6	6
Eml(X) Files	2	2	2
CSV Documents	1	1	1
Microsoft Excel Documents	66	66	63
Microsoft PowerPoint Documents	22	22	22
Microsoft Word Documents	333	336	312
OpenOffice Calc Documents	1	1	1
OpenOffice Writer Documents	22	22	22
PDF Documents	154	154	137
RTF Documents	9774	9782	3385
Text Documents	626	629	521
WordPerfect Files	1	1	1
Apple Disk Images	1	1	1
Feature Usage	30	32	32
Instaled Mictosoft Programs	185	185	185
Instaled Programs	13	13	13
Windows Defender Logs	3	3	3
$LogFile Analysis	14610	9467	2
AmCache Device Containers	24	24	24
AmCache Driver Binaries	376	376	376
AmCache Driver Packages	2	2	2

AmCache File Entries	376	375	374
AmCache Pnp Devices	104	104	107
AmCache Program Entries	146	106	146
AmCache Shortcuts	117	117	117
AutoRun Items	369	369	369
Default Browser	2	2	2
File Associations	1105	1105	1105
File System Information	3	3	3
Jump Lists	241	221	222
Known DLLs	32	32	32
LNK Files	1189	1229	1024
MRU Folder Access	5	3	3
MRU Opened-Saved Files	21	13	13
MRU Recent Files & Folders	160	136	136
MRU Run Commands	2	2	2
MUICache	411	420	665
Network Interfaces (Registry)	6	6	6
Network Profiles	2	2	2
Operating System Information	1	1	1
Prefetch Files - Windows 8-10	769	769	769
Recycle Bin	45	43	43
Scheduled Tasks	209	221	209
Shellbags	96	96	96
Shim Cache	741	741	741
SRUM Application Resource Usage	155	155	155
SRUM Energy Usage (Long Term)	11	11	11
SRUM Network Connections	1	1	1
SRUM Network Usage	23	23	23
SRUM Push Notification Data	5	5	5
Startup Items	16	17	17
System Services	639	619	636
Timezone Information	1	1	1
User Accounts - Windows	9	9	9
UserAssist	144	94	98
Windows Event Logs	134905	133827	130365
Windows Event Logs - Firewall Events	962	962	908
Windows Event Logs - Networking Events	94	94	74
Windows Event Logs - Office Alert Events	13	13	17
Windows Event Logs - Script Events	101	117	116
Windows Event Logs - Service Events	281	281	276
Windows Event Logs - Storage Device Events	10	10	18
Windows Event Logs - System Events	58	13	2
Windows Event Logs - User Events	3789	3967	3967
Windows Event Logs - User PNP Events	11	11	11

Windows Notification Center	13	13	13
Windows Timeline Activity	333	346	363
Encrypted Files	32	28	22
Windows Stored Credentials	1	1	1
USB Devices	45	45	45
Your Phone Devices	2	2	2
Google Maps Tiles	27	19	0
Carved Archives (content not searched)	908	909	805
ISO Files	1	1	1
QuickBooks Files	9	9	9
Celkem	**339813**	**327920**	**279234**

Tabulka 16. Výsledky analýzy pevného disku (vzorek #02)

	250GB systémový disk #02		
Artefakty	Původní	CC	CC_wipe
Classifieds URLs	3913	2524	2523
Cloud Passwords and tokens	26	23	23
Cloud Services URLs	11585	5853	5852
Facebook URLs	79439	35697	35694
Google Analytics First Visit Cookies	138	99	99
Google Analytics Referral Cookies	103	71	71
Google Analytics Session Cookies	33	24	24
Google Analytics URLs	2788	2788	2788
Google Maps Queries	1594	612	612
Google Searches	32174	16839	16837
Google Translate	1102	722	722
Identifiers – Device	798	793	787
Identifiers – People	16380	35660	35711
Loccaly Accessed Files and Folders	2771	2650	2650
Parsed Search Queries	4376	2406	2405
Malware/Pishing URLs	39832	34852	20472
Passwords and Tokens	237	201	201
Rebuilt Desktops – Windows	2	3	3
Rebuilt Webpages	70	4	3
Shipping Sites URLs	4	2	2
Social Media URLs	27364	13418	13417
Torrents URLs	25	17	17
User Accounts	86	86	86
Web Char URLs	2133	1042	1042
Chrome Autofill Profiles	4	4	4
Chrome Autofill	322	239	239
Chrome Bookmarks	136	136	136
Chrome Cache Records	2391	710	710
Chrome Cookies	2487	1395	1395
Chrome Downloads	14	7	7
Chrome Extensions	274	303	302
Chrome FavIcons	6538	5272	5272
Chrome Keyword Search Terms	179	111	111
Chrome Logins	190	162	162
Chrome Media History	506	506	506
Chrome Shortcuts	81	41	41
Chrome Sync Accounts	1	1	1
Chrome Top Sites	23	43	43
Chrome Web History	2692	1886	1886
Chrome Web Visits	4506	3151	3151
Edge Chromium Autofill Profiles	6	6	6

Edge Chromium Autofill	18	18	18
Edge Chromium Cache Records	511	125	125
Edge Chromium Cookies	268	246	246
Edge Chromium Current Session	1	1	1
Edge Chromium FavIcons	38	24	24
Edge Chromium Keyword Search Terms	10	6	6
Edge Chromium Logins	38	31	31
Edge Chromium Media History	2	2	2
Edge Chromium Web History	18	10	10
Edge Chromium Web Visits	22	12	12
Edge Favorites	2	4	4
Edge Top Sites	8	16	16
Edge Typed URLs	6	12	12
Edge-Internet Explorer 10-11 Content	3346	3119	3119
Edge-Internet Explorer 10-11 Cookies	1091	716	716
Edge-Internet Explorer 10-11 Daily-Weekly History	2006	1926	1926
Edge-Internet Explorer 10-11 Dependency Entries	23	5	5
Edge-Internet Explorer 10-11 Downloads	9	9	9
Edge-Internet Explorer 10-11 Main History	1858	1418	1418
Firefox Add-ons	92	92	92
Firefox Bookmarks	2508	2508	2508
Firefox Cache Records	19944	360	71
Firefox Cookies	7717	4604	4604
Firefox Downloads	66	23	23
Firefox FavIcons	7096	7098	7098
Firefox FormHistory	2043	1211	1211
Firefox Input History	129	74	74
Firefox SessionStore Artifacts	575	567	565
Firefox Web History	291531	147683	147698
Firefox Web Visits	629049	319698	319698
Flash Cookies	1	1	1
Google Analytics First Visit Cookies Carved	1190	1226	1222
Google Analytics Referral Cookies Carved	183	204	200
Google Analytics Session Cookies Carved	94	113	111
Google Analytics URLs Carved	2977	2989	2989
IE InPrivate-Recovery URLs	19	16	16
Internet Explorer Cache Records	6	11	8
Internet Explorer Cookies	7	7	1
Internet Explorer Favorites	98	99	99
Internet Explorer Typed URLs	5	4	4
Opera Autofill	2	2	2
Opera Bookmarks	12	12	12
Opera Cache Records	466	466	466

Opera Cookies	948	838	838
Opera FavIcons	327	285	285
Opera Logins	1	0	0
Opera Web History	35	31	31
Opera Web Visits	45	38	38
Potential Browser Activity	177717	174302	173957
Safari History	13	12	12
WebKit Browser Session-Tabs (Carved)	54	52	54
WebKit Browser Web History (Carved)	182822	94187	94151
Discord Messages	11	11	11
Pidgin Accounts	2	2	2
QQ	45	50	50
Skype Accounts	4	4	4
Skype Activity	2320	2192	2320
Skype Calls	659	659	659
Skype Chat Messages	7566	7566	7566
Skype ChatSync Messages	9362	9362	9362
Skype Contacts	572	520	572
Skype File Transfer	145	145	145
Skype Group Chat	91	88	91
Skype IP Addresses	4442	4442	4442
Skype Voicemails	3	3	3
Facebook Chat	4	8	3
Facebook Pages	1	6	6
Facebook Status Updates	1	1	0
Audio	1452	1543	1465
Carved Audio	10425	10525	10504
Photoshop files	573	862	856
Pictures	345067	439880	431967
Potential Facebook Pictures	99	123	12
Thumbnail Pictures	792	80	80
Videos	943	1005	975
VLC Recently Played Files	31	31	31
Calendar Events (ICS)	947	947	947
Email Attachments	6411	23622	23622
Eml(X) Files	36446	10663	10620
MBOX Emails	44859	11022	11019
Outlook Emails	1	1	1
CSV Documents	163	204	184
Microsoft Excel Documents	1658	195	195
Hangul Word Processor	5	7	7
Microsoft PowerPoint Documents	989	1098	1098
Microsoft Word Documents	589	914	912
OpenOffice Calc Documents	0	1	1

OpenOffice Writer Documents	1	3	3
PDF Documents	2742	3977	3961
RTF Documents	7235	8368	7257
Text Documents	4388	4205	6939
WordPerfect Files	2	0	2
Apple Disk Images	3	3	3
Virtual Machines	18	18	18
Bitcoin Addresses	1	1	1
Bitcoin Debug Logs	1	1	1
Cryptocurrency Clients	1	1	1
Cryptocurrency Wallets	1	1	1
Google Drive	2	1	1
Feature Usage	95	95	95
Instaled Mictosoft Programs	251	251	251
Instaled Programs	137	137	137
Windows Defender Logs	1	1	0
$LogFile Analysis	6228	14414	118
.DS_Store Records	26	667	667
AmCache Device Containers	25	25	25
AmCache Driver Binaries	446	446	446
AmCache Driver Packages	22	22	22
AmCache File Entries	2074	2076	2076
AmCache Pnp Devices	145	145	145
AmCache Program Entries	449	449	449
AmCache Shortcuts	465	465	465
AutoRun Items	495	499	499
Default Browser	2	2	2
File Associations	1711	1711	1711
File System Information	2	2	2
Jump Lists	4261	173	173
Keyword Searches	12	0	0
Known DLLs	32	32	32
LNK Files	39338	39702	38880
MRU Folder Access	29	1	1
MRU Opened-Saved Files	242	12	12
MRU Recent Files & Folders	1484	326	326
MRU Run Commands	7	0	0
MUICache	343	350	350
Network Interfaces (Registry)	13	18	18
Network Profiles	9	9	9
Operating System Information	1	1	1
Prefetch Files – Windows 8-10	1754	1673	127
Recycle Bin	7	8	6
Scheduled Tasks	300	302	305

Shellbags	12620	12627	12627
Shim Cache	1024	1024	1024
SRUM Application Resource Usage	277046	261	261
SRUM Energy Usage (Long Term)	191	0	0
SRUM Network Connections	2881	1	1
SRUM Network Usage	76696	2	2
SRUM Push Notification Data	3286	0	0
Startup Items	34	34	34
System Services	770	773	773
Timezone Information	1	1	1
User Accounts – Windows	10	10	10
UserAssist	625	395	395
Windows Event Logs – Firewall Events	951	951	951
Windows Event Logs – Office Alert Events	333	0	0
Windows Event Logs – Script Events	627	633	633
Windows Event Logs – Service Events	1596	1602	1602
Windows Event Logs – Storage Device Events	385	386	386
Windows Event Logs – System Events	29	27	27
Windows Event Logs – User Events	4583	4504	4504
Windows Event Logs – User PNP Events	57	56	56
Windows Event Logs	382793	339572	339572
Windows Notification Center	49	31	31
Windows Timeline Activity	1514	82	82
Encrypted Files	1903	590	543
Encryption / Anti-forensic Tools	9	9	10
Windows Stored Credentials	2	2	2
Remote Desktop Protocol	43	42	42
Remote Desktop Protocol Vitmap Cache	3	2	68
USB Devices	56	56	56
Your Phone Devices	2	2	2
Google Maps	175	180	180
Google Maps Tiles	577	24	16
Carved Archives (content not searched)	10034	11607	11583
EGG Archives	1	1	1
ISO Files	2	2	2
QuickBooks Files	3	11	11
Celkem	**2916760**	**1920747**	**1882610**

PŘÍLOHA P II: ANALÝZA DATOVÝCH DISKŮ

Tabulka 17. Analýza pevného disku 250GB (vzorek #04)

	250GB datový disk (vzorek #04)				
Artefakty	Původní	SmSv	RyFo	UpFo	Wipe
Identifiers - Device	5	2	5	3	0
Identifiers - People	121	107	100	0	0
Potential Browser Activity	24	17	17	0	0
WebKit Browser Web History (Carved)	2	2	2	0	0
Carved Audio	1	1	1	1	0
Photoshop files	0	29	29	0	0
Pictures	6480	7958	7917	0	0
Potential Facebook Pictures	3	0	0	0	0
Videos	286	256	256	0	0
Email Attachments	3	0	0	0	0
Outlook Emails	3	0	0	0	0
CSV Documents	15	0	0	0	0
Microsoft Excel Documents	274	182	179	0	0
Microsoft Word Documents	656	497	383	0	0
OpenOffice Calc Documents	1	1	0	0	0
OpenOffice Writer Documents	24	20	4	0	0
PDF Documents	1154	611	551	0	0
RTF Documents	29	29	29	0	0
Text Documents	2	0	0	0	0
$LogFile Analysis	7619	0	0	0	0
File System Information	1	1	1	0	1
LNK Files	1	1	1	0	0
Encrypted Files	26	0	0	0	0
Carved Archives (content not searched)	855	42	42	0	0
Celkem	**17585**	**9756**	**9517**	**4**	**1**

Tabulka 18. Analýza pevného disku 750GB (vzorek #05)

	750GB datový disk (vzorek #05)				
Artefakty	Původní	SmSv	RyFo	UpFo	Wipe
Cloud Services URLs	1	1	0	0	0
Identifiers - Device	21	18	0	0	0
Identifiers - People	38	37	0	0	0
Internet Explorer Favorites	1	0	0	0	0
Potential Browser Activity	80	67	0	0	0
WebKit Browser Web History (Carved)	6	6	0	0	0
QQ	0	4	0	0	0
Audio	826	0	0	0	0
Carved Audio	785	635	0	0	0
Photoshop files	37	141	0	0	0
Pictures	4069	6057	0	0	0
Potential Facebook Pictures	4	0	0	0	0
Videos	1443	1039	0	0	0
Eml(X) Files	1	0	0	0	0
CSV Documents	2	0	0	0	0
Microsoft Excel Documents	10	9	0	0	0
Microsoft Word Documents	137	129	0	0	0
OpenOffice Calc Documents	1	1	0	0	0
OpenOffice Writer Documents	31	21	0	0	0
PDF Documents	142	69	0	0	0
RTF Documents	38	11	0	0	0
Text Documents	38	0	0	0	0
$LogFile Analysis	5080	0	0	0	0
File System Information	1	1	1	1	1
LNK Files	122	122	0	0	0
Prefetch Files - Windows 8/10	41	41	0	0	0
Windows Event Logs	1547	1547	0	0	0
Encrypted Files	41	0	0	0	0
Carved Archives (content not searched)	195	153	0	1	0
QuickBooks Files	0	2	0	0	0
Celkem	**14738**	**10111**	**1**	**2**	**1**

Tabulka 19. Analýza pevného disku 500GB (vzorek #06)

	500GB datový disk (vzorek #06)				
Artefakty	Původní	SmSv	RyFo	UpFo	Wipe
Cloud Services URLs	1	2	1	0	0
Identifiers - Device	3	0	3	3	0
Identifiers - People	1582	1582	1582	0	0
Firefox FormHistory	1	2	1	0	0
Google Analytics Session Cookies Carved	1	2	1	0	0
Potential Browser Activity	54	108	54	0	0
WebKit Browser Web History (Carved)	308	616	308	0	0
Carved Audio	624	1248	624	0	0
Photoshop files	161	322	161	0	0
Pictures	391	782	391	0	0
Videos	310	620	310	9	9
Eml(X) Files	297	594	297	0	0
MBOX Emails	1546	3092	1546	0	0
PDF Documents	3992	7984	3992	0	0
File System Information	1	1	1	1	1
Google Maps	6	12	6	0	0
Google Maps Tiles	34	68	34	0	0
Carved Archives (content not searched)	222	444	222	0	0
Celkem	**9534**	**17479**	**9534**	**13**	**10**

PŘÍLOHA P III: ANALÝZA FLASH DISKŮ

Tabulka 20. Analýza flash disku (vzorek #14)

	Vzorek #14	
Artefakty	Původní	FrSp
Identifiers - Device	3	3
Identifiers - People	15	6
Potential Browser Activity	18	18
WebKit Browser Web History (Carved)	1	1
Carved Audio	3	3
Photoshop files	2	2
Pictures	892	871
Videos	4	4
Microsoft Word Documents	3	3
PDF Documents	13	2
RTF Documents	139	139
Text Documents	8	8
$LogFile Analysis	718	249
File System Information	1	1
Encrypted Files	9	2
Carved Archives (content not searched)	8	5
Celkem	**1837**	**1317**

Tabulka 21. Analýza flash disku (vzorek #15)

	Vzorek #15	
Artefakty	Původní	FrSp
Identifiers - Device	2	2
Identifiers - People	1	
Pictures	20	10
Microsoft Word Documents	1	1
Pages	2	2
PDF Documents	1	1
File System Information	1	1
Carved Archives (content not searched)	2	2
Celkem	**30**	**19**

Tabulka 22. Analýza flash disku (vzorek #16)

	Vzorek #16	
Artefakty	Původní	FrSp
Cloud Services URLs	1	1
Facebook URLs	267	0

Google Searches	2	0
Identifiers - Device	2	2
Identifiers - People	40	27
Parsed Search Queries	1	0
Social Media URLs	11	0
Google Analytics First Visit Cookies Carved	130	0
Google Analytics Referral Cookies Carved	110	0
Google Analytics Session Cookies Carved	100	0
Google Analytics URLs Carved	11	0
Internet Explorer Favorites	1	0
Potential Browser Activity	7986	164
WebKit Browser Web History (Carved)	101	0
Audio	3	0
Carved Audio	241	33
Photoshop files	17	10
Pictures	21264	2441
Videos	86	10
Eml(X) Files	9	6
CSV Documents	2	2
Microsoft Word Documents	9	1
PDF Documents	108	26
PowerPoint Documents	16	15
RTF Documents	41	28
Text Documents	234	194
Apple Disk Images	5	5
$LogFile Analysis	6	1
File System Information	1	1
Encrypted Files	100	70
Encryption / Anti-forensic tools	10	10
Google maps	7	0
Google Maps Tiles	1	0
Carved Archives (content not searched)	137	85
QuickBooks Files	3	3
Celkem	**31063**	**3135**

Tabulka 23. Analýza flash disku (vzorek #17)

	Vzorek #17	
Artefakty	Původní	FrSp
Google Maps Queries	4	0
Identifiers - Device	7	4
Identifiers - People	94	14
Social Media URLs	8	0
Google Analytics First Visit Cookies Carved	1	0

Potential Browser Activity	55	0
WebKit Browser Web History (Carved)	2	0
Audio	3	0
Carved Audio	2	0
Photoshop files	1	0
Pictures	2694	236
Potential Facebook Pictures	5	0
Videos	7	0
Microsoft Excel Documents	14	4
Microsoft Word Documents	46	5
PDF Documents	378	142
PowerPoint Documents	22	0
RTF Documents	43	0
Text Documents	27	0
$LogFile Analysis	1	1
File System Information	1	1
Encrypted Files	33	0
Google maps	50	0
Carved Archives (content not searched)	83	9
Celkem	**3581**	**416**

Tabulka 24. Analýza flash disku (vzorek #18)

	Vzorek #18	
Artefakty	Původní	FrSp
Identifiers - Device	9	2
Identifiers - People	16	3
Internet Explorer Cache Records	1	0
Potential Browser Activity	225	186
Carved Audio	145	0
Photoshop files	3	2
Pictures	163445	565
Videos	5	0
Microsoft Word Documents	7	0
PDF Documents	56	12
PowerPoint Documents	3	1
RTF Documents	76	17
Text Documents	23	23
File System Information	1	1
LNK Files	95	0
Carved Archives (content not searched)	45	20
Celkem	**164155**	**832**

Tabulka 25. Analýza flash disku (vzorek #19)

	Vzorek #19	
Artefakty	Původní	FrSp
Identifiers - Device	2	2
Identifiers - People	18	9
Parsed Search Queries	2	2
Internet Explorer Cache Records	4	4
Internet Explorer Favorites	1	1
Potential Browser Activity	106	105
Carved Audio	2	2
Photoshop files	29	29
Pictures	2311	2254
Videos	2	0
VLC Recently Played Files	1	1
Eml(X) Files	3	3
Microsoft Excel Documents	1	0
Microsoft Word Documents	5	1
PDF Documents	103	43
RTF Documents	8	7
Text Documents	167	167
Apple Disk Images	1	1
File System Information	1	1
LNK Files	3	3
Encrypted Files	17	19
Encryption / Anti-forensic tools	2	2
Carved Archives (content not searched)	206	204
ISO Files	1	1
QuickBooks Files	6	6
Celkem	**3002**	**2867**

Tabulka 26. Analýza flash disku (vzorek #20)

	Vzorek #20	
Artefakty	Původní	FrSp
Identifiers - Device	2	2
Identifiers - People	219	218
Google Analytics First Visit Cookies Carved	2	2
Google Analytics Referral Cookies Carved	2	2
Google Analytics Session Cookies Carved	2	2
Potential Browser Activity	312	302
Audio	146	146
Carved Audio	133	129
Photoshop files	2	1

Pictures	10737	10212
Videos	31	28
Email Attachments	159	159
Outlook Emails	64	64
Calc Documents	4	4
CSV Documents	15	15
Microsoft Excel Documents	199	195
Microsoft Word Documents	81	80
OpenOffice Writer Documents	1	1
PDF Documents	4954	4943
PowerPoint Documents	3	3
RTF Documents	4	1
Text Documents	559	549
Bitcoin Addresses	16	16
Cryptocurrency Wallets	3	3
File System Information	1	1
Encrypted Files	802	793
Encryption / Anti-forensic tools	1	1
Google maps	695	695
Google Maps Tiles	2	1
Carved Archives (content not searched)	461	440
Celkem	**19612**	**19008**

Tabulka 27. Analýza flash disku (vzorek #21)

	Vzorek #21	
Artefakty	Původní	FrSp
Classifieds URLs	13	2
Dating Sites URLs	1	1
Facebook URLs	3016	2
Google Searches	12	8
Identifiers – Device	17	11
Identifiers – People	223	142
Loccaly Accessed Files and Folders	29	29
Parsed Search Queries	3	3
Web Char URLs	3	3
Social Media URLs	190	57
Edge/Internet Explorer 10-11 Content	810	810
Edge/Internet Explorer 10-11 Daily/Weekly History	18	18
Edge/Internet Explorer 10-11 Main History	16	16
Flash Cookies	2	2
Internet Explorer Cache Records	1	1
Internet Explorer Cookie Records	1	0
Potential Browser Activity	5163	733

Safari History	69	67
WebKit Browser Web History (Carved)	991	83
IP Addresses – Audio/Video Calls	2	0
KakaoTalk Shared Pictures – Windows	1	1
QQ	1	0
Facebook Chat	1	0
Carved Audio	394	36
Photoshop files	129	97
Pictures	96085	5919
Videos	1071	18
Eml(X) Files	91	47
Email Attachments	793	792
Microsoft Excel Documents	2	1
Microsoft Word Documents	14	7
OpenOffice Writer Documents	2	0
PDF Documents	227	87
PowerPoint Documents	23	23
RTF Documents	41	38
Areas Search Keywords	2	2
Carbonite Log File	1	0
File System Information	1	1
LNK Files	31	31
Google maps	34	0
Google Maps Tiles	65	0
Carved Archives (content not searched)	4231	321
QuickBooks Files	10	10
Celkem	**113830**	**9416**

PŘÍLOHA P IV: ANALÝZA SDHC PAMĚŤOVÝCH KARET

Tabulka 28. Analýza SD karty (vzorek #10)

	Vzorek #10	
Artefakty	Původní	FrSp
Identifiers - Device	4	2
Pictures	1681	2
File System Information	1	1
Encrypted Files	83	0
Carved Archives (content not searched)	1	0
Celkem	**1770**	**5**

Tabulka 29. Analýza SD karty (vzorek #11)

	Vzorek #11	
Artefakty	Původní	FrSp
Identifiers - Device	2	0
WebKit Browser Web History (Carved)	1	0
Carved Audio	83	0
Pictures	7182	0
Videos	192	0
File System Information	1	1
Carved Archives (content not searched)	1	0
Celkem	**7462**	**1**

Tabulka 30. Analýza SD karty (vzorek #13)

	Vzorek #13	
Artefakty	Původní	FrSp
Identifiers - Device	3	0
Identifiers - People	23	21
Pictures	105	61
Microsoft Word Documents	13	11
PDF Documents	6	6
Text Documents	2	0
$LogFile Analysis	5	0
File System Information	1	1
Encrypted Files	1	0
Carved Archives (content not searched)	8	1
Celkem	**167**	**101**

Tabulka 31. Analýza SD karty (vzorek #22)

	Vzorek #22	
Artefakty	Původní	FrSp
Identifiers - Device	3	1
Potential Browser Activity	37	5
Audio	904	761
Carved Audio	859	0
Photoshop files	6	6
Pictures	419	141
Videos	3	49
Text Documents	17	0
File System Information	1	1
Encrypted Files	2	2
Carved Archives (content not searched)	2	0
Celkem	**2253**	**966**

Tabulka 32. Analýza SD karty (vzorek #23)

	Vzorek #23	
Artefakty	Původní	FrSp
Identifiers - Device	2	2
Photoshop files	1	0
Pictures	369621	0
Videos	463	0
File System Information	1	1
Celkem	**370088**	**3**

Tabulka 33. Analýza SD karty (vzorek #24)

	Vzorek #24	
Artefakty	Puvodní	FrSp
Identifiers – Device	7	4
Identifiers – People	40	0
Photoshop files	7	0
Pictures	9725	88
Videos	105	0
Eml(X) Files	1	0
Microsoft Excel Documents	21	0
Microsoft Word Documents	232	0
PDF Documents	169	0
PowerPoint Documents	1	0
File System Information	1	1
Carved Archives (content not searched)	12	0
Celkem	**10321**	**93**

PŘÍLOHA P V: DOTAZNÍK

1) Zajímá vás, jakou digitální stopu zanecháváte na internetu?

a) Ano
b) Ne

2) Používáte unikátní a složitá hesla pro různé služby?

a) Ano
b) Ne

3) Využíváte dvoufázovou autentizaci k zabezpečení svých online účtů?

a) Ano
b) Ne
c) Nevím co to je

4) Používáte správce hesel, abyste si pamatovali a ukládali svá hesla?

a) Ano
b) Ne

5) Máte zkušenosti s „hacknutím“ vašeho účtu na sociální síti nebo e-mailu?

a) ano
b) ne

6) Používáte VPN služby k zabezpečení vašeho připojení na internet?

a) Ano
b) Ne
c) Nevím co to je

7) Používáte veřejné a otevřené "hot-spoty" pro připojení k internetovému bankovnictví a jiným důležitým službám?

a) Ano
b) Ne
c) Někdy

8) Máte povědomí o tom, co jsou to "fingerprinty" a jak mohou být použity k identifikaci vašeho zařízení a sledování vašeho chování na internetu?

a) Ano
b) Ne

9) Máte povědomí o tom, co jsou to "zero-day" zranitelnosti a jak mohou být zneužity k útokům na vaše zařízení?

a) Ano
b) Ne

10) Aktualizujete pravidelně svá zařízení s připojením na internet.

a) Ano
b) Ne
c) Nejsem si jistá (ý)

11) Zajímá vás, jaká data o vás shromažďují vaše oblíbené webové stránky a aplikace?

a) Ano
b) Ne
c) Jen u důležitých služeb

12) Máte nastaveny své účty na sociálních sítích jako veřejné nebo soukromé?

a) Soukromě
b) Veřejně
c) Nevím

13) Máte nastavené omezení sdílení dat s třetími stranami na sociálních sítích?

a) Ano
b) Ne
c) Nevím

14) Máte nastavené omezení shromažďování polohových dat vašeho zařízení?

a) Ano
b) Ne
c) Nevím

15) Jak často kontrolujete své nastavení soukromí na sociálních sítích a webových stránkách, které navštěvujete?

a) Při prvním použití
b) Týdně
c) Měsíčně
d) Nahodile
e) Neřeším to

16) Jak často se vzdáváte soukromí ve prospěch získání nějaké výhody, jako jsou například slevy nebo nabídky na internetových stránkách?

a) Nikdy
b) Sporadicky
c) Často
d) Nejsem si jistý

17) Jak často sdílíte své osobní informace na internetu, jako jsou například jméno, příjmení, e-mailová adresa, telefonní číslo nebo adresa bydliště?

a) Nikdy
b) Sporadicky
c) Často
d) Za určitým účelem (nákupy, registrace apod.)

18) Používáte anonymní okna v prohlížečích internetových stránek?

a) Ano
b) Ne
c) Nevím

19) Používáte „ad-blocker“ k omezení nevyžádaných reklam na internetu?

a) Ano
b) Ne
c) Nevím

20) Máte vědomosti o tom, co jsou soubory cookies, k čemu slouží a jak fungují?

a) Ano
b) Ne
c) Částečně

21) Jak často využíváte funkci "odstranit historii prohlížení" na svém zařízení?

a) Nikdy
b) Měsíčně
c) Sporadicky, když si vzpomenu

22) Máte zkušenosti s phishingovými útoky nebo podobnými útoky na vaše osobní údaje?

a) Ano
b) Ne
c) Nevím o tom

23) Jak často klikáte na odkazy v e-mailech od neznámých odesílatelů nebo přijímáte žádosti o přátelství od neznámých lidí na sociálních sítích?

a) Nikdy
b) Občas
c) Často

24) Používáte více e-mailových účtů pro různé účely?

a) Ano
b) Ne

25) Pohlaví

a) Žena
b) Muž
c) Jiné
d) Nechci uvést

26) Dosažené vzdělání

a) Základní
b) Středoškolské
c) Vysokoškolské
d) Nechci uvést

27) Věk

a) Méně než 10 let
b) 10-15 let
c) 15-25 let
d) 25-50 let
e) 50-70 let
f) 70 a více let
g) Nechci uvést
h) Věk (přesný)