Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Prevence ochrany osobních údajů uživatelů

Klára Humrová

© 2022 ČZU v Praze

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Klára Humrová

Informatika

Název práce

Prevence ochrany osobních údajů uživatelů

Název anglicky

Prevention of User's Personal Data Protection

Cíle práce

Hlavním cílem bakalářské práce bude stanovit preventivní postupy a opatření, vedoucí k minimalizaci rizika ztráty osobních dat uživatelů v online prostředí.

Dílčími cíli jsou:
- Vyhodnotit hrozby a rizika
- Zmapovat aktuální trendy v oblasti zabezpečení
- Navrhnout způsoby informování uživatelů

Metodika

Teoretická část bude zpracována na základě dostupné české i zahraniční literatury, odborných publikací a online zdrojů. Důraz bude kladen na možné způsoby ochrany dat, trendy v této oblasti, zmapování největších hrozeb a ukotvení ochrany osobních údajů v zákoně.

Data pro zpracování praktické části budou získána prostřednictvím vlastního experimentu. Subjekty budou vystaveny simulacím, ve kterých bude zkoumáno jejich chování a nakládání s osobními daty.

Doporučený rozsah práce

30 – 40 stran

Klíčová slova

osobní údaje, uživatel, online prostředí, ochrana dat, prevence

---

Doporučené zdroje informací

BARTÍK, Václav a Eva JANEČKOVÁ. Ochrana osobních údajů v aplikační praxi. 4. aktualizované vydání. Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-141-5.

KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

KROPÁČOVÁ, Andrea. Uživatel a počítačová bezpečnost. Zpravodaj ÚVT MU [online]. 2006, XVI(3), 16-20 [cit. 2021-4-30]. ISSN 1212-0901. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/353.html

NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ a Jan TOMÍŠEK. GDPR – obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-765-3.

TATARU, Georgiana Florentina a Ștefan Răzvan TATARU. HUMAN RESOURCES AND PERSONAL DATA PROTECTION: AN INDISSOLUBLE RELATIONSHIP. Journal of Public Administration, Finance & Law. 2020, (18), 303-311.

Předběžný termín obhajoby

2021/22 LS – PEF

Vedoucí práce

Ing. Jana Hřebejková

Garantující pracoviště

Katedra informačních technologií

Konzultant

Ing. Václav Lohr, Ph.D.

Elektronicky schváleno dne 10. 8. 2021

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 5. 10. 2021

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 15. 03. 2022

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Prevence ochrany osobních údajů uživatelů" jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15. března 2022 _____

Poděkování

Ráda bych touto cestou poděkovala Ing. Janě Hřebejkové za vedení a pomoc při zpracování mé bakalářské práce. Dále bych chtěla poděkovat Ing. Václavu Lohrovi, Ph.D. za užitečné rady a ochotu dělat konzultanta.

Prevence ochrany osobních údajů uživatelů

Abstrakt

Bakalářská práce se zabývá prevencí ochrany osobních údajů uživatelů. V první části práce jsou charakterizovány osobní údaje a jejich ukotvení v zákoně, dále jsou popsány hrozby a rizika, která vedou k možnému ohrožení těchto údajů, a zároveň také způsoby, jak je minimalizovat. Druhá část je zaměřena na vlastní experiment, jehož cílem bylo získat informace o tom, jak uživatelé nakládají se svými osobními údaji. Uživatelé jsou dle svého dosaženého výsledku rozděleni do skupin, kterým se věnuje závěr práce. V závěru jsou do práce vloženy situace s největší chybovostí, které jsou popsány, a zároveň je každé skupině podle jejího výsledku stanoveno doporučení, na co se zaměřit v oblasti vlastní online ochrany a navrženy preventivní postupy, jak co nejefektivněji zlepšit své znalosti v oblasti ochrany osobních údajů.

Klíčová slova: osobní údaje, uživatel, online prostředí, ochrana dat, prevence, rizika, hrozby

Prevention of User's Personal Data Protection

Abstract

This bachelor thesis deals with the prevention of user's personal data protection. The first part of the thesis characterizes personal data and their enshrined in the law, then describes the threats and risks that lead to a possible threat to this data and way how to minimize them. The second part is focused on my own experiment, which is aimed to obtain information about how users manipulate their personal data. Users are divided according to their achieved result into groups, which are mentioned in the conclusion. In the end, the situations with the highest error rates are inserted into the bachelor thesis, which are described, and at the same time each group is given recommendations according to its results, what to focus on in their own online protection and proposed preventive procedures to improve their knowledge in personal data protection as effectively as possible.

Keywords: personal data, user, online environment, data protection, prevention, risks, threats

Obsah

1 Úvod ... 8

2 Cíl práce a metodika ... 10

2.1 Cíl práce ... 10

2.2 Metodika ... 10

3 Teoretická východiska ... 11

3.1 Osobní údaje ... 11

3.2 Kybernetická bezpečnost ... 11

3.3 Ukotvení ochrany osobních údajů v zákoně ... 12

3.3.1 GDPR ... 12

3.3.2 Zákon o zpracování osobních údajů ... 12

3.3.3 Autorský zákon ... 13

3.3.4 Právní regulace ochrany dat nezletilých ... 13

3.3.5 ÚOOÚ ... 13

3.3.6 Vybrané právní problémy/situace ... 13

3.4 Hrozby a rizika ... 15

3.4.1 Subjektivní ... 17

3.4.2 Objektivní ... 18

3.5 Způsoby ochrany ... 24

3.5.1 Základní bezpečnostní zásady ... 24

3.5.2 Bezpečnostní školení, sebevzdělávání ... 24

3.6 NÚKIB ... 30

3.6.1 Trendy kybernetické bezpečnosti bezpečnosti podle NÚKIB za leden 2022 ... 31

3.7 Shrnutí ... 32

4 Vlastní práce ... 33

4.1 Charakteristika vlastního experimentu ... 33

4.2 Dokumentace experimentu ... 34

4.2.1 Soubory cookies ... 35

4.2.2 Phishing – dvoufázové ověřování ... 35

4.2.3 Zákonná legislativa ... 35

4.2.4 Honeypoty ... 36

4.2.5 Pop-up okna ... 36

4.2.6 Škodlivé softwary ... 36

4.2.7 Licenční podmínky ... 36

4.2.8 Phishing – sociální sítě ... 37

4.2.9 Hlášení antivirového programu ... 37

4.2.10 DDos útoky 38
4.2.11 Digitální certifikáty 38
4.2.12 Vzdělání 38

5 Zhodnocení a doporučení 40
5.1 Zhodnocení výsledků hry 40
5.1.1 Výsledky úkolu Soubory cookies 40
5.1.2 Výsledky úkolu Zákonná legislativa 41
5.1.3 Výsledky úkolu Honeypoty 42
5.1.4 Výsledky úkolu Škodlivé softwary 43
5.1.5 Výsledky simulace Antivirový program 44
5.1.6 Výsledky Vzdělání 45
5.2 Doporučení 47
5.2.1 Preventivní postupy a opatření 47
5.2.2 Návrhy způsobů informování 48

6 Závěr 50

Seznam použitých zdrojů 53

7 Přílohy 57

Seznam obrázků

Obrázek 1 - Správné užití režimu opt-out 14
Obrázek 2 - Schéma zajišťování bezpečnosti 17

Seznam tabulek

Tabulka 1 - Porovnání firewallů 26

Seznam grafů

Graf 1 Podíl malwarů zachycených honeypoty 27
Graf 2 NÚKIB bezpečnostní incidenty 30
Graf 3 - Výsledky úkolu soubory cookies 41
Graf 4 - Výsledky úkolu Zákonná legislativa 42
Graf 5 - Výsledky úkolu Honeypoty 43
Graf 6 - Výsledky úkolu Škodlivé softwary 44
Graf 7 - Výsledky simulace Antivirový program 45
Graf 8 - Výsledky Vzdělání 46

Seznam použitých zkratek

GDPR – z angl. General Data Protection Regulation
DPIA – z angl. Data Protection Impact Assessment
DPO – z angl. Data Protection Officer
VPN - z angl. Virtual Private Network
SSL – z angl. Secur Sockets Layer
TLS – z angl. Transport Layer Security
HTTPS – z angl. Hypertext Transfer Potocol Secure
NÚKIB – Národní úřad pro kybernetickou informační bezpečnost

1 Úvod

S neustálým vývojem v oblasti technologií a pokračující digitalizací stále vzrůstá potřeba využívat internet. V dnešní době si už existenci bez internetu není možné představit, protože velkou měrou život usnadňuje. Věci jako jsou na příklad internetové bankovnictví, sociální sítě nebo nakupování online prostřednictvím e-shopů se staly součástí každodenního života většiny lidí. Na internetu je závislá i většina firem a organizací, které ho využívají nejen ke zjednodušení své činnosti, ale také třeba ke komunikaci s úřady nebo k obchodování se zahraničím.

Internet se zdá být dokonalým nástrojem, který velkou měrou přispívá k tomu, aby svět mohl fungovat takovým způsobem, na jaký jsme dnes zvyklí. Jako většina věcí má však i tato na pohled dokonalá technologie druhou stranu mince. Díky tomu, že je využíván prakticky všude, stal se internet skvělým prostředkem, jak se dostat k informacím a údajům, které by neměly být zveřejňovány, a zároveň umožňuje dokonalejší provozování trestné činnosti.

Tato práce se bude věnovat právě prevenci ochrany těchto dat, konkrétně ochraně osobních údajů. Budou vyhodnoceny hrozby a rizika, které by mohly vést ke ztrátě či odcizení dat uživatelů, zmapovány aktuální trendy v oblasti zabezpečení a v neposlední řadě budou navrhnuty způsoby informování uživatelů o aktuální hrozbách a trendech, a také jak těmto hrozbám co nejefektivněji předcházet, popřípadě bránit.

V první části práce bude vymezen rozsah pojmu osobní údaje uživatelů a ukotvení těchto údajů a jejich ochrany v zákoně. Bude popsáno, jak tyto údaje právní předpisy v České republice vnímají a jak jsou v nich definovány, dále také čím se řídí a jak se v čase vyvíjely. Detailnější prostor bude věnován rizikům a hrozbám, které mohou ztrátu uživatelských dat zapříčinit. Rozděleny budou na několik kategorií a pro každou budou uvedeny konkrétní příklady jednotlivých hrozeb. Závěrem této části budou představeny způsoby a trendy, jak se těmto hrozbám bránit, nebo, pokud je to možné, úplně vyhnout.

Druhá část práce se bude zaobírat vlastním experimentem. Nejprve bude vytvořena úniková hra s cílem zkoumat chování uživatelů v souvislosti s nakládáním s jejich osobními daty. Subjekty budou vystaveny co možná nejreálnějším situacím a úkolům a následně bude zaznamenáno jejich chování a znalosti. Získaná data poté budou zpracována, vyhodnocena a subjekty rozděleny do několika skupin na základě jejich schopností, znalostí a dovedností prokázaných ve hře.

V závěru práce budou na základě získaných dat vyfiltrovány situace, ve kterých bylo nejvíce chybováno, a podáno možné vysvětlení, proč tomu tak bylo. Každé skupině bude také navrhnuto optimální řešení, jak nejefektivněji posunout své znalosti a způsoby ochrany na vyšší úroveň, a co udělat pro to, aby v reálných situacích dopadly lépe.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem bakalářské práce je stanovit preventivní postupy a opatření, vedoucí k minimalizaci rizika ztráty osobních dat uživatelů v online prostředí.

Dílčí cíle jsou navrženy následovně:

- vyhodnotit hrozby a rizika,
- zmapovat aktuální trendy v oblasti zabezpečení,
- navrhnout způsoby informování uživatelů.

2.2 Metodika

Teoretická část je zpracována na základě dostupné české i zahraniční literatury, odborných publikací a online zdrojů. Důraz je kladen na možné způsoby ochrany dat, trendy v této oblasti, zmapování největších hrozeb a ukotvení ochrany osobních údajů v zákoně.

Data pro zpracování praktické části byla získána prostřednictvím vlastního experimentu. Subjekty byly vystaveny simulacím, ve kterých bylo zkoumáno jejich chování a nakládání s osobními daty.

3 Teoretická východiska

3.1 Osobní údaje

Pro účely této bakalářské práce zahrnuje pojem „osobní údaje“ veškerá elektronická, tištěná nebo šifrovaná data, která slouží k bližší identifikaci uživatele. Osobními údaji je myšleno zejména:

- jméno a příjmení,
- pohlaví,
- adresa trvalého bydliště,
- rodné číslo,
- číslo platební karty a bankovní údaje,
- e-mailová adresa a telefonní číslo,
- současná poloha (například z mobilního telefonu),
- IP adresa,
- veškeré údaje, týkající se činnosti uživatele na elektronických zařízeních.

Tyto citlivé údaje mohou v určité formě obsahovat i osobní média jako jsou dokumenty, účty, soubory nebo fotky. (ec.europa.eu)

3.2 Kybernetická bezpečnost

Kybernetická bezpečnost je obecně považována za proces, mající za úkol co nejbezpečnějším způsobem uchovávat osobní data. Tento proces bývá označován zkratkou C.I.A., která definuje tři základní principy:

- confidentiality (důvěrnost dat) – přístup k datům by měl mít pouze vlastník, popřípadě autorizované osoby,
- integrity (integrita dat) – nikdo by neměl mít právo cokoli měnit bez vědomí vlastníka,
- access (dostupnost dat) – vlastník by měl mít k datům kdykoli přístup.

Tyto pojmy, tvořící pomyslný trojúhelník, bývají považovány za tři nejzásadnější v rámci informační bezpečnosti. (Chai, 2021)

3.3 Ukotvení ochrany osobních údajů v zákoně

S rozrůstajícím se online světem postupem času vznikla potřeba upravit a doplnit legislativu takovým způsobem, aby mohly být situace, přestupky a trestné činy, ke kterým dochází v prostředí internetu, řešeny právní cestou.

3.3.1 GDPR

Jedním z nejznámějších souborů, definujícím pravidla pro ochranu dat je Obecné nařízení o ochraně osobních údajů. Vstoupilo v účinnost 28. května 2018 a reguluje nakládání s daty občanů států, nacházejících se na území Evropské unie. Jeho vznik byl zapříčiněn rozvojem komunikačních technologií, využíváním cloudových úložišť a vzrůstající popularitou sociálních sítí.

„ *GDPR představuje nový právní rámec ochrany osobních údajů v evropském prostoru s cílem hájit co nejvíce práva občanů EU proti neoprávněnému zacházení s jejich daty včetně osobních údajů.* “ (Škorničková). Týká se jak fyzických, tak právnických osob i internetových služeb, a jeho případné porušení je vysoce sankcionováno. Při zpracování a nakládání s daty je v některých případech nutné provést posouzení vlivu na ochranu osobních údajů DPIA, na němž se obvykle podílí pověřenec pro ochranu osobních údajů DPO a zpracovatel. Zpracovatel dat je dále povinen zabezpečit data proti zneužití (včetně jejich pseudonymizace), vést záznamy o jejich zpracování, a veškerá jeho manipulace s daty podléhá kontrole ze strany Úřadu pro ochranu osobních údajů. (Nulíček, 2017)

3.3.2 Zákon o zpracování osobních údajů

Zákon č. 110/2019 Sb., Zákon o zpracování osobních údajů, vznikl pro upřesnění a doplnění podmínek nařízení GDPR pro Českou republiku. Jeho přijetím byl zrušen Zákon o ochraně osobních údajů, který reguloval nakládání s osobními daty od roku 2000. Tento soubor předpisů například snižuje výši sankcí, povoluje zaměstnavatelům výjimku z DPIA, umožňuje správcům poskytovat informace o zpracování osobních údajů prostřednictvím internetu a stanovuje odlišnou věkovou hranici pro udělení souhlasu se zpracováním osobních údajů. Již ze zákona vyplývá, že na zpracovatele, případně správce osobních dat, jsou kladené vysoké technologické nároky, aby byl schopen data zabezpečit před zneužitím. Jedná se

zejména o vhodný software, spolehlivé úložiště a výkonný hardware, tyto požadavky mohou vyžadovat nemalé finanční náklady. (Nulíček, 2019)

3.3.3 Autorský zákon

Zákon č. 121/2000 Sb., Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, nepřímo souvisí s ochranou osobních údajů. Tento zákon mimo jiné definuje práva autora k nehmotným dílům, např. počítačovým programům, fotografiím nebo databázím. V rámci autorského zákona musí být nahlíženo na licenci, pod kterou je program vydán. Nejčastějšími typy licencí v rámci IT bývají open sourcové, cloudové nebo GPL a GNU licence. V rámci licenčních podmínek je třeba rozlišovat, zdali se jedná o licenci na uživatele tzv. per user nebo na zařízení tzv. per device. S licenčními podmínkami jde ruku v ruce uchovávání a ochrana uživatelských dat před zneužitím. (Chaloupková, 2012)

3.3.4 Právní regulace ochrany dat nezletilých

V České republice je uzákoněn věk, od kterého může osoba udělit právoplatný souhlas se zpracováním osobních údajů, dovršením 15 let. Této právní způsobilosti ale osoba nabývá pouze v souvislosti s nabídkou služeb informační společnosti (například za účelem marketingové propagace). Tato věková hranice byla stanovena zejména kvůli užívání sociálních sítí. (Nulíček, 2019)

3.3.5 ÚOOÚ

Úřad pro ochranu osobních údajů je ústřední správní orgán, který je oprávněn vydávat rozhodnutí, dozorovat, prošetřovat a konzultovat nakládání s daty v oblasti ochrany osobních údajů. Tato instituce je zcela nezávislá na činnostech a rozhodnutích realizovaných státem. V rámci svojí vnitřní struktury disponuje řadou protikorupčních opatření, která mají za cíl co nejefektivnější vykonávání činnosti. (uoou.cz)

3.3.6 Vybrané právní problémy/situace

V červenci 2021 nebyl schválen návrh novely zákona o elektronických komunikacích z roku 2005, který je vzhledem k technologickému pokroku v určitých částech zastaralý a pro dnešní aplikaci nepoužitelný, proto je třeba mnohdy hledat právní oporu v jiných zákonech a nařízeních.

3.3.6.1 Režim opt-in a opt-out

Tyto principy jsou nejčastěji využívány v případě zasílání elektronických obchodních sdělení a nabídek, pro uživatele je tak možné si ověřit, zda firma zasílá emaily legální cestou, a učinit příslušné právní kroky, když tomu tak není.

Režim opt-in vyžaduje výslovný, doložitelný a informovaný souhlas adresáta se zasláním obchodního sdělení a zároveň společnost není oprávněna zaslat žádost opakovaně na stejnou e-mailovou adresu. Častý způsobem, jak toto obejít, je doručení informačního e-mailu s předvyplněným formulářem, obsahujícím políčko s již zaškrtnutým souhlasem. Tato praktika je považována za nezákonnou, protože se nemusí jednat o vědomý souhlas adresáta.

Naproti tomu režim opt-out nevyžaduje výslovný souhlas příjemce, za předpokladu, že bude mít jasnou a jednoduše proveditelnou možnost odmítnout adresování dalších sdělení. V tomto případě jde o snahu dát firmám možnost šířit o sobě povědomí a zvyšovat svoje tržby prostřednictvím oslovení více zákazníků, tento princip je využíván ve většině propagační korespondence, zpravidla je na konci e-mailu uvedena možnost odhlášení odběru obchodních sdělení. (Bartík, 2016)

Obrázek 1 - Správné užití režimu opt-out

Tento e-mail byl odeslaný na adresu: [redacted] Doufáme, že informace týkající se značky [redacted] jsou pro Vás zajímavé a hodnotné. Nepřejete-li si, aby Vám byla obchodní sdělení odesílatelem nadále zasílána, klikněte zde.

Tento email byl vygenerován automaticky. Neodpovídejtetedy na něj, použijte výše uvedený odkaz nebo kontaktujte naše call centrum na telefonním čísle [redacted]

[redacted] zapsaná v obchodním rejstříku Městského soudu v Praze, oddíl [redacted]

Zdroj: vlastní zpracování

3.3.6.2 Odpovědnost accessproviderů, hostproviderů, poskytovatelů úložišť a provozovatelů sociálních sítí za obsah

Co se týče poskytovatelů připojení k internetu a hostingu, jim není zákonem udávána odpovědnost za obsah informací dostupných na internetu, pokud se na něm aktivně nepodílejí, dále jim není uložena povinnost vyhledávat a prověřovat přenášené a ukládané informace.

V případě poskytovatelů úložišť a sociálních sítí, kde je možnost chatování, komentování, vkládání příspěvků a inzerátů, jsou za obsah dat odpovědni jen do určité míry. Zejména pokud mohli z nějakého důvodu o protiprávní činnosti vědět, nebo se o ní dozvěděli a nepodnikli příslušné kroky k odstranění obsahu. Stejně jako v případě accesproviderů a hostproviderů nejsou povinni aktivně vyhledávat a prověřovat případná nezákonná jednání uživatelů. Závěrem je ale nutné dodat, že provozovatelé sociálních sítí se v posledních letech aktivně podílejí na prohledávání protiprávního obsahu na svých platformách, což může mnohdy způsobovat konflikty s uživateli, kteří se ničeho nezákonného nedopustili, ale pokud poskytovatel jejich profil nebo příspěvky vyhodnotí z nějakého důvodu jako ilegální, má ve většině případů poslední slovo on a uživatel se musí podřídit. (Bartík, 2016)

3.3.6.3 Využívání online plateb

Nakupování přes internet v posledních letech získávalo čím dál větší oblibu a s příchodem pandemie COVID-19 zažily online platby ještě větší rozmach, který do určité míry stále přetrvává. V důsledku navýšení elektronických transakcí a rizik spojených se ztrátami dat vydal Evropský sbor pro ochranu osobních údajů dokument s doporučeními, týkající se uchovávání údajů z kreditních karet zákazníků. Dokument mimo jiné stanovuje podmínky, za kterých může správce platební údaje přechovávat, například k usnadnění příštího nákupu. Opět zde platí, že držitel karty musí jednoznačně, svobodně, informovaně a konkrétně udělit souhlas s uchováním údajů z jeho kreditní nebo debetní karty, a to ještě před tím, než jsou jeho data uložena. (PARLAMENTNÍ LISTY.cz, 2021)

3.4 Hrozby a rizika

Množství a důležitost uchovávaných dat se zvyšuje a k jejich ztrátě může dnes dojít velmi snadno, proto je důležité, aby uživatelé byli seznámeni s možnými riziky a hrozbami jak při manipulaci se svými osobními daty, tak při jejich uchovávání, a minimalizovali svoje zranitelná místa v zabezpečení. Hrozba určuje možnost využití zranitelného místa k útoku a způsobení škody, riziko určuje pravděpodobnost využití zranitelného místa a potenciální způsobená škoda vyplývající z hrozby. Útok je považován za realizaci hrozby.

Obecně lze rizika a hrozby rozdělit do různých kategorií podle toho, z jakého pohledu je na ně nahlíženo. Nejčastějším rozdělením je na subjektivní a objektivní. Za subjektivní jsou považovány ty, které jsou přímo ovlivněny lidským faktorem:

- úmyslné – zpravidla se jedná o útok,
- neúmyslné – způsobené nevědomostí nebo nedbalostí.

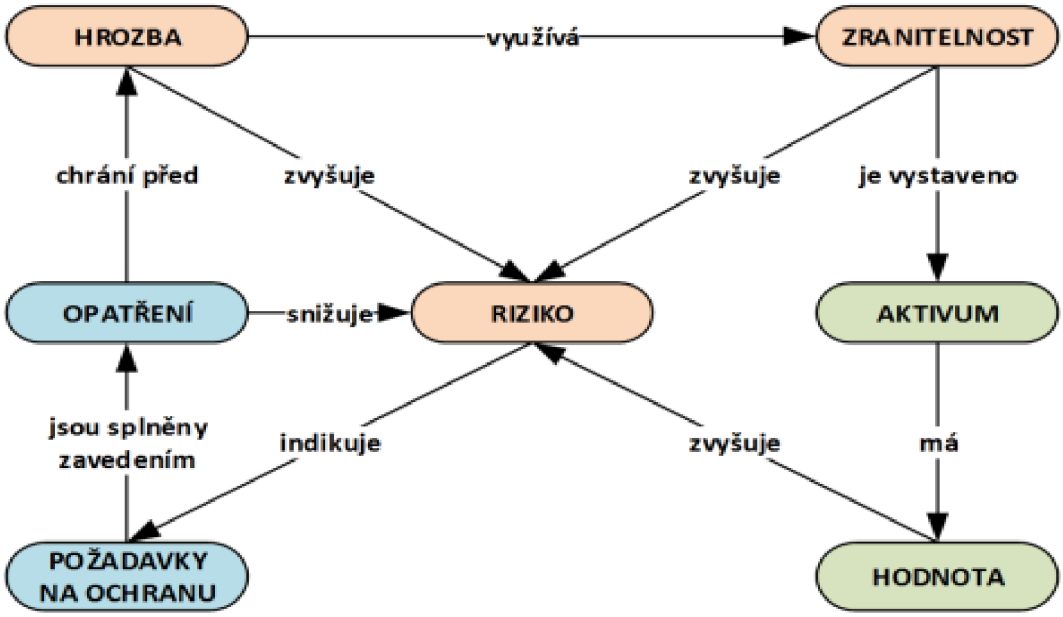
Za objektivní jsou naopak považovány ty, které uživatelem být ovlivněny z velké části nemohou:

- přírodní – např. tornáda, požáry, povodně,
- fyzikální – elektromagnetické záření
- technické- např. selhání paměťového média,
- softwarové – škodlivé softwary. (Požár, 2010)

Softwarových hrozeb, které potenciálně ohrožují data uživatelů, je mnohem více než hardwarových. Vše jde ruku v ruce s neustálým technologickým pokrokem, šikovností hackerů a v neposlední řadě hodně uživatelů podceňuje základní bezpečnostní zásady jako je antivirová ochrana počítače nebo struktura hesla, a vystavují se tak možnému ohrožení svých dat. Výrobci operačních systému a antivirových programů nabízejí širokou škálu aplikací, které jsou uživatelsky přívětivé i pro méně zkušené uživatele oblasti IT, a tak je použití těchto systémů jednodušší než dříve, více o tomto tématu bude uvedeno v další části práce.

Ve schématu Národního úřadu pro kybernetickou a informační bezpečnost, viz níže, je znázorněno zajišťování bezpečnosti, jehož cílem je řízení rizik spojených s ochranou osobních údajů. Jako úspěšné řízení rizika lze označit soubor úkonů, které vedou k jeho minimalizaci či eliminaci. Schéma sestává ze tří skupin bodů. První skupinou je hrozba, zranitelnost a riziko, druhou aktivum a hodnota, a třetí požadavky na ochranu a opatření. Za aktivum lze považovat cokoli, co má pro subjekt, který je předmětem ohrožení, hodnotu. První krokem k realizaci opatření je zmapování vyhodnocení aktiv a přiřazení jejich hrozeb a zranitelností, jedno aktivum jich může mít zpravidla více. Dalším krokem je určení hodnoty rizika a následná sumarizace požadavků. V závěru jsou na základě požadavků na ochranu zrealizována konkrétní opatření, která mají za úkol snížit nebo nejlépe eliminovat bezpečnostní hrozby. Obecným předpokladem k funkčnosti schématu je, že náklady na bezpečnostní opatření by neměly být vyšší než náklady spojené s následky zrealizování rizika. (nukib.cz, 2019)

Obrázek 2 - Schéma zajišťování bezpečnosti



Zdroj: NÚKIB (2019)

3.4.1 **Subjektivní**

3.4.1.1 Pokročilá nastavení počítače

Jedná se zejména o neodborná přenastavení základních funkcí počítače, která mohou způsobit změnu fungování zařízení a vytvořit pomyslná slabá místa v zabezpečení. Obecně uváděnými příklady jsou BOIS, případně UEFI nebo operační systém. Téměř vždy jsou tato přenastavení prováděna s dobrým úmyslem, například změna pořadí bootování nebo ztišení větráku, během nich ale může dojít k nějaké nechtěné změně. Ve většině případů je toto riziko ošetřeno výrobcem, který umožňuje uživateli měnit pouze věci, které zásadním způsobem neohrozí činnost počítače, stále je ale možné s trochou snahy přenastavit některé klíčové funkce.

3.4.1.2 Zastaralé zabezpečení

Ne nadarmo IT specialisté apelují na uživatele, aby si zálohovali svá data a pravidelně aktualizovali operační systém a softwary, které mají za úkol co možná nejefektivněji chránit počítač proti zneužití. Starší technika nebo neaktuální protivirová ochrana může hackerům vydláždit snadnou cestu k osobním údajům, bankovním účtům i souborům, které mohou sloužit jako nástroj pro vydírání.

3.4.1.3 Nevědomost

Neznalost možných softwarových rizik bývá tou nejčastější příčinou úniku dat nebo ztráty kontroly nad svým zařízením. V dnešní době jsou dobrá informovanost, znalost svých práv a sebevzdělání v této oblasti jedněmi z nejzásadnějších preventivních opatření, které může uživatel učinit, aby uchránil svoje osobní údaje v online světě.

3.4.2 **Objektivní**

Tato kategorie zahrnuje rizika a hrozby, která uživatel nemá možnost i přes veškerou snahu jako je dodržování veškerých bezpečnostních doporučení z velké části ovlivnit. Jedná se například o technické poruchy, přerušení dodávky elektrického proudu, nevyžádané e-maily, vyskakovací okna, viry, malwary atd. Softwary a metody, které nějakým způsobem napadají soubory s daty nebo mají za úkol získat přístup k osobním údajům jsou velmi často kombinovány, aby co nejefektivněji odvedly svou práci.

3.4.2.1 Selhání paměťového zařízení

Mnoho uživatelů si svoje osobní data stále ukládá na přenosná paměťová zařízení jako jsou například karty, USB Flash disky a externí hard disky. Kromě rizika krádeže nebo ztráty zařízení může nastat problém technického rázu, kdy v případě opomenutí zálohování uživatelem dochází ke ztrátě veškerého obsahu.

V dnešní době dává řada uživatelů po vzoru velkých firem přednost využívání úložných serverů, kde odpadá chyba lidského faktoru při nesprávné manipulaci s paměťovým zařízením při jeho používání.

3.4.2.2 Selhání PC komponentu

Klíčovou částí pro práci s daty bylo, a ještě nějakou dobu bude, funkční elektronické zařízení. Příčin selhání některé z počítačových komponent může být mnoho, od špatné manipulace přes vniknutí prachových částic nebo vody, výrobní vady po napadení virem anebo jednoduše opotřebení a stáří. Ve spoustě případů lze

z HDD, SSD nebo SSHD disku získat alespoň část dat uložených v počítači nazpět, v každém případě je nutné údržbu hardwaru počítače nepodcenit.

- Škodlivé softwary

Tento pojem zahrnuje jednu z nejrozšířenějších kategorií softwarových hrozeb, které ohrožují osobní údaje a data uživatelů. Program, který se šíří bez vědomí uživatele může mít za cíl pouze ho obtěžovat, ale také převzít kompletní kontrolu nad zařízením, vymazávat, šifrovat a zamezit přístup k souborům a šířit se do dalších zařízení. V poslední době je řada programů mířena na infikování mobilních zařízení, na kterých bývají uživatelé méně opatrní a tráví na nich podstatně více času než na počítači. Vznik virů sahá až do 20. století a jejich množství se rok od roku zvyšuje. Některé nabývají na oblíbenosti, jiné upadají a jsou nahrazovány jinými, dokonalejšími.

3.4.2.3 Malware

Odhalení malwaru v počítači může zabrat nějaký čas. Nejčastějšími projevy jsou zpomalení, zamrznutí nebo pád operačního systému, vyskakování reklamních oken, Blue Screen of Death, ztráta místa na paměťovém disku nebo přístupu k souborům, změna nastavení prohlížeče atd. V konečném případě je uživateli pouze zobrazena zpráva, že kontrolu nad jeho počítačem převzali hackeři. V mnoha případech může být malware odstraněn jiným, konkurenčním. (malwarebytes.com)

3.4.2.4 Ransomware

Typ malwaru, který zašifruje data prostřednictvím kódu, při infikování tímto druhem viru zpravidla nedochází ke kompletní ztrátě souborů, ale ke znemožnění jejich přístupnosti. Uživatel může takto ohrozit své soubory například spuštěním zavirované přílohy z e-mailu, návštěvou infikovaného prohlížeče nebo webové stránky, a je následně vydírán, aby zaplatil určitý finanční obnos, nejčastěji v podobě bitcoinů, za zpřístupnění. Napadeno může být kterékoli elektronické komunikační zařízení, typicky se jedná o počítač nebo mobilní telefon s operačním systémem Android. Jsou ale zaznamenány případy, kdy byly napadeny i nejrůznější kontrolní systémy. (eset.com)

Jedná se o hojně rozšířený typ viru, který napadá jak soubory běžných uživatelů, tak systémy vládních organizací. V roce 2017 se rozšířil z Národní bezpečnostní agentury ve Spojených státech amerických ransomware s názvem Wanna Cryptor, který napadal zařízení

s operačním systémem Windows. Při vypuknutí pandemie COVID-19 došlo k rozšíření aplikace CovidLock, která slibovala přístup k datům, týkajících se šíření nákazy, po instalaci zablokovala mobilní zařízení a pod výhružkou odhalení uloženého obsahu vyžadovala zaplacení výkupného. (gatefy.com, 2021)

3.4.2.5 Trojský kůň

Tento typ malwaru, jehož název je příhodně odvozen od dobytí města Tróje, si uživatel nainstaluje do počítače sám jako součást neškodného programu (s koncovkou .exe), například hry nebo nástroje k usnadnění práce na počítači. Mnohdy je malware v nečinnosti a aktivuje se při navštívení určité stránky nebo otevření aplikace a získává data, přebírá kontrolu nad zařízením, stahuje jiný škodlivý software – podle toho, jak je naprogramovaný. Typicky se využívá k vytvoření backdoors, umožňující získat přístup do ostatních zařízení přes počítačovou síť. (McCarthy, 2013)

3.4.2.6 Worm

Počítačový červ je typem malwaru (někdy bývá nesprávně označován jako počítačový virus), jehož cíl je stejný jako u ostatních škodlivých softwarů a psychologických podvodných metod, a to připravit uživatele o jeho data nebo je poškodit, zásadně se ale liší způsobem šíření. Worm se dokáže sám replikovat a odesílat své kopie do ostatních zařízení. Během toho může využívat systémové chyby v počítači, například pokud si uživatel neodborně přenastaví BIOS, usnadní mu převzetí kontroly nad síťovou komunikací. (McCarthy, 2013)

3.4.2.7 Spyware

Jedná se o těžko odhalitelný druh viru, který nemá za úkol aktivně zablokovat přístup k souborům, ale sledovat činnost uživatele a shromažďovat informace, které následně odesílá jeho tvůrci. Mezi nejznámější typy spywarů patří:

- Infostealer – monitoruje zařízení a odesílá osobní data (historii vyhledávání, uživatelská jména, hesla, e-mailové adresy atd.),
- Password Stealer – speciálně vytvořený pro získání přihlašovacích údajů,
- Keylogger – nahrává znaky stisknuté na klávesnici. (SoftwareLab.org)

3.4.2.8 Adware

Advertising-supported software má, jak již vyplývá z názvu, upozornit na inzerovanou reklamu. Bývá doprovázen pop-up okny, zpomaluje webový prohlížeč, přesměrovává na infikované stránky a reklamy překrývají velkou část obrazovky. Primárně slouží k přesměrování uživatele k jinému viru, který napadne jeho soubory. (McCarthy, 2013)

3.4.2.9 Spam

S tímto typem internetové hrozby přišel do kontaktu každý uživatel. Spam sice přímo neohrozí osobní data, může ale v uživateli vyvolat jednání, které je ohrozí. Součástí spamu bývají hoaxy, které podporují psychologickou manipulaci. V minulosti se vyskytoval výhradně v e-mailové komunikaci, zřídka ve formě SMS zpráv, v současné době je hojně rozšířený zejména na sociálních sítích, právě ve spojení s hoaxy a fake news, případně je šířen za účelem marketingové propagace. (Polčák, 2007)

3.4.2.10 Cookies

Soubory cookies jsou mezi uživateli hojně diskutované téma. Při navštívení téměř jakékoli webové stránky je zobrazeno pop-up okno, které po uživateli vyžaduje informovaný souhlas s používáním souborů cookies a dalších síťových identifikátorů, které mohou obsahovat informace s osobními údaji a činnostech uživatele. Pro provozovatele webů a firmy je tento nástroj vysoce užitečný ke zdokonalování svých služeb, identifikaci návštěvníků, statistický účelům a personalizování stránek. Obecně lze cookies rozdělit podle účelu použití do následujících skupin:

- sledovací a konverzní – k analyzování prodeje,
- marketingové – k personalizaci obsahu a reklam,
- analytické a esenciální – k zefektivnění uživatelského prostředí.

I přesto, že je uživatel chráněn Zákonem o zpracování osobních údajů, mohou tyto soubory představovat riziko – pokud někdo získá přístup k jeho zařízení, kde se trvalé soubory cookies ukládají na disk, dají se data zneužít. Řada uživatelů navíc neví o možnosti zakázání používání síťových identifikátorů v nastavení prohlížeče, která není webovými stránkami dostatečně zdůrazňována, protože pro provozovatele nepředstavuje chtěnou variantu. Zakázání využívání souborů cookies ale mívá za následek omezení některých

funkcí stránek. Pro získání souhlasu s použitím souborů je využíván opt-in, pouze zřídka opt-out režim. (McCarthy, 2013)

3.4.2.11 DoS a DDoS útoky

Typickým cílem Denial of Service útoků bývá vyřazení serverů z provozu, znepřístupnění služby nebo sítě, za použití exploitu, během čehož útočníci využívají chyb a vyčerpání systémových prvků. V případě DDoS útoku se jedná o distribuovaný DoS útok, který se liší v tom, že k útoku využívá více počítačů, ze kterých ve stejném čase odešle požadavek a způsobí již zmíněné vyčerpání zdrojů.

Tento aktuální typ hrozby je ve větší míře směřován proti firmám a organizacím, uživatele ale může připravit například o přístup k datům umístěných na serveru nebo znemožnit připojení modemu k internetu. Tvůrci DoS a DDoS útoků následně požadují po firmách výkupné, aby jejich služby opět zpřístupnili zákazníkům. Zajímavé je, že podle současné právní legislativy nelze tyto útoky jednoznačně označit jako trestné. (Keary, 2020)

- Sociální inženýrství

Tento pojem se čím dál více dostává do obecného povědomí. Jedná se o formu počítačového napadení, která je cílena na lidský faktor, je totiž snazší přimět k chybě uživatele nežli software. Metody sociálního inženýrství využívají nejčastěji manipulativního nátlaku, důvěřivosti, ale mnohdy jen prosté neznalosti rizik nebo věcí technického rázu ze strany uživatelů. (Kožíšek, 2016)

3.4.2.12 Phishing

Od malwarů a virů se toto riziko liší tím, že se více zaměřuje na lidskou psychiku. Psychologický nátlak, využívaný zejména v elektronické komunikaci, má za úkol získat přístup k nejcitlivějším údajům jako jsou přihlašovací údaje, hesla, čísla bankovních účtů nebo kreditních karet. Autor phishingového útoku se snaží pod falešnou identitou zmanipulovat uživatele takovým způsobem, aby uvěřil jeho tvrzením. Metody manipulace se stále zdokonalují a je čím dál tím těžší je odhalit, typicky je uživatel obviněn z nelegální činnosti a je po něm vyžadováno na falešných webových stránkách věrně připomínajících web Policie ČR nebo Exekutorského úřadu

zaplacení pokuty. Občas je tato metoda doprovázena zobrazením vyskakovacího okna a infikováním počítače, které způsobuje spuštění beep kódu, který lze například slýchat při průběhu POST testů, vše má za úkol vyvinout ještě věrohodnější nátlak na uživatele. (Kožíšek, 2016)

3.4.2.13 Vishing

Vishing na rozdíl od phishingu nevyužívá k získání dat webové stránky. Jedná se o metodu sociálního inženýrství a uživatel je zprávami vyzván pod záštitou falešné organizace (například zpráva od banky nebo správce sociální sítě), aby zavolal na uvedené telefonní číslo, kde jsou z něj vymámeny osobní údaje jako je heslo, PIN, autorizační kódy atd. Časté je v rámci vishingu také otevření přílohy v podvodném e-mailu od exekutorského úřadu, která se napojí na internetové i mobilní bankovnictví a připraví majitele účtu o přístup a finanční prostředky. (Moravčík, 2021)

3.4.2.14 Kyberšikana

K tomu, aby byl uživatel připraven o své osobní údaje, mnohdy není zapotřebí tvorby složitých programů. Kyberšikana pracuje především s lidskou psychikou a sebelepší technické zabezpečení na ni zpravidla nemá vliv. Probíhá prostřednictvím běžné elektronické komunikace jako jsou e-maily, chatování nebo skrz sociální aplikace. Uživatelé jsou dlouhodobě zastrašováni, vydíráni a nuceni k poskytnutí přístupu k osobním údajům. Kyberšikana nemusí být vždy osobního charakteru a probíhat mezi lidmi, kteří se navzájem znají. Útočníci se především na sociálních sítích pod falešnou identitou sblíží s uživatelem, který jim mnohdy nevědomky poskytne prostředky k vydírání, typická je v tomto případě krádež online identity. (Kožíšek, 2016)

3.4.2.15 Interní chyba

K úniku dat nemusí dojít přímým zaviněných ze strany jejich vlastníka, ale také ze strany osob či institucí, kterým jsou data svěřena. Typickým příkladem může být nedodržení, ignorování nebo pouhé opomenutí předepsaných postupů zaměstnanci banky nebo selhání bezpečnostních systémů v bankovnictví. Z těchto důvodů jsou zaměstnanci, pracující s nejcitlivějšími údaji klientů, opakovaně podrobováni bezpečnostním prověrkám.

3.5 Způsoby ochrany

3.5.1 Základní bezpečnostní zásady

Do této kategorie spadají především tři základní zásady:

- vytvořit silné heslo a dvě e-mailové adresy – první pro komerční účely a druhou pro spravování svého soukromí,
- neotevírat podezřelé e-maily a hypertextové odkazy,
- nesdělovat identifikační údaje a hesla, především na sociálních sítích.

3.5.2 Bezpečnostní školení, sebevzdělávání

Nejdůležitějším aspektem ochrany dat uživatelů je jejich informování o škále rizik, schopností nových technologií, principů funkčnosti antivirových programů a celkové prohloubení znalostí v oblasti IT.

Nejčastěji využívanou metodou a nejsnadnějším přístupem k přehledným informacím jsou bezpečnostní školení. Zpravidla této metody využívají firmy, školy a nejrůznější instituce ke školení svých zaměstnanců, ať už nově příchozích nebo pro přeškolení stávajících, právě za účelem eliminování interních chyb při vykonávání běžných pracovních činností.

Dalším klíčových prvkem ochrany osobních údajů je sebevzdělávání. Nejefektivněji uživatel zabrání úniku svých dat tím, že se vyvaruje rizikového jednání a chyb, vedoucích ke ztrátě jeho údajů. Způsobů sebevzdělání je celá řada, od bezpečnostních a naučných školení a kurzů, přes čtení odborných knih, článků a příruček, vyslechnutí rad odborníků až po prosté pročítání informací na internetu. Novinkou posledních let se stávají projekty a vzdělávací programy, které mají za cíl šířit osvětu právě v oblasti prevence ochrany osobních údajů.

Neméně důležitým bodem prevence je školení nezletilých v oblasti ochrany osobních údajů. Nezletilí a mladiství sice nenabývají takových práv jako dospělí, ale je jim stejnou měrou umožňován pohyb na internetu a využívání sociálních sítí. Děti a dospívající jsou sice od útlého věku obklopeni technologiemi, ale málokdy jsou jim vštěpovány možná rizika a způsoby ochrany. Tuto skutečnost se pokoušejí podchytit základní a střední školy pořádáním preventivních programů a začleňováním své školy do projektů, týkajících se gramotnosti v oblasti IT. (Kožíšek, 2016)

3.5.2.1 Trendy v oblasti zabezpečení dat

Trendy v oblasti zabezpečení se neustále rozvíjí. Škála nabídek zabezpečení a množství IT specialistů, zabývajících se touto problematikou, musejí pružně reagovat na nejnovější metody hackerů.

3.5.2.2 Antivirový program

Pravděpodobně nejznámější forma ochrany před viry je antivirový program. Dnešní antiviry disponují vícevrstvou ochranou, tedy kromě detekce a odstranění virů, malwarů, ransomwarů, spamů atd., napomáhají k ochraně proti krádeži hesel, účtů, kreditních karet a šifrují soubory. I obyčejná verze antivirového programu, kterou lze stáhnout zdarma na internetu, může zachytit nejen škodlivý kód, ale také aplikace a soubory. Tento typ ochrany je uživatelsky velmi přívětivý a k jeho užívání není třeba hlubších technických znalostí. Na rozvíjející se trendy sociálního inženýrství reagují i vývojáři antivirů. Jimi vyvinuté programy dokážou v mnoha případech odhalit například phishing. (eset.com)

3.5.2.3 Firewall

Firewall bývá označován jako primární ochrana počítače před napadením. Je již součástí novějších operačních systémů Windows a jeho činnost běžný uživatel v podstatě nezaznamená, aktuální třetí generace dokáže rozeznat i protokoly FTP a HTTP. Na zařízeních uživatelů je běžně softwarový firewall, cenově náročnější, hardwarový, je využíván zejména v případech, kdy je pro uživatele žádoucí připojit více zařízení do sítě.

Výhodou je vyšší rychlost, efektivnější ochrana a nezávislost na operačním systému. Výběr některých typů firewallů, je pro přehlednost porovnán v tabulce. (Scarfone, 2009)

Tabulka 1 - Porovnání firewallů

Typ firewallu	Výhody	Nevýhody
Paketový (nestavový) filtr	vysoká rychlost přenosu, flexibilita	malá úroveň kontroly spojení, nízká bezpečnost
Stavový inspekční firewall	vysoká rychlost kontroly a bezpečnost	náročnost na výkon
Aplikační - proxy brány	vysoká bezpečnost a míra kontroly, filtrování obsahu paketu	náročnost na výkon, pomalejší přenos

Zdroj: vlastní zpracování, Scarfone, 2009

3.5.2.4 VPN

S výskytem Covidu-19 se služby VPN dostaly do širokého povědomí díky služebním počítačům, kdy byli zaměstnavatelé nuceni zajistit co možná nejefektivnější ochranu firemních dat během homeofficů a zároveň splňovat požadavky Obecného nařízení o ochraně osobních údajů. Během aktivního VPN připojení nejsou údaje odesílány přímo webu, ale zašifrovány a poslány na zvolený VPN server, který je až poté předá webu, stejný princip je uplatňován i při získávání údajů z webu. Pro útočníka je tak obtížnější získat IP adresu konkrétního uživatele. Nevýhodou v tomto případě může být nižší přenosová rychlost dat a zpoplatnění VPN služeb. (Bořánek, 2017)

3.5.2.5 Honeypot

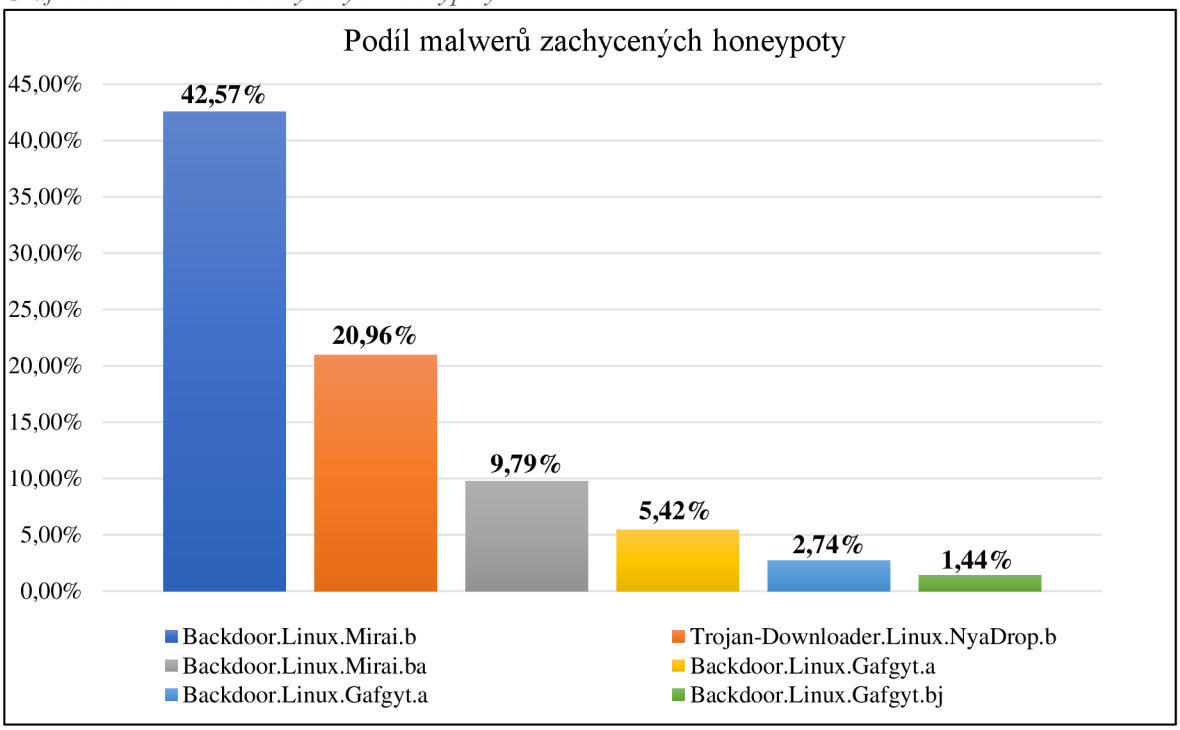
Zajímavým trendem v oblasti ochrany dat je honeypot. Jedná se o uměle vytvořený prvek v síti, který simuluje reálné zařízení s uživatelem nebo server se všemi jeho vlastnostmi.

Tato simulace s nízkou mírou zabezpečení má za cíl nalákat, analyzovat a odhalit techniky útoků, zdržet útočníka nebo odvést jeho pozornost. Může mít formu aktivní, kdy interaguje s prostředním webu, nebo pasivní, kdy nevyvíjí žádnou aktivitu a vyčkává na okamžik, kdy bude moci začít sbírat data. Pokud by honeypoty svojí užitečností a výhodami převyšovaly míru nevýhod jako je možná náročnost na vytvoření a požadavky na výkon, mohly by se v budoucnu stát součástí standardních

způsobů zabezpečení, běžnou natolik jako vytvoření hesla. (DIGITÁLNÍ PEVNOST, 2018)

V následujícím grafu je zobrazen procentuální podíl prvních šesti nejúspěšnějších útoků malwarů, které byly načteny honeypot zařízeními. Graf byl vytvořen na základě dat ze Security bulletinu od firmy Kaspersky, získaných z webových stránek secure.com, zabývajících se sumarizací hrozeb, informováním o rizicích a analyzováním útoků. Statistická data jsou získána v rámci států Evropské unie. (Kaspersky Security Bulletin, 2021)

Graf 1 Podíl malwarů zachycených honeypoty



Zdroj: vlastní zpracování, Kaspersky Security Bulletin (2021)

3.5.2.6 Dvoufázové ověřování

Tímto druhem zabezpečení disponují nejčastěji emailové účty, online bankovnictví, platební brány nebo mobilní bankovní aplikace. Jedná se o zdokonalený způsob ověřování identity uživatele. V první fázi je požadována tvorba bezpečného hesla s malou pravděpodobností prolomení a ve druhé doplňkové ověření totožnosti, které může být například v podobě otisku prstu, skenování obličeje na mobilním zařízení, přihlášení do přidružené aplikace a potvrzení prováděné aktivity, zaslání SMS nebo emailu s autorizačním kódem. Tento typ ověřování se rozšířil zejména s rozvojem online nákupů a plateb a

ustávající potřebou fyzicky navštěvovat úřady a finanční instituce jako jsou například banky a pojišťovny.

3.5.2.7 Digitální certifikáty

Digitální certifikáty jsou efektivním prostředkem k ověření totožnosti osoby (případně serveru). Do širokého povědomí uživatelů se dostaly již před lety, když jejich užívání začaly vyžadovat bankovní instituce pro přístup do online bankovnictví. Dnes jsou pravděpodobně nejznámější díky očkovacímu certifikátu proti Covidu-19, jejich využití je ale daleko širší. Certifikační autority neboli vydavatelé certifikátů je využívají k ověření digitálního podpisu, například k potvrzení o studiu. Povinnými prvky certifikátu jsou zpravidla informace o Certifikační autoritě, datum platnosti a jeho jednoznačné určení (například identifikačním kódem).

Mezi certifikáty se řadí i SSL a TLS protokoly, přičemž novější TLS postupně nahrazuje SSL. Tyto certifikáty mají dvojí funkci, zaprvé ověření identity a zadruhé šifrování komunikace například mezi klientem a serverem. Uživatel s nimi běžně přichází do kontaktu v internetovém prohlížeči, kdy je adresový řádek označen zkratkou HTTPS. Certifikáty fungují na principu asymetrické kryptografie, kdy se k šifrování a dešifrování používají odlišné klíče – veřejný a soukromý. Veřejný klíč slouží k zašifrování dat, s jeho pomocí ale nelze zprávy dešifrovat, k tomu slouží klíč soukromý.

Seznam některých certifikátů je do zařízení načten již při instalaci operačního systému za účelem okamžité komunikace s požadovaným serverem. (Hanák, 2016)

3.5.2.8 Umělá inteligence

V souvislosti s bezpečností dat nelze mluvit o umělé inteligenci jako takové, ale pouze o tzv. slabé umělé inteligenci. Tato forma je charakteristická tím, že je pečlivě naprogramována k řešení pouze jednoho, detailně strukturovaného problému. Takto naprogramovaná zařízení jsou schopna se učit a zdokolovat v řešení přiděleného úkolu na základě své předešlé aktivity a nasbíraných dat. Celý proces funguje na bázi opakujících se vzorců, z nichž si zařízení se slabou umělou inteligencí vytváří vlastní modely chování, na základě kterých vylepšuje svoji následnou činnost. (acronis.cz, 2018)

3.5.2.9 Aktualizace a zálohování

Aktualizace a zálohování dat asi nelze označit přímo za trend, důležitost těchto kroků ale uživatelé často opomíjejí. Výrobci a vývojáři se snaží s tímto problémem bojovat a nabízejí možnosti automatických aktualizací, aby se uživatel nemusel o aktualizace starat, ale přesto byla jeho osobní data co nejlépe chráněna. Co ale nabývá na popularitě, je zálohování dat na cloudová úložiště. Uživatele láká vidina toho, že mají ke svým souborům a datům přístup prakticky odkudkoli a nemusejí mít po ruce žádné paměťové medium. Jedinou podmínkou bývá uživatelský účet, v některých případech jsou služby zálohování zpoplatněny, ale zpravidla se nejedná o závratné částky, u cloudových úložišť pro velké společností je tomu ovšem jinak. Populární je také využívání webových aplikací, například od nástrojů Microsoft Office, které umožňují nejen online editaci obsahu, ale také automatické ukládání. (McCarthy, 2013)

3.5.2.10 Hotspoty

Dočasnou, ale přesto efektivní metodou může být využívání internetového připojení prostřednictvím hotspotu v mobilním telefonu. V případě zjištění IP adresy zařízení nebo pouze pokud uživatel nechce mít viditelnou svoji obvyklou IP adresu, může využít datového připojení na mobilním telefonu a jeho IP adresa se změní. Nevýhodou je tato metoda v případě, že uživatel potřebuje přistoupit k informacím, které jsou omezeny na základě geografické polohy. (McCarthy, 2013)

3.5.2.11 Vlastní testování zabezpečení

Nejlepším způsobem, jak ověřit míru zabezpečení je jeho otestování. Pro běžné uživatele není příliš reálný v nějakém větším měřítku. O bezpečí svých údajů se mohou přesvědčit například kontrolami zabezpečení, které nabízejí internetové domény v případě, že u nich vlastní uživatelský účet. Během této analýzy je uživatel proveden sadou úkonů, které mají navýšit míru ochrany, jedná se o změnu hesla, dvoufázové ověření, stažení digitálního certifikátu atd.

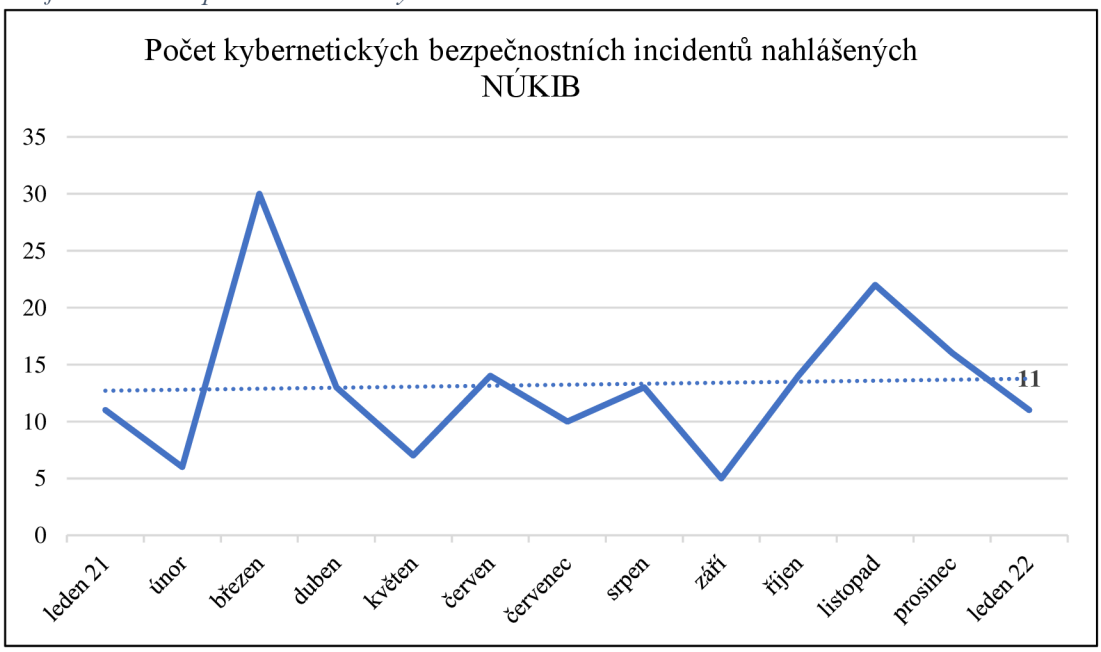
Na rozdíl od omezených možností běžných uživatelů je tento trend ve velké míře využíván státními i soukromými institucemi najímajícími firmy, které mají za úkol prověřit a případně vylepšit zabezpečení dat a systémů. Zajímavým trendem jsou tzv. friendly hackeři, někdy jsou také nazývaní jako white hat hackeři. Jedná se o IT specialisty, kteří mají

za úkol prověřit bezpečnost. Nabourají se do systému daného subjektu a získají přístup k jeho datům a souborům. Daný subjekt může na základě tohoto přátelského hackerského útoku vylepšit systém zabezpečení a vyzkoušet si své krizové postupy. (kaspersky.com)

3.6 NÚKIB

Dalším, pro uživatele prakticky neovlivnitelným rizikem narušení bezpečnosti osobních údajů, je jejich ztráta ze strany jiného subjektu. Útočník se naboura do systému nějaké organizace a získá tak přístup k údajům, které daná organizace spravuje. Pokud může mít takováto ztráta nebo samotné nabourání do systému vážnější následky, nahlásí se Národnímu úřadu pro kybernetickou a informační bezpečnost neboli NÚKIB.

Graf 2 NÚKIB bezpečnostní incidenty



Zdroj: vlastní zpracování, Národní úřad pro kybernetickou a informační bezpečnost (2022)

Z grafu jsou vidět počty nahlášených kybernetických incidentů Národnímu úřadu pro kybernetickou a informační bezpečnost. Na první pohled je patrný velký nárůst počtu hlášených případů v březnu roku 2021. Důvodem byla zranitelnost ProxyLogon. Jedná se o zranitelnost serveru Microsoft Exchange Server, která umožňuje útočníkovi obejít ověřování a vydávat se za správce. (proxylogon.com, 2021)

Hackeři využívali útok ke dvěma hlavním účelům. Jednak se dostali k citlivým informacím a údajům, které měli možnost zašifrovat a následně subjekt vydírat, za druhé mohli na serveru těžit kryptoměnu. Toto se jim podařilo pomocí malwaru Lemon_Duck, který se zaměřuje právě na těžbu kryptoměn tzv. cryptominer a aktuálně je jedním z nejpokročilejších typů těžebního malwaru. Tyto cryptominery spotřebovávají na hostitelském systému výpočetní výkon a přináší i dodatečné náklady za elektřinu. Podle odhadů byly těmito útoky ohroženy až desítky tisíc společností. Microsoft pohotově reagoval vydáním aktualizace zabezpečení, které by zranitelnost v Exchange Serveru měly odstranit. Zákazníci si je ovšem musí nainstalovat sami, což způsobilo značnou prodlevu v řešení tohoto problému. (Palyza, 2021)

Druhý viditelný nárůst nahlášených incidentů byl v listopadu roku 2021. Zde se jednalo o zneužívání zranitelnosti ProxyShell a nárůstu ransomwarových útoků. Opět byly postiženy servery Microsoft Exchange Server, kdy tento útok umožnil na server nahrát webshell a díky tomu mohli útočníci vzdáleně spouštět kód s nejvyšším oprávněním a zcela kompromitovat daný server. (nukib.cz, 2021)

Mimo těchto dvou výraznějších výkyvů ale k žádným dalším za uplynulý rok nedošlo a trend za celý rok je tedy zhruba 13-14 hlášených případů za měsíc. NÚKIB rozlišuje incidenty dle závažnosti na méně významné, významné a velmi významné, závažnost je definována ve vyhlášce č. 82/2018 Sb. a v interní metodice NÚKIB. Velmi významné incidenty se objevují pouze ojediněle, za minulý rok 2021 jich bylo 8. Významné a méně významné incidenty byly zastoupeny ve vzájemně srovnatelném poměru. (nukib.cz, 2021)

3.6.1 Trendv kybernetické bezpečnosti bezpečnosti podle NÚKIB za leden 2022

V lednu roku 2022 došlo celkem k 11 nahlášeným incidentům, což je méně, než byl trend za předcházející rok 2021. Skoro dvě třetiny nahlášených incidentů v lednu zasáhly veřejný sektor. Jednalo se o úspěšné phishingové kampaně, ransomwary a také využití zranitelnosti Log4Shell.

Phishingové kampaně evidoval NÚKIB na začátku roku dvě. Byly zacíleny zejména na české veřejné instituce. Oba případy začaly tak, že se útočníkům podařilo kompromitovat uživatelské účty a z nich dále podnikat phishingové útoky na různé domény a další veřejné instituce. V jedné z kampaní byl útočníkem použit tzv. thread hijacking, což znamená, že byly použity již existující komunikace oběti, na ty útočník navázal a zprávy se škodlivými odkazy poslal v odpovědi na tato vlákna.

Ransomware se v lednu tohoto roku řešil také dvakrát. To je oproti předchozím dvěma měsícům z hlediska počtu těchto útoků pokles. První ransomware Jigsaw se objevil ve státní organizaci, druhý NightSky v soukromé společnosti. V případě ransomwaru NightSky útočníci napřed využili zranitelnosti Log4Shell, tím se dostali do sítě subjektu a poté zašifrovali jeho systém. Tento ransomware patří k novým svého druhu, poprvé začal útočit ve druhé polovině prosince roku 2021, chvíli poté, co byla zveřejněna zranitelnost.

NÚKIB řešil v lednu roku 2022 dva incidenty v souvislosti s využitím zranitelnosti Log4Shell. V první situaci byl kompromitován server pro správu mobilních zařízení, ale nebyly zaznamenány žádné jiné škody. Druhý případ je popsán výše, kdy byl použit ransomware a útočník subjektu data zašifroval. (nukib.cz, 2021)

3.7 Shrnutí

V teoretické části práce byl vymezen rozsah pojmu osobní údaje a jejich ukotvení v legislativě České republiky. Zmíněn byl koncept procesů C.I.A., sestávající ze 3 základních pilířů ochrany dat. Dále byly obecně popsány hrozby a rizika, následuje jejich rozdělení do dvou skupin na subjektivní, které má uživatel možnost do určité míry ovlivnit, a objektivní, které přímo nezávisejí na jeho činnosti. Další část práce byla věnována způsobům ochrany dat, zmapování nejnovějších trendů a zdůraznění míry důležitosti osobního rozvoje v oblasti ochrany dat v IT světě. V závěru teoretické části byly porovnány statistické údaje o kybernetických útocích ze stránek Národního úřadu pro kybernetickou a informační bezpečnost za období leden 2021 až leden 2022.

4 Vlastní práce

Dle dat Národního úřadu pro kybernetickou a informační bezpečnost je patrné, že trend kybernetických útoků nebude mít v nejbližší době klesající charakter, spíše naopak. Na základě této skutečnosti je třeba zvyšovat zabezpečení a informovanost o těchto problémech nejen ve státních institucích a obchodních korporátech, ale především mezi běžnými uživateli, kteří se stávají čím dál snadnějším terčem. Vzhledem k této skutečnosti je v praktické části zjišťováno povědomí uživatelů o bezpečnostních prvcích a mapováno jejich jednání v online prostředí a manipulace s osobními daty.

Praktická část práce je realizována prostřednictvím vlastního experimentu, kdy byly subjekty (uživatelé) vystaveny simulacím a úkolům, ve kterých bylo zkoumáno jejich chování a nakládání s osobními údaji. Pro získání dat v rámci vlastního experimentu byla vytvořena úniková hra, která obsahuje jedenáct modelových situací. Sběr dat formou hry byl vybrán s cílem co nejvěrohodněji simulovat reálnou situaci, aby uživatel odpověděl co nejpravdivěji a ne tak, jak si myslí, že se od něj očekává. Dokumentace celé únikové hry je vložena prostřednictvím příloh, odkaz na hru samotnou je obsažen v příloze č. 15.

4.1 Charakteristika vlastního experimentu

Pro realizaci hry byl vybrán prezentační program Google Slides od společnosti Google, především na základě skutečnosti, že umožňuje bezplatně využívat nejrůznější nástroje jako jsou animace či videa, jeho ovládání je pro uživatele intuitivní a hra je po vygenerování odkazu dostupná komukoli bez nutnosti registrace či přihlášení.

Hra nese název „YOUR DATA OR MY DATA?“ a skládá se z dvanácti úkolů, přičemž v jedenácti z nich je zkoumáno chování a znalosti testovaných subjektů, v poslední (bezbodové) úloze jsou mapovány jejich preference rozvoje znalostí v oblasti zabezpečení dat. Tématu z každé simulace se věnovala teoretická část práce. Celkový počet bodů, kterého je možno dosáhnout, je dvacet pět.

Ke spuštění hry je doporučeno využít počítač, je však možné ji otevřít i na jakémkoli jiném zařízení. Na samém počátku hry jsou uživateli zobrazeny instrukce k jejímu hraní a QR kód, který je možné oskenovat prostřednictvím mobilního telefonu a otevřít formulář pro zaznamenání odpovědí. Formulář byl vytvořen v softwaru pro správu průzkumů Google Forms, který umožňuje anonymní evidenci odpovědí. V úvodu záznamového archu musí uživatel odpovědět na tři otázky, které mají ucelit základní představu o věku, vzdělání a je

zde vyhrazen prostor k osobnímu zhodnocení znalostí v oblasti kybernetické bezpečnosti na škále od 1 do 10 (1 – amatér, 10 – expert). Jednotlivé úkoly ve hře a odpovědní archy ve formuláři jsou pro lepší orientaci provázány prostřednictvím shodného symbolu. V případě nefunkčnosti QR kódu je k dispozici odkaz pro spuštění formuláře.

V další fázi je subjektu nastíněn příběh hry. Jeho zařízení bylo napadeno tzv. white hat hackerem, který je zmiňován v teoretické části práce, jehož cílem není uživatele o jeho data nenávratně připravit. Subjekt je vyzván ke hraní hry, která má sloužit k prověření jeho znalostí v oblasti kybernetické bezpečnosti. V případě, že subjekt prokáže, že jsou jeho znalosti dostačující, o hackerovi již nikdy neuslyší. Pokud neuspěje, přístup k jeho datům mu bude na dobu šesti měsíců odepřen, tuto dobu považuje hacker za dostatečnou k doplnění znalostí.

Hra sestává z hlavní hrací plochy, na které se po absolvování každé simulace objeví interaktivní ikona, vedoucí k simulaci následující. Celé prostředí je vytvářeno v souladu s metodami UI designu. Formulář je realizován prostřednictvím single choice a z velké části multiple choice odpovědí. K formátu multiple choice odpovědí bylo přistoupeno z důvodu znesnadnění tipování ze strany subjektu, aby byl poskytnut co nejreálnější obraz o jeho znalostech a schopnostech.

V závěru hry je testovanému subjektu zobrazen souhrn jeho výsledků se správnými odpověďmi. Na základě počtu získaných bodů zvolí ve hře jednu ze tří skupin možných výsledků, které jsou rozděleny dle úspěšnosti následujícím způsobem:

a) 0 – 12 bodů,
b) 13 – 18 bodů,
c) 19 – 25 bodů.

V případě, že subjekt spadá do skupiny a), ve hře neuspěl a je mu zobrazena zpráva od white hat hackera, že jeho data jsou na šest měsíců zablokována. Pokud subjekt dosáhl počtu bodů odpovídajících skupině b), je informován, že jeho data jsou v bezpečí, ale zároveň je mu doporučeno, aby své znalosti nepřestával rozvíjet. V případě zařazení subjektu do skupiny c), je mu dáno najevo, že jeho výsledek je velmi dobrý.

4.2 Dokumentace experimentu

V této kapitole budou popsány jednotlivé simulace a úkoly, kterým byly subjekty vystaveny. Dále bude zdůvodněna volba single choice nebo multiple choice odpovědí.

4.2.1 Soubory cookies

První zkoumanou položkou ve hře jsou znalosti subjektu o souborech cookies, konkrétně jakým způsobem uděluje souhlas s jejich užíváním, zdali automaticky volí možnost „Povolit vše“ nebo potvrzuje jednotlivé typy zvlášť. Dále zda uživatelé ví, kam se soubory ukládají, k čemu slouží marketingové cookies a které jsou vždy povinné. Pro ilustraci jsou na několika obrázcích zobrazena vyskakující okna s udělením souhlasu používání. Úkol se soubory cookies, je zobrazen v příloze č. 2 – Soubory cookies.

4.2.2 Phishing – dvoufázové ověřování

V tomto případě byla prověřována reakce subjektu na zdokonalenou formu phishingu. Uživateli byla nastíněna situace, kdy je dlouholetým klientem banky a jakékoli odchozí platby dvoufázově ověřuje prostřednictvím mobilního telefonu. Právě mu dorazil email s odkazem a instrukcemi k dvoufázovému ověření příchozí online platby pomocí zadání klientského čísla a autorizačního SMS kódu. V případě zadání klientského čísla je uživatel přesměrován na další stránku, která požaduje vložení autorizačního SMS kódu. Klientská čísla nejsou takto propojena s telefonními čísly klientů, tudíž pouze po zadání klientského čísla nemůže být SMS kód obdržen. Této neznalosti některých uživatelů autor phishingu využívá a spoléhá, že po neobdržení SMS zvolí subjekt variantu „nebo znovu Poslat kód“, kde bude následně vyzván k zadání telefonního čísla. V tu chvíli bude tvůrce držitelem jak uživatelského e-mailu, klientského a telefonního čísla, tak autorizačního SMS kódu. S těmito údaji už je útočník schopen dostat se k bankovnímu účtu.

Pro autentičnost jsou na dvou obrázcích zobrazeny stránky banky a subjekt je tázán, zdali by pokračoval v ověřování dle instrukcí v emailu. Hlavní indikátor by pro uživatele měla představovat adresa v adresní řádku prohlížeče, dále nevšední ověření příchozí platby, a propojení klientského čísla s telefonním. Simulace phishingu je zobrazena v příloze č. 3 - Phishing - dvoufázové ověřování.

4.2.3 Zákonná legislativa

Znalost právních předpisů v online světě je jednou ze zásadních součástí informační bezpečnosti. Subjekt vybíral ze série možností, které měly za úkol zjistit, zda ví, k čemu slouží Úřad pro ochranu osobních údajů, jaký je uzákoněný věk, kdy mohou nezletilí udělit právoplatný souhlas se zpracováním osobních údajů, jakým zákonem ČR a nařízením

Evropské unie jsou definovány právní regulace a zda je správné tvrzení o režimu opt-out. Zadání úkolu s právní legislativou je k dispozici v příloze č. 4 – Zákonná legislativa.

4.2.4 Honeypoty

Dalším položkou, která byla zkoumána, byl přehled o moderních technologiích, podílejících se na ochraně dat. S velkou pravděpodobností běžní uživatelé nemají o existenci honeypotů nijak velké povědomí, proto obsah tohoto úkolu nebyl rozváděn do hloubky. V rámci tohoto úkolu je uživatel dotazován, zdali honeypoty slouží k ochraně před hackery a zkoumání jejich chování pro zefektivnění ochrany před nimi, nebo zdali mají obalamutit běžné uživatele pod rouškou nenápadnosti, a získat tak přístup k jejich datům. Dále byly předkládány základní tvrzení, zdali mohou honeypoty mít aktivní či pasivní formu a být náročné na vytvoření a výkon. Úkol se zadáním je k dostupný v příloze č. 5 – Honeypoty.

4.2.5 Pop-up okna

Pop-up okna bývají nejčastějším projevem adwaru nebo marketingové propagace. Cílem této simulace je zjistit, zdali subjekt vnímá pop-up okna jako potencionální hrozbu. Pro ilustraci je do hry vložen obrázek, zobrazující pop-up okno, které požaduje vyplnění e-mailové adresy, lze však pokračovat v prohlížení stránky zavřením příslušného okna. Jednou z možností výběru je, zdali jsou tato okna formou agresivního advertisingu. Simulace s pop-up okny je přiložena v příloze č. 6 – Pop-up okna.

4.2.6 Škodlivé softwary

V tomto úkolu byly zjišťovány znalosti subjektu v oblasti škodlivých softwarů, které tvoří nejpočetnější skupinu kybernetických a informačních hrozeb. Je zkoumáno, zdali uživatel považuje antivirus za kompletní ochranu před viry a malwary, dále jaké jsou jeho znalosti o ransomwarech, počítačových červech, spywarech (konkrétně Keyloggeru), spamech, a příčinách tzv. Blue Screen of Death neboli Modré obrazovky smrti. Škodlivé softwary jsou zobrazeny v příloze č. 7 – Škodlivé softwary.

4.2.7 Licenční podmínky

Oblast softwarových licencí do určité míry souvisí s legislativou a autorským zákonem. Povědomí o licenčních podmínkách stahované aplikace je naprosto zásadní

v oblasti ochrany osobních údajů, uživatel se udělením souhlasu přímo podílí na jejich uchovávání.

Subjektu byla nastíněna situace, kdy si chce stáhnout aplikaci na úpravu fotografií. Licenční smlouva, kterou musí potvrdit, mimo jiné obsahuje souhlas s uchováváním a využíváním jeho údajů v souladu se zásadami ochrany osobních údajů, dále že veškerá komunikace mezi ním a vlastníkem aplikace bude probíhat elektronickou formou, a že vlastník aplikace nenese odpovědnost za újmu způsobenou prozrazením přihlašovacích údajů.

V další fázi aplikace žádá o oprávnění k využívání následujících funkcí a služeb zařízení: kontakty, fotoaparát, fotografie a mediální obsah zařízení. Uživatel určuje, jaké licenční podmínky odsouhlasil a jaká povolení aplikaci udělí. Zadání licenčních podmínek je vloženo v příloze č. 8 – Licenční podmínky.

4.2.8 Phishing – sociální sítě

Jedním z nejčastějších míst, kde dochází k phishingu prostřednictvím zprávy, jsou právě sociální sítě. Tato simulace je cílena především na mladší generaci, nicméně provedena je tak, aby i subjekt, který neužívá sociální sítě, dokázal situaci správně vyhodnotit.

Uživateli je na instagramový účet doručena zpráva, že se stává výhercem mobilního telefonu. Ve zprávě je na obdarovaného kladen časový nátlak, aby klikl na přiložený odkaz, zaregistroval se a ofocenou registraci zaslal odesílateli zprávy. Firma, vyrábějící tento telefon, skutečně vyhlašovala soutěž prostřednictvím svého oficiálního profilu, jehož nickname (uživatelská přezdívka) i s profilovou fotografií a modrým symbolem s fajfkou, označujícím, že se jedná o oficiální, ověřený profil, je předložen při nastínění situace. Podvodná zpráva byla ovšem odeslána z profilu s jiným nicknamem bez symbolu. Uživatel může zvolit tři možnosti, jak zareaguje.

První je dodržení instrukcí ve zprávě, druhá nedodržení instrukcí ve zprávě a nahlášení profilu jako podvodného, a třetí snaha zjistit prostřednictvím chatu, zdali se nejedná o podvod. Simulace phishingu je k dispozici v příloze č. 9 – Phishing – sociální sítě.

4.2.9 Hlášení antivirového programu

Subjekt je postaven do situace, kdy mu přátelé zaslali složku s poklady ke společné dovolené. Když se snaží složku stáhnout a otevřít, antivirus mu zobrazí hlášení, že jeden ze

souborů obsahuje malware, přičemž ani jednomu z přátel, které zná osobně, se toto hlášení nezobrazilo. Je dotazován za a) zdali vytvoří výjimku v antiviru a spustí soubor; b) nebude otevírat složku a nespustí soubor; c) hlášení ignoruje; d) přesune soubor do karantény a složku otevře na mobilu, který takovéto hlášení nezobrazuje nebo nahlásí hlášení jako falešný obsah s soubor spustí. Hlášení antivirového programu je přiloženo v příloze č. 10 – Hlášení antivirového programu.

4.2.10 **DDos útoky**

I když DDos útoky nejsou typicky směřovány přímo proti uživatelům, mohou ohrozit přístup k jejich datům, a proto patří do možných hrozeb, o kterých by uživatelé měli mít povědomí. Subjekt je tázán, zdali DDos útoky primárně slouží k vyřazení serverů, webových stránek a znepřístupnění služeb nebo k napadení domácích sítí, bankovních účtů a zařízeních běžných uživatelů. Dále jsou zkoumány jeho znalosti v rozdílech Dos a DDos útoků. Zadání úkolu DDos útoku je zobrazeno v příloze č. 11 – DDos útoky.

4.2.11 **Digitální certifikáty**

Poslední úkol, kterému je subjekt vystaven je posouzení jeho znalostí digitálních certifikátů a šifrovacích protokolů. Těmito znalostmi opět disponují spíše uživatelé, kteří se v oboru IT pohybují, nicméně certifikáty a šifrování jsou velmi důležitým prvkem Uživatel je tázán, jakou mají funkci (ověření identity a šifrování), jestli fungují na principu asymetrické kryptografie, k čemu slouží veřejný a soukromý klíč, zdali mezi povinné prvky certifikátu patří informace o certifikační autoritě a jaký je rozdíl mezi SSL a TSL protokolem. Digitální certifikáty jsou k dispozici v příloze č. 12 – Digitální certifikáty.

4.2.12 **Vzdělání**

Cílem posledního úkolu hry není zkoumat chování či znalosti subjektu, ale zjistit co možná nejvíce ohledně preferencí, týkajících se vzdělání v oblasti ochrany osobních údajů. Pokud by nové informace v této oblasti byly sdělovány pro uživatele atraktivní formou, zvýšila by se jejich ochota zjišťovat více o nových poznatcích a trendech. Testovaný subjekt dostal za úkol formou multiple choice odpovědi sdělit, jakým způsobem by pro něj bylo nejefektivnější rozšiřovat své obzory v této oblasti. Dále bylo prostřednictvím úkolu mapováno, jaké bylo jeho dosavadní vzdělání, nabídnuty byly tři možnosti: dosud se žádným způsobem nevzdělával, jeho znalosti byly rozšiřovány prostřednictvím bezpečnostních

školení a kurzů (nejčastěji ve spojení s prací), a problematice osobních údajů se věnuje na profesionální úrovni (například v rámci svého zaměstnání).

V otázce preferovaných způsobů ohledně získávání nových informací mohl uživatel vybrat z následujících variant: bezpečnostní školení (typicky zajištěné zaměstnavatelem), sociální sítě (prostřednictvím postů a příběhů), pravidelné reporty v tištěné nebo elektronické podobě, internetové články, na které by vyskočilo upozornění na telefonu, a mobilní aplikace, týkající se aktuálních témat v oblasti kybernetické a informační bezpečnosti. Úkol s preferencemi v oblasti vzdělání je zobrazen v příloze č. 13 – Vzdělání.

5 Zhodnocení a doporučení

5.1 Zhodnocení výsledků hry

Celkem se vlastního experimentu zúčastnilo 126 testovaných subjektů, z čehož 19 dosahovalo věku nižšího než 17 let, 61 věku 18-39 let, 32 uživatelů bylo v rozmezí 40-59 let a 14 starších 60 let. Nejlepších výsledků vzhledem k věku dosáhli hráči ve věku 18-39 let, což lze označit za očekávaný výsledek vzhledem k tomu, že jsou v rámci studia nebo zaměstnání nuceni využívat jak internet, tak moderní technologie.

Nejčastější dosažené vzdělání představovalo vysokoškolské (48), poté středoškolské s maturitou (37), následně základní (23) a nakonec středoškolské bez maturity (18). Nejvýše bodů získali hráči, kteří mají dokončené vysokoškolské vzdělání, což pravděpodobně souvisí s vykonávaným povoláním, ve kterém je potřeba se dále vzdělávat, a jejich předchozím studiem na vysoké škole, kdy se s některými věcmi již mohli setkat.

Sebehodnocení v oblasti ochrany dat bylo uvedeno prostřednictvím procent vzhledem ke škále hodnocení 1-10. Nejvíce dotázaných, celkem 26 %, ohodnotilo své znalosti hodnotou 5, dalšími největšími skupinami byly subjekty, které své znalosti ohodnotily číslem 7, celkem 18 % z celkového počtu, a číslem 8, což bylo 14 % z celkového počtu. Hodnotu 1 a 10 si nepřidělil nikdo, 9 pouze jeden člověk.

Zajímavým faktem je, že téměř 40 % testovaných, kteří své znalosti ohodnotili číslem 7 nebo 8 dopadli stejně nebo hůře než ti, kteří se ohodnotili číslem 5, které tvořilo průměr sebehodnocení. Možným vysvětlením tohoto jevu je, že zejména mladší generace nadhodnocují své znalosti na základě toho, že na počítači tráví značnou část času, například hraním her.

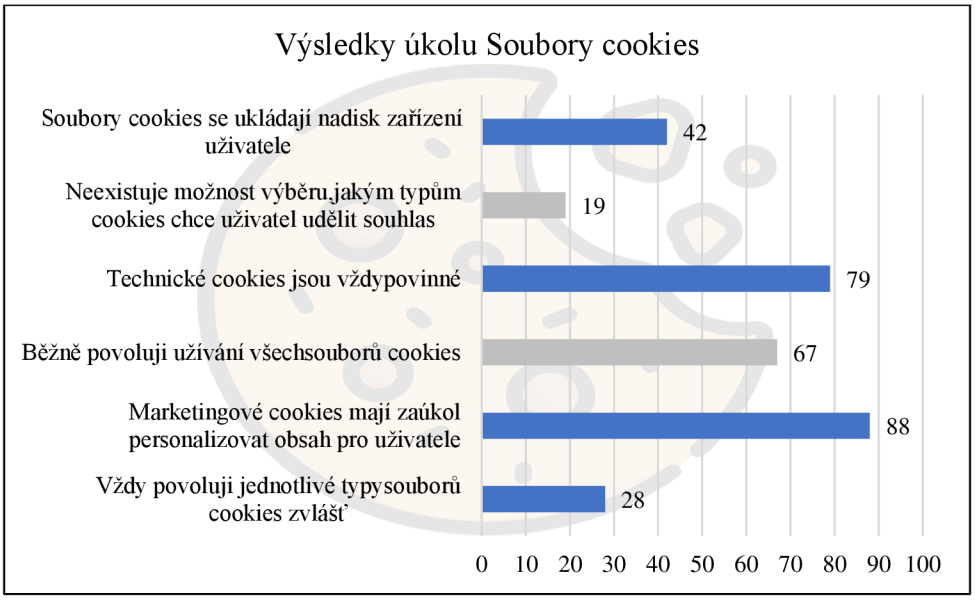
Z dostupných výsledků hry byly vybrány čtyři úkoly a jedna simulace, v nichž dotazovaní chybovali nejčastěji. Zjištění jsou prezentována prostřednictvím grafu, chybně zodpovězené otázky jsou zobrazeny šedivě, správné modře. Šestý graf se týká uvedení preferencí vzdělání v oblasti kybernetické bezpečnosti.

5.1.1 Výsledky úkolu Soubory cookies

V tomto úkolu 67 subjektů uvedlo, že běžně povolují užívání všech souborů. Tato skutečnost je pravděpodobně zaviněna nízkou informovaností, jak a k čemu soubory slouží. Pouhých 42 subjektů vědělo, že se ukládají na disk zařízení, sbírají data a následně jsou při

dalším připojení odeslána, oproti tomu 79 hráčů prokázalo znalost o povinnosti technických cookies. Na skutečnost nízké informovanosti poukazuje i fakt, že jednotlivé typy cookies pročítá a povoluje zvlášť pouze 28 uživatelů.

Graf 3 - Výsledky úkolu soubory cookies

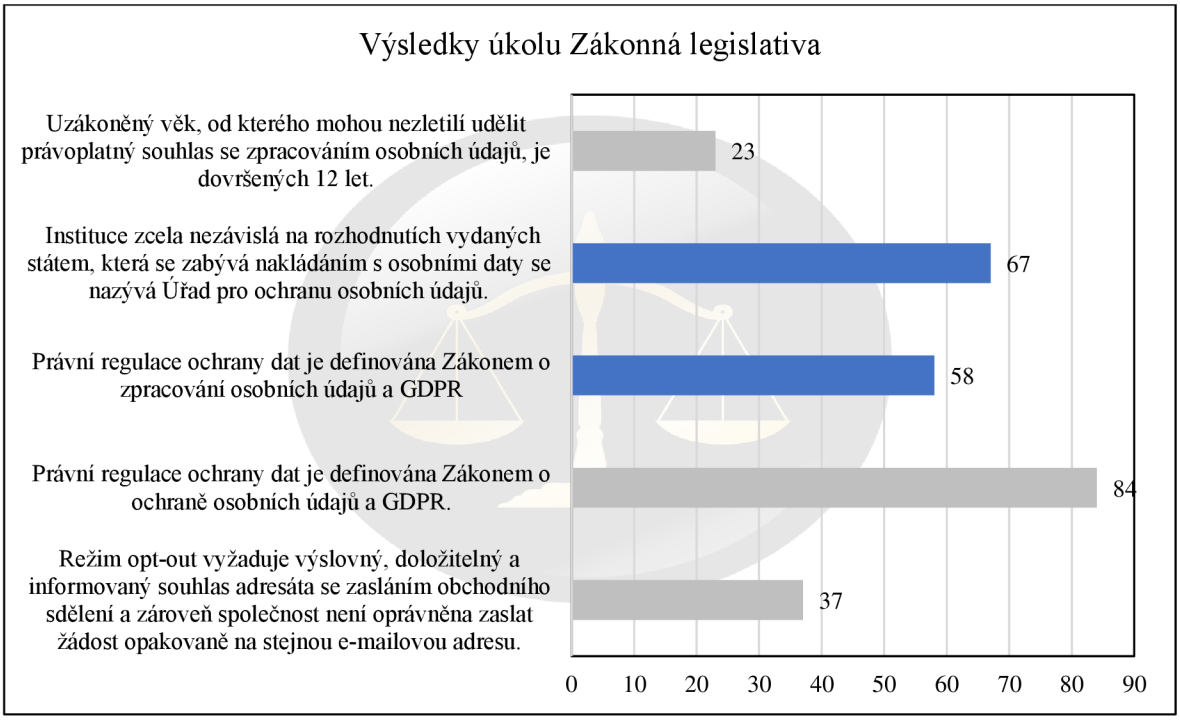


Zdroj: vlastní zpracování

5.1.2 Výsledky úkolu Zákonná legislativa

Nejvíce chybně zodpovězeným tvrzením bylo, že regulace ochrany dat je definována Zákonem o ochraně osobních údajů, který byl v roce 2019 nahrazen Zákonem o zpracování osobních údajů. O této skutečnosti nebylo informováno 84 testovaných subjektů. Za neutrální výsledek lze považovat povědomí o Úřadu pro ochranu osobních údajů.

Graf 4 - Výsledky úkolu Zákonná legislativa

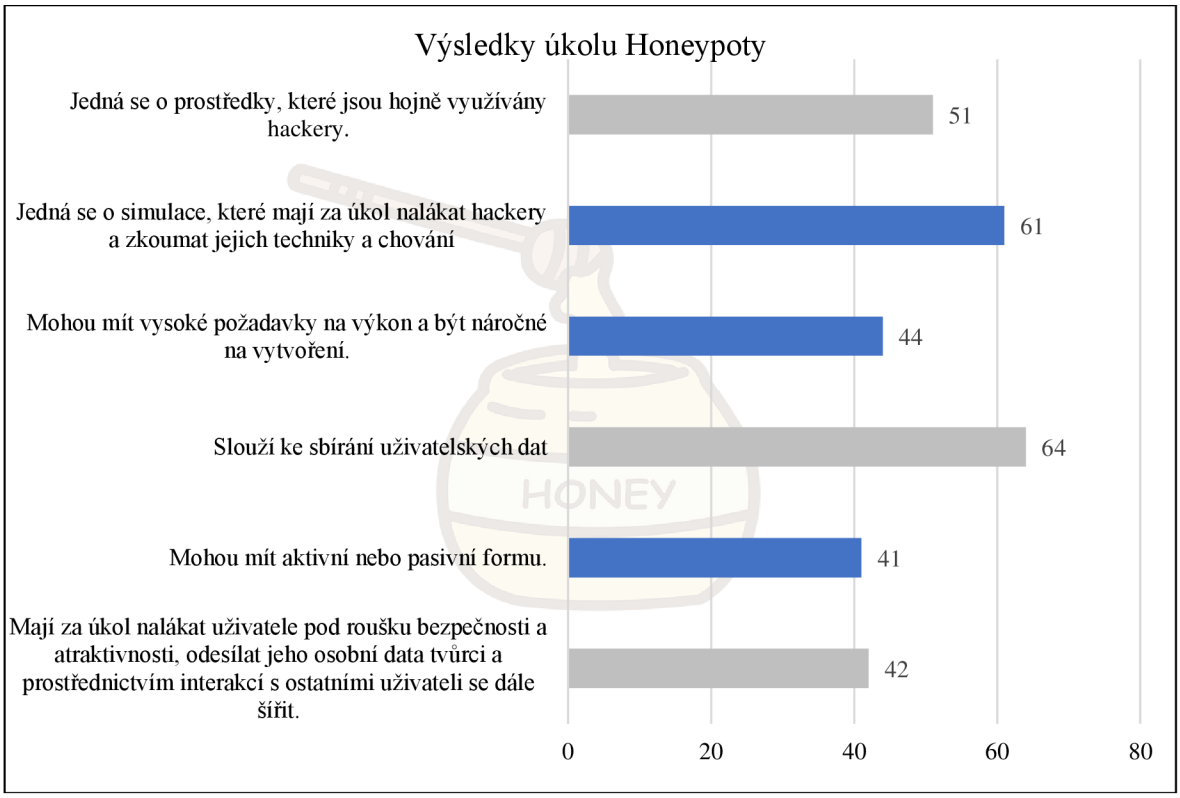


Zdroj: vlastní zpracování

5.1.3 **Výsledky úkolu Honeypoty**

Nízké znalosti byly prokázány v úkolu s honeypoty, vzhledem k výsledkům lze předpokládat, že uživatelé správnosti tvrzení spíše odhadovali. Řada subjektů se mylně domnívala, že honeypoty jsou využívány hackery a slouží ke sběru uživatelských dat, toto stanovisko zaujímalo v první případě 51 a ve druhém 64 z nich. Dále bylo subjekty uvedeno, že honeypoty mohou mít vysoké požadavky na vytvoření a výkon, aktivní či pasivní formu, a že jejich úkolem je nalákat uživatele pod rouškou bezpečí a dále se skrz ně šířit bez jejich vědomí.

Graf 5 - Výsledky úkolu Honeypoty

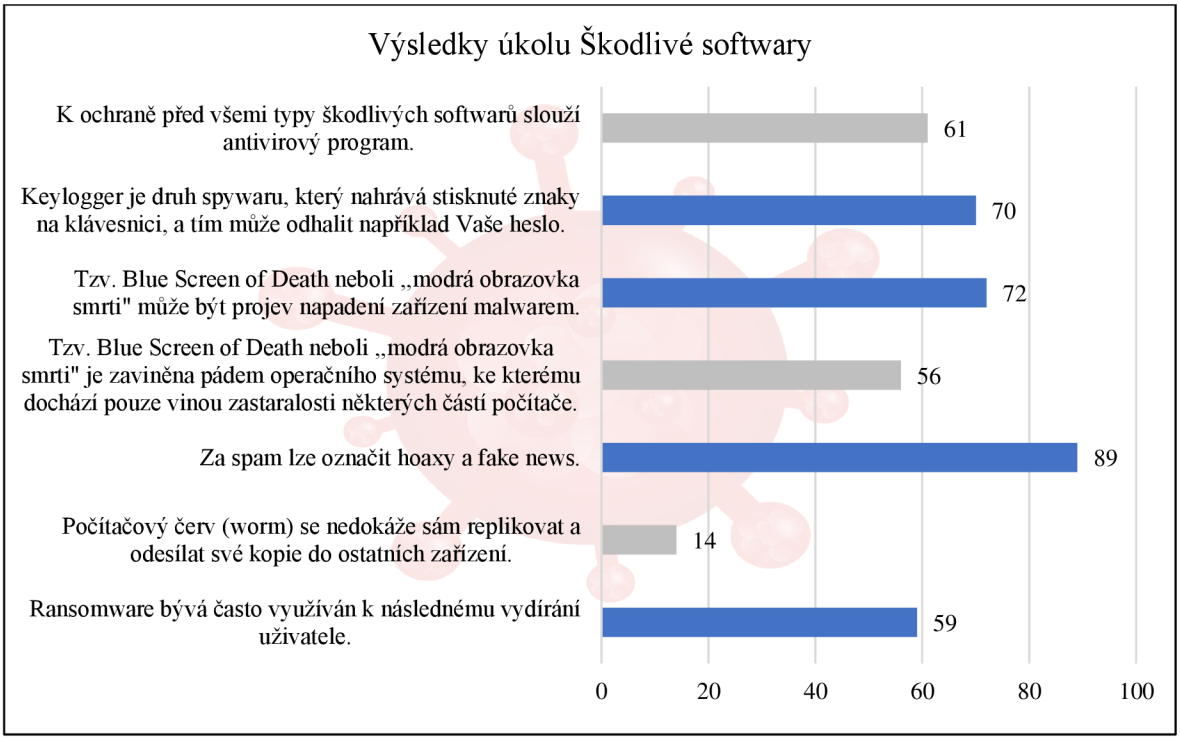


Zdroj: vlastní zpracování

5.1.4 Výsledky úkolu Škodlivé softwary

K poměrně překvapivému výsledku u tohoto úkolu došlo v prvním tvrzení. 61 testovaných subjektů se domnívá, že antivirový program slouží k ochraně před všemi typy škodlivých softwarů. Tento fakt značí velkou míru důvěry v antivirové programy. Znalost možný hrozeb v kategorii Škodlivých softwarů patří mezi nejlepší z celého experimentu. Nejvíce rozšířené je povědomí o spamech, jak ukazují čísla v grafu. Poměrně dobrých výsledků dosáhlo tvrzení o tzv. Modré obrazovce smrti a definice keyloggeru a v menší míře využití ransomwaru. Indikátorem dobrých znalostí o počítačovém červu značí pouze 14 špatných odpovědí na tvrzení, že se nemůže sám replikovat.

Graf 6 - Výsledky úkolu Škodlivé softwary

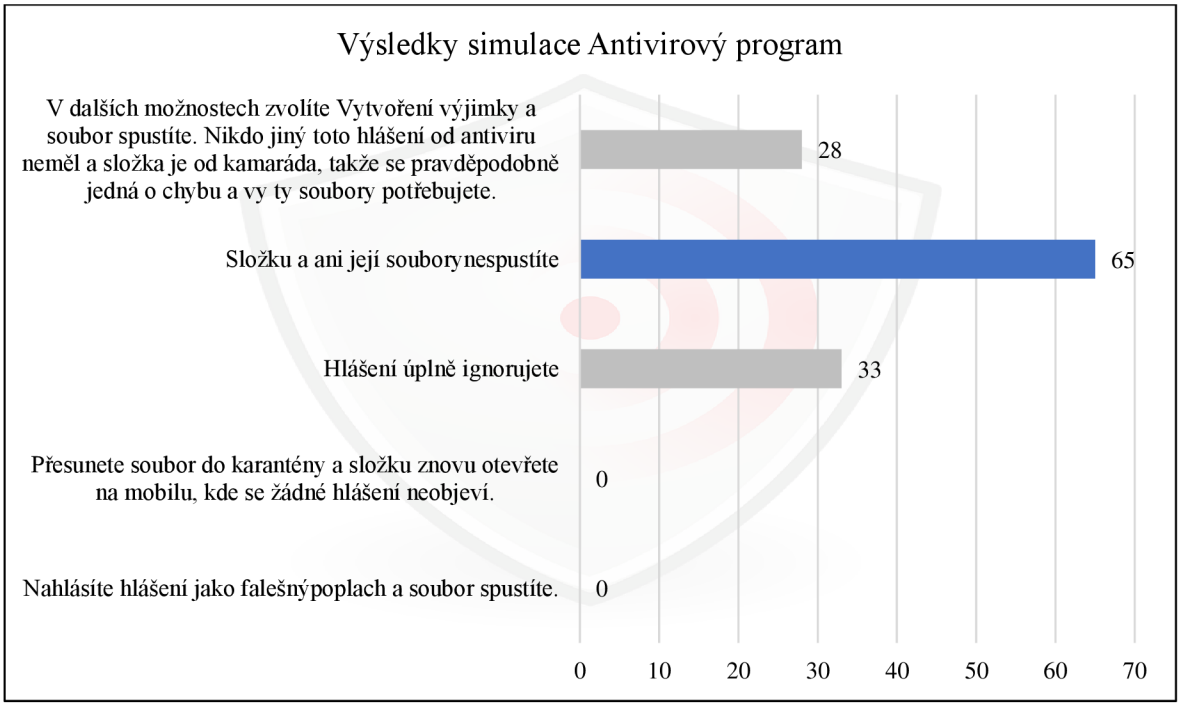


Zdroj: vlastní zpracování

5.1.5 Výsledky simulace Antivirový program

Na předchozí výsledky úkolu se škodlivými softwary navazují výsledky simulace s antivirovým programem. Míra důvěry v antivirový program byla v tomto případě potvrzena, protože nahlášený soubor by nespustilo 65 testovaných uživatelů. Něco málo přes čtvrtinu subjektů by hlášení ignorovalo úplně. Méně než čtvrtina uživatelů by souboru vytvořila výjimku a hlášení neuposlechla z důvodu toho, že soubor byl zaslán jedním z přátel.

Graf 7 - Výsledky simulace Antivirový program



Zdroj: vlastní zpracování

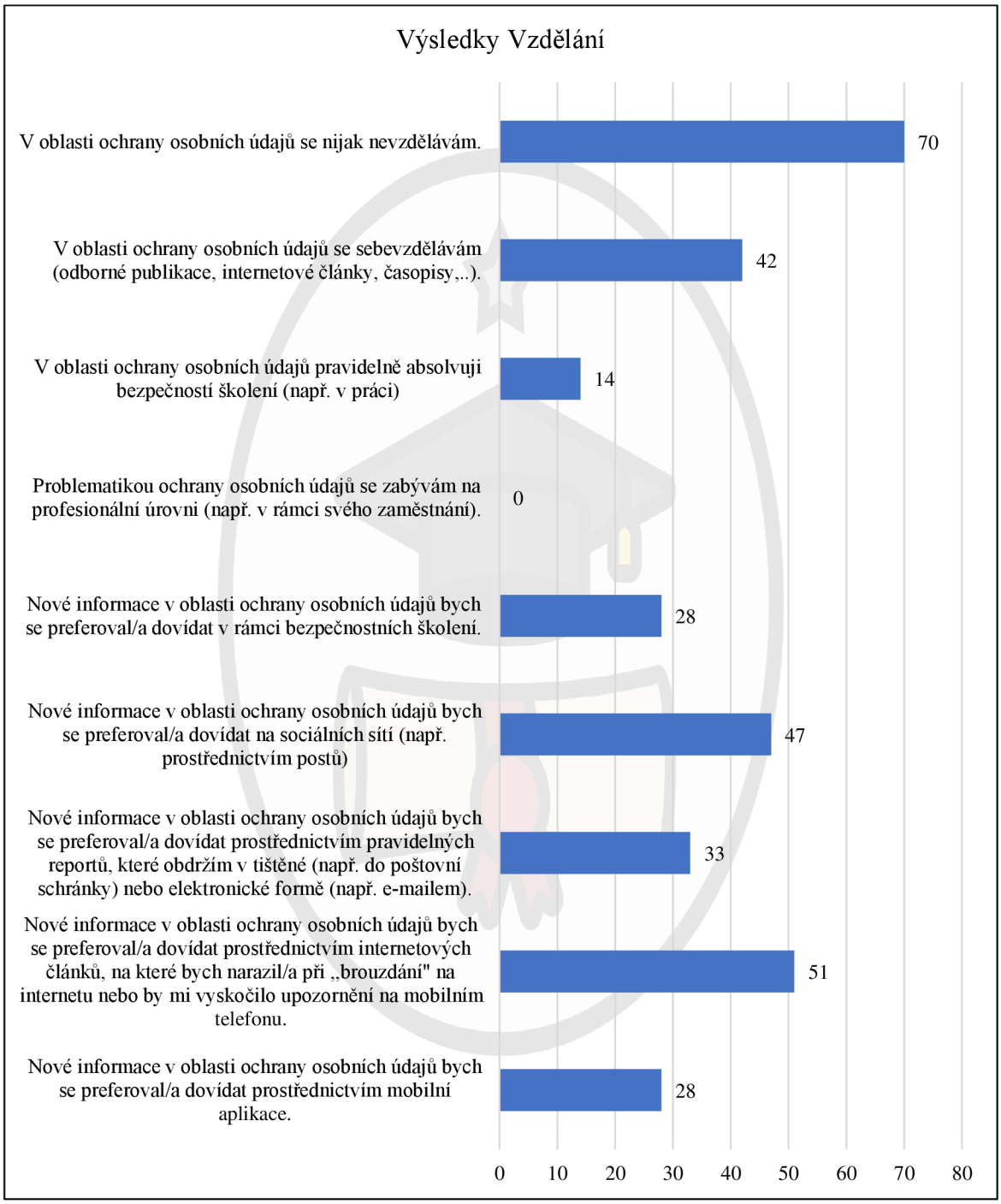
5.1.6 **Výsledky Vzdělání**

V úkolu s názvem Vzdělání uváděly testované subjekty osobní preference ohledně vzdělávání v oblasti ochrany dat, a také jak jejich vzdělání v této problematice probíhalo doposud. Celkem 70 uživatelů uvedlo, že se v této oblasti nijak nevzdělává, což lze označit za poměrně vysoké číslo. Přesně třetina uživatelů využívá k rozšíření svých obzorů odborné publikace, internetové články nebo časopisy. Překvapivě malý počet subjektů, konkrétně 14, pravidelně absolvuje bezpečností školení například v rámci svého zaměstnání. Značný vliv na tento fakt může mít vysokoškolské nebo středoškolské studium či povinná školní docházka. Nikdo z testovaných neuvedl, že by se tímto oborem zabýval na profesionální úrovni.

Co se týče preferencí vzdělávání, nejvyšší počet hlasů dostalo vzdělávání prostřednictvím upozornění na mobilním telefonu (např. když vyjde na nějakém odborné webové stránce nový článek). Důležité je v rámci tohoto úkolu upozornit, že jeden subjekt mohl označit více svých preferencí. 42 testovaných uživatelů by preferovalo dovídat se o této problematice na sociálních sítí. V případě nižší věkové kategorie se tato forma jeví jako vysoce efektivní, protože zejména mladí lidé tráví na sociálních sítích značnou část času. 33

dotazovaných by preferovalo zasílání publikací tištěnou nebo elektronickou formou. A stejný počet subjektů zvolil jako efektivní variantu mobilní aplikaci a bezpečnostní školení.

Graf 8 - Výsledky Vzdělání



Zdroj: vlastní zpracování

5.2 Doporučení

5.2.1 Preventivní postupy a opatření

5.2.1.1 Skupina se ziskem 0-12 bodů

Prvotním krokem subjektu z této skupiny by mělo být ověřování veškerých informací, se kterými přijde do styku v online prostředí a týkají se jeho osoby. Před jakýmkoli činem jako je reakce na podezřelý email či SMS by měl zkusit vypátrat na internetu bližší informace, případně se poradit s odborníkem. Svoje znalosti by měl rozvíjet postupně, od samých základů, jako je vytvoření silného hesla, ochrana přihlašovacích údajů, základní verze antivirového programu, a především informování o nejčastějších hrozbách jako je phishing či spuštění přílohy nedůvěryhodného emailu. Princip asymetrického šifrování by v tomto případě nebyl efektivní. Řada bank a státních institucí vydává pro své klienty zprávy o aktuálních hrozbách, ty mohou být v těchto směrech velmi užitečné. Významným prvkem by mohlo být i absolvování základního bezpečnostního školení o tom, jak se chovat v online prostředí a na sociálních sítích, pro začátek mohou být vhodné i ne příliš odborné publikace, které se věnují problematice ochrany osobních údajů v online světě. Závěrečné doporučení se týká zjištění práv subjektu a nastudování právních předpisů jeho chování na internetu.

5.2.1.2 Skupina se ziskem 13-18 bodů

Tato skupina uživatelů by měla klást velký důraz na sebevzdělávání. Může si pomoci řadou technologií, které umožňují být v obraze. Například odběrem odborných publikací nebo vyfiltrováním upozornění na telefonu týkajících se světa IT. Při instalaci softwaru či aplikace je třeba dbát zvýšené pozornosti při odsouhlasení licenčních podmínek. Důvěra v antivirové programy by neměla být stoprocentní, zejména u free verzí, určitou formou antiviru jsou při pohybu na internetu i samotní uživatelé. Stejně jako v předchozím případě by se měli informovat o potenciálních hrozbách. Vysoce efektivní pro tuto skupinu je absolvování nejrůznějších pokročilejších bezpečnostních školení, při kterých se naučí pod vedením expertů propojit nové znalosti s těmi předchozími. Vhodná dovednost k naučení může být například využití VPN nebo porozumění principům digitálních certifikátů a dvoufázového ověřování.

5.2.1.3 Skupina se ziskem 19-25 bodů

Jak již bylo v práci mnohokrát zmíněno, sebevzdělání a informovanost o nejnovějších trendech je základ v ochraně osobních údajů. Subjekty v této skupině disponují rozšířenými znalostmi v této problematice, ale i jim je doporučeno se co možná nejvíce vzdělávat prostřednictvím vědeckých článků, expertních školení, nebo - pokud je to náplní jejich práce - vědeckých výzkumů. Závěrečné doporučení pro tuto skupinu je předávat své znalosti dál a pomáhat méně zkušených uživatelům, čímž si sami mohou rozšířit své znalosti, případně na celou problematiku změnit úhel pohledu.

5.2.2 **Návrhy způsobů informování**

Tato kapitola vychází z posledního úkolu vlastního experimentu. Na základě preferencí subjektů ohledně vzdělání jsou zde vyhotoveny návrhy, jak co nejefektivněji zvýšit povědomí uživatelů o možných hrozbách a rizicích.

Nejméně preferovanou variantou ve hře bylo absolvování bezpečnostních školení. Alternativou k několikahodinovým školením mohou být krátké týdenní meetingy, cca půlhodinové, které jsou vedeny online, nejlépe v rámci pracovní doby. U řady uživatelů by opadla nechuť udržovat pozornost po dobu několika hodin, a naopak by se mohl zvýšit jejich zájem, pokud by školení probíhalo během jejich pracovní doby, přičemž délka školení by byla pro zaměstnavatele provozně přijatelná. Zajímavý způsob školení nabízí firma CYBERSEC. Školení je rozděleno do několika kurzů, které jsou přístupné online v libovolnou dobu. Po absolvování všech kurzů a splnění podmínek závěrečného testu je uživateli udělen certifikát. Výhodou tohoto školení pro zaměstnavatele je, že není potřeba rezervovat prostory a platit školitele, zaměstnanci kurzy projdou postupně dle svých časových možností, a zároveň to zásadním způsobem neomezí výkon jejich práce.

Širokou škálu školení v rámci rozvoje bezpečnostních znalostí nabízí i NÚKIB. Možné je se zúčastnit v rámci vlastního sebevzdělávání nebo také jako zaměstnanec firmy, která školení zajistí.

Druhou nejméně preferovanou alternativou pro subjekty představovala mobilní aplikace. Příčinu menší atraktivnosti tohoto způsobu informování může představovat nutnost instalace další aplikace a její požadavky na paměť v zařízení. Alternativou k tomuto postupu může být aktivace upozornění v již stávajících aplikacích (například bankovních), které upozorňují klienta na možné hrozby.

Prostřední, třetí preferovanou možností bylo informování prostřednictvím reportů v tištěné nebo elektronické podobě. Nejdůvěryhodnějším zdrojem těchto reportů je Národní úřad pro kybernetickou a informační bezpečnost. Tento web bohužel nenabízí možnost pravidelného odběru informací, nicméně online kurzy dostupné na osveta.nukib.cz mohou představovat příjemný kompromis. Velmi důvěryhodným zdrojem je také Úřad pro ochranu osobních údajů, který taktéž pravidelně vydává reporty s aktuálními trendy. Řada časopisů v tištěné podobě bohužel nedosahuje dostatečné odborné úrovně. Efektivním způsobem tedy může být vytvoření portálu, prostřednictvím něhož mohou uživatelé dostávat jak elektronické, tak tištěné krátké, výstižné a aktuální reporty. Důležitým aspektem tohoto způsobu je bezplatné užívání portálu.

Dalším nejvíce preferovaným způsobem informování byly subjekty zvoleny sociální sítě. Dá se předpokládat, že tuto možnost volili spíše mladší uživatelé. V tomto případě se nabízí řešení začít sledovat na sociálních sítích ověřené organizace a zapnout u nich upozornění.

Nejčastěji upřednostňovanou variantou bylo čtení odborných publikací na internetu, případně hlášení o nově vydaném článku. Tento způsob informování jde efektivně zkombinovat s předchozím. Po zapnutí upozornění na preferovaném profilu bude uživatel dostávat upozornění o jeho činnosti.

O všech výše zmíněných způsobech musejí být uživatelé efektivně poučeni prostřednictvím nejrůznějších informačních kampaní. Málokterý uživatel se o tyto varianty bude zajímat sám od sebe, pokud se ale stane znalost této problematiky trendem, například se o ni začnou zajímat známé osobnosti, osloví největší možný počet běžných uživatelů. Velmi efektivním nástrojem jsou v tomto ohledu sociální sítě, na kterých by příspěvky související s touto problematikou byly zobrazovány v hojné míře. Dalším nástrojem mohou být média, protože uživatelé vnímají nejvíce problémy, které jsou jimi prezentovány.

6 Závěr

Problematika bezpečnosti osobních údajů v online světě je stále častěji diskutované téma. Touha získat osobní data vede v mnoha případech ke konání činů, které jsou vedené jako přestupky, či dokonce trestné činy.

Česká legislativa se problematice ochrany osobních údajů sice věnovala již dříve, ale významným způsobem byla ovlivněna zásahem Evropské unie, kdy v roce 2018 vstoupilo v účinnost tzv. GDPR. V České republice vznikl zákon č. 110/2019 Sb., Zákon o zpracování osobních údajů, ve kterém je na zpracovatele, případně správce osobních údajů kladen velký tlak, aby byly údaje řádně zabezpečeny před zneužitím a anonymizovány. Dohled a řadu dalších věcí týkajících se osobních údajů má na starosti v rámci českého území Úřad pro ochranu osobních údajů, který představuje nezávislý dohled nad předpisy stanovenými v zákoně.

Úvodní část práce byla věnována právě osobním údajům, zejména jejich obsahu a právním předpisům, které se jich týkají, a konceptu C.I.A.. Dále byly definovány a zmapovány možná rizika a hrozby, které mohou vést k ohrožení nebo ztrátě těchto dat. Rizika a hrozby byly rozděleny z pohledu toho, jakým způsobem má uživatel možnost je ovlivnit na subjektivní a objektivní. Subjektivní jsou uživatelem přímo ovlivňována a na jejich vzniku se do určité míry podílí, je možné je rozdělit na úmyslná, např. cílený útok, a neúmyslná, např. nedbalost či neznalost. Naproti tomu jako objektivní jsou označovány ty, na jejichž vzniku se uživatel přímo nepodílí. Stejně jako v případě objektivních je možné je dále rozdělit podle jejich příčiny, v tomto případě na přírodní, fyzikální, technické a softwarové. Softwarovým rizikům a hrozbám je věnována větší část práce, protože z hlediska množství tvoří nejpočetnější skupinu. Jedná se jak o škodlivé softwary (např. malware či ransomware), tak i o metody sociálního inženýrství, jakými jsou například phishing nebo vishing.

Dalším tématem byly způsoby ochrany. Zmíněny byly jak základní bezpečnostní zásady, důležitost sebevzdělání a informovanost, tak i nejnovější trendy v této oblasti, jakou jsou digitální certifikáty, umělá inteligence a honeypoty.

V závěru teoretické části práce byla popsána činnost a statistiky útoků z dokumentů Národního úřadu pro kybernetickou a informační bezpečnost. Rozebíráno bylo zejména období od ledna 2021 do ledna 2022.

Úvod praktické části byl věnován představení únikové hry. Hra byla sestavena v prezentační programu Google Slides, motivací k výběru daného softwaru bylo bezplatné užívání, intuitivní ovládání pro uživatele a možnost vygenerování odkazu, který je přístupný komukoli bez nutnosti registrace či přihlášení.

Hra nese název „MY DATA OD YOUR DATA?“ a skládá se z jedenácti simulací a úkolů, ve kterých bylo zjišťováno, jak subjekty nakládají s osobními údaji a jaké jsou jejich znalosti v oblasti ochrany dat. Účelem posledního úkolu bylo zjistit, jaké jsou preference uživatelů v oblasti bezpečnostního vzdělávání a jejich dosavadní způsob získávání informací. K zaznamenání odpovědí byl využit software pro správu průzkumů Google Forms, který mohl hráč načíst prostřednictvím QR kódu či odkazu. Celkový možný počet bodů, kterého bylo možno dosáhnout, je dvacet pět.

Subjekty byly na základě výsledků ze hry rozděleny do tří skupin: a) 0 – 12 bodů; b) 13 – 18 bodů; c) 19 – 25 bodů, celkem bylo testováno 126 subjektů. V práci byly zdokumentovány a podrobně popsány jednotlivé simulace a úkoly.

Zhodnocení výsledků hry probíhalo formou výběru pěti nejchybovějších situací a úkolu s preferovaným způsobem vzdělání, konkrétně úkoly se soubory cookies, zákonnou legislativou, honeypoty, škodlivými softwary a simulace s antivirovým programem.

V případě cookies velký počet uživatelů (67) automaticky povolil ukládání všech jejich typů na disk počítače, tato odpověď byla vyhodnocena jako nesprávná, protože cookies umožňují stránce sledovat veškeré činnosti uživatele, což zvyšuje riziko. Dalším důvodem bylo, že soubory cookies zahlcují disk zařízení uživatele.

V úkolu se zákonnou legislativou subjekty (84) mylně označily jako aktuální Zákon o ochraně osobních údajů, který byl po příchodu GDPR nahrazen Zákonem o zpracování osobních údajů.

Výsledky subjektů ohledně honeypotů byly více méně srovnatelné, což značí, že většina uživatelů nemá o honeypotech dostatečné znalosti. Nejčastější odpověď subjektů (64) byla, že honeypoty jsou nástrojem ke sbírání dat uživatelů. Z toho vyplývá, že většina subjektů vnímá honeypot jako potenciální hrozbu. Ten má však opačný účel, má za úkol zkoumat činnost hackerů a informovat o nich.

V otázce týkající se škodlivých softwarů skoro polovina uživatelů (61) uvedla, že antivirový program je ochrání před všemi typy softwarových hrozeb. To je častý omyl, který má zafixovaný velký počet běžných uživatelů. Antivirový program je

bezpochyby velmi užitečný nástroj v boji proti škodlivému softwaru, nikdy však není jistota, že odhalí všechny hrozby.

Výsledek simulace týkající se antivirového programu ukazuje, že téměř polovina uživatelů (61) by ignorovala hlášení antiviru o souboru obsahující škodlivý software v případě, že by jim soubor zaslal kamarád či známý, který s tím neměl žádný problém a hlášení se mu nezobrazilo. V takovém případě se uživatelé vystavují zvýšenému riziku infikování zařízení. Jejich známý například nemusí mít antivirový program aktualizovaný.

V závěru uživatelé ve většině případů uvedli, že se v oblasti ochrany osobních dat nijak nevzdělávají. Důvodem může být pro ně vcelku neatraktivní téma, kterému se věnovala poslední část otázky. Uživatelé v ní uvedli, že by preferovali rozvíjet své znalosti zejména pomocí informací na sociálních sítí nebo článků na internetu. K rozšíření znalostí v oblasti ochrany osobních údajů by tedy jednoznačně přispěla kampaň zaměřená právě na sociální sítě a poutavé články.

Hlavním cílem práce bylo navrhnout preventivní postupy a opatření, vedoucích k minimalizaci ztráty osobních údajů. Doporučení jsou rozdělena pro každou skupinu, podle výsledku hry. Pro skupinu a) by bylo vhodné ověřovat informace, které se budou týkat jejich osobních údajů. Například řada bank vydává svým klientům zprávy o aktuálních hrozbách, buď prostřednictvím zpráv nebo při přihlášení do internetového bankovnictví. Doporučení pro skupinu b) je rozvíjet své znalosti o tomto tématu. Existuje například řada technologií, které v ochraně před hrozbami mohou pomoct, pokud je uživatel dokáže správně použít. Dalším návrhem je věnovat zvýšenou pozornost licenčním podmínkám při instalaci softwaru či aplikace, se kterou nemá zkušenosti. Uživatelé spadající do skupiny c) mají znalosti na dobré úrovni, nicméně není od věci je ještě více zdokonalovat. Mohou také své znalosti předávat méně zkušeným uživatelům a díky tomu třeba změnit pohled na danou problematiku, nebo ještě více rozšířit své obzory.

Seznam použitých zdrojů

Tištěné zdroje

1. NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ a Jan TOMÍŠEK, 2017. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer. ISBN 978-80-7552-765-3.

2. NULÍČEK, Michal, Josef DONÁT, Bohuslav LICHNOVSKÝ, František NONNEMANN, Petr HABARTA a Kateřina KAŠPÁRKOVÁ, 2019. *Zákon o zpracování osobních údajů*. Praha: Wolters Kluwer. ISBN 978-80-7598-467-8.

3. VLACHOVÁ, Barbora a Martin MAISNER, 2019. *Zákon o zpracování osobních údajů*. Praha: C.H.Beck. ISBN 978-80-7400-760-6.

4. BAČA, Ján, Radek BURŠÍK, Jakub KLODWIG, Alice SELBY, Jan SVOBODA a Veronika ŠÍPOŠOVÁ, 2020. *Zákon o zpracování osobních údajů: Praktický komentář*. Plzeň: Aleš Čeněk. ISBN 978-80-7380-804-4.

5. CHALOUPKOVÁ, Helena a Petr HOLÝ, 2012. *Autorský zákon: komentář*. 4. vyd. V Praze: C.H. Beck. Beckovy komentáře. ISBN 978-80-7400-432-2.

6. BARTÍK, Václav a Eva JANEČKOVÁ, 2016. *Ochrana osobních údajů v aplikační praxi*. 4. aktualizované vydání. Praha: Wolters Kluwer. ISBN 978-80-7552-141-5.

7. MÍŠEK, Jakub, 2020. *Moderní regulatorní metody ochrany osobních údajů*. Brno: Masarykova univerzita. ISBN 978-80-210-9736-0.

8. POLČÁK, Radim, 2007. *Právo na internetu: spam a odpovědnost ISP*. Brno: Computer press. ISBN 978-80-251-1777-4.

9. KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

10. MCCARTHY, Linda a Denise WELDON-SIVIY, ed., 2013. *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha: CZ.NIC. ISBN 978-80-904248-6-9.

Online zdroje

1. Co jsou to osobní údaje? *Evropská komise* [online]. [cit. 2021-8-15]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_cs

2. CHAI, Wesley, 2021. Confidentiality, integrity and availability (CIA triad). *Whatls.com* [online]. leden 2021 [cit. 2021-08-15]. Dostupné z: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

3. ŠKORNIČKOVÁ, Mgr. Eva. Co je GDPR? *GDPR: Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2021-8-16]. Dostupné z: https://www.gdpr.cz/gdpr/

4. RÜCKLOVÁ (ŠVANDELÍKOVÁ), JUDr. Bc. Klára, 2018. GDPR: Co se skrývá pod tajemným „DPIA“? *Právní prostor* [online]. 22.02.2018 [cit. 2021-8-16]. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/gdpr-co-se-skryva-pod-tajemnym-dpia

5. *Úřad pro ochranu osobních údajů* [online]. [cit. 2021-8-16]. Dostupné z: https://www.uoou.cz/

6. Úřad pro ochranu osobních údajů: Evropský sbor pro ochranu osobních údajů k uchovávání údajů z kreditních karet. *PARLAMENTNÍ LISTY.cz* [online]. 08.06.2021 [cit. 2021-8-22]. Dostupné z: https://www.parlamentnilisty.cz/zpravy/tiskovezpravy/Urad-pro-ochranu-osobnich-udaju-Evropsky-sbor-pro-ochranu-osobnich-udaju-k-uchovavani-udaju-z-kreditnich-karet-666677

7. KROPÁČOVÁ, Andrea. Uživatel a počítačová bezpečnost. Zpravodaj ÚVT MU [online]. 2006, XVI(3), 16-20 [cit. 2021-4-30]. ISSN 1212-0901. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/353.htm

8. TATARU, Georgiana Florentina a Ștefan Răzvan TATARU. HUMAN RESOURCES AND PERSONAL DATA PROTECTION: AN INDISSOLUBLE RELATIONSHIP. Journal of Public Administration, Finance & Law. 2020, (18), 303-311.

9. doc. RNDr. JOSEF POŽÁR, CSc. Vybrané hrozby informační bezpečnosti organizace. In: *CyberSecurity.cz: Kybernetická bezpečnost a obana* [online]. 2010 [cit. 2021-08-15]. Dostupné z: https://www.cybersecurity.cz/data/Pozar2.pdf

10. Metodika k varování ze dne 17. prosince 2018, 2019. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. 04.01.2019 [cit. 2022-02-20]. Dostupné z: https://nukib.cz/download/publikace/podpurne_materialy/2019_01_04_metodika_k_varov%C3%A1n%C3%AD_z_17-12-2018_v1.0.pdf

11. *Eset* [online]. [cit. 2021-8-28]. Dostupné z: https://www.eset.com/cz/

12. All about malware. *Malwarebytes: CYBER PROTECTION FOR EVERYONE* [online]. [cit. 2021-8-28]. Dostupné z: https://www.malwarebytes.com/malware

13. What is Spyware? The 5 Examples You Need to Know. *SoftwareLab.org* [online]. [cit. 2021-8-28]. Dostupné z: https://softwarelab.org/what-is-spyware/

14. 11 real and famous cases of malware attacks. *Gatefy* [online]. 04.06.2021 [cit. 2021-8-28]. Dostupné z: https://gatefy.com/blog/real-and-famous-cases-malware-attacks/

15. KEARY, Tim, 2020. Dos vs DDos Attacks: The Differences and How To Prevent Them. *Compiratech* [online]. [cit. 2021-11-05]. Dostupné z: https://www.comparitech.com/net-admin/dos-vs-ddos-attacks-differences-prevention/

16. MORAVČÍK, plk. Ondřej. Současné trendy podvodníků - vishing a spoofing. *Policie České republiky* [online]. 23.04.2021 [cit. 2021-8-29]. Dostupné z: https://www.policie.cz/clanek/web-informacni-servis-zpravodajstvi-soucasne-trendy-podvodniku-vishing-a-spoofing.aspx

17. SCARFONE, Karen a Paul HOFFMAN. Guidelines on Firewalls and Firewall Policy: Recommendations of the National Institute of Standards and Technology. *National Institute of Standards and Technology* [online]. září 2009, 2-2 - 2-6 [cit. 2021-11-05]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

18. BOŘÁNEK, Roman, 2017. VPN pro začátečníky: princip fungování, výhody a nevýhody. *Root.cz* [online]. [cit. 2021-11-05]. Dostupné z: https://www.root.cz/clanky/vpn-pro-zacatecniky-princip-fungovani-vyhody-a-nevyhody/

19. Honeypot. *DIGITÁLNÍ PEVNOST: Bojujme za bezpečnější digitální svět* [online]. 2018 [cit. 2021-11-05]. Dostupné z: https://www.digitalnipevnost.cz/viki/honeypot

20. Kaspersky Security Bulletin 2020-2021. EU statistics. *SECURELIST by Kaspersky* [online]. 26.05.2021 [cit. 2021-11-05]. Dostupné z: https://securelist.com/kaspersky-security-bulletin-2020-2021-eu-statistics/102335/

21. Jak umělá inteligence napomáhá s ochranou vašich dat. *Acronis* [online]. 07.11.2018 [cit. 2021-11-05]. Dostupné z: https://www.acronis.cz/jak-umela-inteligence-napomaha-s-ochranou-vasich-dat/

22. HANÁK, Jiří. Vysvětlení SSL certifikátů: Co jsou, jak fungují a proč je používat. *MasterDC* [online]. 29.03.2016 [cit. 2021-11-05]. Dostupné z: https://www.master.cz/blog/co-jsou-ssl-certifikaty-a-ssl-protokoly-jak-funguji-vysvetleni-navod/

23. *White Hat Hackers: The Good, the Bad, or the Ugly?* [online]. [cit. 2021-11-05]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/white-hat-hackers

24. Klienty Raiffeisenbank zkouší nachytat nový phishing. Takto vypadá, 2021. *Měšec.cz* [online]. 15.01.2021 [cit. 2022-03-14]. Dostupné z: https://www.mesec.cz/aktuality/klienty-raiffeisenbank-zkousi-nachytat-novy-phishing-takto-vypada/

25. Pop-up okna pro sběr emailů. *WEBMIUM* [online]. 29.05.2016 [cit. 2022-12-17]. Dostupné z: https://blog.webmium.cz/posts/pop-up-okna-pro-sber-emailu

26. What is ProxyLogon?. *ProxyLogon* [online]. 2021 [cit. 2022-02-20]. Dostupné z: https://proxylogon.com/

27. PALYZA, Jiří, 2021. Další zneužití bezpečnostní mezery Exchange Serveru: malware na těžbu kryptoměny. *CHIP* [online]. 18.02.2021 [cit. 2022-02-20]. Dostupné z: https://www.chip.cz/novinky/dalsi-zneuziti-bezpecnostni-mezery-exchange-serveru-malware-na-tezbu-kryptomeny/

28. Upozornění na aktivní zneužívání zranitelnosti Microsoft Exchange server - ProxyShell, 2021. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. 13.08.2021 [cit. 2022-02-20]. Dostupné z: https://www.nukib.cz/cs/infoservis/hrozby/1739-upozorneni-na-aktivni-zneuzivani-zranitelnosti-microsoft-exchange-server-proxyshell/

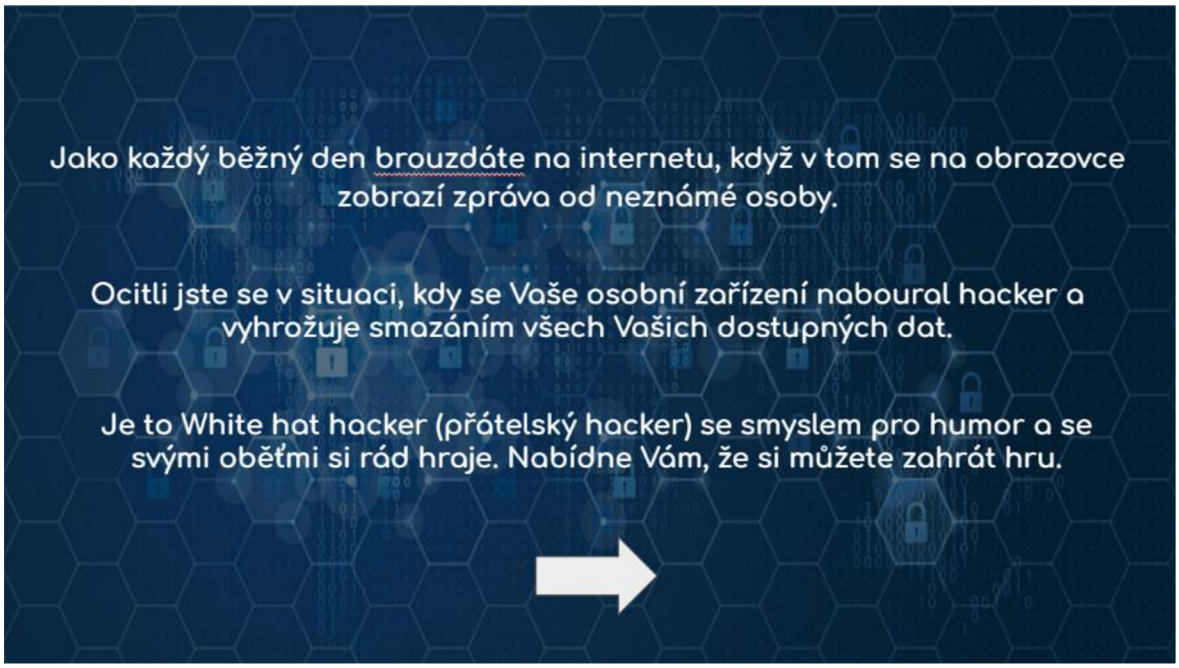
29. Kybernetické incidenty pohledem NÚKIB: LEDEN 2022, 2022. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. 2022 [cit. 2022-02-20]. Dostupné z: https://www.nukib.cz/download/publikace/vyzkum/2022-01_Kyberneticke_incidenty_leden.pdf

7 Přílohy

Příloha č. 1 – Úvod hry

Zdroj: vlastní zpracování

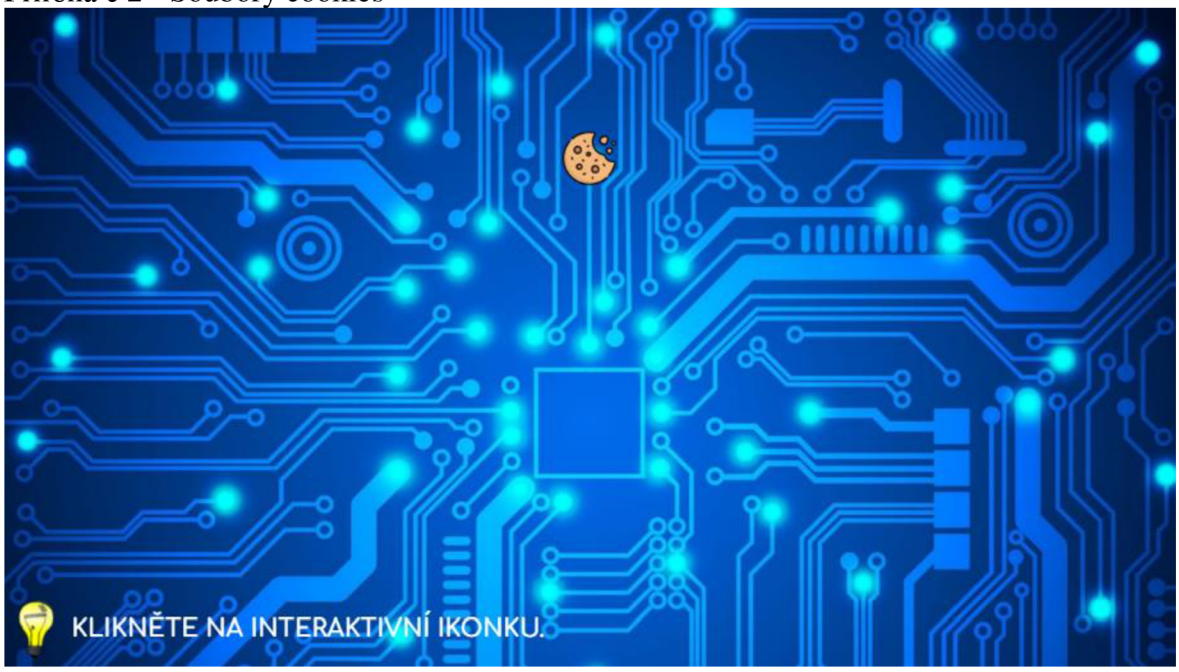
Zdroj: vlastní zpracování



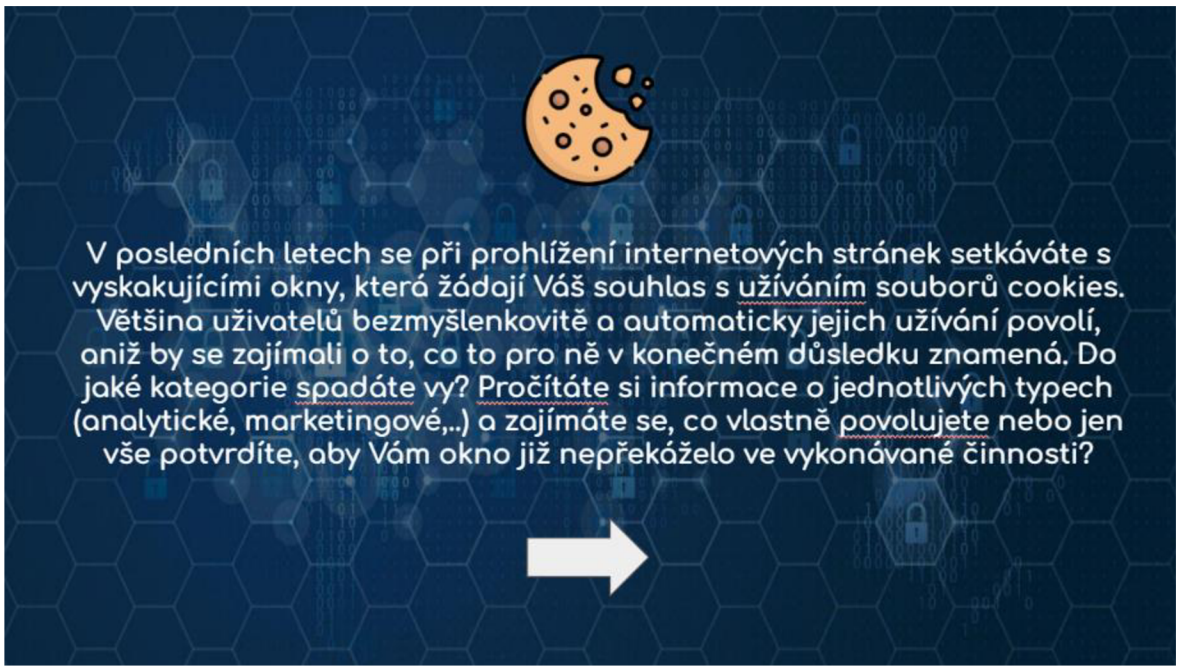
Zdroj: vlastní zpracování

Zdroj: vlastní zpracování

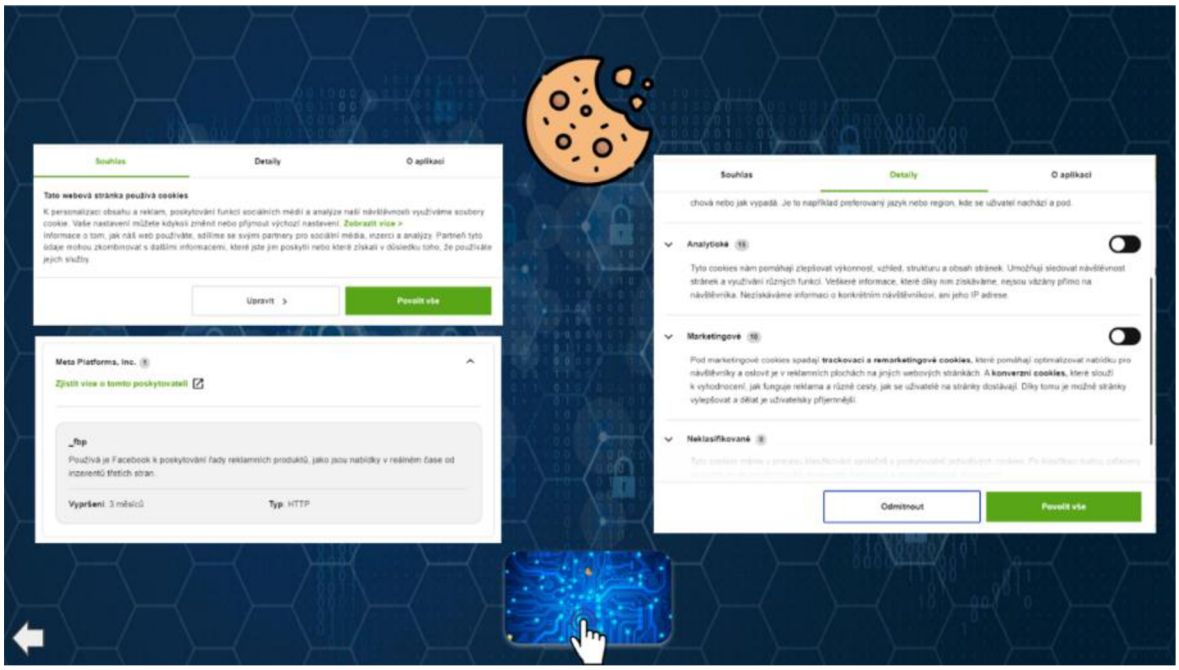
Příloha č 2 - Soubory cookies



Zdroj: vlastní zpracování

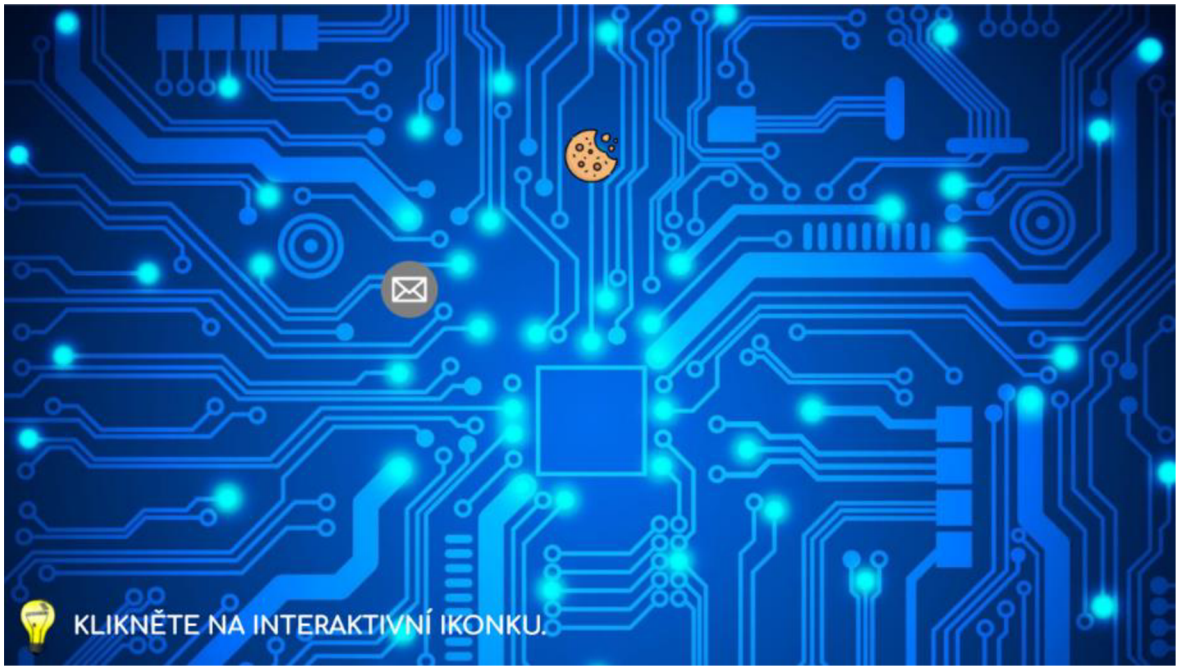


Zdroj: vlastní zpracování



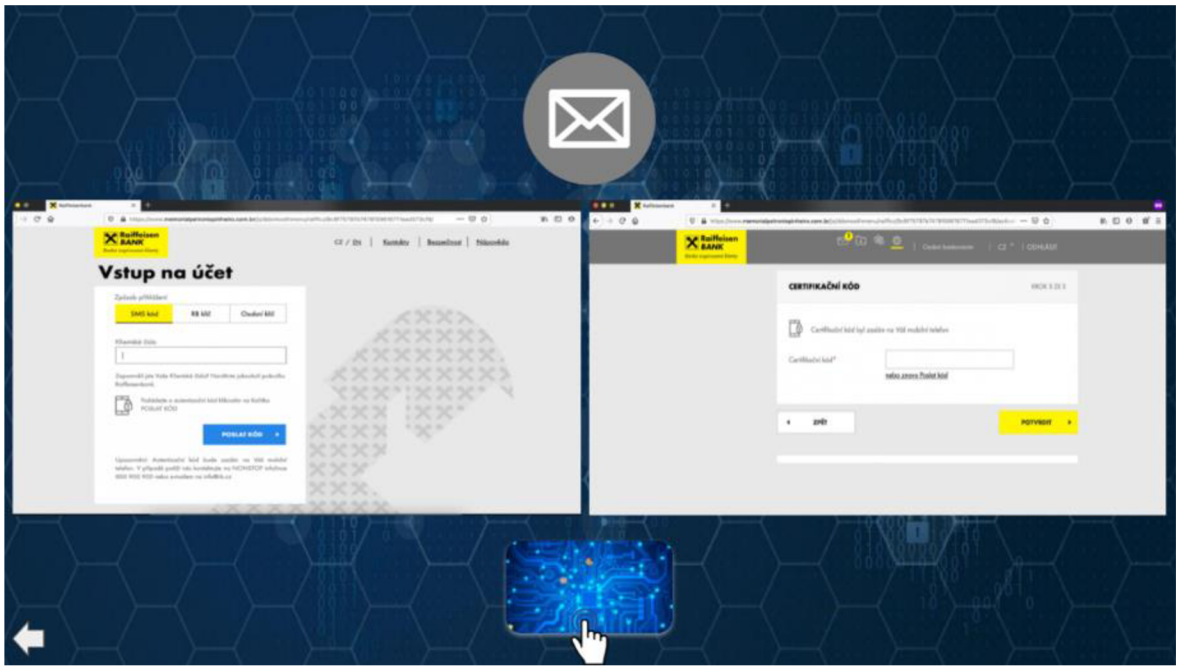
Zdroj: vlastní zpracování

Příloha č. 3 - Phishing - dvoufázové ověřování



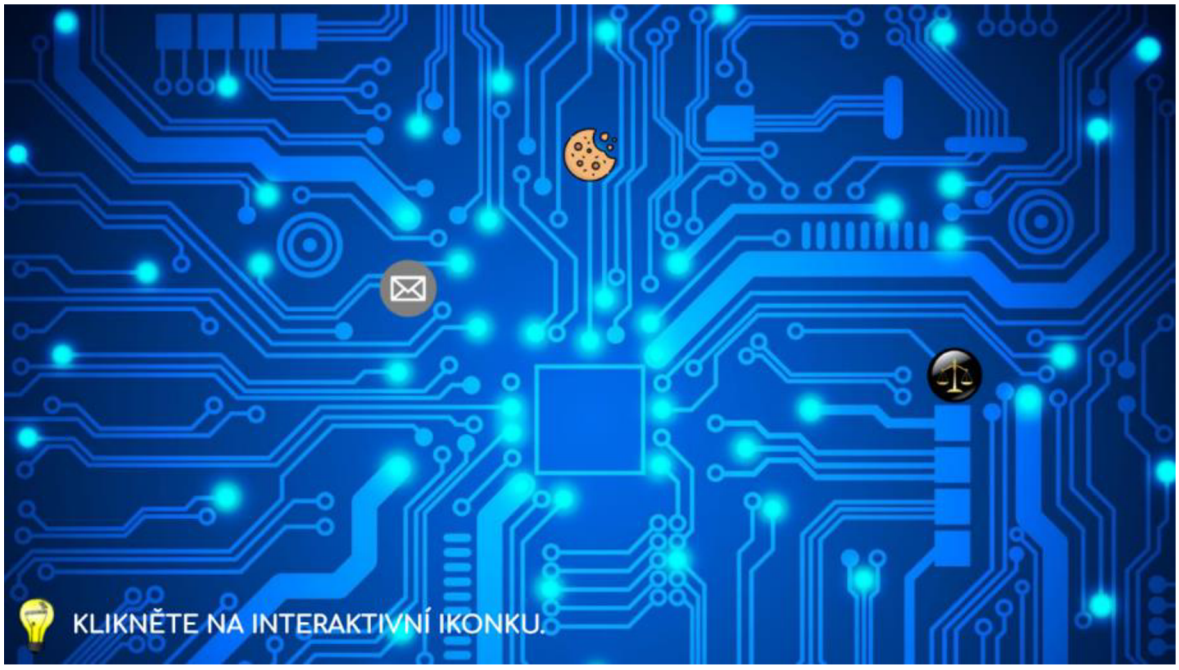
Zdroj: vlastní zpracování

Zdroj: vlastní zpracování

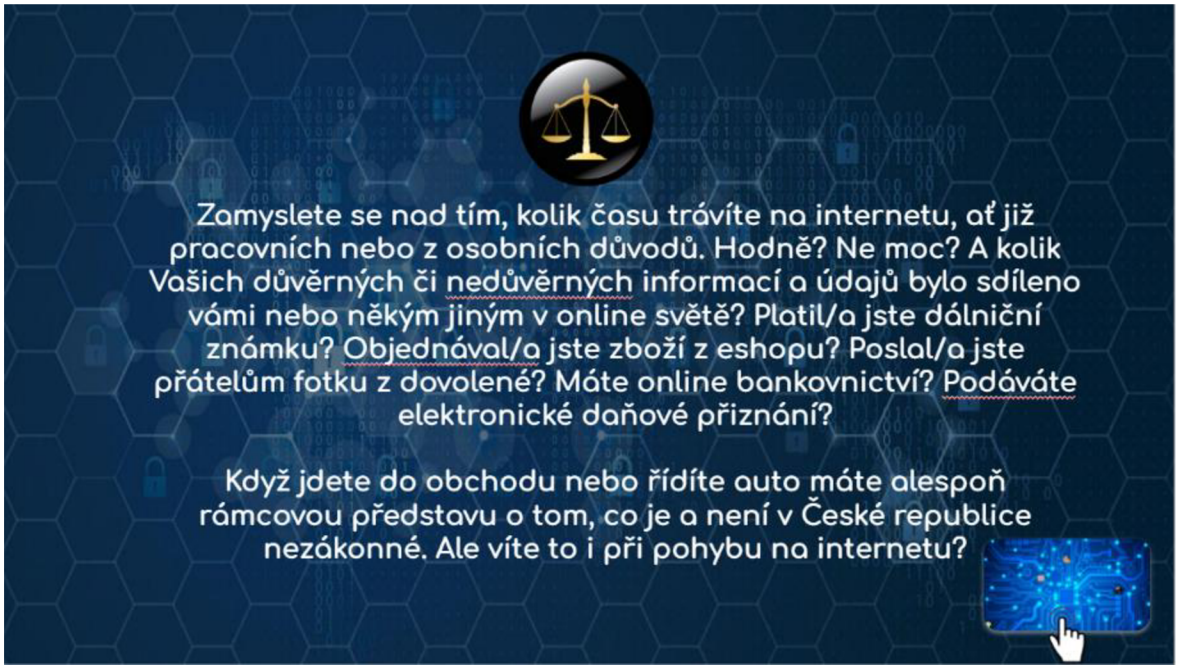


Zdroj: vlastní zpracování, měšec.cz 2021

Příloha č. 4 - Zákonná legislativa

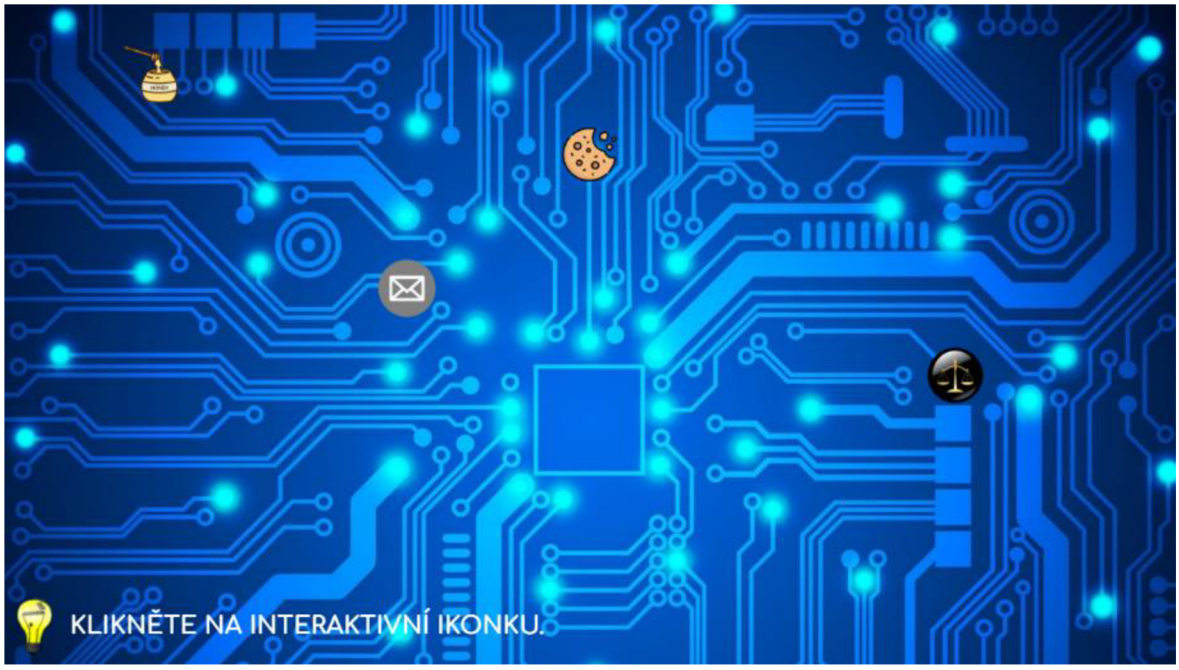


Zdroj: vlastní zpracování



Zdroj: vlastní zpracování

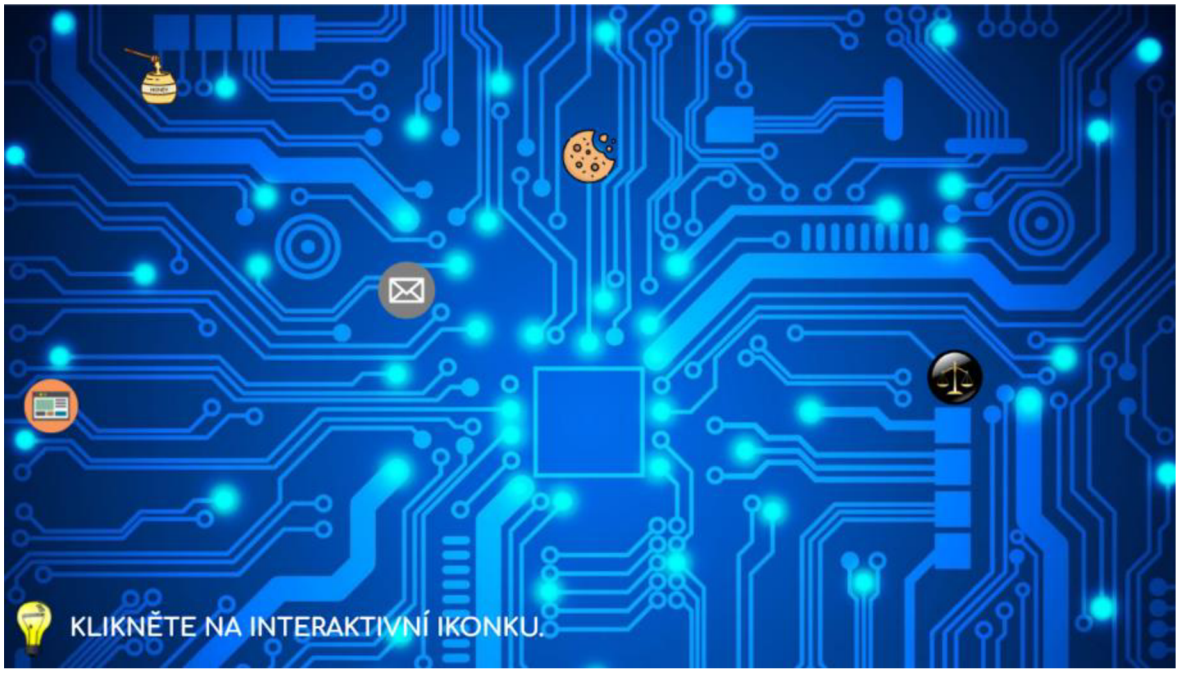
Příloha č 5 - Honeypoty



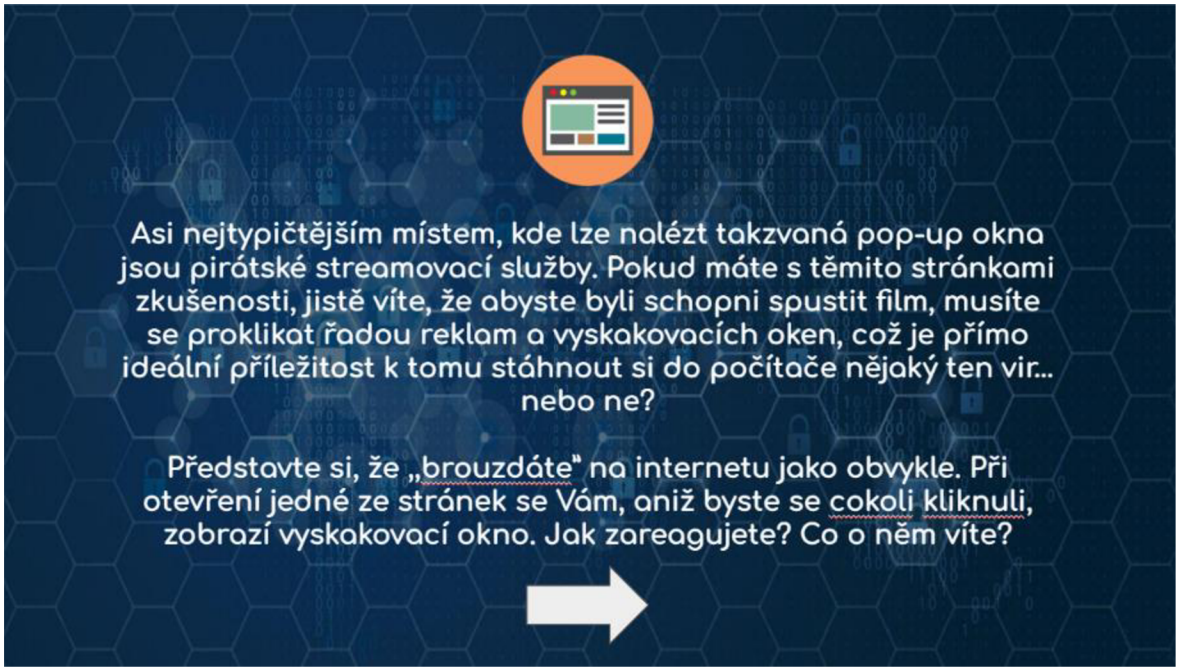
Zdroj: vlastní zpracování

Zdroj: vlastní zpracování

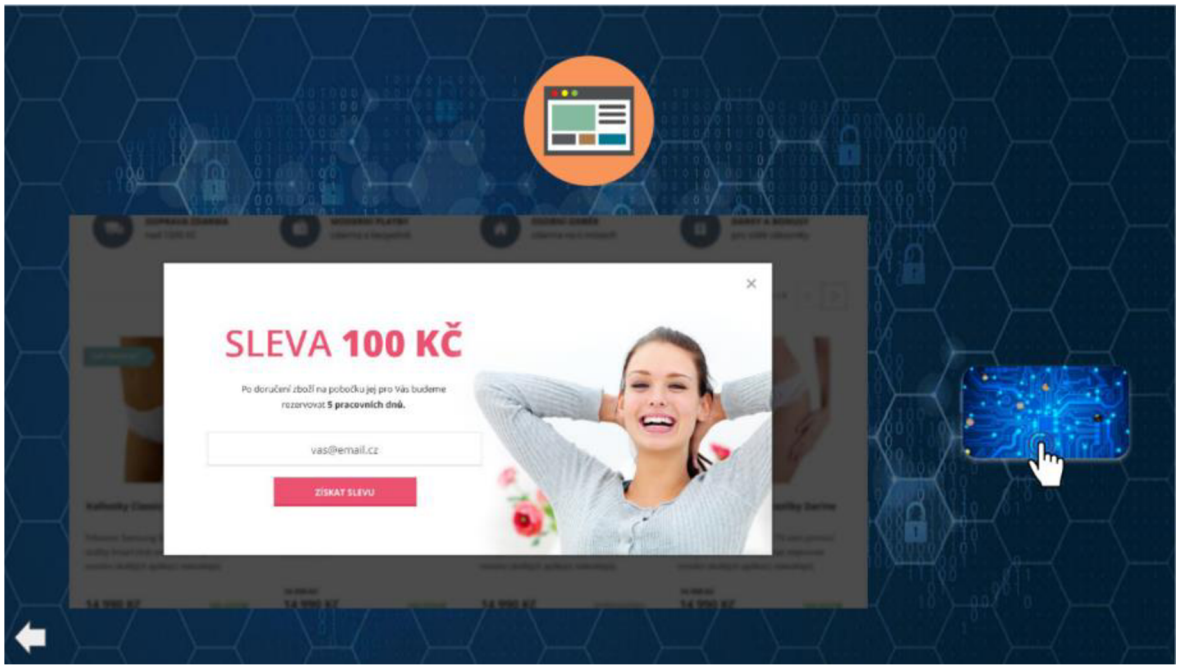
Příloha č. 6 - Pop-up okna



Zdroj: vlastní zpracování

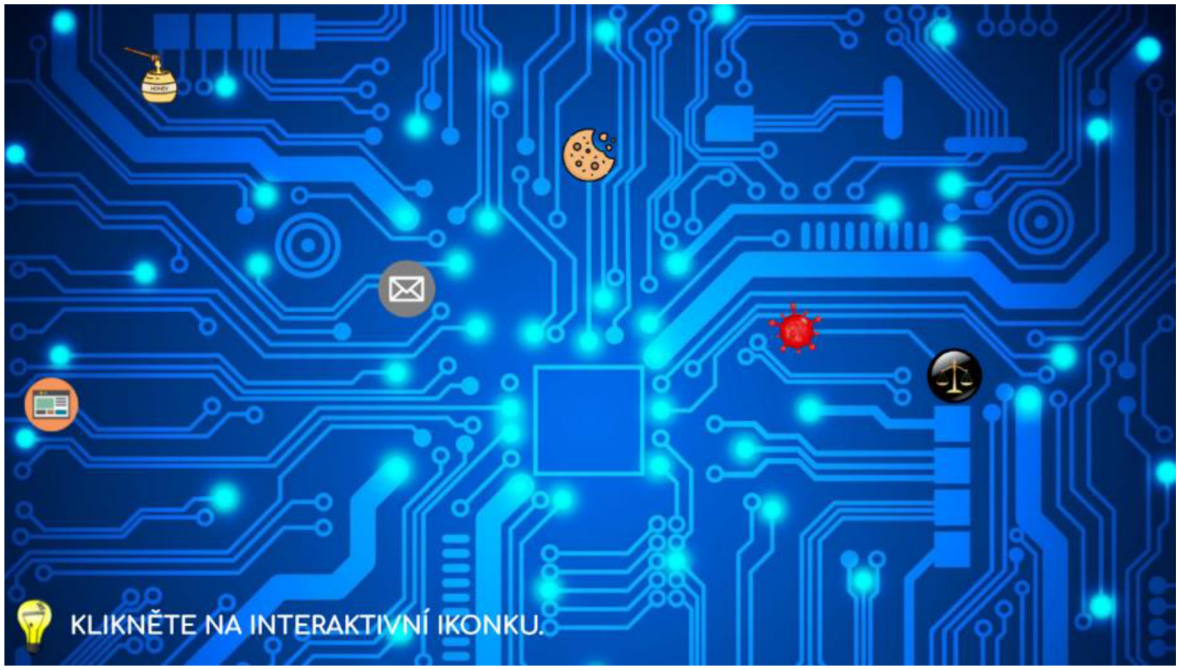


Zdroj: vlastní zpracování

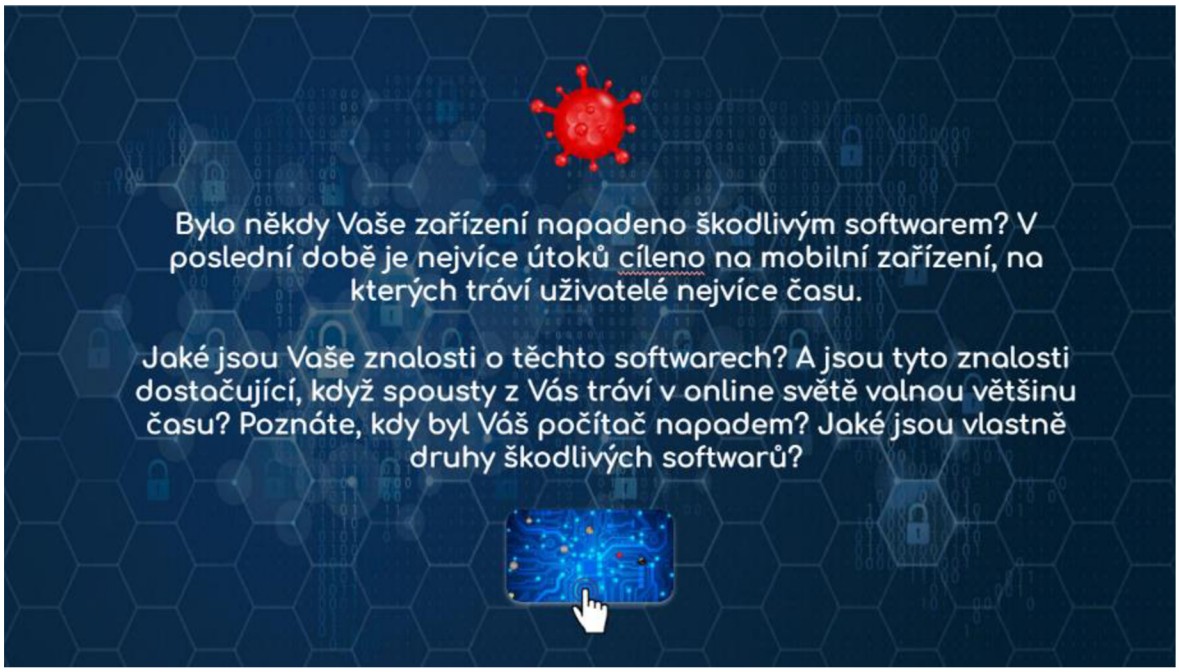


Zdroj: vlastní zpracování, WEBMIUM 2016

Příloha č. 7 - Škodlivé softwary

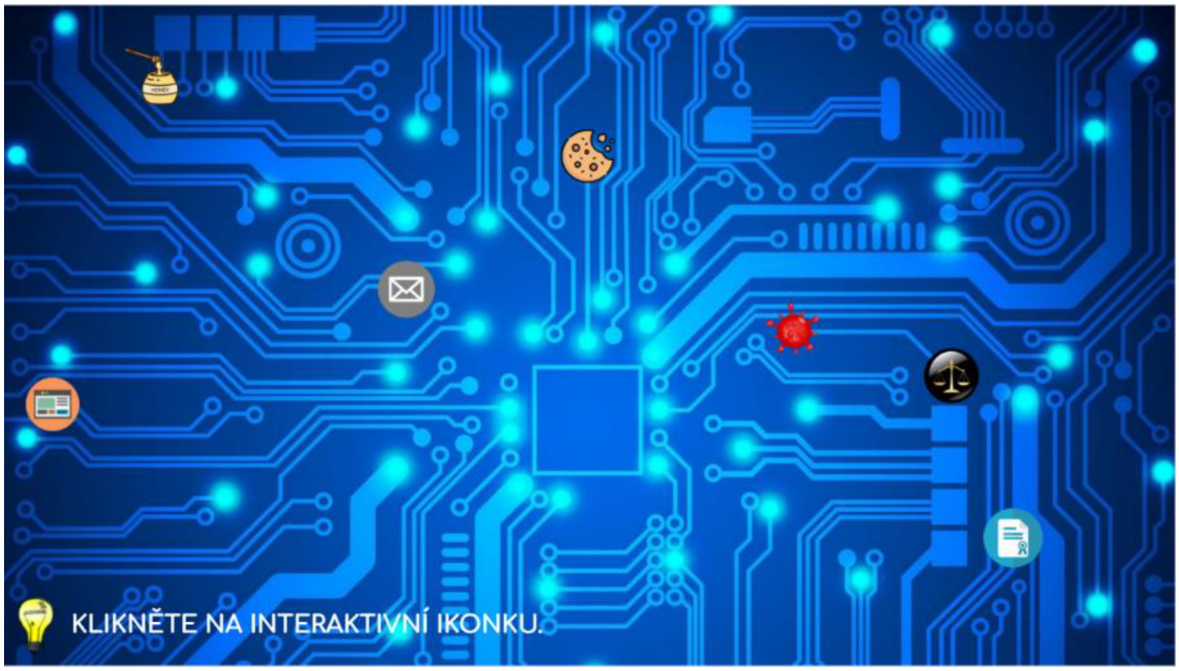


Zdroj: vlastní zpracování

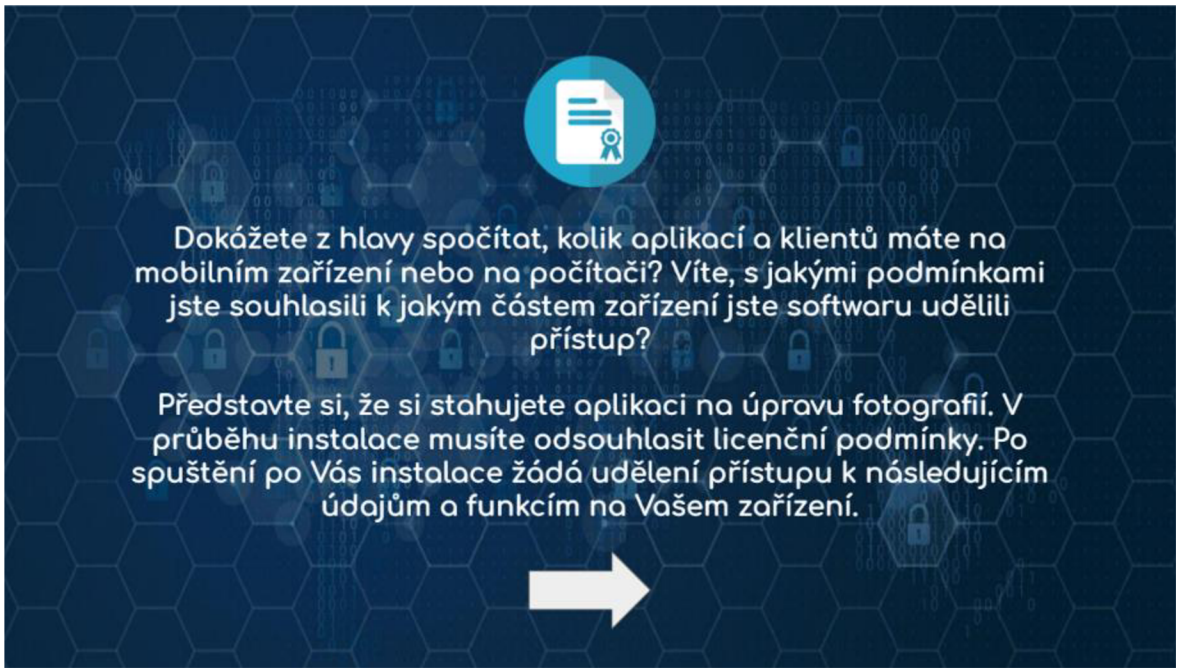


Zdroj: vlastní zpracování

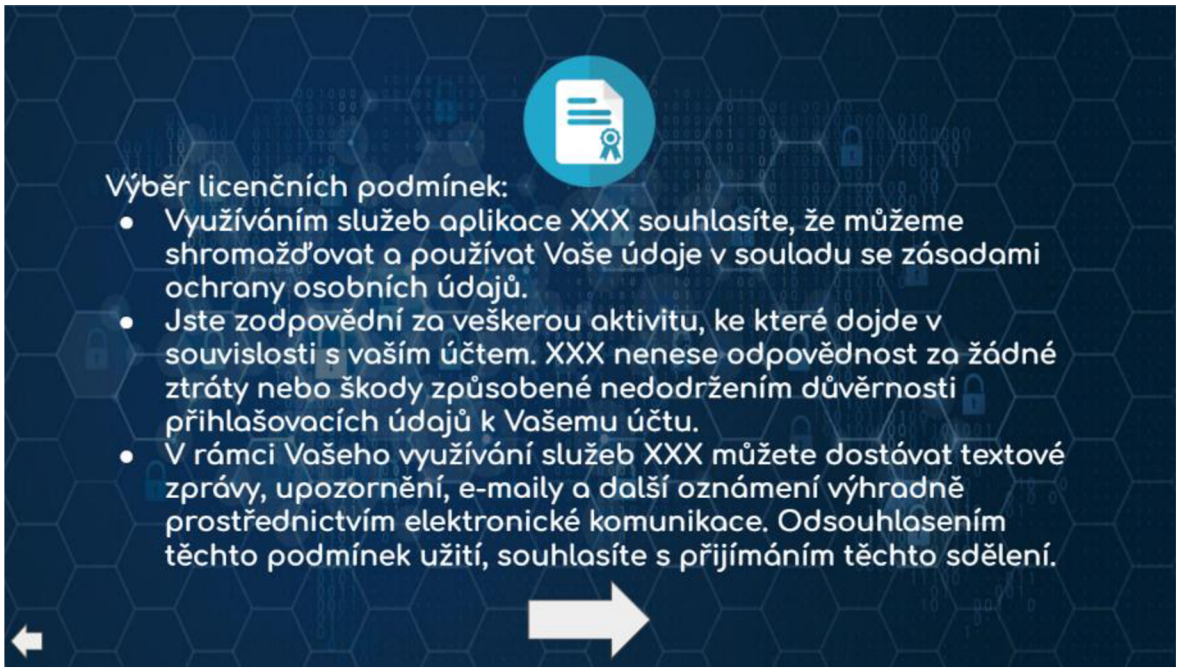
Příloha č. 8 - Licenční podmínky



Zdroj: vlastní zpracování



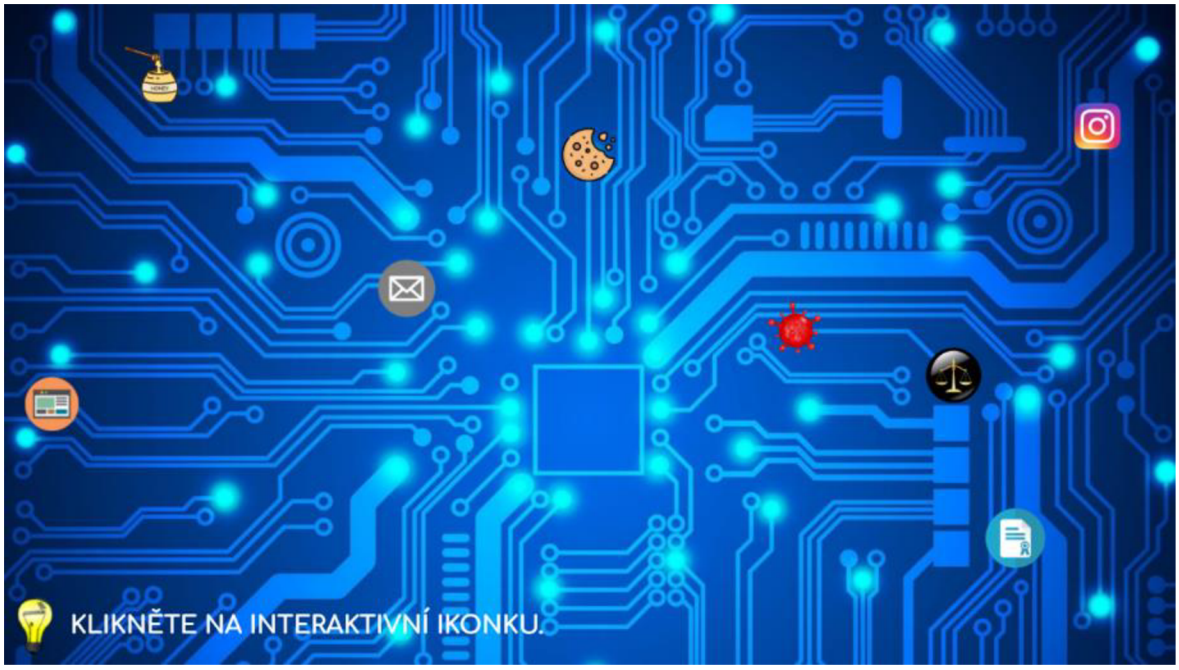
Zdroj: vlastní zpracování



Zdroj: vlastní zpracování

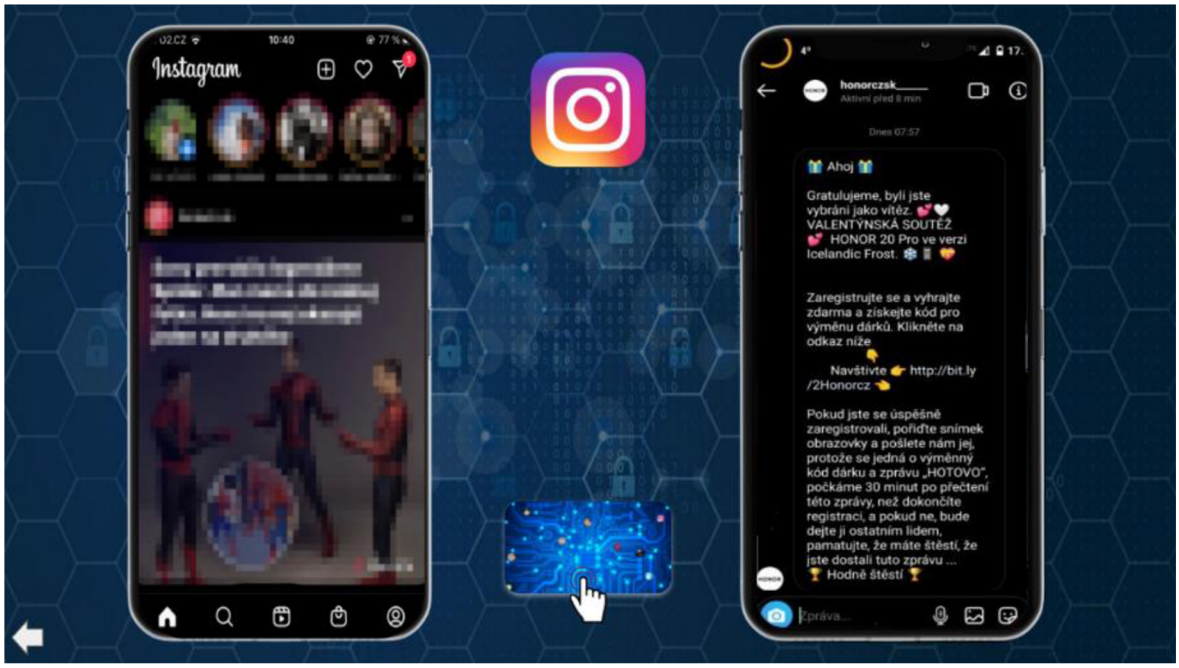
Zdroj: vlastní zpracování

Příloha č. 9 - Phishing – sociální sítě



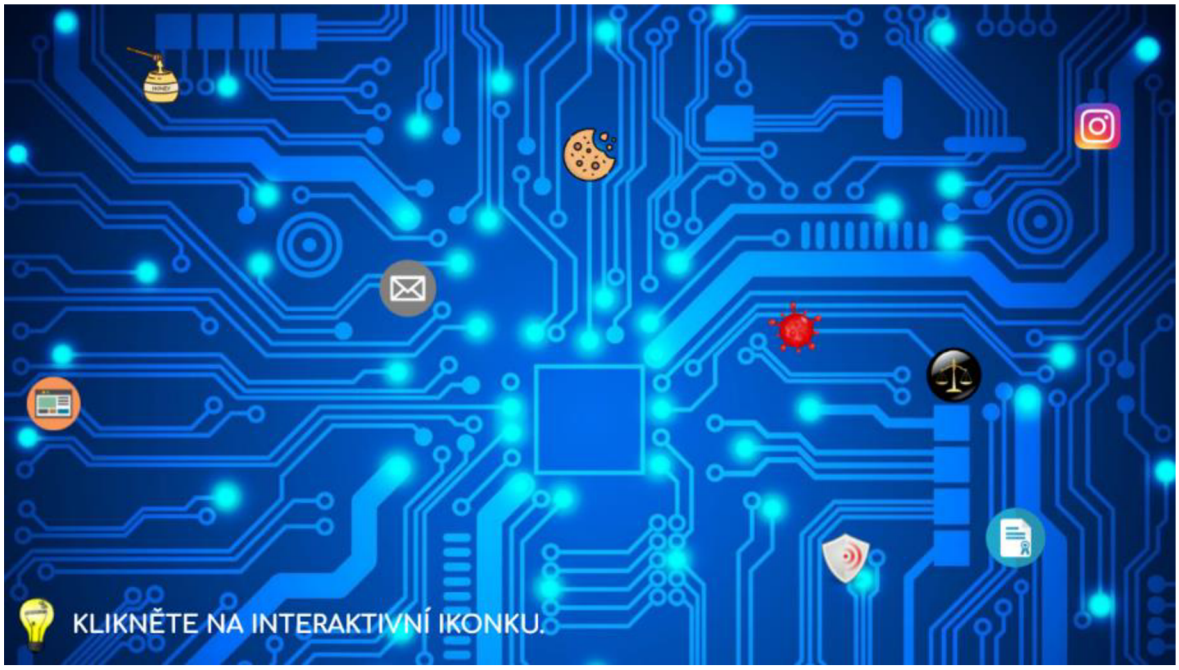
Zdroj: vlastní zpracování

Zdroj: vlastní zpracování

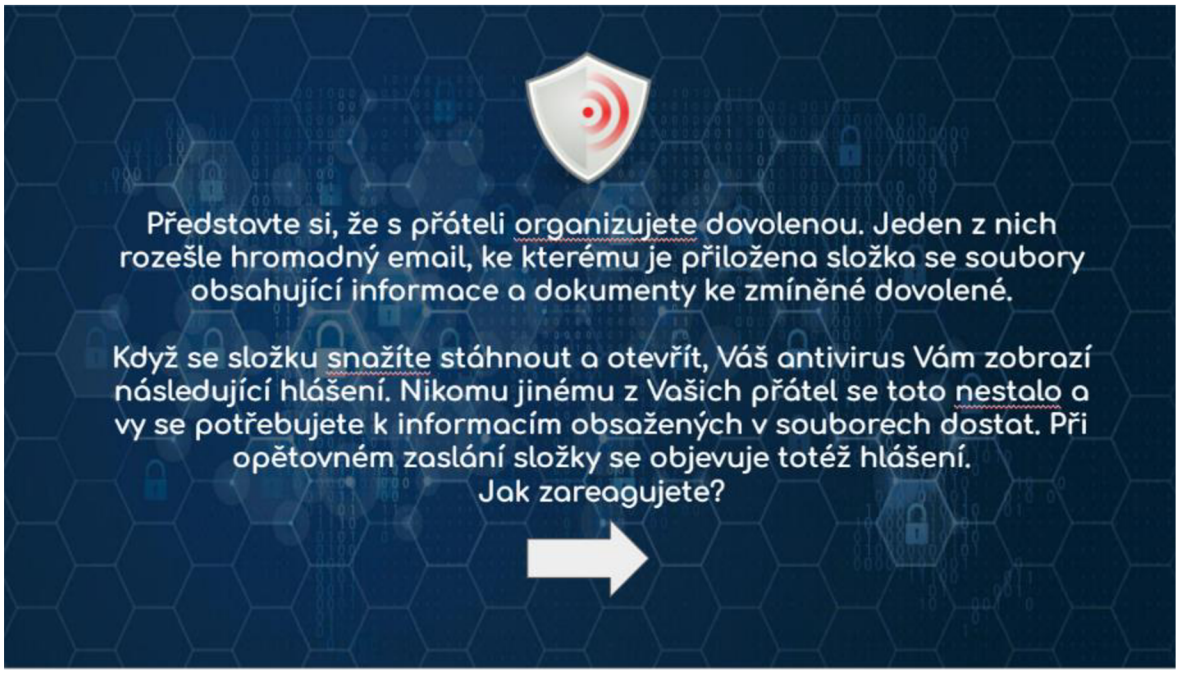


Zdroj: vlastní zpracování

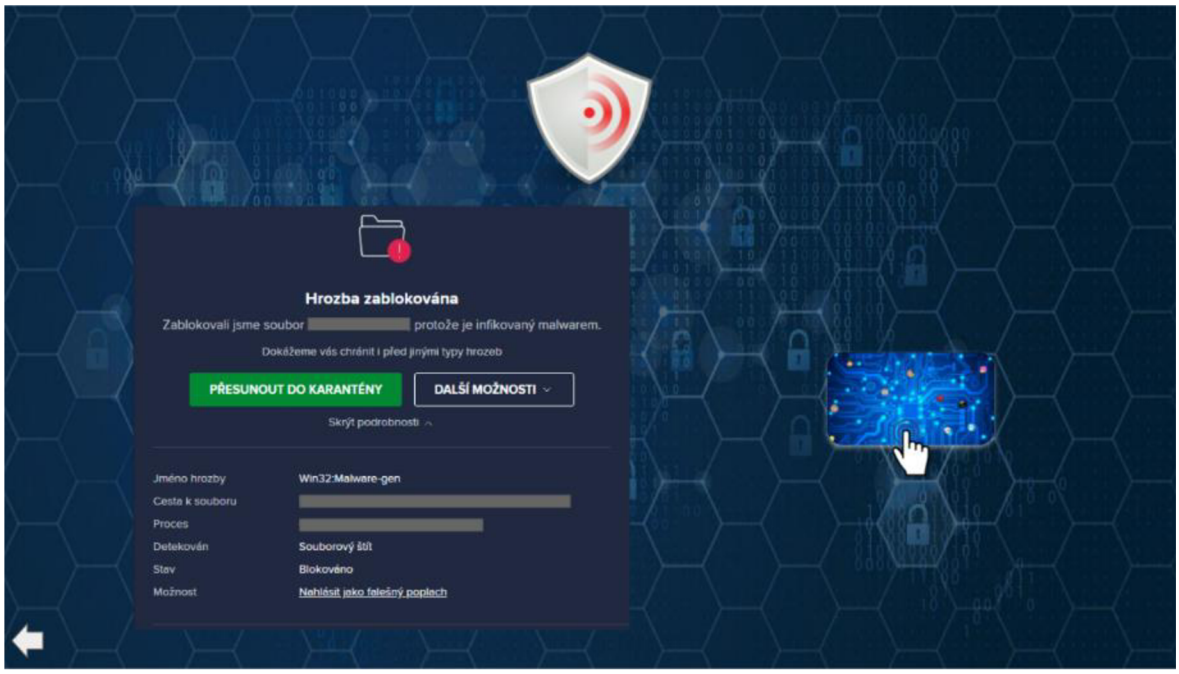
Příloha č. 10 - Hlášení antivirového programu



Zdroj: vlastní zpracování

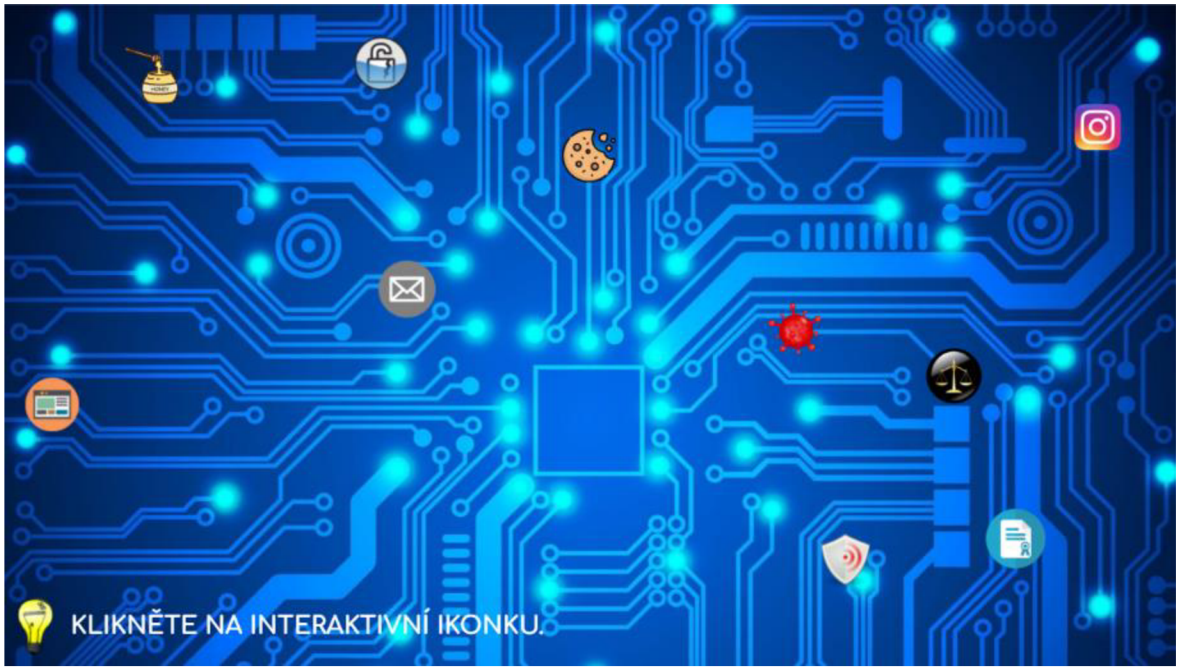


Zdroj: vlastní zpracování

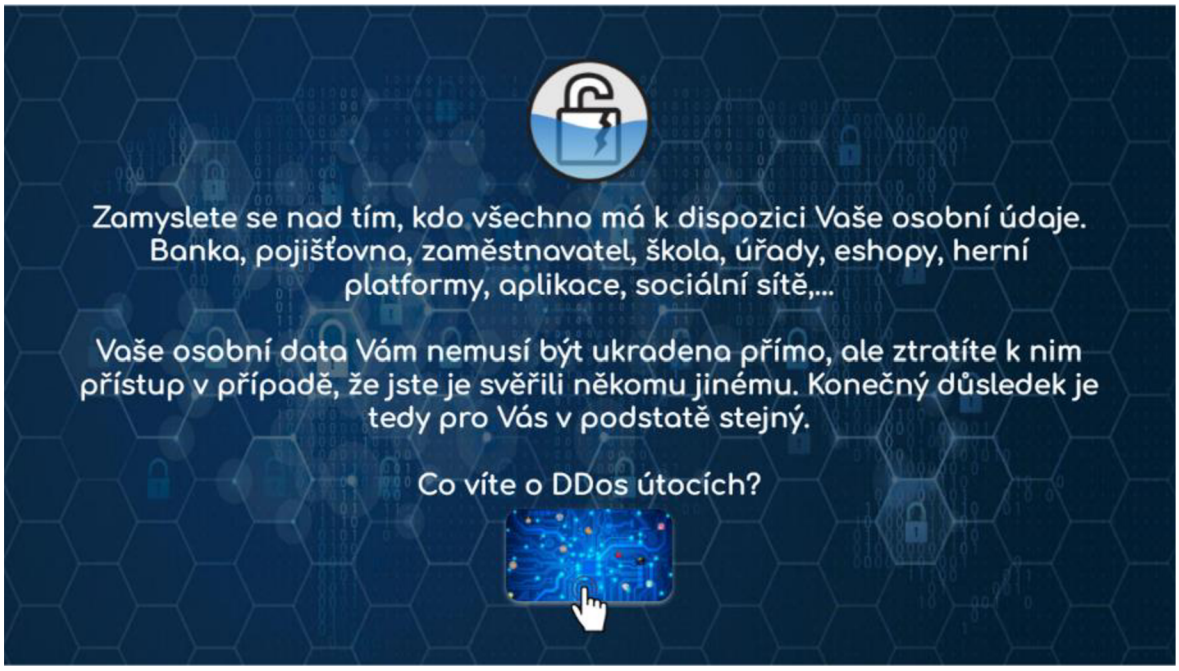


Zdroj: vlastní zpracování

Příloha č. 11 - DDos útoky

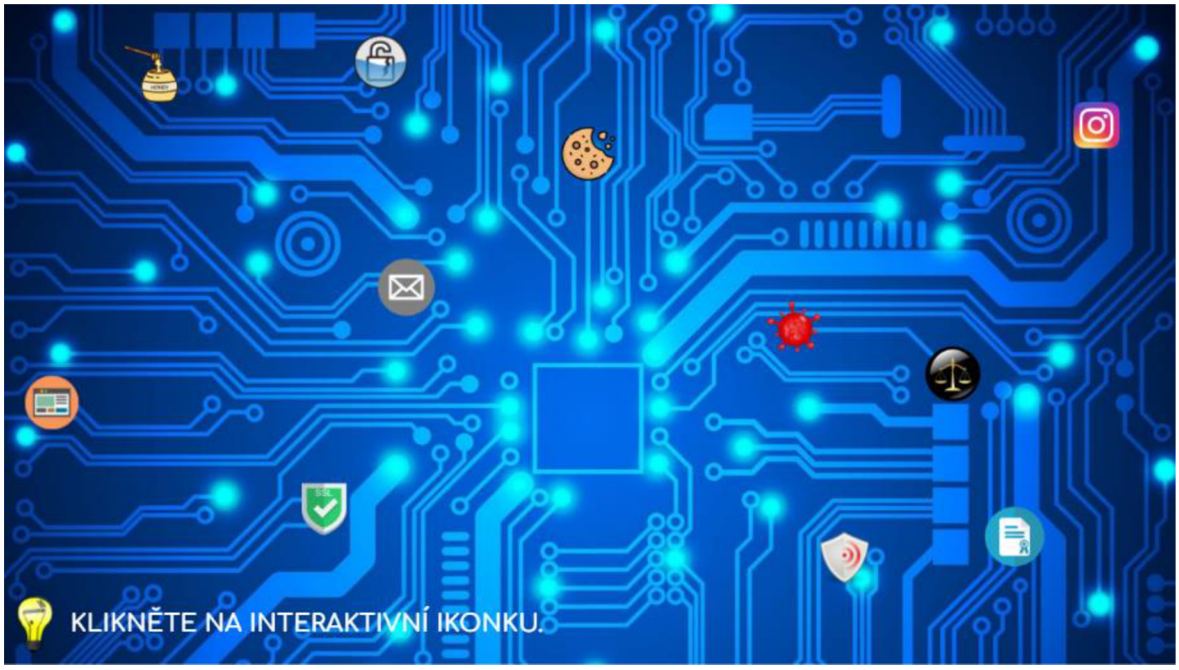


Zdroj: vlastní zpracování

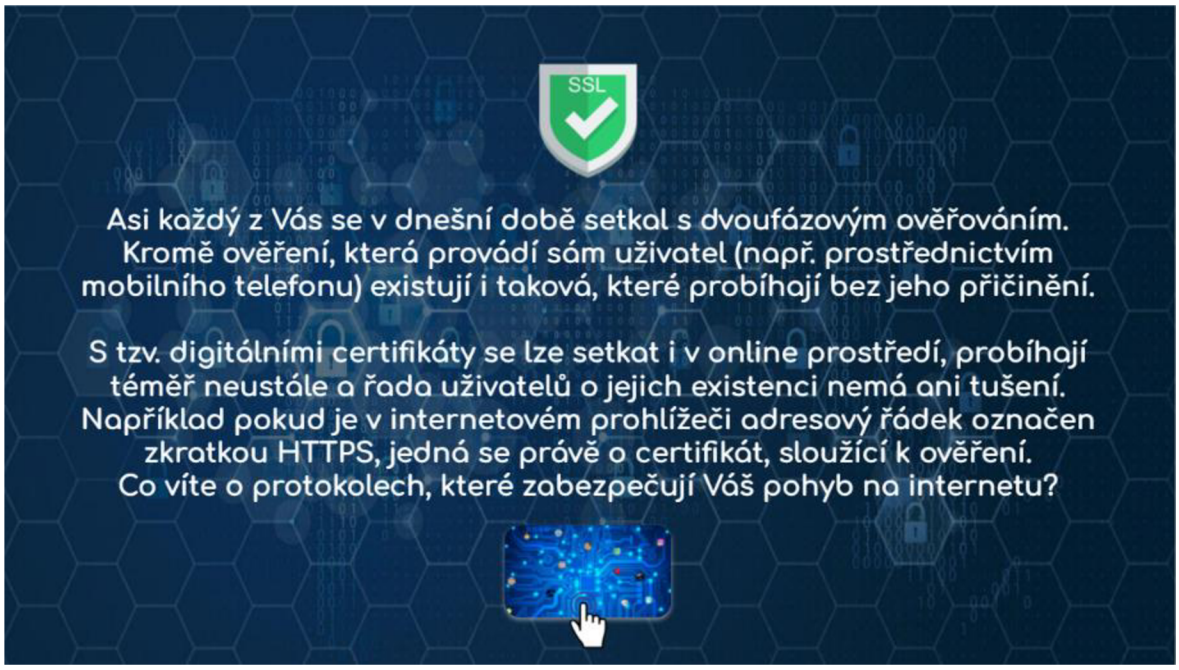


Zdroj: vlastní zpracování

Příloha č. 12 - Digitální certifikáty

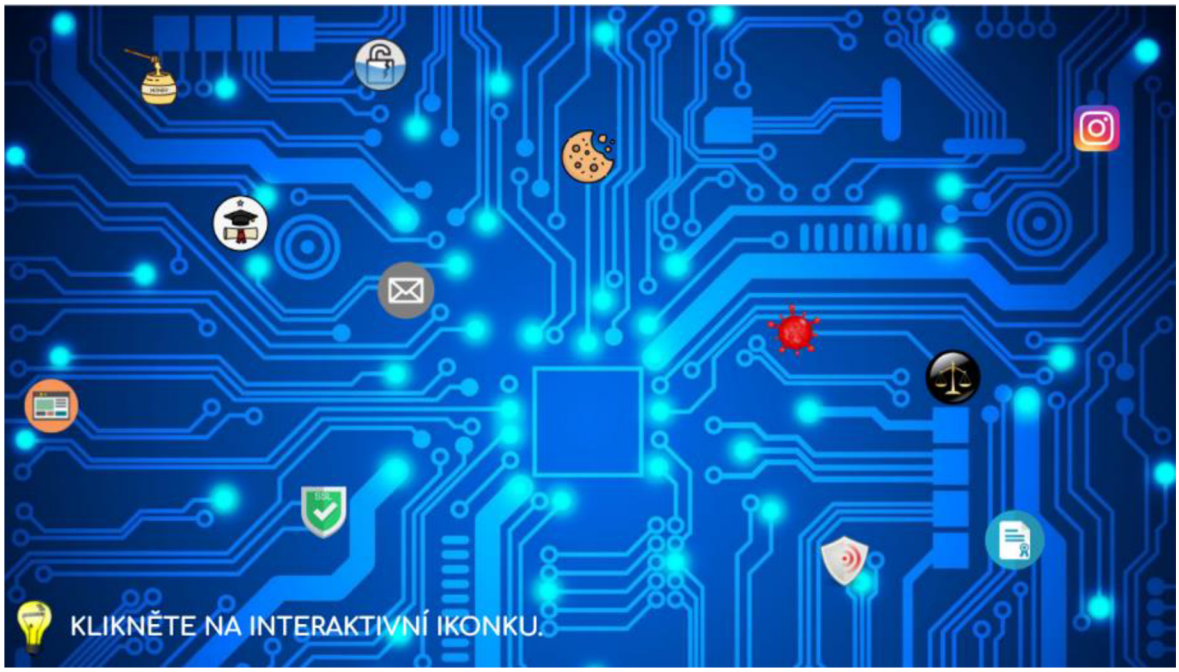


Zdroj: vlastní zpracování

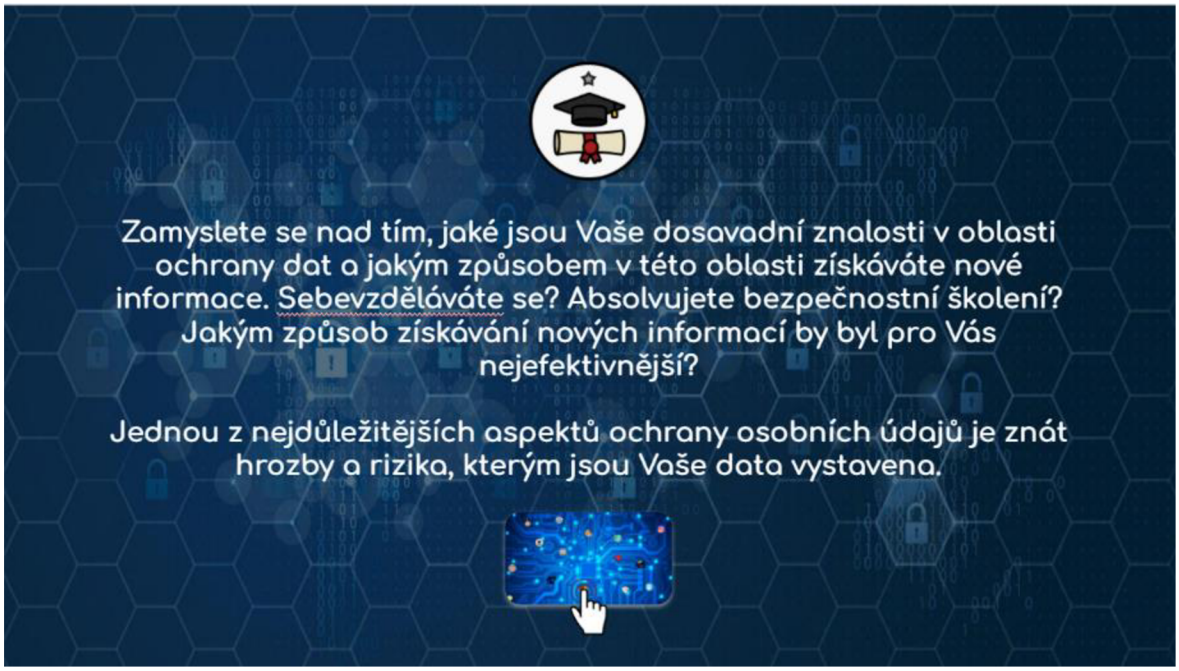


Zdroj: vlastní zpracování

Příloha č. 13 - Vzdělání



Zdroj: vlastní zpracování



Zdroj: vlastní zpracování

Příloha č. 14 – Závěr hry

Zdroj: vlastní zpracování

Zdroj: vlastní zpracování

Zdroj: vlastní zpracování

Zdroj: vlastní zpracování

Zdroj: vlastní zpracování

Zdroj: vlastní zpracování

Příloha č. 15

https://docs.google.com/presentation/d/e/2PACX-1vSj8_-HpEuCKMYhPKlH0ocQ0JpSUlgBtKlcac_bi_aTbt7nKXIBVQ9v9wVEh9pyTFJT50GQPg1N6h3q/pub?start=false&loop=false&delayms=3000&slide=id.g11684b9e808_0_25