Prevence v ochraně soukromí

Bc. David Kučera

Diplomová práce

2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. David Kučera**
Osobní číslo:	**A18576**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Prevence v ochraně soukromí**
Téma práce anglicky:	**Prevention in Personal Privacy Protection**

Zásady pro vypracování

1. Analyzujte podstatu prevence při zajištění bezpečnosti referenčních objektů. Specifikujte, co je primární a sekundární prevence, jakými opatřeními se zajišťuje.
2. Pojednejte o soukromí jako novému druhu aktiva. Zaměřte se na jeho formální, obsahové a právní vymezení.
3. Identifikujte a analyzujte bezpečnostní hrozby, které ohrožují soukromí.
4. Pojednejte o způsobech ochrany soukromí. Identifikujte jednotlivá opatření a zhodnoťte jejich účinnost. Zaměřte se především na preventivní opatření.
5. Vytvořte hypotetický model soukromí, identifikujte hrozby a rizika, jež je ohrožují. Navrhněte dva způsoby ochrany soukromí, tyto prostřednictvím vícekriteriálního hodnocení zhodnoťte a vyberte vhodnější.
6. Rozpracujte preventivní opatření vybraného způsobu ochrany soukromí.

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

Seznam doporučené literatury:

1. VALOUŠEK, Martin. Ochrana osobnosti, soukromí a osobních údajů. Praha: Leges, 2019. ISBN 978-80-7502-346-9.
2. PLECITÝ, Vladimír. Problematika ochrany osob a majetku z pohledu soukromého a veřejného práva. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 9788073802479.
3. ŠIMÍČEK, Vojtěch. Právo na soukromí. Brno: Masarykova univerzita, 2011. ISBN 9788021054493.
4. Listina základních práv a svobod v aplikační praxi ČR. Praha: C.H. Beck, 1997. ISBN 8071791490.
5. Zákon č. 1/1993 Sb., Ústava České republiky. Praha: Armex, 2009. ISBN 978-80-86795-78-2.
6. LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. ISBN 9788073188894.
7. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 9788087500057.
8. MATES, Pavel. Ochrana soukromí ve správním právu. Praha: Linde, 2006. ISBN 80-7201-589-3.

Vedoucí diplomové práce: **doc. Ing. Luděk Lukáš, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **15. ledna 2021**
Termín odevzdání diplomové práce: **17. května 2021**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

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

Ve Zlíně dne 15. ledna 2021

Jméno, příjmení: Bc. David Kučera

Název diplomové práce: Prevence v ochraně soukromí

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně, dne 9. 6. 2021

Bc. David Kučera, v. r.

…….

Podpis diplomanta

ABSTRAKT

Diplomová práce je zaměřena na prevenci v ochraně soukromí. V první části je vyspecifikován pojem prevence a její rozdělení. V další části práce je analyzováno bezpečnostní a právní pojetí soukromí. Zároveň je součástí teoretické části také analýza bezpečnostních hrozeb a návrh preventivních opatření, včetně zhodnocení. Praktická část obsahuje model hypotetického soukromí, včetně popisu preventivních opatření určených k ochraně tohoto celku. Opatření byla vytvářena na základě analýz možných opatření a dotazníkového šetření, které posloužilo jako podpora závěrů uvedených v této práci.

Klíčová slova: prevence, soukromí, ochrana, osobní údaje, identita

ABSTRACT

The diploma thesis focuses on prevention in privacy protection. The first part specifies the concept of prevention and its division. The next part of the thesis analyzes the security and legal concept of privacy. At the same time, the theoretical part also includes an analysis of security threats and a proposal for preventive measures, including evaluation. The practical part contains a model of hypothetical privacy, including a description of preventive measures designed to protect this whole. The measures were created on the basis of analysing possible measures and a questionnaire survey, which was used to support the conclusions presented in this work.

Keywords: prevention, privacy, protection, personal data, identity

Poděkování patří vedoucímu práce panu doc. Ing. Luďkovi Lukášovi, CSc. a to především za trpělivost, odborné vedení a cenné rady, které mi po celou dobu psaní této práce poskytoval.

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

OBSAH

ÚVOD

Prevence v ochraně soukromí je v této době velmi aktuálním tématem, protože ochrana osobních údajů a identity se stává velmi cennou komoditou. Důvodem, proč je tato ochrana tak aktuální je především fakt, že s růstem využívání moderních technologií, roste také počet jeho napadení. Lidé k většině úkonů, ať už v práci nebo v osobním životě využívají internet, důvodem je především jednoduchost, ale také úspora času. Bohužel může využívání internetu a některé neopatrné kroky uživatelů vést k útokům na osobní údaje, fotografie, dokumenty a další aktiva, která se v elektronických zařízeních často nachází.

Častokrát jsou útoky zrealizované za účelem obohacení. Takovým útokům může předcházet právě krádež identity, platebních údajů nebo jiných osobních údajů, které mohou k obohacení vést. V některých případech však nejsou motivací pouze peníze, ale také sledování a následný nátlak, popřípadě vydírání. Případem takové hrozby je například kyberstalking nebo fyzické sledování. V kybernetickém prostoru se navíc v poslední době setkáváme s rostoucí žádostí o schválení tzv. cookies a žádostí o zpracování osobních údajů. Velké společnosti a správci webových stránek po nás žádají čím dál víc osobních údajů a jejich jednání začíná narušovat naše soukromí.

Cílem diplomové práce je analyzovat skutečnost, jak je možné chápat soukromí člověka a co jej vlastně utváří. Dále popsat, jak je na soukromí nahlíženo z pohledu legislativy a dále jakým způsobem může být soukromí ohrožováno. Na základě analýzy a ošetření rizik poté vyhotovit soubor preventivních opatření, vedoucích ke zmírnění dopadů a snížení pravděpodobnosti expozice.

V praktické části této práce je provedena analýza veřejného mínění o tom, jak lidé nahlíží na preventivní opatření a ochranu soukromí. Tato analýza dále slouží jako odrazový můstek pro návrh preventivních opatření k modelu hypotetického celku a jeho soukromí, který je také obsahem praktické části. Model obsahuje popis tříčlenné rodiny, která je finančně zaopatřená a má zájem chránit své soukromí. Je zde podrobně popsáno bydlení a činnosti jednotlivých členů rodiny, na základě kterých jsou poté popsány hrozby ohrožující soukromí. V poslední části jsou popsány způsoby preventivní ochrany soukromí.

I. TEORETICKÁ ČÁST

1 PREVENCE

Každý druh bezpečnosti zahrnuje různá opatření a tato opatření lze především časově rozdělit na opatření, která vznikla před narušením bezpečnosti a ta, která se aplikují až po vzniku narušení bezpečnosti. Jedná se o preventivní a represivní opatření [1].

Prevence pochází z latinského slova „preventio“ a znamená „předcházení“. Je to tedy slovo převzaté z latiny, které se v poslední době často využívá v řadě jazyků a je spojeno především s událostmi negativního charakteru a jejich předcházení. Jedná se o proaktivní přístup, který má zamezovat těmto negativním událostem [2].

Pojem prevence je tedy možno chápat jako soubor opatření, jejichž prostřednictvím se má předcházet škodícím účinkům a jejich působení. Cílem těchto opatření je především, aby újma v ideálním případě vůbec nevznikla a pokud vznikne, tak aby došlo k co nejmenší újmě [1].

1.1 Podstata prevence

Podstata prevence je v každém odvětví chápana podobně. Nejčastěji je pojem prevence využíván v oboru lékařství, kde je prevence rozdělena na primární, sekundární, terciální a kvarterní prevenci. Naopak v pojetí kriminality je prevence rozdělena na primární, sekundární a terciální. Ve všech případech je však úkolem zamezit negativním událostem ještě před jejich vznikem, případně dalšími opatřeními zmírňovat možné dopady. Dělení prevence může být v každém odvětví rozdílné [2].

Abychom lépe pochopili pojem prevence je potřeba definovat i další pojmy, jako jsou bezpečnost, hrozba, riziko, újma a jejich vzájemný vztah. Poté budeme schopni podstatu prevence pochopit v rámci kontextu teorie bezpečnosti, na který se budeme v rámci této práce soustředit.

1.1.1 Bezpečnost

Pojem bezpečnost je definován jako „Stav, kdy je riziko, plynoucí z bezpečnostních hrozeb, minimalizováno na akceptovatelnou úroveň“. Existují různé druhy bezpečnosti a proto také různé možnosti, jak snižovat riziko daných hrozeb, ale vždy je bezpečnost závislá na tom, o jaký referenční objekt se jedná. Referenční objektem je určitá entita, kterou se snažíme ochránit, tedy zamezit vzniku újmy. Může se jednat například o člověka, stát nebo organizaci [1; 3].

V rámci preventivních opatření se snažíme právě o to, aby rizikové incidenty ideálně v žádném případě nenastaly nebo, aby byla újma co možná nejmenší. Pokud budeme hovořit o bezpečnosti, tak k ní také neodmyslitelně patří pojmy hrozba a riziko.

1.1.2 Hrozby

"Hrozba představuje skutečnost (jev se škodícím účinkem), která se svým působením projevuje na určitém celku negativně. Může mu v případě expozice způsobit újmu nebo na něj mít negativní dopad. Jedná se o škodící účinek (působení), které má materiální nebo nemateriální povahu" [1, str. 24].

Pro pochopení pojmu hrozba můžeme uvést příklady z praxe, jakou jsou například teroristické útoky, autonehody nebo přepadení. Tyto typy hrozeb mohou být ohrožením pro naše zdraví. Existují však také logické hrozby, které nevedou přímo k ohrožení života, ale zaměřují se například na zcizení osobních údajů nebo fotografií. Logické hrozby plynou často z využívání technického vybavení, kterými může být například mobilní telefon nebo notebook.

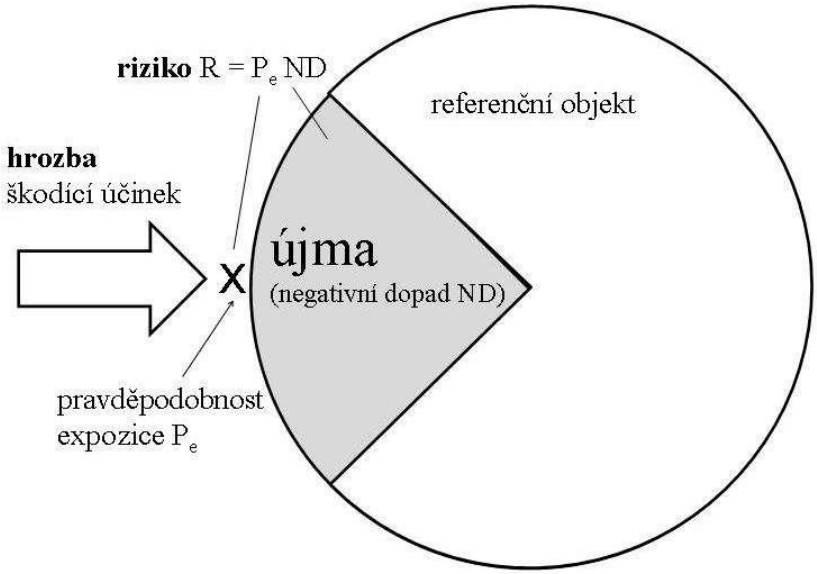
1.1.3 Riziko

Riziko je veličina, která vyjadřuje možnost negativního dopadu. Její vyjádření se uvádí součinem pravděpodobnosti vzniku újmy a její předpokládané velikosti. Riziko je často používaný pojem, například pokud chce chodec přecházet semafor na červenou, tak hrozí riziko, že jej zastaví policie nebo v horším případě, že dojde k újmě na zdraví [4].

Pro jednotku, v níž se uvádí riziko je určující jednotka, v níž se vyčísluje újma, například Kč, EU a jiné. Důležitým nástrojem pro určení rizika je analýza rizik, za pomocí které určíme, kde je objekt nejzranitelnější a jsme tak schopni připravit efektivní preventivní opatření.

1.1.4 Újma

Újma představuje nežádoucí projev nebo negativní změnu na aktivech referenčního objektu. Újmu bývá většinou možné vyčíslit a to nejčastěji v penězích. Negativní dopad naopak nelze v penězích vyčíslit a hodnotí se kvalitativně (malý, střední a velký). Jedná se například o negativní dopady živočišného druhu. Tuto spojitost mezi újmou, hrozbou a rizikem zobrazuje obrázek č. 1.



Obr. 1: Základní bezpečnostní model [1]

Z obrázku č. 1 je patrné, že hrozba má škodící účinek, který působí na referenční objekt. Tento škodící účinek způsobuje referenčnímu objektu určitou újmu a riziko je mírou nebezpečnosti hrozby.

Jinými slovy je možné si představit, že rodinný dům je aktivem referenčního objektu, na který může působit hrozba ve formě zloděje. Újmou by byla krádež cenností a osobních věcí, které v tomto domě jsou. Riziko krádeže je tím větší, čím větší bude pravděpodobnost, že bude možné do domu vniknout a zároveň díky jeho hodnotě, může být atraktivní pro zloděje lup.

Pokud však bude potenciální útočník upozorněn cedulí na plotě, že je objekt střežen a po zahradě bude běhat pes, který bude objekt hlídat, tak je možné tato opatření považovat za preventivní, vedoucí ke snížení rizika, resp. ke snížení pravděpodobností expozice.

1.2 Typy prevence

V současnosti se v rámci pojetí teorie bezpečnosti nejčastěji setkáváme s dělením prevence na primární prevenci a sekundární prevenci. Hlavním důvodem tohoto dělení je to, že primární prevence se soustředí na dobu před škodícím účinkem a sekundární prevence působí až po zahájení působení škodícího účinku. Můžeme také hovořit o tom, že pro různé odvětví platí různá dělení prevence.

Lékařství má k dispozici primární, sekundární, terciální a kvarterní prevenci. Důvodem jsou různé stupně v boji s nemocí, ale také možné dopady a postupy při samotném procesu léčby. Stejně tak základní dělení na primární prevenci, sekundární prevenci a terciální prevenci bude obsahově jiné pro prevenci v kriminalitě, nebo jiném odvětví [2].

1.2.1 Primární prevence

Primární prevence si klade především za cíl předcházet hrozbám, jevům a vlivům, které by mohly vytvořit škodící účinky. Jinými slovy díky působení prevence by nemělo dojít k expozici hrozby. Působení primární prevence také shromažďuje informace o možném vzniku nových hrozeb. Těmto nashromážděným informací potom odpovídají preventivní opatření vedoucí k zamezení újmy.

Případ primární prevence si můžeme uvést například z oblasti dopravy. Abychom zamezili nehodám tedy újmě na silnicích, měli bychom aplikovat několik primárních opatření. Mezi tyto primární opatření může patřit testování řidičů, tzn. řidičské zkoušky, dále značení silnic nebo dohled na silniční provoz pomoci moderních kamerových systému, popřípadě přímo policií.

Dalšími primárními opatřeními mohou být například z oblasti teorie bezpečnosti - školení bezpečnosti, nebo perimetrická ochrana. Dále se může jednat například o opatření z oblasti lékařství, jako jsou pravidelné očkování nebo zdravé podmínky pro žití [2].

1.2.2 Sekundární prevence

Sekundární prevence přímo navazuje na prevenci primární. Jejím úkolem je předejít újmě i za situace, kdy dojde ke škodícímu účinku a jeho působení. Opět tento termín rozvedeme za pomocí příkladu z dopravní praxe.

O sekundární prevenci se může jednat v případě, kdy dojde ke srážce dvou automobilů, tedy k již zmíněnému škodícímu účinku, ale automobil je dostatečně bezpečný a tedy například díky airbagům nedojde k újmě na zdraví člověka. Jde tedy o ochranu ve formě vhodně zkonstruované karosérie – deformační zóny jsou vytvořeny tak, aby absorbovaly kinetickou energii nárazu. Dále může jít o ochranu ve formě bezpečnostních pásů, které mají v rámci nárazu zamezit zraněním pasažérů. V neposlední řádě může jít o systém e-call, který při nehodě posílá základní data na IZS.

Mezi sekundární prevenci můžeme také zařadit z oboru lékařství například preventivní prohlídky a včasnou diagnostiku. Z oblasti teorie bezpečnosti může jít například o anti-theft aplikace, které při krádeži daného zařízení zasílají majiteli informace o poloze a majitel má zároveň možnost obsah zařízení smazat nebo na zařízení upozornit, například za pomocí spuštění nějaké zvuku, většinou ve formě sirény.

1.3 Preventivní opatření

Preventivní opatření označují ta opatření, která se zavádějí před expozicí hrozby a vznikem újmy a zavádějí se za účelem snížení rizika. Důležitým faktorem je především to, aby zaváděná opatření nebyla například finančně náročnější než negativní finanční dopad, který by mohl být způsoben referenčnímu objektu.

Preventivní opatření mohou být aplikována fyzickou cestou, tedy především zamezením přístupu k referenčnímu objektu. Konkrétně můžeme říci, že pokud nebudeme chtít, aby se někdo dostal do námi chráněného obydlí, tak na okraji pozemku vybudujeme oplocení.

Popřípadě mohou být preventivní opatření aplikována logickou cestou. To platí v případě, kdy je k referenčnímu objektu přístup, ale snažíme se zamezit negativnímu dopadu. Modelovým příkladem může být například mobilní telefon s cennými daty, který položíme na pracovní stůl. Fyzická cesta preventivního opatření by byla, zamezit přístupu k tomuto mobilnímu zařízení, ale logická cesta je ta, že mobilní telefon zajistíme příslušným heslem nebo biometrickým ověřením, které zloději zamezí přístupu k informacím v zařízení.

2 SOUKROMÍ

Pojem soukromí je v poslední době velmi často využívaný a to v různých oblastech našeho života. Pro každého může mít však jiný význam. Někteří vidí soukromí jako například svou „osobní zónu“, do které by nikdo neměl vstupovat, jiný za soukromí považuje zprávy, které si posílá se spolužákem a někdo další by mohl namítat, že se jedná o věci, které ukrývá za plotem, aby je nikdo neviděl. Všichni mohou mít pravdu, ale jak konkrétně soukromí vypadá a odkud, kam sahá, by nám měla pomoci ujasnit tato kapitola.

V dnešním světě sociálních sítí někteří lidé vyměňují náhled do svého soukromí za velké obnosy peněz. Na druhou stranu jsou také lidé, kteří jsou ochotni obětovat nemalé částky, aby své soukromí ukryli a jejich digitální a tím i fyzická stránka život zůstala v anonymitě [5].

Pojem soukromí, je znám již zhruba 3 tis. let. Tehdy lidé nevěděli, že se jedná o soukromí, ale jednalo se spíše o jakési pocity “provinění”. Jsou známé důkazy, které definují především ostych rodičů, které nechtěli mít pohlavní styk, když byli v okolí děti. Našly se domy, ve kterých byly místnosti pro děti a rodiče oddělené a má se za to, že důvodem bylo právě soukromí, které pro sebe dospělí chtěli mít [6].

Dalším příkladem z historie soukromí jsou Řekové, kteří v období 4. - 6. stol. n. l. přemýšleli za pomocí geometrie nad zmenšením oken, ale s maximalizací prostupnosti světla. V podstatě se jednalo o to, aby lidé procházející ulicí neviděli lidem do místností a díky tomu bylo zachováno soukromí lidí obývajících onu domácnost [6].

Do 18. století bylo soukromí dosahováno především za pomocí architektonických úprav místností, popřípadě průzoru oken, ale koncem 18. století se na tuto problematiku začalo spolu s rozvojem práva nahlížet také z jiných úhlů a to například jako na ochranu sdělování informací. Tuto skutečnost dokazovala listina, která ve Spojených státech amerických zakazovala, aby zaměstnanci pošty třídili listování zásilky pomocí pročítání sdělovaných zpráv a tím se mělo zamezit úniku informací [6].

Pojetí soukromí bylo zaměřeno pouze na člověka a jeho fyzično, do jehož prostoru nesměl nikdo bez dovolení zasáhnout, pokud tedy zákon nehovořil jinak. Později však došlo k úpravě právního pohledu a za soukromí se považovalo tzv. “soukromí čtyř stěn”. Avšak dnešní vyjádření se nezaměřuje pouze na místo, kde člověk žije nebo tráví svůj čas, ale také na právo budovat vztahy s dalšími lidmi [7].

2.1 Právní vymezení pojmu soukromí

Odborníci, kteří se právem zabývají, souhlasně tvrdí, že pojem „právo na soukromí“ nelze jasně definovat. Důvodem je, že hodnoty, které se týkají soukromí, se neustále mění a vyvíjí. Proto například Evropský soud pro lidská práva prohlásil, že není nutné pokoušet se o přesnou definici [8].

Ochranou soukromí se v České republice zabývá obecné ustanovení §81 Občanského zákoníku a tentýž zákon upravuje ustanovení §86. Dále je soukromí chráněno také Listinou základních práv a svobod z roku 1992 [8].

2.1.1 Občanský zákoník – zákon č. 89/2012 Sb.

Občanský zákoník má za úkol upravovat všechny soukromoprávní vztahy, které jsou sebrány do jednoho právního kodexu. Důležitým faktorem tohoto zákona je dodržování demokratických práv, pro jehož sepsání byl základem návrh občanského zákoníku bývalého Československa z roku 1937 [9].

Občanský zákoník je zákon č. 89/2012 Sb. z roku 2012 s aktuální úpravou z roku 2020. V tomto zákoně stojí, že:

“§3

(1) Soukromé právo chrání důstojnost a svobodu člověka i jeho přirozené právo brát se o vlastní štěstí a štěstí jeho rodiny nebo lidí jemu blízkých takovým způsobem, jenž nepůsobí bezdůvodně újmu druhým.

(2) Soukromé právo spočívá zejména na zásadách, že každý má právo na ochranu svého života a zdraví, jakož i svobody, cti, důstojnosti a soukromí“ [6].

Dále je velmi zajímavé jakým způsobem občanský zákoník nahlíží na jméno, zacházení se jménem a jeho ochranou:

„§ 77

(1) Jméno člověka je jeho osobní jméno a příjmení, popřípadě jeho další jména a rodné příjmení, která mu podle zákona náležejí. Každý člověk má právo užívat své jméno v právním styku, stejně jako právo na ochranu svého jména a na úctu k němu.

(2) Člověk, který v právním styku užívá jiné jméno než své vlastní, nese následky omylů a újem z toho vzniklých.“

Na § 77 občanského zákoníku navazuje také oddíl č. 6 s názvem „Osobnost člověka“, který hovoří o ochraně důstojnosti života [10].

„§ 81

(1) Chráněna je osobnost člověka včetně všech jeho přirozených práv. Každý je povinen ctít svobodné rozhodnutí člověka žít podle svého.

(2) Ochrany požívají zejména život a důstojnost člověka, jeho zdraví a právo žít v příznivém životním prostředí, jeho vážnost, čest, soukromí a jeho projevy osobní povahy“ [10].

Následuje ustanovení o možnosti obrany proti porušení práva.

„§ 82

(1) Člověk, jehož osobnost byla dotčena, má právo domáhat se toho, aby bylo od neoprávněného zásahu upuštěno nebo aby byl odstraněn jeho následek.

(2) Po smrti člověka se může ochrany jeho osobnosti domáhat kterákoli z osob jemu blízkých.

§ 83

(1) Souvisí-li neoprávněný zásah do osobnosti člověka s jeho činností v právnické osobě, může právo na ochranu jeho osobnosti uplatnit i tato právnická osoba; za jeho života však jen jeho jménem a s jeho souhlasem. Není-li člověk schopen projevit vůli pro nepřítomnost nebo pro neschopnost úsudku, není souhlasu třeba.

(2) Po smrti člověka se právnická osoba může domáhat, aby od neoprávněného zásahu bylo upuštěno a aby byly odstraněny jeho následky“ [10].

Jednou z nejdůležitějších částí zákona popisující ochranu soukromí je bezesporu tato část:

„§ 86

Nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Zejména nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, nebo takové záznamy o jeho soukromém životě šířit. Ve stejném rozsahu jsou chráněny i soukromé písemnosti osobní povahy.

§ 87

(1) Kdo svolil k použití písemnosti osobní povahy, podobizny nebo zvukového či obrazového záznamu týkajícího se člověka nebo jeho projevů osobní povahy, může svolení odvolat, třebaže je udělil na určitou dobu.

(2)Bylo-li svolení udělené na určitou dobu odvoláno, aniž to odůvodňuje podstatná změna okolností nebo jiný rozumný důvod, nahradí odvolávající škodu z toho vzniklou osobě, které svolení udělil“ [6].

Dále se zákon zabývá případy, ve kterých je nutné svolení k použití písemností a podobizen, popřípadě ve kterých výjimečných případech není nutné povolení přijmout.

„§ 88

(1) Svolení není třeba, pokud se podobizna nebo zvukový či obrazový záznam pořídí nebo použijí k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob.

(2) Svolení není třeba ani v případě, když se podobizna, písemnost osobní povahy nebo zvukový či obrazový záznam pořídí nebo použijí na základě zákona k úřednímu účelu nebo v případě, že někdo veřejně vystoupí v záležitosti veřejného zájmu.

§ 89

Podobizna nebo zvukový či obrazový záznam se mohou bez svolení člověka také pořídit nebo použít přiměřeným způsobem též k vědeckému nebo uměleckému účelu a pro tiskové, rozhlasové, televizní nebo obdobné zpravodajství“ [10].

Pro všechny výjimky platí omezující podmínka, že je možné výjimku použít jen přiměřeným způsobem.

„§ 90

Zákonný důvod k zásahu do soukromí jiného nebo k použití jeho podobizny, písemnosti osobní povahy nebo zvukového či obrazového záznamu nesmí být využit nepřiměřeným způsobem v rozporu s oprávněnými zájmy člověka“ [10].

Občanský zákoník obsahuje mnoho ustanovení, která chrání soukromí občanu České republiky. Především se zabývá ochranou jména a s ním spojených záležitostí jako jsou ochrana důstojnosti a cti. Dále je důležitá ochrana soukromých záležitostí jako i prostor a to včetně pořizování, ať už zvukových či obrazových nahrávek.

2.1.2 Základní listina práv a svobod – ústavní zákon č. 2/1993 Sb. ve znění ústavního zákona č. 162/1998 Sb.

Jedná se o zákon č.2/1993 Sb., Listina základních práv a svobod, která pojednává především o samosprávě demokratických tradic, zabezpečení svobodných hodnot a jejímž cílem je zachovat tyto hodnoty pro budoucí generace [11].

Hlava druhá tohoto zákona se zabývá Lidskými právy a základními svobodami. Zajímavý je čl. 7, který hovoří o zaručení soukromí takto:

„(1) Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.

(2) Nikdo nesmí být mučen ani podroben krutému, nelidskému nebo ponižujícímu zacházení nebo trestu“ [11].

Další částí zákona, který hovoří o soukromí je čl. 10, ve které je popsána ochrana před zásahem do soukromí, zveřejňování nebo zneužívání údajů o osobách.

„*Článek 10*

(1) Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.

(2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.

(3) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě" [11].

V tomto zákoně je mnoho částí zabývajících se ochranou soukromí, například také čl. 12, který říká:

„(1) Obydlí je nedotknutelné. Není dovoleno do něj vstoupit bez souhlasu toho, kdo v něm bydlí.

(2) Domovní prohlídka je přípustná jen pro účely trestního řízení, a to na písemný odůvodněný příkaz soudce. Způsob provedení domovní prohlídky stanoví zákon.

(3) Jiné zásahy do nedotknutelnosti obydlí mohou být zákonem dovoleny, jen je-li to v demokratické společnosti nezbytné pro ochranu života nebo zdraví osob, pro ochranu práv a svobod druhých anebo pro odvrácení závažného ohrožení veřejné bezpečnosti a pořádku. Pokud je obydlí užíváno také pro podnikání nebo provozování jiné hospodářské činnosti, mohou být takové zásahy zákonem dovoleny, též je-li to nezbytné pro plnění úkolů veřejné správy" [11].

Základní listina práv a svobod obsahuje celou řadu článků, které nám pomáhají definovat práva a možnosti ochrany soukromí. V druhém oddíle tohoto zákona je zaručena také svoboda slova, což může samozřejmě velmi souviset se zásahem do soukromí. Kdy jsou v dnešní době především známé osobnosti napadány slovním projevem novinářů, popřípadě tzv. „haterů" za pomocí sociálních sítí [11].

V dnešní době se na základní svobody zapomíná a někteří mají pocit, že druhým mohou určovat, co smí říkat na veřejnosti, jakým způsobem se chovat a za co vše jsou dané osoby vlastně historicky zodpovědné. Tímto způsobem však dochází k formování jedinců, kteří jsou cenzurováni a jejichž soukromí je porušováno.

2.1.3 Trestní zákoník – zákon č. 40/2009 Sb.

Trestní zákoník upravuje především trestní právo hmotné. Obsahuje základy trestní odpovědnosti, trestní sankce a zvláštní ustanovení o některých pachatelích. Součástí jsou také trestné činy spáchané proti lidské důstojnosti, proti rodině, dětem nebo životnímu prostředí [12].

Jedná se tedy o zákon č. 40/2009 Sb., podle kterého se rozhoduje o vině případného pachatele. Za protiprávní jednání se mohou považovat například trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství [8; 13].

Neoprávněné nakládání s osobními údaji

„§ 180

(1) Kdo, byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti.

(2) Stejně bude potrestán, kdo, byť i z nedbalosti, poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají“ [13].

Dalším případem porušení zákona je porušení tajemství dopravovaných zpráv. Přesné znění zákona popisuje § 182.

„§ 182

(1) Kdo úmyslně poruší tajemství

a) uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením,

b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo

c) neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

(2) Stejně bude potrestán, kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch

a) prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu, telefonního hovoru nebo přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu, nebo takového tajemství využije" [13].

Pomluva může být také jednou z možností narušení soukromí. Častokrát se v současnosti setkáváme s tímto trestným činem. V některých případech jsou domněnky vysloveny jako pomluvy a mohou lidem skutečně ublížit a pošpinit i jejich dobré jméno.

„§ 184

Pomluva

(1) Kdo o jiném sdělí nepravdivý údaj, který je způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu, bude potrestán odnětím svobody až na jeden rok.

(2) Odnětím svobody až na dvě léta nebo zákazem činnosti bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem" [13].

Trestní zákoník se ze tří popsaných zákonů zabývá ochranou soukromí nejpodrobněji a je zde popsán také následek protiprávního jednání. Důležité je, že nejde pouze o krádež informací, ale především o člověka jako součást celku. Chrání dobré jméno dané osoby, jeho pověst mezi ostatními lidmi, což může mít velký dopad na jeho soukromí.

Zajímavá je část zabývající se uchováním informací od dané osoby. Lidé v některých případech zneužívají informace, které jim jsou předkládány a to především pro vlastní prospěch. Příkladem těchto událostí mohou být mnohačetné otázky na internetových fórech, ve kterých se píše o sledování zaměstnanců za pomocí služebních telefonů využívaných k osobním účelům. Sledování zpráv odcházejících ze služebního e-mailu nebo dokonce trasování za pomocí GPS ve služebním automobilu. Tyto případy většinou nekončí u soudu, ale ukončením pracovního poměru a na daných fórech se objevují právě proto, že se některým zdá tato jednání v nepořádku.

2.1.4 GDPR - Nařízení Evropského parlamentu a Rady (EU) č. 2016/679

Název GDPR znamená „Obecné nařízení o ochraně osobních údajů“ a je to nařízení Evropského parlamentu a Rady (EU) z roku 2016. Platnost toho nařízení je v českém právním prostředí nutné dodržovat od 25. května 2018. Nařízení představuje právní rámec ochrany osobních údajů [14].

Toto nařízení vzniklo především z důvodu sjednocení právního rámce ve všech zemích Evropské unie a má za cíl zvýšit a sjednotit ochranu osobních dat občanů. Především jde o to, že v minulosti byly některé osobní údaje využívány nesprávně nebo bez vědomí osob. Proto bylo nutné upřesnit jejich použití a podmínky za jakých mohou být tyto údaje zpracovány [14; 15].

Co je to zpracování údajů a o jaké údaje může jít? Zpracováním se rozumí především manipulace, shromažďování, získávaní a případná likvidace dat. Jedná se o zpracování osobních údajů, mezi které patří data, která identifikují fyzickou osobu. Především jméno, příjmení, adresa nebo popřípadě číslo občanského průkazu a rodné číslo. Může se ale také jednat o genetické nebo biometrické údaje typu: DNA, otisk prstu nebo snímek obličeje [15; 16].

2.1.5 Dílčí závěr

Z výše analyzovaných zákonů plyne, že právo na soukromí patří neodmyslitelně k lidským životům. Každý zákon má na celou věc mírně odlišný úhel pohledu. Proto je nutné tyto pohledy definovat pro přesnější popis v této práci.

Občanský zákoník, jelikož chrání soukromoprávní vztahy, se zabývá především ochranou osob, jejich důstojností, spojenou s tímto jménem, ale také ochranou soukromých prostor,

které tato osoba využívá. S tím je spojena také ochrana s nahráváním osob, vytvářením podobizen a jsou zde také výjimky pro případné užití těchto údajů [10].

Základní listina práv a svobod se zabývá především elementární částí soukromí a tou je svoboda projevu, ochrana jména a svoboda shromažďování. Podobně jako v občanském zákoníku je zde zmíněno zachování důstojnosti spojené s vlastním jménem, tedy jedincem [11].

Trestní zákoník se více soustředí na porušení tajemství, plynoucích od dané osoby. Je zde popsáno, že využívání informací plynoucích ze zásahu do zpráv, ať už zvukových či jiných může vést k trestnímu stíhání. Celkově je v trestním zákoníku hlouběji popsán postih za jednotlivá porušení zákonů. Neméně důležitou částí trestního zákoníku je definice pomluvy, tedy znevažování dobrého jména osob a šíření lživých či nepodložených zpráv o dané osobě [13].

V neposlední řadě se soukromí týká také GDPR, které chrání osobní údaje před zneužitím. Je to ze zmíněných zákonů/nařízení nejnovější dokument a vznikl především díky rozvoji moderních technologií a sjednocení Evropských právních předpisů. V minulosti bylo zneužití dat velmi snadné a díky tomuto nařízení už by tomu tak být nemělo [15].

Soukromí je podle každého ze zákonů definováno odlišně, a proto je nutné vzít jednotlivé výše uvedené myšlenky a soukromí definovat. Soukromí definuje soubor práv, myšlenek, osobních údajů, ale může se také jednat o dokumenty a věci, které pro člověka mohou mít určitou citovou nebo finanční hodnotu.

Za soukromí se považují věci, které pro daného jedince mají osobní význam a mohou jej charakterizovat, například soukromím je také lidské tělo, které má nezaměnitelnou podobu, resp. otisk prstu nebo oční duhovky, které se používají k identifikaci osob. Soukromím je svoboda projevu a ochrana důstojnosti.

2.2 Druhy soukromí

Pro někoho je soukromí velmi důležité a pro jiného neznamená mnoho. Důležitá je však skutečnost, že se dá soukromí v jakékoliv formě, ať už jako fotka, jméno nebo profil na sociální síti velmi snadno zneužít. Soukromé informace by měl mít člověk pod kontrolou a přístup k těmto informacím vždy pečlivě střežit.

Podle zákonů, které byly výše popsány, je na každém, jak se svými citlivými údaji naloží. Je těžké specifikovat, co vše soukromí obsahuje. Soukromí spadá do jakési fuzzy množiny, ve které hranice určuje pouze dotyčná osoba. Je možné však specifikovat, co jsou osobní údaje a jak se rozdělují.

Osobní údaje

1. Obecné osobní údaje:
    a. jméno a příjmení,
    b. věk,
    c. pohlaví,
    d. národnost,
    e. číslo občanského nebo řidičského průkazu,
    f. vzdělání,
    g. fotografie.
2. Biometrické údaje:
    a. DNA,
    b. krevní skupina,
    c. otisky prstů,
    d. oční duhovka,
    e. obličej.

2.2.1 Finanční soukromí

Do této kategorie spadají útoky na soukromí za účelem krádeže financí, popřípadě informací vedoucích ke krádeži financí. Tato oblast je v poslední době ohrožována především pomocí internetu. Nejčastěji se vyskytují ve formě phishingu. Phishing je vydávání se za důvěryhodnou autoritu s účelem získat citlivá data, popřípadě zasílání falešných e-mailů s cílem navnadit příjemce k odeslání peněz [17; 18].

Nejčastějšími případy jsou krádeže přihlašovacích údajů k internetovému bankovnictví, ale existují také daleko sofistikovanější metody. Existují přístroje, tzv. NFC čtečky, které dokážou z kreditní karty vybavené právě NFC technologií ukrást peníze pouhým přiblížením těchto zařízení [19].

Neobvyklé nejsou ani případy zneužití osobních údajů, nejčastěji za účelem vytvoření půjčky. V obchodech je možné za použití dvou dokladů totožnosti získat půjčku například

na zboží v obchodě s elektrospotřebiči, ale také půjčku u bankovní instituce. Nevýhodou je, že pokud taková transakce proběhne, tak se to oběť dozví nejčastěji v okamžiku, kdy jí přijde výzva k úhradě pohledávky. Často to bývá nejméně po jednom a více měsících, což jsou nejčastější frekvence splátek půjček.

2.2.2 Ochrana lidských práv

Ochranou lidských práv se zabývá ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ale v tomto zákoně se hovoří především o svobodě slova a pohybu. Z pohledu soukromí to však je možné brát jako ochranu před sledováním nebo cenzurou našeho názoru, který pro může být pro jednotlivce charakterizující. Případná cenzura by mohla být právě útokem na lidskou důstojnost, která se v již zmíněném zákoně popisuje [11].

O zásahu do soukromí z pohledu porušení lidských práv mohli lidé v Evropě hovořit především ve 20. stol., kdy byli neustále někým utlačování za to, jaké jsou rasy nebo národnosti. V 70. letech docházelo především ke shromažďování informací a sledování pohybu osob. V tomto období se na území Spojených států amerických hovoří především o utlačování menšin. Tento problém je na denním pořádku v řadě zemí dodnes.

2.2.3 Osobní soukromí

Osobním soukromím je v tomto kontextu myšleno především střežení vlastního majetku, věcí které mohou mít pro jednotlivce určitý hlubší význam. Na začátku této kapitoly bylo zmíněno, že lidé v sobě mají zakořeněnou ochranu před vnějším světem. Snaží se především chránit svou rodinu a nechtějí, aby je někdo sledoval, jak se baví se svými blízkými a jak spolu tráví volný čas. Samozřejmě je důležité také chránit majetek, který člověk vlastní. Proč by jinak lidé vynalezli dveře, kdyby chtěli všechno sdílet se svými sousedy. Důvodem je právě zachování soukromí [17].

V dřívějších dobách lidem záleželo především na ochraně majetku hmotného. Lidé z vyšších vrstev ukazovali, jakým bohatstvím disponují. Především formou drahých šatů a šperků. V dnešních dobách se však situace u některých bohatých jedinců změnila a je naopak zájem o ochranu soukromí a s tím spojenou ochranu majetku a blízkých osob.

2.2.4 Soukromí na internetu

Problémem dnešní doby je bezesporu zneužívání dat o pohybu uživatelů na internetu. Při vstupu prakticky na každou webovou stránku je vyžadováno potvrzení cookies. Tedy

shromažďování informací o aktivitě na dané stránce. Uživatel má dvě možnosti, buď nesouhlasit a díky tomu se tedy na stránku nedostat, popřípadě v omezeném režimu nebo souhlasit, ale veškerá aktivita bude zaznamenána. Otázkou je, co se s těmito daty dále děje a proč má někdo potřebu takové věci shromažďovat? Webové stránky je užívají především k tomu, aby umožňovaly poskytování reklam a produktů, které jsou nejčastěji vyhledávány [17; 20; 21].

Dalším ohrožením soukromí na internetu je vytváření smyšlených profilů na sociálních sítích a využívání buď smyšlených, nebo duplikovaných údajů, fotek a dalšího obsahu. Tímto způsobem je možné zneužít identitu osob velmi často za účelem obohacení. Příkladem může být muž, který zduplikoval profil pohledné mladé dívky, oslovoval starší muže a s nabídkou zaslání intimních fotografií od nich získával peníze. Přišel si takto na 1,5 mil. Kč.

Dalším případem ohrožení může být také hacking. U hackingu dochází k narušování dat a případně i zneužívání zařízení. Hacker se dostává přímo do zařízení a může „libovolně“ nakládat s daty, které jsou v zařízení uloženy. Může tak docházet ke krádeži citlivých dat, ale také ovládání účtů na sociálních sítích, e-mailů a přístupu k cenným dokumentům. Součástí tohoto činu může být také následné vydírání, spojené s krádeží například citlivých fotek. Z minulosti jsou známé útoky na světové celebrity, kterým se hacker vlámal do zařízení a zcizil tam intimní fotografie, kterými osoby nejprve vydíral a později je umístil na veřejně přístupné stránky. Objetí těchto činů se staly například herečky Jennifer Lawrence, Scarlett Johansson nebo Mila Kunis [17; 22; 23].

V neposlední řadě a zdaleka nejhorším činem, který se na internetových sítích odehrává, je zneužívání identity ke kontaktování dětí mladších 18 let. Útočníci často oběť kontaktují, komunikují s ní a po čase žádají intimní fotografie, pokud je však dostanou tak dochází k dalšímu vydírání. Toto jsou vážné přečiny proti lidskosti a důstojnosti [22].

2.3 Soukromí jako nový druh aktiva

V minulých stoletích se lidé pokud byli bohatí vyznačovali především tím, jaké měli šaty, v jakých bydleli domech, kolik měli šperků a později jaký měli dopravní prostředek nebo na jaké adrese bydleli. Zkrátka záleželo na věcech, které byly v ideálním případě vidět nebo se daly nějak představit.

S rozvojem technologií se začíná nad bohatstvím uvažovat jinak. Lidé si hmotných statků začínají vážit méně a to proto, že jsou nahraditelné. Pokud například pes rozbije televizi, je možné v obchodě koupit novou. V případě vyloupení bytu, kdy má většina lidí pojištění, analyzuje škodu likvidátor a pojišťovna vyplatí náhradu škod. Co se však stane, v případě zneužití osobních údajů. Jakým způsobem je možné smazat osobní fotografii, která se dostala na internet, ale dal jí tam naprosto cizí člověk. Soukromí se stává stále důležitější skutečností, protože je nenahraditelné. Důležitějšími se stávají naše osobní údaje, fotky, ale také například sdílení polohy.

3 BEZPEČNOSTNÍ HROZBY OHROŽUJÍCÍ SOUKROMÍ

S rozvojem sociální a technologické oblasti se objevují také nové druhy aktiv, které je nutné chránit. Aktivem, jak již bylo zmíněno, se může stávat to, na čem si daná osoba vytvoří závislost a co také často používá. A právě z rozvoje nových druhů aktiv se vytváří i nové hrozby. Příkladem nových hrozeb ohrožujících soukromí může být krádež identity, zneužití platebních údajů, zkrátka vše co souvisí s osobními údaji, ať už se jedná o jakýkoliv druh.

Nejčastěji se setkáváme s krádeží profilů na sociálních sítích, za účelem vydírání nebo obohacení. Zneužití osobních údajů za účelem poskytnutí finančního produktu nebo přímo krádež peněz za pomocí zneužití platební karty. V dnešní době lidé využívají k platbě mobilní telefon, ve kterém mohou mít „svou platební kartu“ a právě toho mohou útočníci využít k obohacení. Újma však nemusí být pouze na majetku nebo financích, ale častokrát se stává, že dochází ke zneužití dobrého jména nebo také využívání osobních fotografií k nelegální činnosti.

3.1 Klasifikace hrozeb

“Hrozba představuje skutečnost (jev se škodícím účinkem), který se svým působením projevuje na určitém celku negativně. Může mu v případě expozice způsobit újmu nebo na něj mít negativní dopad. Jedná se o škodící účinek (působení), které má materiální nebo nemateriální povahu“ [1, str. 24].

Podle výše zmíněné citace, která je definicí hrozby, je možné zařadit hrozby do dvou kategorií, podle toho na jaké aktivum hrozba působí. Existuje tedy buď materiální působení, nebo nemateriální působení.

Materiální působení

Materiálním působením je myšleno, že hrozba může způsobit újmu na materiálních statcích daného referenčního objektu. V našem případě se jedná o osoby nebo jedince, proto je nejčastější hrozbou například krádež. Myšleno krádež peněženky nebo notebooku, který byl například uložený v autě. Popřípadě může jít i o fyzické napadení, ať už má jakýkoliv podtext. Materiální působení může mít tedy fyzikální nebo chemickou povahu [1].

Nemateriální působení

Nemateriální působení má z pravidla informační a logickou povahu. Jedná se o druh činnosti spojený s krádeží identity, dat a informací, které mají dopad na život člověka po stránce finanční a psychické [1].

Hrozby můžeme dále rozdělit podle formy provedení, kterou útočník využije. Jde tedy buď o fyzický kontakt, nebo se může jednat o logickou cestu.

Fyzická hrozba

V tomto případě se jedná o fyzický střet s pachatelem, kdy může dojít k narušení soukromí ve formě ublížení na zdraví, krádeži předmětů nebo peněz, popřípadě k sexuálně motivovanému útoku.

Logická hrozba

Jedná se o hrozbu, u které nedochází k fyzickému střetu, ale naopak je útok vytvářen psychickým nátlakem, vydíráním nebo krádeží peněz či identity a to převážně za použití internetu nebo jiného technického vybavení, kterými může být také fotoaparát nebo mobilní telefon.

3.2 Posouzení hrozeb

V této části práce se budeme zabývat tím, jaké konkrétní hrozby mohou ohrožovat soukromí. Dojde také na diskuzi o některých reálných příkladech z praxe. Pro pozdější analýzu je nutné hrozby specifikovat, uvést v jaké formě se vyskytují a jakým způsobem mohou člověka napadnout. Nejprve budou zmíněny fyzické hrozby a další část bude věnovaná hrozbám logickým.

3.2.1 Fyzické hrozby

Jak již bylo zmíněno, jedná se o hrozbu, při které dochází ke kontaktu s pachatelem a může vést k narušení soukromí ve formě krádeže, tedy odcizení předmětů, popřípadě dokladů. Další újmou může být také ohrožení zdraví, násilí se sexuálním podtextem nebo může jít i o formu násilí vedoucí k ponížení druhé osoby.

Jedná se především o fyzické hrozby:

- krádež cenností, mobilního telefonu nebo notebooku,

- krádež osobních dokladů,
- vyloupení domu/bytu.

Krádež cenností, mobilního telefonu nebo notebooku

Vyústěním fyzického napadení může být krádež. Ke krádeži nemusí vést cesta pouze přes fyzické napadení, ale může jít také o krádež, které si okradený všimne až už je pozdě, tedy kdy nemá přehled o tom, kdo jej mohl okrást. Pachatelem takové činu je nejčastěji cizí osoba, ale bohužel není vyloučeno, že může jít o osobu blízkou. Riziko se samozřejmě zvyšuje, pokud jedinec nemá své věci pod kontrolou a nechává je bez dozoru. Krádeže typu kapsářství se odehrávají prakticky všude, ale nejčastěji jsou prováděny v nákupních centrech, kde je více lidí a vznikají zde méně přehledné situace.

Příkladem krádeže může být případ ze začátku října roku 2020, který se odehrál na území Olomouckého kraje. Starší paní si v jednom ze supermarketu nechala ve vozíku batoh, který jí byl v nestřežené chvíli odcizen. Spolu s peněženkou, ve které měla hotovost, jí byl zcizen také mobilní telefon a další cenné předměty [25].

V případech krádeže peněz a cenností dochází k újmě na financích, popřípadě jsou spolu s peněženkou odcizeny také doklady a kreditní karta, která může později vést ke zneužití osobních údajů.

Dalším příkladem je případ z poloviny října roku 2020, který se stal na území Olomouckého kraje. Muž zde nalezl volně ležící mobilní telefon a platební kartu. S touto kartou později několikrát zaplatil a pomocí mobilního telefonu dobil kredit na několik telefonních čísel, což nakonec znamenalo škodu ve výši 29 000Kč [26].

Ke krádeži mobilního telefonu může docházet při chvilce nepozornosti, například když telefon zůstane položený na stole v restauraci. Nezřídka se stává, že je mobilní telefon ukraden také z automobilu, kde byl dříve majitelem zanechán. V těchto případech může jít o krádež fotografií, ale především se může pachatel přiblížit soukromí vlastníka. Může zjistit, kde oběť pracuje, kde bydlí a kdo je dalším členem rodiny. Tento typ narušení soukromí je velmi podobný vzdálenému přístupu do zmíněných zařízení. S tím rozdílem, že vzdáleně nakládá s informacemi a v druhém případě pachatel vlastní také fyzickou podobu přístroje, kterou je možné zpeněžit.

Krádež notebooku bývá také často spojena s vykradením automobilu. V poslední době se často objevují případy, kdy lidé nechávají ve svých automobilech cennosti, ale také již zmíněné peněženky s osobními doklady. Tím se samozřejmě zvyšuje riziko krádeže, rozbitých oken v autech je nespočet a tím častěji, čím je místo zaparkovaného automobilu opuštěnější nebo odlehlejší. Není však výjimkou, že se pachatel odváží také na automobil v obsazeném podzemním parkovišti.

Krádež osobních dokladů

Jednou z nejnepříjemnějších záležitostí je krádež dokladů. Dochází k ní podobně jako k předchozí krádeže mobilního telefonu, ale újma může být velmi značná a to především z pohledu financí. Nejčastěji se osobní doklady zneužívají ke sjednávání úvěrů, ale také menších půjček ve formě například půjčky na elektrospotřebiče. Známé jsou také případy, kdy pachatelé zneužili osobních dokladů za účelem falšování pokut. Nejčastěji se jednalo o pokuty za dopravní přestupky.

Bohužel dochází k těmto činům nejen náhodně, ale také cíleně a to například i v rámci blízkých přátel. V dřívějších letech byly například půjčky na elektrospotřebiče velmi dostupné, bylo potřebné předložit dva doklady a mít stálý příjem. Půjčka byla častokrát schválena i například invalidnímu důchodci. V okamžiku, kdy byla půjčka schválená, odcházel zákazník s vybraným výrobkem. Jenže v některých případech se stávalo, že na zákazníka čekal někdo, kdo mu přístroj odebral, později prodal a dotyčnému zákazníkovi tak zbyl pouze dluh. Prakticky se tedy jednalo o zneužití osoby, která těmito doklady disponovala.

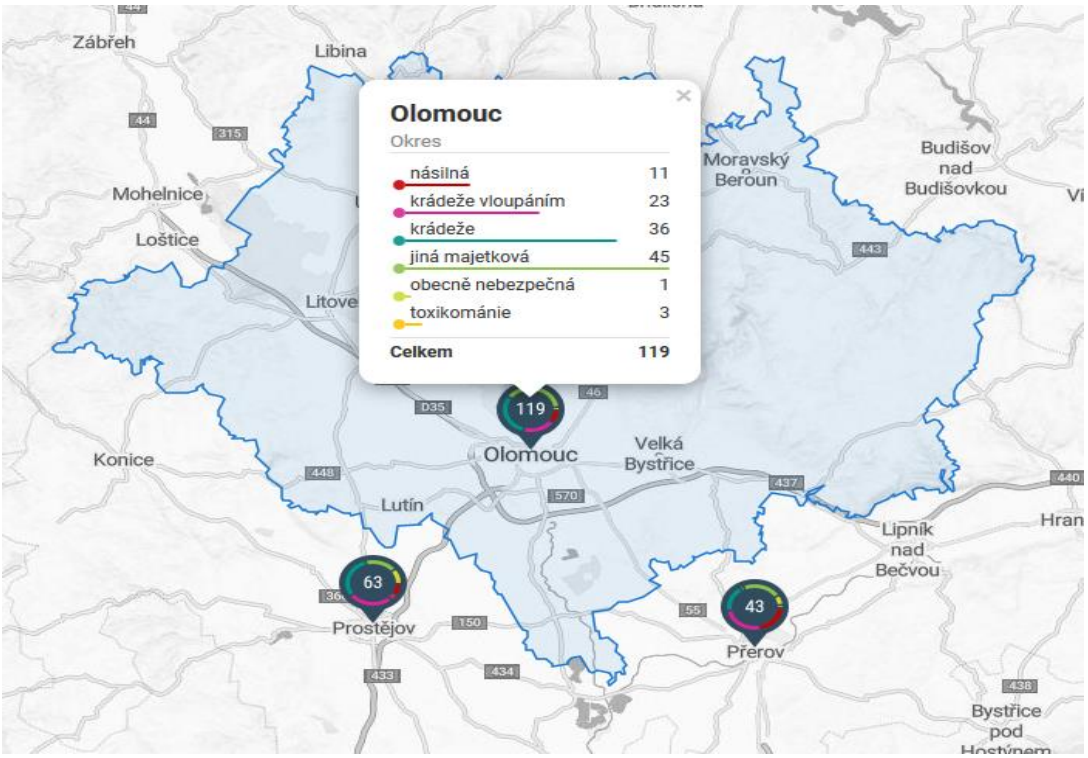
Vyloupení domu/bytu

Předchozí případy se zabývaly především útoky na osobu nebo případy, kdy hrozilo zcizení věcí. V tomto případě se však bude jednat o zcela jiný druh hrozby. Fyzicky prakticky nemusí být pachatel s obětí v kontaktu, ale jelikož se v místě, kde oběť žije, nachází nejvíce osobních věcí, je nutné tuto hrozbu určitě zmínit. Nejčastěji dochází ke krádeži úmyslně a pachatelem může být člověk z blízkého okolí, ale častěji jde o neznámého pachatele, který však může být informovaný o místě bydliště oběti, může znát i prostor bytu či domu například z fotografií, které někdo sdílel na internetu.

Dochází zde k největší újmě na majetku, protože se v místě bydliště většinou nachází mnoho předmětů, cenností a peněz, ale zároveň zde může být také nashromážděno nejvíce

osobních informací. Osobní dokumenty, cenné papíry, informace o dalších nemovitostech, které oběť vlastní. Při vyloupení domu se bohužel často stává, že pachatel narazí na majitele a v takových případech může dojít také k újmě na zdraví.

Na obrázku č. 2 je možné vidět různé druhy kriminální činnosti, která se páchala na území okresu Olomouc v měsíci listopadu roku 2020. Nejčastěji se zde, vyskytovaly krádeže a jiná majetková kriminalita - tyto dvě skupiny byly zastoupeny v téměř 70 % případů. Bohužel zde však byly zastoupeny také případy zneužití informací, resp. osobních údajů.



Obr. 2: Kriminalita v Olomouci [27]

3.2.2 Logické hrozby

Mezi logické hrozby řádíme útoky, při kterých nedošlo k fyzickému kontaktu, ale mohou poškozenému způsobit újmu. Nejčastěji se jedná o krádež financí, ale může jít také o zneužití osobních údajů nebo případně poškození důstojnosti dané osoby.

Měkkými místy těchto hrozeb jsou především slabá hesla, která lidé využívají. Tedy krátká hesla, nebo běžně používané kódy, které jsou snadno zapamatovatelné. Zároveň neměnnost hesel a jejich časté opakování na různých webových portálech vedou ke zvýšení pravděpodobnosti napadení. Dalším problémem je také důvěřivost lidí, především starších

lidí, ale také naivita některých mladých lidí, kteří zatím neměli možnost získat zkušenosti s podvody na internetu.

Jedná se především o tyto logické hrozby:

- phishing,
- hacking,
- kyberstalking,
- vydírání,
- krádež identity.

Phishing

Phishing je forma útoku, kdy se útočník vydává za důvěryhodnou autoritu s cílem získat citlivá data. Průběh je většinou takový, že oběti přijde e-mail, který se tváří jako velmi závažný nebo lákavý, ale zpravidla je psaný velmi zkomoleně. Většinou je obsahem také žádost o zaslání hesla k bankovnictví nebo údajů o platební kartě [18].

Pokud však dojde k zadání těchto údajů, dochází buď k odcizení financí z účtu, nebo zneužití dat, které byly danému pachateli zaslány. Dále je nutné zmínit, že dochází také ke kombinaci phishingu s dalším škodlivým softwarem a průběh může být také takový, že při přijetí zprávy stačí pouze kliknout na odkaz nebo přílohu e-mailu, tím se stáhne škodlivý software, který potřebná data získá [18].

Je nutné zmínit, že se jedná o předem připravenou formu hrozby, kterou může v dnešní době zneužít prakticky každý s přístupem k internetu. Zároveň se nezřídka stává, že pachatel oběť vydírá výměnou za zcizená data.

Průzkum dokonce v České republice ukázal, že se zhruba čtvrtina obyvatel s phishingem již setkala. U třetiny se tak stalo pomocí e-mailu a druhá třetina byla kontaktována pomocí SMS zprávy. V 74 % však pokus o útok nikdo neoznámil a v 62 % došlo k úniku osobních dat [28].

Hacking

Hacking je způsob jak získat neoprávněným způsobem přístup do počítače. Jedná se o techniku, kdy hacker překonává zabezpečení počítačového systému za pomocí skriptů

nebo programů, které ovlivňují přenášená data. Přístroje jsou většinou napadány pomocí virů nebo červů [29; 30].

Tato technika má velmi podobné dopady jako phishing, jediný rozdíl je však v přístupu k osobním nebo jiným údajům v daném zařízení. Jak již z postupu hackingu vyplývá, je k takovému útoku nutná příprava.

Stalking

Stalking je označení pro sledování oběti. Jedná se o techniku, při které pachatel sleduje svou oběť. Může ji sledovat pomocí fotek na sociálních sítích, kde většina lidí sdílí také svou polohu a díky tomu může pachatel později sledovat dotyčnou osobu také osobně. Pokud jde o sledování na sítích čili kyberprostoru, můžeme o něm hovořit také jako o **kyberstalkingu**.

Tuto činnost může provádět osoba, se kterou se potenciální oběť nikdy nesetkala. Může se však jednat i o nějakého přítele z minulosti nebo dokonce bývalého partnera. Vždy jde o dlouhodobější záležitost, při které pachatele shromažďuje informace o místech, kde se osoba pohybuje, ale může také pořizovat fotografie.

Dopadem stalkingu bývá nejčastěji fyzická konfrontace, ale může dojít také k psychické frustraci z nedostatku soukromí. Zřídka se stává, že je tento čin motivován financemi.

Vydírání

Vydírání může být způsobeno prakticky všemi logickými hrozbami, které byly uvedeny. Může dojít k odcizení citlivých dat z počítače, může se jednat o špatně ukryté fotky na sdíleném disku. Velmi často se stává, že jsou osoby vydírány právě i v případě stalkingu.

Pokud někdo odcizí osobní data, tak nejčastěji požaduje za jejich navrácení finanční odměnu. Stejné je to i v případě soukromých fotografií. Ale například u stalkingu pro pachatele většinou nejsou důležité peníze. Dochází tedy například k požadování intimních fotek, vyhrožování s uveřejněním soukromích informací. Ve všech případech je oběť velmi psychicky ponižována a v některých případech může docházet i k sebevraždám.

Krádež identity

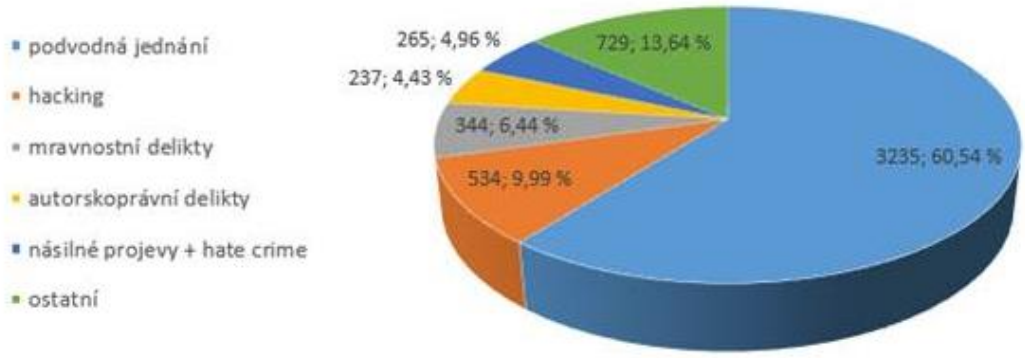
Na sociálních sítích často dochází ke krádežím jednotlivých profilů a poté jsou získávána data o přátelích a rodině. Pokud se totiž pachatel za oběť vydává, získá tak potřebné

informace velmi snadno. Samozřejmě je možné tímto způsobem také požadovat od blízkých osob nebo rodiny této osoby peníze.

Podobně se vkrádají pachatelé do soukromí také tím, že celý profil napodobují, tedy kopírují fotografie a osobní údaje. Tato technika má podobné dopady, ale s menší odezvou. Nejčastěji se tedy pachatel pokouší o obohacení nebo diskreditaci oběti.

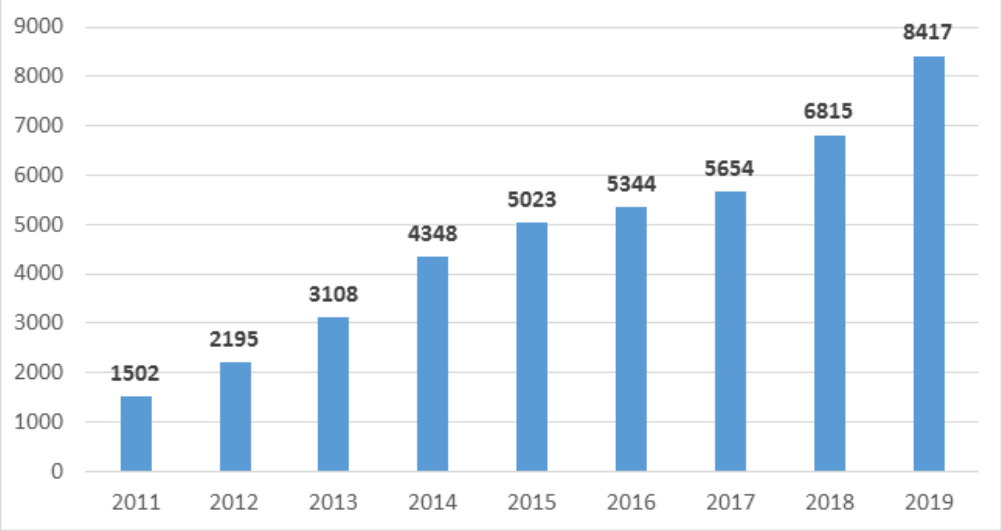
Možným příkladem může být případ, který se stal na začátku září roku 2020 na území Olomouckého kraje. Muž se zde prostřednictvím sociálních sítí vydával za společníka, který oslovil starší paní. Později došlo k bližšímu spojení a muž tvrdil, že ženě zaslal ze zahraničí šperky v hodnotě několika milionu Kč, ale že zůstaly na celnici a proto je nutné zaslat nějaký obnos, aby se celá zásilka uvolnila. Tímto způsobem získal muž od oběti 1,2 milionu Kč [31].

Obrázek č. 3 zachycuje jednotlivé druhy kyberkriminality a jejich vazby. Pod pojmem podvodná jednání je zařazen již zmíněný phishing. Do struktury násilné projevy a hatecrime patří vydírání, pronásledování a extremistické projevy.



Obr. 3: Struktura kyberkriminality za rok 2016 [30]

Z obrázku č. 3 je evidentní, že největší zastoupení s 60 % mají na poli kyberkriminality skutečně podvodná jednání, tedy například phishing, ale také hacking s 10 % není úplně neobvyklý. Obrázek č. 4 zaznamenává počet napadení v oblasti kyberkriminality v období let 2011-2019.



Obr. 4: Počet napadení na internetu v letech 2011-2019 [30]

Na vertikální ose grafu je uveden počet obětí a na horizontální ose grafu je vyobrazen rok, ve kterém se trestná činnost v oblasti kyberkriminality zkoumala. Mezi lety 2011-2013 byl nárůst více než dvojnásobný a mezi lety 2013-2019 skoro trojnásobný. Samozřejmě je nutné počítat s tím, že existuje přímá úměra mezi počtem napadení a zvyšujícím se využitím moderních technologií.

3.3 Analýza rizik

Analýza rizik je proces, ve kterém budeme identifikovat hrozby a určovat jejich nebezpečnost. Dále nás bude zajímat, jak již z názvu vyplývá, jaké je riziko výskytu takovéto hrozby. Je nutné tedy identifikovat aktivum. Dále stanovit význam aktiva a tím tedy stanovit dopady případné ztráty, či poškození. V této části bude nutné stanovit druhy událostí, které mohou negativně ovlivnit hodnotu aktiv a umožňují tak působení hrozeb. V neposlední řadě je nutné určit pravděpodobnost výskytu hrozeb a míru zranitelnosti vůči dané hrozbě [32].

Aktivem je v našem případě identita (například na sociálních sítích), osobní údaje, fotografie, poloha nebo také dokumenty, obsahující osobní údaje a cenné informace. Pokud bychom měli tato aktiva nějak ohodnotit, tak by to bylo bodovým hodnocením, konkrétně od 1 do 5 bodů. Bodové hodnocení je velmi snadným, ale přesto účinným prostředkem ke zhodnocení a proto jej také zvolíme.

Riziko lze chápat jako možnou újmu a výpočet je:

$$R = P * D \quad (1)$$

kde R je riziko, P je pravděnepodobnost expozice a D je újma (velikost dopadu).

Každé aktivum by tedy mělo mít hodnocení pravděpodobnosti expozice a velikosti dopadu. Tabulka č. 1 zobrazuje škálu hodnocení velikosti újmy (negativního dopadu) a jejich popis.

Tab. 1: Škála hodnocení velikosti újmy (negativního dopadu) [vlastní zdroj]

Body	Velikost újmy	Popis dopadu
5	Krizové	Zásadně ohrožuje danou osobu na majetku a zdraví
4	Významné	Postihuje výrazně danou osobu, ale nejedná se o ohrožení zdraví
3	Střední	Může ovlivnit soukromí dané osoby, ale pouze s minimálním dopadem
2	Nevýznamné	Může ovlivnit soukromí dané osoby, ale se zanedbatelným dopadem
1	Zanedbatelné	Prakticky se jedná o běžnou situaci, která nemusí znamenat újmu

Tabulka č. 2 zobrazuje pravděpodobnost expozice jednotlivých hrozeb.

Tab. 2: Škála pravděpodobnosti expozice [vlastní zdroj]

Body	Pravděpodobnost	Popis výskytu
5	Jisté	Událost se téměř vždy vyskytne nebo s pravděpodobností 90%
4	Pravděpodobné	Událost se pravděpodobně vyskytne
3	Možné	Událost se může vyskytnout (např. za vhodných podmínek)
2	Nepravděpodobné	Událost se může vyskytnout, ale je to nepravděpodobné
1	Téměř žádné	Událost se vyskytne ve výjimečných případech

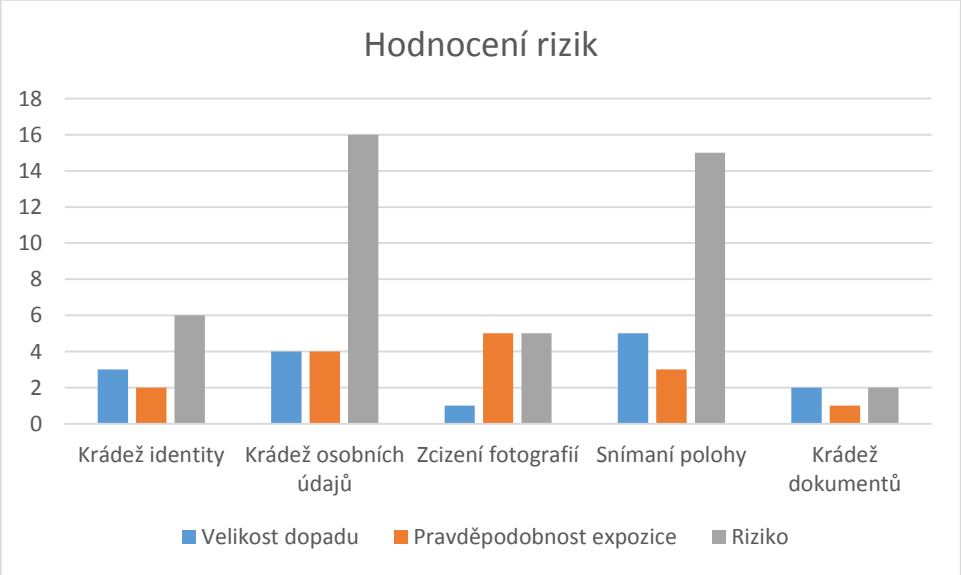
Krádež identity - 3 body za velikost dopadu, protože zpravidla dochází pouze k finanční ztrátě, ale pravděpodobnost je velmi malá díky zabezpečení heslem a z pravidla také ještě ověřením telefonního čísla, tzv. dvojí ověření, proto 2 body za pravděpodobnost expozice.

Krádež osobních údajů - 4 body za velikost dopadu, protože může dojít k velké finanční ztrátě a problémům v soukromí a zároveň 4 body za pravděpodobnost expozice, protože z uvedených je nejsnadnější někomu ukrást například doklady.

Zcizení fotografií -1 bod za velikost dopadu a zároveň 5 bodů za pravděpodobnost expozice, protože většina lidí má fotky veřejně dostupné a každý k nim má přístup, občas někdo fotky zneužije, ale dopad je z pravidla zanedbatelný.

Snímaní polohy - 5 bodů za velikost dopadu, protože je pro nás prioritní zdraví a například při stalkingu může dojít k újmě na zdraví, zároveň 3 body za pravděpodobnost expozice, protože je v dnešní době snadné zjistit ze sociálních sítí, například kde dotyčná osoba tráví dovolenou nebo, kam pravidelně chodí za zábavou či sportem.

Krádež dokumentů - 2 body za velikost dopadu, protože se opět jedná o finanční ztrátu a zároveň 1 bod za pravděpodobnost expozice, protože je hacking a vloupání do domu nejsložitějším úkonem.



Graf 1: Analýza rizik pomocí bodového systému [vlastní zdroj]

Graf č. 1 ukazuje rizika pro jednotlivá aktiva. Je zde vidět sloupec s velikostí dopadu, tak jak byla aktiva uvedena. Druhý sloupec poukazuje na pravděpodobnost expozice. Poslední sloupec je sloupec rizika a je součinem velikosti dopadu a pravděpodobnosti expozice, podle postupu ze vzorce č. 1. Je zde tedy vidět, že nejrizikovější je krádež osobních údajů s 16 body z celkových 25 bodů, dále snímání polohy s 15 body, poté je vidět pokles na 6 bodů rizika krádeže identity, 5 bodů pro zcizení fotografií a nejméně riziková je krádež dokumentů se 2 body. Tabulka č. 3 osvětlí, jaké hrozby mohou ohrožovat výše zmíněná

aktiva. Jaké újmy mohou hrozby svým působením způsobit a v závěru, jaké opatření může pomoci riziko snížit.

Tab. 3: Hrozby, rizika, újmy a opatření soukromí [vlastní zdroj]

	Název	**Podstata**
Hrozby	Krádež cenností/mobilu/notebooku	Útok za účelem obohacení, popřípadě získání soukromých fotografií, osobních údajů.
	Krádež osobních dokladů	Získání osobních dokladů za účelem zneužití k obohacení nebo vydírání.
	Vyloupení domu/bytu	Útok za účelem obohacení, tj. zcizení hmotných i nehmotných statků a jejich zpeněžení, popřípadě zneužití.
	Phishing	Finanční ztráta, ale také ztráta soukromí s případným vydíráním.
	Hacking	Finanční ztráta, ale také ztráta soukromí s případným vydíráním.
	Stalking	Ohrožení soukromí s účelem získání informací o dotyčné osobě vedoucí k vydírání.
	Vydírání	Vyhrožování zveřejněním fotografií nebo údajů vedoucí k obohacení a ztrátě důstojnosti poškozené osoby.
	Krádež identity	Získání osobních dat a jejich následné zneužití k obohacení nebo získání informací o soukromí dalších osob.
Újmy	Ohrožení zdraví	Ublížení na zdraví, zmrzačení nebo smrt.
	Majetková ztráta	Ztráta materiálního a finančního vlastnictví.
	Omezení pohybu	Ztráta možnosti volného pohybu vyvolaná sledováním.
	Poškození zdraví a snížení	Psychické zatížení vlivem nátlaku a

	kvality života	vydírání.
	Snížení kvality života blízkých	Komplikace spojené se zásahem do soukromí vlivem zneužití sociálních sítí.
	Omezení lidských práv a svobod	Omezení domovní svobody, pohybu a ochrany před násilím.
	Veřejné poškození osoby	Zveřejnění choulostivých fotografií.
Opatření	Vzdělání v IT bezpečnosti	Vzdělání v IT pomocí kurzů nebo školení.
	Zabezpečení majetku	Prostorová, obvodová, plášťová a předmětová ochrana. PZTS nebo kamerový systém.
	Zabezpečení zařízení (kybernetická bezpečnost)	Instalace firewallu, zabezpečení internetových prohlížečů, zabezpečení silným heslem a především informovanost o dané problematice.
	Kontrola sdílených informací	Sdílet co nejméně osobních údajů na internetu, v ideálně případě žádné a kontrolovat, kdo k nim má přístup.

3.4 Trendy vývoje hrozeb

Na základě informací, které byly zmíněny v této kapitole, je možné říci, že hrozby ohrožující soukromí se budou dále rozvíjet a měnit. Především v oblasti informačních technologií, kde jak jsme podle obrázku č. 4 znázorňujícím výskyt napadení mohli vidět, bude útoků přibývat a zřejmě budou čím dál více propracovanější a sofistikovanější.

Je možné předpokládat, že co se týče fyzických hrozeb, nebude vývoj nijak strmě stoupat. Kapsářství zůstane zřejmě na stejné úrovni, možná s poklesem příchozích turistů vlivem pandemie jich naopak ubude. Ochrana domů a aut je stále cenově dostupnější a proto by se mohl odbyt výrobků spojených s jejich ochranou zvýšit. V poslední době je možné zpozorovat například častější výskyt kamer v automobilech. Tento trend brzy dozná i prodej zabezpečovacích zařízení, především kamer, které se používají k ochraně domu. Dále se čím dál častěji začíná používat pojem „smarthome“ nebo „smartliving“, tedy chytré bydlení. Do tohoto konceptu zapadá ovládání spotřebičů bezdrátově a k tomu se právě pojí také ochrana, kamerové systémy a zabezpečení domů či bytů.

Společnost Kasperky provedla v roce 2020 průzkum v oblasti internetového bankovnictví a předpokládá, že bude útoků na bankovní instituce přibývat. Také tvrdí, že krádeže platebních údajů a karet bude více sofistikované. Tento styl útoků bude vést k častějšímu okrádání, ale také může být díky tomu na vzestupu vydírání a stalking. Společnost Kaspersky také tvrdí, že budou stále častější krádeže bitcoinu. Důvodem může být především to, že vlivem pandemie, bude klesat důvěra lidí ve státy a tedy také tuzemskou měnu. Vlivem toho se budou lidé obracet spíše k měně alternativní, což může být například bitcoin nebo jiný druh coinu [33].

Dalším trendem, který je na vzestupu, je samozřejmě seznamování přes internet a s tím je také spojeno ohrožení ve smyslu sdílení osobních údajů neznámým osobám. Sociální sítě se zároveň stávají místem, kde se stále častěji propagují různé výrobky a tím se stává novým trhem pro nabídku, ale také poptávku. Shlukuje se tím na těchto sociálních sítích čím dál více lidí a tím tyto sítě získávají větší moc ovládat masy. Ten, kdo dnes není na sociálních sítích, může mít pocit omezení v určitých oblastech života. Tato skutečnost samozřejmě závisí na věku daného člověka. Nejvíce to postihuje mladší lidi do třiceti let věku a děti. Na druhou stranu se i starší lidé mohou cítit sociálně vyloučení, když se někdo baví o nějakém výrobku nebo službě, které se prezentuje právě pouze na sociálních sítích.

4 ZPŮSOBY OCHRANY SOUKROMÍ

V této kapitole budou popsány způsoby ochrany soukromí, jejich rozdělení a konkrétní postupy jejich realizace. Ochrana soukromí je zásadním pilířem lidských životů a proto je nutné k této tématice sdělit některé podrobnosti. Ochrana soukromí je také důležitá, protože při jejím narušení může docházet ke ztrátě identity, financí a dalších cenností, které mohou mít pro mnohé hluboký význam. Narušením se může útočník dostat k důležitým informacím a využít je tak proti oběti.

4.1 Varianty a modely ochrany soukromí

V této kapitole o způsobech ochrany soukromí budou zmíněny varianty, jakými lze soukromí chránit, a budou popsána konkrétní preventivní opatření. Pro lepší přehlednost o využitelnosti budou preventivní opatření zhodnocena. Způsoby ochrany soukromí je možné pro lepší orientaci rozdělit na ochranu fyzickou cestou a kybernetickou cestou.

Ochrana soukromí fyzickou cestou

Pod fyzickou cestou ochrany soukromí je možné si představit především zamezení přístupu k jednotlivým zařízením, popřípadě omezení ve formě dohledu nad užíváním. Dalším způsobem je také zamezení přístupu k cenným dokladům či informacím.

Fyzický způsob ochrany se bude lišit podle toho, zda se jedná o ochranu zařízení, které se nachází v domácnosti nebo které je využito také například v pracovním prostředí. Nicméně je nutné, aby bylo zařízení vždy uzamčené tak, aby nebylo možné s ním libovolně manipulovat. Toto se týká především mobilních telefonů a notebooků. Zařízení je nutné mít neustále pod dohledem, čemuž je možné napomoci, pokud jej uživatel nosí s sebou a nenechává je bez dozoru.

Podobný postup se týká také důležitých dokumentů popřípadě dokladů. Doklady je nutné nosit stále u sebe a mít je pod dohledem. Pokud tak není možné učinit, je potřeba zajistit jejich bezpečné uložení. V domácím prostředí se může jednat o uzamykatelné skříňky nebo trezory a v pracovním prostředí o uzamykatelnou skříňku nebo uzamčení celé kanceláře. Především v domácím prostředí bychom měli zajistit ochranu proti vstupu do obydlí, tzn. bezpečnostní dveře a perimetrickou ochranu ve formě plotu.

Ochrana soukromí logickou cestou

Logický způsob ochrany soukromí spočívá především v ochraně v okamžiku, kdy může mít podezřelá osoba přístup k elektronickým zařízením, popřípadě dokladům - v tomto případě například platební kartě. Pokud není možné zamezit fyzickému přístupu k zařízení, což se stává zcela běžně, je nutné zamezit alespoň přístupu k informacím a to především zabezpečením zařízení pomocí hesla nebo jiného autorizačního procesu.

V dnešní době jsou mobilní zařízení zajišťována také biometrickou identifikací nebo tzv. gestem, což je nákres symbolu z pravidla na devíti-místné šachovnici, který si uživatel může zvolit. Dalším běžným způsobem zabezpečení je otisk prstu, který se využívá jak u notebooků, tak u mobilních telefonů. V neposlední řadě je možné využít sken oční duhovky nebo obličeje, pokud to mobilní telefon nebo vybrané zařízení umožňuje.

Předchozí způsob kybernetické ochrany se týká přístupu do zařízení, ale pokud je nutné, aby se zařízením pracovaly další osoby nebo, aby bylo uchráněno soukromí, při užívání je nutné využívat antivirovou ochranu, kontrolovat pohyb na internetu a sdílení informací. Postupy a realizace k minimalizaci rizik budou popsány dále v této kapitole.

Modely k zajištění ochrany soukromí

1. **Režimový model**

Do režimového modelu ochrany soukromí patří především dodržování pravidel a jakýsi řád činností, které by měly vést ke snížení škodícího účinku. V ideálním případě budit dojem neproniknutelnosti a tím zamezení incidentu. Příkladem režimového opatření může být namátková kontrola pohybu osob v blízkosti objektu a především přizpůsobení objektu vůči danému umístění [1].

Režimový model využijeme i při ochraně logickou cestou a to například tak, že budeme v pravidelných intervalech měnit svá hesla u účtů. Dále je možné kontrolovat zařízení, která se k účtu přihlašují. Díky dodržování pravidel, lze docílit větší bezpečnosti.

2. **Bariérový model**

Bariérový model je nejběžněji používaný model k zajištění bezpečnosti. Spočívá především v zachování trvalé ochrany objektu, k čemuž přispívá vytvoření bariér. Obecně lze říct, že se jedná o opatření, která mají fyzický nebo logický charakter zabraňující negativní interakci.

Konkrétně se může jednat například o oplocení, tedy o perimetrickou ochranu, která však filtruje a propouští na základě kritérií, takže například videotelefon přes který je nutné se identifikovat, kvůli vstupu do objektu. Tyto příklady bariérových modelů jsou využívány spíše pro ochranu fyzickou cestou [1].

Pro ochranu logickou cestou můžeme za bariérový model označit například firewall v používaný v počítačích nebo také antivirovou ochranu. Zkrátka vše, co může vést k trvalé ochraně.

3. Model participace

U modelu participace jde o spojení určité skupiny lidí za účelem dosažení cíle, v našem případě ochrany soukromí. Jinými slovy se nejčastěji stává, že se lidé se zájmem ochránit své obydlí spojí, aby jej společně bránili. Jedná se o formu tzv. domobrany, kdy skupiny lidí vytváří hlídky a kontrolují své ulice, popřípadě čtvrti za účelem zamezení újmy. Příkladem může být domobrana z části Prahy, kde v letech 2019-2020 docházelo k častým vloupáním do rodinných domů [1].

4. Proaktivní model

Jelikož tato práce pojednává o preventivních opatřeních, nesmíme zapomenout na proaktivní model, který myslí na budoucnost a snaží se předvídat, jaké události by mohly přijít. Snaží se předejít negativním dopadům [1].

Jde především o vyhledávání nežádoucích stavů a návrh řešení, která mají těmto stavům zabránit. Může jít o vytváření podmínek – pokud bude například u domu vysoký plot s ostnatým drátem a kamerovým systémem, je riziko napadení nižší než bez těchto věcí. Pokud bude mít uživatel velmi silné heslo a bude se přihlašovat stále pouze z jednoho zařízení, ke kterému nikdo další nemá přístup, je riziko napadení opět nižší.

Právní ochrana obyvatel

Ochranu soukromí legislativně vymezují v České republice především zákony. Právní ochrana je sepsána především v:

- občanském zákoníku,
- základní listině práv a svobod,
- trestním zákoníku.

Jakým způsobem a na co konkrétně se výše zmíněné zákony zaměřují, bylo popsáno především ve druhé kapitole této práce. Důležité je, že v případě problémů, například stalkování na internetu nebo sdílení osobních fotografií bez souhlasu vlastníka je možné řešit právní cestou. Samozřejmě tím není možné vzít situaci zpět, ale je možné získat alespoň například očištění dobrého jména nebo částečnou finanční kompenzaci.

GDPR (General Data Protection Regulation)

Ochrana soukromí je zajištěna také pomocí GDPR, která chrání před zneužitím především osobní údaje. Jedná se o legislativu, která platí v rámci Evropské unie, takže její využití je vskutku široké. Tuto směrnici lze využít jak v kybernetickém, tak i fyzickém prostoru. Je nutné vnímat, že pro ochranu soukromí se snaží stát potažmo Evropská unie dělat maximum.

4.2 Typy opatření, jejich realizace a zhodnocení

Pro účinnou ochranu soukromí je nutné navrhnout preventivní opatření, která by zamezila jednotlivým hrozbám. V této části budou navrhována preventivní opatření, jejich realizace a v poslední části budou pomocí párového srovnání preventivní opatření zhodnocena.

Jelikož se v diplomové práci zabýváme prevencí v ochraně soukromí, budeme se zaměřovat na preventivní opatření, tedy předcházení jednotlivým hrozbám.

4.2.1 Typy preventivních opatření a jejich realizace

Typy preventivních opatření můžeme rozdělit na technické a organizační. Po určení jednotlivých typů budeme popisovat konkrétní zavedení a jejich důvody.

Organizační opatření:

- vzdělání v sebeobraně,
- vzdělání v oblasti IT bezpečnosti,
- umístění obydlí,
- přístup do objektu,
- kontrola smluvních podmínek,
- kontrola osobních dokladů a předmětů,
- regulace chování na sociálních sítích.

Vzdělání v sebeobraně

Vzdělání v sebeobraně je zařazeno do opatření, protože hrozby vedoucí ke zcizení předmětů, ať už elektronických zařízení nebo dokladů mohou vést přes napadení. Napadení, tedy fyzickému útoku na osobu se předejít nedá, pokud si oběť útočník „vyhlédne“ pro případnou krádež, tak tomu není možné předejít, ale pro snížení rizika, je možné cvičit a vzdělávat se v sebeobraně, tímto se úspěšnost násilníka nebo zloděje výrazně sníží.

Vzdělání v oblasti IT bezpečnosti

Předejít problémům především s elektronickým zařízením lze vzděláváním v této oblasti. Možností vzdělávání je celá řada, ať už ve formě návštěvy přednášek, které o problematice zabezpečení elektronických zařízení hovoří nebo návštěvy kurzu, který uživatele na zprovoznění a práci se zařízením připraví, až po studium informatiky jako oboru na úrovni středoškolské nebo vysokoškolské.

Možností je poměrně mnoho a jedná se pouze o rozhodnutí jednotlivců, jaké úrovně informovanosti chtějí dosáhnout, ale zároveň samozřejmě záleží na vědomostech, časových možnostech a zkušenosti jakou s IT doposud mají.

Umístění obydlí

Důležitým aspektem je umístnění obydlí, které chceme chránit. Je velký rozdíl mezi rizikem, že se pachatel pokusí dostat do opuštěného rodinného domu na samotě, kde nejsou žádná další obydlí a v pokusu o vniknutí do bytu na frekventovaném sídlišti. Důležitým aspektem ochrany je tedy umístění.

Pokud jde o byt, je podstatnou věcí, v jakém patře se nachází. Nižší patra vybízejí k vnějšímu vniknutí a u vyšších pater se riziko snižuje. Důležité je také umístění samotného domu, tedy pokud jde o konec slepé ulice nebo o otevřený prostor s vhodným přístupem také pro příjezd vozidel. V neposlední řadě je důležité zabezpečení celého domu, tj. zabezpečení vstupních dveří a případně kamerový systém ve vstupní hale a společných prostorách. Posledním stupněm zabezpečení je samotné zajištění bytu odolnými vstupními dveřmi s bezpečnostní vložkou.

U domu jsou důležitým parametrem ochrany umístění domu, ve smyslu řádový dům nebo volně stojící. Zda se jedná o frekventovanou oblast a otázkou také je, jaký je k místu přístup například automobilem, ale také pěšky.

Přístup do objektu

V případě přístupu k objektu je nutné volit vhodné zabezpečení ve formě bran a branek, ideálně bez možnosti otevření pouhou klikou. Ideální je instalace koule pouze v kombinaci se zámkem na klíč. Dalším způsobem může být přístup na základě elektrického impulsu, přes vzdálené ovládání, ale až poté co je ověřena identita vstupující osoby. Nejvhodnější je použití videotelefonu, kde je možné vpouštěnou osobu nejen slyšet, ale také vidět.

Pokud by se pachatel dostal až na pozemek, je vhodné mít bezpečnostní dveře se speciální bezpečnostní vložkou pro klíče, aby se zamezilo snadnému vypáčení nebo otevření pomocí paklíče či šperháku.

Kontrola smluvních podmínek

Kontrola smluvních podmínek je opatřením, kterým lze zamezit úniku informací z elektronických zařízení. Postup je velmi jednoduchý a to při každé návštěvě stránek nebo registraci pečlivě prostudovat podmínky, za kterých je možné dále postupovat.

Častokrát se stává, že podmínky obsahují právě hrozby týkající se narušení soukromí a to ve formě sledování pohybu na stránkách. Dále sledování pohybu jednotlivých zařízení, aby cílené reklamy byly relevantní pro umístění sledované osoby.

Častým problémem smluvních podmínek a využívání souborů cookies je, že pokud nejsou odsouhlaseny, tak o souhlas při každé návštěvě dané stránky budou žádat o potvrzení tím způsobem, že se přes 75 % obrazovky objeví základní pravidla a požadavky. Uživatel nemůže na stránce dál pokračovat, tedy alespoň ne pohodlným způsobem, který by uživatel očekával.

Kontrola osobních dokladů a předmětů

Opatřením, které se může zdát zcela jednoznačné, je kontrola osobních dokladů a předmětů, ale není tomu tak vždy. Někteří nosí své peněženky a mobilní telefony v zadní kapse kalhot, ke které mohou mít kapsáři velmi snadný přístup. Nechávají své věci volně na stole v restauraci nebo na sedadlech aut, do kterých je vidět a dávají tak zlodějům záminku ke krádeži.

Jednoduchým pravidlem proto je, nenechávat své věci bez dozoru a na snadno dostupných místech. Ideálně je mít na bezpečném místě, kam se žádný zloděj nedostane. Mobilní telefon nosit v přední kapse nebo tam, kde se dá kapsa zapnout.

Regulace chování na sociálních sítích

Případ nadměrného sdílení informací, resp. vytváření digitálních stop je v rámci sociálních sítí nespočet. Lidé si vůbec neuvědomují, kolik toho vlastně sdílí se svými známými nebo dokonce zveřejňují k nahlédnutí naprosto cizím lidem. Je běžné sdílení obrázků z dovolených, fotek svých dětí nebo rodiny a sdílení polohy. Lidé se na sociálních sítích svěřují s tím, jaký styl hudby poslouchají, jaké filmy se jim líbí, ale už si neuvědomují, že se tak stávají snadným terčem marketingových kampaní nebo také snadným terčem pro útok zlodějů či násilníků. Nezřídka tak dochází ke krádeži identity.

Při každém sdílení informací, textu, fotografii nebo v nejhorším případě umístění, je nutné být velmi obezřetný. Je možné kontrolovat pro koho je příspěvek viditelný a většinou se jedná o celé skupiny. Proto je nutné pravidelně kontrolovat, kdo patří do jednotlivých skupin, kterým je umožněn přístup k informacím o naší osobě. Není také nutné přihlašovat se do všech skupin nebo sdělovat jakých sezení, přednášek a akcí se daná osoba bude účastnit.

Technická opatření:

- perimetrická ochrana,
- kontrola vyplňování osobních údajů,
- kontrola digitálních stop,
- zamezení sdílení přístupu k datům a účtům,
- identifikace a autentizace,
- blokování reklamního sledování a ukládání hesel,
- antispamová, antivirová a firewall,
- anonymní proxy servery.

Perimetrická ochrana

V tomto případě budeme hovořit o ochraně obydlí, do které budou zahrnuty jednotlivé ochranné vrstvy. První věc, kterou jako útočník můžeme zaznamenat, je oplocení. Poté obydlí mohou chránit také světla, dále se na místě může vyskytovat například pes bránící „své obydlí“ a v neposlední řadě kamerové systémy, popřípadě různé typy detektorů narušení.

Oplocení lze realizovat mnoha způsoby, Důležitým faktorem je provedení, výška nebo také druh. Ideálním způsobem je použití tenzometrického plotového systému, který

zaznamenává tlak na napínací dráty a tím může zachytit příchod útočníka. Tato varianta realizace je však nepravděpodobná a nákladná. Častěji se setkáme s klasickým pletivovým oplocením, popřípadě panelovým oplocením. U obou těchto případu, lze instalovat nad samotné oplocení ostnatý drát v jedné nebo více úrovních, popřípadě žiletkový drát. Žiletkový drát se sice častěji využívá ve věznicích, ale jeho použití je možné. V neposlední řadě je bezpečné také namísto drátěného typu oplocení postavit zeď, ideálně do výšky přesahující dosah člověka.

Další možností ochrany je instalace detektorů pohybu, například pomocí PIR detektoru, který je napojený k PZTS nebo alespoň k vnějšímu světlu. Po zaznamenání pohybu osob se světlo rozsvítí a tím může odradit případné útočníky. Je samozřejmě také možné nainstalovat pouze světla, která budou přes noc osvětlovat předem zvolená místa.

Důležitým faktorem při ochraně soukromí může být také to, zda má dotyčná domácnost psa, popřípadě jiné zvíře, které by mohlo budit dojem ochrany a respektu. U psa je samozřejmě důležitá jeho velikost, plemeno, ale také zda je cvičený k ochraně.

Vnější okruh chráněného objektu mohou také snímat kamery a působit tak jako odstrašení. Kamery mohou být umístěny z vnější strany oplocení, to se však používá spíše u komerčních objektů. Častěji jsou umístěny na samotné budově a snímají vstup a okolí budovy.

Kontrola vyplňování osobních údajů

Kontrola vyplňování osobních údajů je základní bod preventivní ochrany soukromí. Vždy když dochází k registraci nebo jsou zadávány osobní údaje, musí být ověřeno, že stránky nejsou nijak pochybné, že mají ideálně nějakou historii nebo jsou viditelné recenze, protože se může jednat i o prodejní stránky. Dále je nutné si prostudovat podmínky, za kterých osobní údaje uživatel sděluje a jak s nimi bude nakládáno.

Důležité je, že některé registrace a také uložení zadaných údajů lze zrušit. Mnohokrát se totiž stává, že například pokud daná osoba nakoupí zboží na webových stránkách, tak je povinná zadat svou e-mailovou adresu a další údaje. Po doručení zboží však neustále chodí z těchto stránek různé nabídky a akční slevy, tomuto jednání je možné zabránit. V mnoha případech je totiž možné odhlásit odběr a ideálně zažádat o vymazání osobních údajů.

Kontrola digitálních stop

Pohyb na internetu není zcela anonymní a každý příspěvek nebo prohlášení je velmi snadno dohledatelné. Kontrola digitálních stop spočívá v určitém maskování, mazání a skrývání svých počinů, které na internetu provádíme. Nejčastěji se jedná o sdílení různých informací na sociálních účtech a přihlašování k různým odběrům a stránkám. Dále se může jednat o příspěvky nebo komentáře na různých fórech [34].

Ochranou digitálních stop může být jednoduchá přezdívka ve fórech, kam uživatel píše tak, aby nikdo nevěděl, že jde o určitou konkrétní osobu nebo zamezení viditelnosti příspěvků lidem, kteří jsou cizí. Kroky po internetu mohou být ukládány do historie prohlížeče a především se mnoho webových stránek ptá, zda přijímáme a souhlasíme s použitím a uložením souborů cookies.

Soubory cookies se ukládají do počítače a při každé návštěvě takovéto stránky je může daná stránka využít. Jedná se především o informace týkající se pohybu na stránce a nejčastěji se využívají k cílené reklamě na základě „potřeb“ návštěvníka. Tyto soubory cookies a samotnou historii vyhledávání lze vymazat a pro ochranu soukromí je zcela nezbytné kroky na internetu kontrolovat a případné stopy mazat.

Zamezení sdílení přístupu k datům a účtům

Dalším způsobem, jak zamezit zneužití soukromí je nesdělovat své přihlašovací údaje třetí osobě. Toto pravidlo platí jak při přihlašování do jednotlivých aplikací nebo na stránky, či sociální sítě, tak při přihlášení do zařízení. Toto opatření se může jevit banálně, ale bývá často příčinou problémů.

Nejtěžšími případy jsou bohužel úniky citlivých dat z jednotlivých korporací, kdy je na vině sdělení přístupů svým kolegům, kteří je mohou zneužít. Častokrát však může jít o sledování komunikace partnera nebo dítěte.

Identifikace a autentizace

Důležitým aspektem při preventivní ochraně soukromí je to, aby se nikdo nedostal k účtům, na kterých uživatel působí, proto je nutné mít vysokou ochranu ve formě silného hesla. Aspekty, které rozhodují o síle, resp. náročnosti prolomení hesla jsou tyto:

- složení hesla,
- délka hesla,

- použití hesla,
- frekvence změny hesla.

Dále je dnes na většině účtů, ať už k e-mailům, sociálním sítím nebo jiným zavést tzv. dvojí ověření, což v praxi znamená, že pokud je heslo správně zadáno, je na mobilní telefon zaslán ještě ověřovací kód, kterým je nutné přihlášení potvrdit [1].

Blokování reklamního sledování a ukládání hesel

Soubory cookies byly již zmíněné u kontroly smluvních podmínek, ale jelikož je frekvence jejich využívání poměrně velká, je nutné na tuto problematiku poukázat znovu. Zapnutí souborů cookies je pouze na volbě jednotlivce, je však nutné si uvědomit, kdo s těmito daty pracuje a za jakými účely. Proto je důležité pečlivě zvažovat jejich schválení a nejlépe při každém uzavření prohlížeče nastavit jejich smazání.

Ukládání hesel je samostatná záležitost, která vede k přístupu neoprávněných osob do účtů. Pokud se uživatel na svém počítači někam přihlásí a uloží své přihlášení, znamená to, že každý kdo toto zařízení používá nebo má k tomuto zařízení přístup, může předchozí přihlášení snadno zopakovat a dostat se tak k soukromí dané osoby. Proto je nutné hesla neukládat a ideálně odstranit i procházení, protože často na jednotlivých stránkách zůstává přihlašovací jméno.

Antispamová, antivirová a firewall

Antispamová ochrana slouží především k ochraně e-mailových schránek. Častokrát se stává, že do schránky e-mailu chodí nevyžádaná pošta a ta může být ve formě nevhodné reklamy, ale také za účelem vydírání a podvodu s cílem zneužití. Antispamová ochrana se stará o to, aby takových e-mailů bylo co nejméně, a tím bylo soukromí chráněno. Antispamovou ochranu většinou poskytují samotné antivirové programy a to ve formě doplňku svých programů [35].

Antivirová ochrana slouží k zamezení napadení pomocí viru, malwaru, ransomwaru nebo dalších. Principiálně jde o zabezpečení zařízení před škodlivými útoky, které by mohli vést k hacknutí zařízení, ztrátě dat nebo také poškození, resp. znehodnocení softwarové stránky zařízení.

Firewall chrání zařízení v rámci počítačové sítě a podle určitých pravidel povoluje nebo naopak blokuje komunikaci zařízení s dalšími. Firewall mají například zařízení

s operačním systémem Windows, již předinstalovanou. Jde jí také pořídit v rámci doplňků některých antivirových programů [36].

Anonymní proxy servery

Využití proxy serveru dává možnost být při některých operacích v rámci internetu méně pozorován. Jedná se totiž o šifrovaný přenos dat a tím je složitější dostupnost k informacím o pohybu na internetu. Je možné jej využít přímo v rámci některých prohlížečů, například Firefox má přímo službu FoxyProxy. Proxy server je možné využívat při zacházení s citlivými údaji, třeba v rámci internetového bankovnictví, ale není na škodu jej použít také při využívání sociálních sítí a dalších činností.

4.2.2 Zhodnocení opatření

Cílem této části práce je preventivní opatření zhodnotit a určit tak, jejich pořadí v rámci požadované ochrany. Opatření budou hodnocena pomocí párového srovnání, protože je to snadný a efektivní způsob srovnání, díky tomu, že bude srovnáno každé opatření s každým, tak vyjde jasný výsledek o tom, která opatření jsou nejvhodnější. Rozhodujícím faktorem pro hodnocení bude účinnost opatření.

Tabulka č. 4 a 5 porovnává jednotlivé preventivní opatření mezi sebou a v případě, že je jedno opatření účinnější než jiné získává „1“, pokud není účinnější, získává „0“ a po všech porovnáních jsme schopny kolik „1“ dané opatření získalo a díky tomu vyhodnotit pořadí. Zvlášť budou hodnocena opatření technická a zvlášť také organizační.

Tab. 4: Porovnání organizačních opatření pomocí párového srovnání [vlastní zdroj]

Označení	Opatření	1	2	3	4	5	6	7	Součet	Pořadí
1	Vzdělání v sebeobraně	x	1	1	1	1	1	1	6	1.
2	Vzdělání v oblasti IT bezpečnosti	0	x	0	0	1	0	1	2	5.
3	Umístění obydlí	0	1	x	1	1	0	1	4	3.
4	Přístup do objektu	0	1	0	x	1	0	1	3	4.
5	Kontrola smluvních podmínek	0	0	0	0	x	0	0	0	7.

6	Kontrola osobních dokladů a předmětů	0	1	1	1	1	x	1	5	2.
7	Regulace chování na soc. sítích	0	0	0	0	1	0	X	1	6.

Tab. 5: Porovnání technických opatření pomocí párového srovnání [vlastní zdroj]

Označení	**Opatření**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**Součet**	**Pořadí**
1	Perimetrická ochrana	x	1	1	1	1	1	1	6	1.
2	Kontrola vyplňování os. údajů	0	x	0	0	0	0	0	0	7.
3	Zamezení sdílení přístupu k datům a účtům	0	1	x	1	1	1	1	5	2.
4	Identifikace a autentizace	0	1	0	x	1	1	1	4	3.
5	Blokování reklamního sledování a ukládání hesel	0	1	0	0	x	0	1	2	5.
6	Antispamová, antivirová ochrana a firewall	0	1	0	0	1	x	1	3	4.
7	Anonymní proxy server	0	1	0	0	0	0	x	1	6.

4.2.3 Dílčí závěr

Na základě párového hodnocení bylo zjištěno, že nejúčinnějším preventivním opatřením z oblasti organizačních opatření je vzdělání v sebeobraně. Vzdělání v sebeobraně vede především ke snížení rizika odcizení osobních dokladů či elektronických zařízení v okamžiku napadení. Dalším velmi účinným opatřením je kontrola osobních dokladů a předmětů. Důvodem je především to, že účinnost tohoto opatření je velká – pokud nebudou

lidé nechávat své věci bez dozoru, velmi tak snižují riziko odcizení cenných předmětů. Následujícím opatřením v žebříčku účinnosti je umístění obydlí, které má za následek výrazné snížení rizika vloupání. Dále je přístup do objektu, zde se jedná o opatření, které má útočníka odradit od vloupání, podobně jako tomu bylo v předchozím případě u umístění obydlí. A následují vzdělání v oblasti IT bezpečnosti, regulace chování na sociálních sítích a kontrola smluvních podmínek. Tato tři opatření velmi výrazně snižují riziko napadení v oblasti internetu, nejsou však tak účinná jako předchozí opatření, která zároveň chrání nebo spíše nesměřují k fyzické újmě.

Co se týče preventivních technických opatření, tak se podle bodového hodnocení ukázalo, že je nejúčinnější perimetrická ochrana, která nejlépe zabraňuje vniknutí útočníka do zájmového objektu. Dále zamezení sdílení přístupu k datům a účtům, protože dopad například sdělení přístupových údajů k zařízení může vést k velkým ztrátám na soukromí. Identifikace a autentizace je další vysoce hodnocené opatření, které se týká podobného tématu jako sdílení přístupů, ale důležitá část je především způsob uzamčení a síla hesla, které uživatel použije, aby zamezil získání soukromých dat a fotografií, které mohou být v zařízení uloženy. Antispamová, antivirová ochrana a firewall jsou také velmi důležitým preventivním opatřením, které chrání elektronické zařízení a velkou měrou přispívají k ochraně osobních dat. Na závěr je tu blokování reklamního sledování a ukládání hesel, anonymní proxy server a kontrola vyplňování osobních údajů. Všechna tato preventivní opatření mají společný jmenovatel a tím je skrývání pohybu na internetu, což je samozřejmě také velmi důležité pro ochranu soukromí.

II. PRAKTICKÁ ČÁST

5 ANALÝZA PREVENCE V OCHRANĚ SOUKROMÍ Z POHLEDU RESPONDENTŮ

Cílem dotazníkového šetření bylo zjistit, jak respondenti vnímají roli prevence v ochraně soukromí. Názory a odpovědi na jednotlivé dotazy, které jsou v dotazníku uvedeny, mají napomoci při tvorbě preventivních opatření a mají také odhalit, jak nad soukromím lidé přemýšlí.

5.1 Dotazník

Dotazník obsahoval celkem 27 otázek, které se týkaly prevence v ochraně soukromí. Otázky byly rozděleny do určitých sekcí, kvůli lepší orientaci hodnotitele. První část dotazů byla zaměřená na rozřazení respondentů a to podle věku, pohlaví a vzdělání. Účelem tohoto rozřazení bylo především ukázat, že se dotazování účastnila rozmanitá skupina lidí a díky tomu budou výsledky relevantnější.

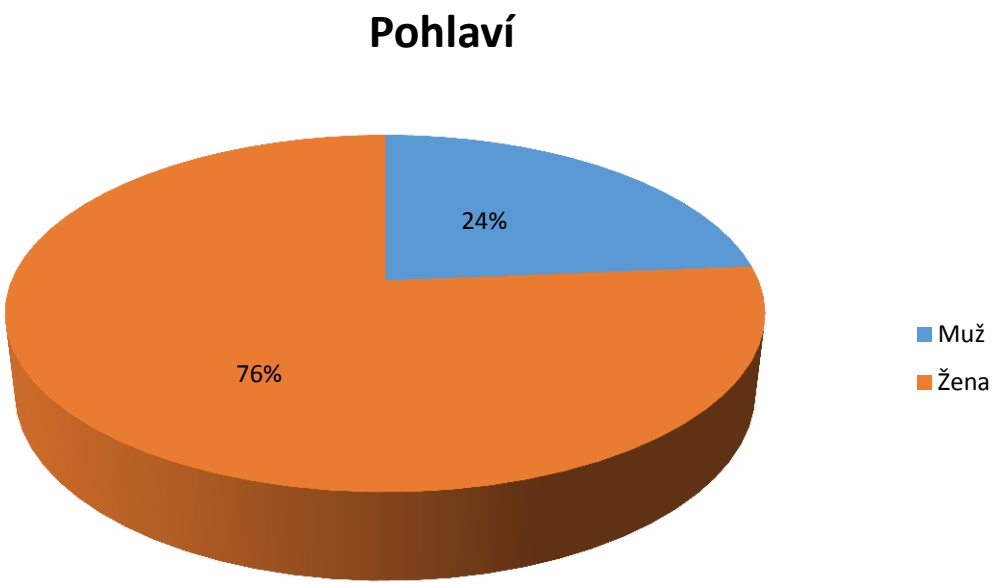
Druhá část otázek byla z oblasti hrozeb, tzn., byly zde především dotazy týkající se zkušeností nebo setkáním s určitými druhy hrozeb, které mohou narušovat soukromí. Další část otázek směřovala především k vnímání soukromí. Otázky v této části se zabývaly tím, jak respondenti hodnotí své soukromí, jak si ho váží a zda je pro ně vůbec důležité.

Poslední část otázek se zaměřovala na prevenci. Dotazy byly pokládány tak, abychom zjistili, jaká preventivní opatření respondenti využívají a jakým způsobem prevenci vnímají. Poslední tři dotazy v této sekci byly volně položené otázky, u kterých se měli respondenti zamyslet nad prevencí a její důležitostí v našich životech.

Průzkumu se zúčastnilo celkem 140 respondentů, což je dostatečný počet pro to, aby se dotazník dal považovat za přiměřeně objektivní a přinesl tak dostatečné výsledky ve vnímání prevence v ochraně soukromí. Dotazování probíhalo anonymně, formou elektronického dotazníku, vytvořeného na webu vyplnto.cz.

Otázka č. 1: Pohlaví

První otázka zjišťovala pohlaví osob, které se dotazníku účastnily. Je důležité, aby odpovědi byly od obou pohlaví, protože žena i muž mohou roli prevence vnímat jinak, zároveň mohou být i jiným způsobem vnímány hrozby.

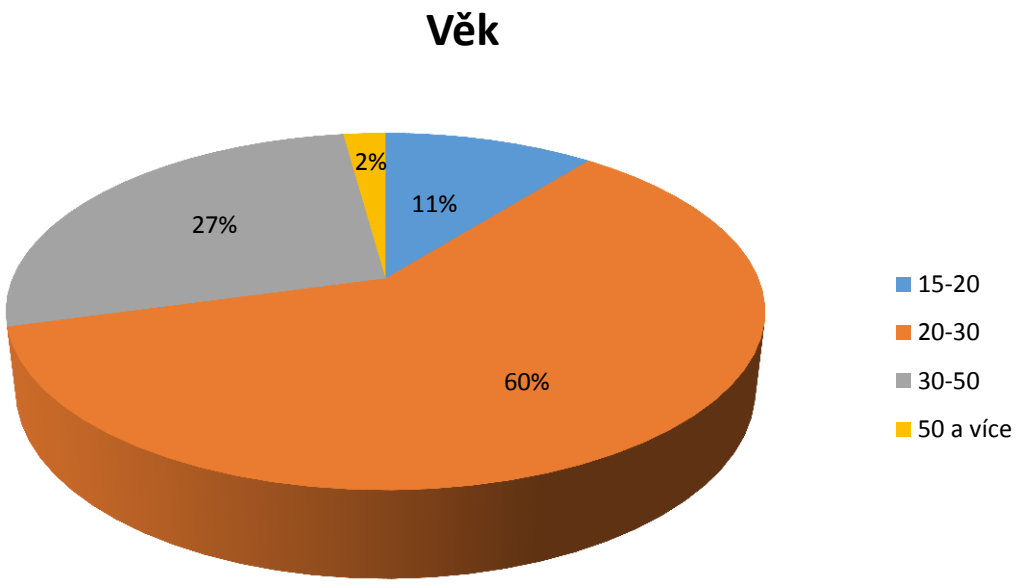


Graf 2: Pohlaví [vlastní zdroj]

Z výsledků uvedených na obrázku výše můžeme vidět, že ženy se dotazníku účastnily ve větším počtu než muži a to v poměru 76 % žen a 24 % mužů. Je důležité, že skupina odpovídajících je i přes větší podíl žen zastoupena oběma pohlavími.

Otázka č. 2: Věk

Druhá otázka, která vedla k rozřazení respondentů, se týkala věku. Podobně jako u pohlaví se různé věkové skupiny mohou na prevenci v ochraně soukromí dívat jinak. Starším lidem například mohou vadit inovace v oblasti ochrany, a proto je považují za zbytečné, naopak mladí lidé mohou brát roli prevence na lehkou váhu. Kvůli těmto a dalším důvodům, je důležité, aby respondenti byli v různých věkových skupinách.

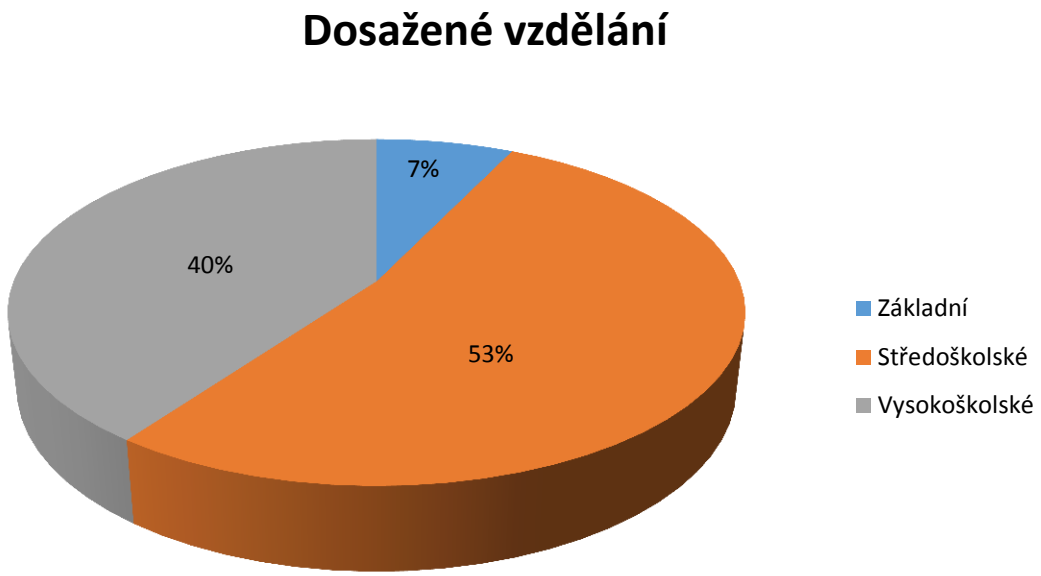


Graf 3: Věk [vlastní zdroj]

Nejobsáhlejší skupinou odpovídajících byli lidé ve věku 20-30 let a to s 60 % podílem. Další velkou skupinou byli respondenti ve věku 30-50let s podílem 27 %. Zbývajících 13 % zúčastněných byla ve věku 15-20let, konkrétně 11 % a ve věku nad 50let odpověděla 2 % dotazovaných. Skupiny ve věku 20-30 a 30-50 odpovídali nejčastěji, k tomu přispělo zřejmě také to, že dotazník byl šířen elektronickou formou.

Otázka č. 3: Dosažené vzdělání

Poslední otázka, která má za úkol ukázat rozmanitost respondentů, je otázka týkající se dosaženého vzdělání.



Graf 4: Dosažené vzdělání[vlastní zdroj]

Nejvíce odpovídajících na tuto otázku mělo dosažené středoškolské vzdělání a to 53 % odpovídajících, dále se dotazníku zúčastnilo 40 % vysokoškolsky vzdělaných respondentů a v nejmenším zastoupení byli lidé se základním vzděláním v 7 % poměru.

Otázka č. 4: Setkali jste se někdy s některými druhy nebezpečí na internetu?

Tato otázka je první ze sady otázek týkající se hrozeb. Otázkou je, zda se s některými hrozbami ohrožujícími soukromí respondenti již setkali a které to jsou. Na základě této otázky budeme schopni vyhodnotit nejčastěji hrozby a reagovat adekvátním preventivním opatřením.

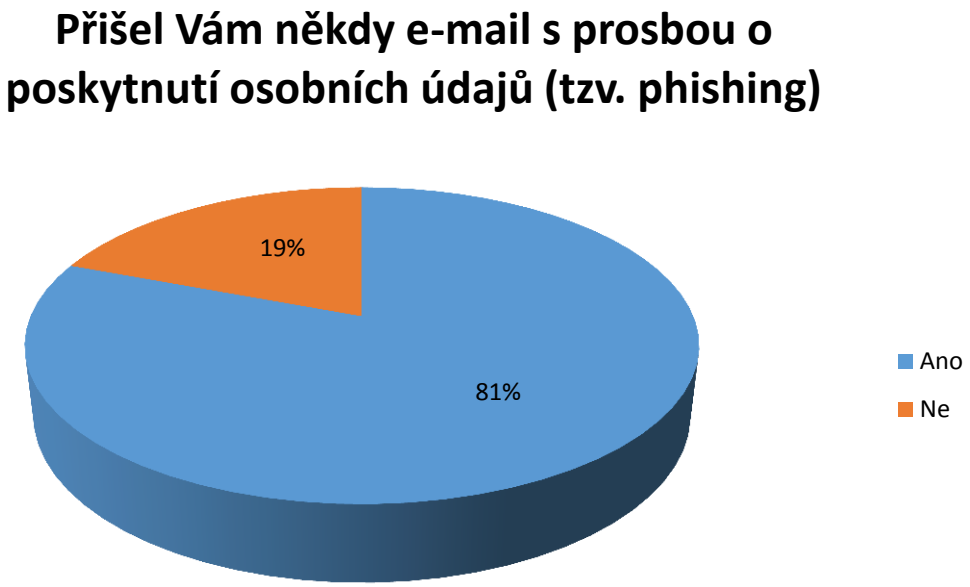
Graf 5: Nebezpečí na internetu [vlastní zdroj]

U této otázky, mohli respondenti označit více odpovědí, přičemž nejčastější odpovědí bylo s 54 % setkání s phishingem, dále s 20 % kyberstalking a s 15 % kyberšikana. Důležité také je, že 9 % respondentů se někdy s žádným druhem nebezpečí nesetkalo.

Poslední 2 % dotazovaných reagovali jinou odpovědí, než byly nabídnuty. Nejčastěji se v této skupině odpovědí objevoval kybergrooming, tedy využití komunikačních prostředků k navázání důvěrného vztahu, častokrát je bohužel záměrem sexuální obtěžování a zneužití důvěry.

Otázka č. 5: Přišel Vám někdy e-mail s prosbou o poskytnutí osobních údajů (tzv. phishing)?

V této otázce se zabýváme konkrétně phishingem a účelem je zjistit, jaký byl konkrétní počet obětí phishingu. Abychom respondentům pojem phishing a jeho podobu přiblížili, byla otázka položena konkrétně takto: "Přišel Vám někdy e-mail s prosbou o poskytnutí osobních údajů (tzv. phishing). Například, bylo v e-mailu uvedeno, že jste něco vyhrál a proto máte poskytnout – jméno, číslo účtu atd.".



Graf 6: Poskytování osobních údajů [vlastní zdroj]

Výsledkem této otázky je zjištění, že 81 % respondentů, tedy v přepočtu 114 lidí z celkových 140 se setkalo s phishingem, je tedy evidentní, že se jedná o hrozbu, která je velmi rozšířená. Pouhých 19 % dotazovaných se s phishingem vůbec nesetkalo.

Otázka č. 6: Stali jste se někdy obětí stalkingu (sledování), nebo kyberstalkingu (sledování na sociálních sítích)?

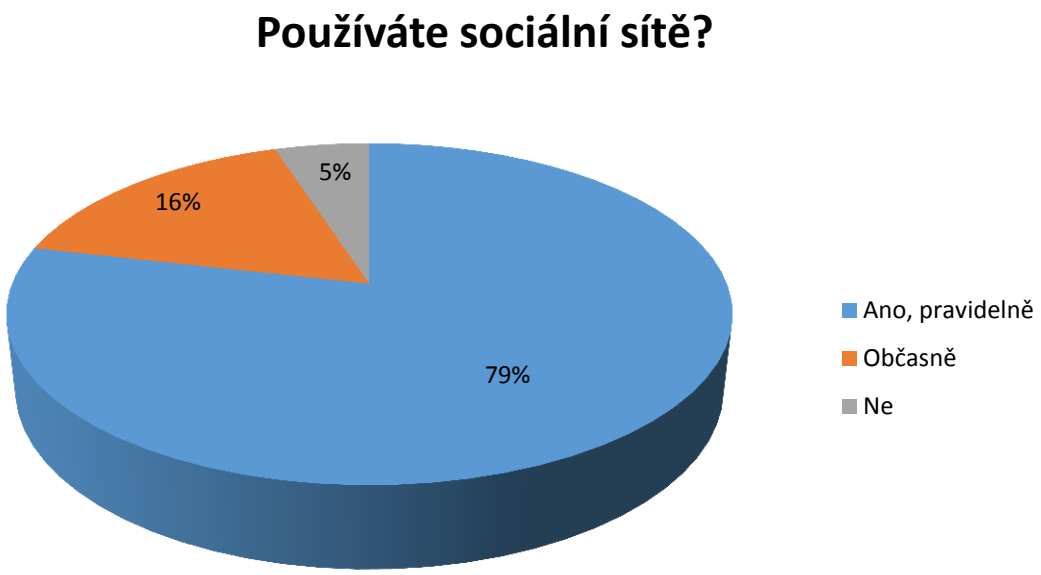
Podobně jako u předchozí otázky nám šlo o upřesnění počtu respondentů, kteří se setkali s tímto způsobem narušení soukromí.

Graf 7: Oběti stalkingu/kyberstalkingu[vlastní zdroj]

U této otázky byly odpovědi překvapující, 79 % dotazovaných se s tímto druhem ohrožení nesetkalo a 21 % respondentů mělo určitou zkušenost se stalkingem a kyberstalkingem. Je samozřejmě možné, že dotazování o tom, že byli sledování, vůbec nevědí a díky tomu je nutné věnovat více času a úsilí například v oblasti sebeobrany, popřípadě vzdělání v kybernetické bezpečnosti.

Otázka č. 7: Používáte sociální sítě?

Otázka dotazující se na aktivitu na sociálních sítích, byla zařazena z toho důvodu, že se na těchto sítích častokrát objevují osobní údaje. Případný pachatel může z těchto sítí získat spoustu cenných informací, které mohou vést ke stalkingu.

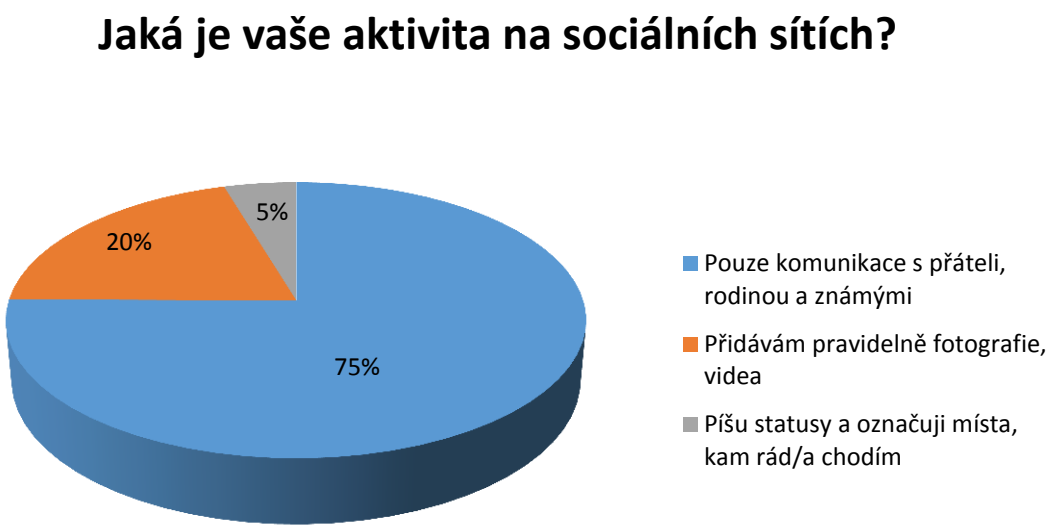


Graf 8: Používání sociálních sítí [vlastní zdroj]

Odpovídající téměř v 95 % potvrdili, že využívají sociální sítě. Konkrétně 79 % respondentů potvrdilo pravidelné využívání a 16 % pouze občasné. Pouhých 5 % dotazovaných sociální sítě nevyužívá. Tyto výsledky mohou být samozřejmě ovlivněny věkem dotazovaných, ale je evidentní, že využití sociálních sítí je významné.

Otázka č. 8: Jaká je vaše aktivita na sociálních sítích?

U této otázky bychom se měli dozvědět konkrétní činnost respondentů na sociálních sítích. Na základě odpovědí, bychom se mohli dozvědět, jak dbají respondenti o své soukromí na sociálních sítích.



Graf 9: Aktivita na sociálních sítích [vlastní zdroj]

U této otázky bylo možné označit více odpovědí. Nejčastěji respondenti využívají sociální sítě ke komunikaci, konkrétně v 75 % případů, téměř každý měl zaškrtnutý tento typ odpovědi. Přidávání fotografií potvrdilo 20 % odpovídajících a 5 % odpovědělo, že označují místa, kam chodí.

Z těchto odpovědí je možné vyvodit, že čtvrtina respondentů provozuje určitý způsobem rizikovou činnost na sociálních sítích a je nutné zaměřit svou pozornost k preventivním opatřením typu: kontrola digitálních stop, kontrola sdílení určitého obsahu, popřípadě věnovat čas zabezpečení svých zařízení.

Otázka č. 9: Ponecháváte někdy, třeba i omylem svůj mobil nebo notebook bez dozoru?

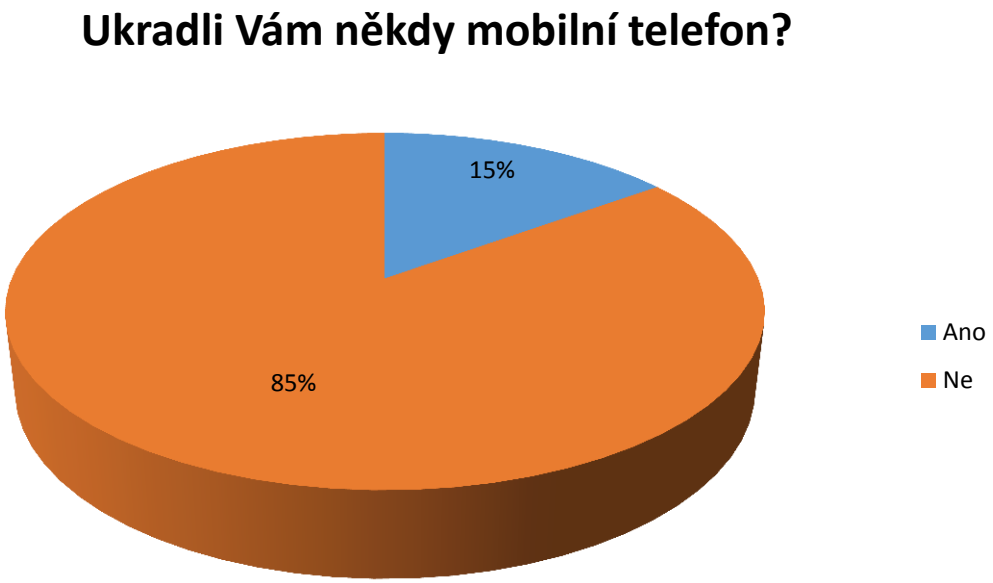
Cílem této otázky bylo zjistit, zda si lidé střeží své věci a nedávají je všanc krádežím. Konkrétní znění otázky bylo: "Ponecháváte někdy, třeba i omylem svůj mobil nebo notebook bez dozoru? V autě nebo na stole v restauraci apod."

Graf 10: Mobil nebo notebook bez dozoru [vlastní zdroj]

Na tuto otázku lidé v 80 % případů odpověděli, že nenechávají své věci bez dozoru, což je rozhodně správné. Co je však zarážející, že 20 % odpovídajících své věci nechává volně bez dozoru a snadno dostupné. Dva lidé z deseti dobrovolně dopouští, aby jim někdo předměty bez větší námahy ukradl, a ohrožují tím tak své soukromí.

Otázka č. 10: Ukradli Vám někdy mobilní telefon?

Tato otázka souvisí s otázkou předchozí a jejím cílem je zjistit v kolika případech skutečně došlo ke krádeži mobilního telefonu. Zcizení mobilního telefonu může častokrát vést k narušení soukromí a rozhodně se řadí mezi nebezpečné hrozby.



Graf 11: Ukradený mobilní telefon [vlastní zdroj]

Odpověď byla nejčastěji ne, tedy 80 % odpovídajících mobilní telefon odcizen nebyl. Pouze v 15 % případů se stalo, že byl mobilní telefon odcizen. Můžeme si však povšimnout, že počty okradených a těch z předchozí otázky, kteří svoje zařízení nechrání je velmi podobný.

Lze s určitostí říci, že 21 lidí ze 140, kteří o svůj mobilní telefon přišli, mohou pomocí preventivních opatření krádeži buď předejít, nebo alespoň zamezit ztrátě citlivých údajů obsažených v zařízení.

Otázka č. 11: Myslíte, že je soukromí důležité?

Tato otázka je z další kategorie otázek, která se týká vnímání soukromí. Cílem otázek je zjistit, jak respondenti vnímají své soukromí, jak si ho váží. Tedy v pozdějším důsledku, zda je důležité si jej vůbec chránit.

Graf 12: Důležitost soukromí [vlastní zdroj]

Na základě odpovědí je možné říci, že 98 % respondentů si váží svého soukromí. Soukromí je pro ně důležité a tudíž je předpoklad, že budou mít zájem si jej chránit. Pouhá 2 % dotazovaných si myslí, že soukromí není důležité.

Toto je jedno z nejdůležitějších zjištění v rámci tohoto dotazování, protože díky tomu, že lidé považují soukromí za důležité, tak budou chtít své soukromí chránit a využívat tak preventivní opatření.

Otázka č. 12: Je pro vás důležitější ochrana majetku nebo soukromí?

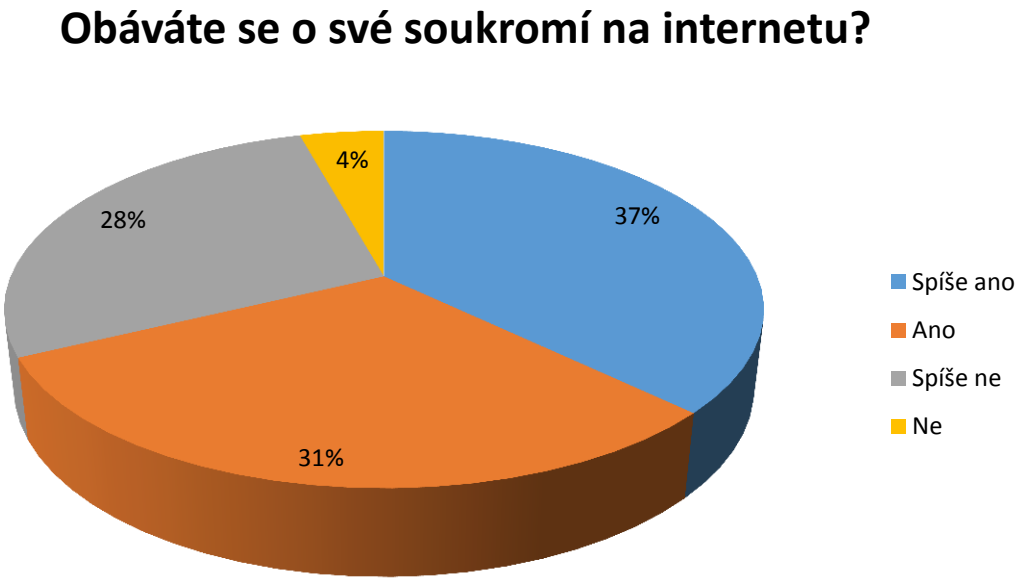
Cílem této otázky je zjistit, zda je pro respondenty ochrana soukromí alespoň, tak důležitá jako ochrana majetku. V dřívějších dobách by totiž nebylo pochyb o tom, že by lidé chránili spíše svůj majetek. Půjde tedy o vnímání soukromí v porovnání s něčím, co lidé znají a co umí například finančně ohodnotit.

Graf 13: Ochrana soukromí nebo majetku [vlastní zdroj]

Vzhledem k tomu, že je ochrana majetku velmi důležitá, odpovědělo 36 % respondentů, že si více váží právě majetku. Co je však pro naše závěry důležitější, tak 64 % respondentů si váží více svého soukromí, tedy téměř dvě třetiny dotazovaných. Z toho plyne, že v dnešní době si lidé hodnotu soukromí velmi dobře uvědomují a jsou si ochotni přiznat, že je pro ně důležitější než majetek.

Otázka č. 13: Obáváte se o své soukromí na internetu?

Otázka patřící do skupiny vnímaní soukromí. S internetem je jistě spojeno velké množství hrozeb vedoucí k narušení soukromí, je proto vhodné zjistit, jak vnímají lidé pohyb na internetu.



Graf 14: Soukromí na internetu [vlastní zdroj]

Pokud bychom spojili skupiny, které se obávají o své soukromí (31 %) a které se spíše obávají o své soukromí (37 %), máme 68 % což je více než dvě třetiny odpovídajících, kteří se pohybují na internetu a bojí se o své soukromí. Což je velmi podstatné, protože tito lidé mohou mít zájem se chránit, protože tak doposud neučinili nebo jsou chráněni, ale mají pocit, že ochrana není dostatečná.

Dále si zbylých 28 % respondentů myslí, že se o své soukromí na internetu nemusí obávat a 4 % odpovídajících se nebojí vůbec. Tyto dvě skupiny naopak buď nemají zájem se chránit, nebo mají takovou ochranu, která jim připadá bezpečná.

Otázka č. 14: Věnujete pozornost smluvním podmínkám a pročítáte si je před potvrzením?

Tato otázka se týká pročítání smluvních podmínek, bohužel se častokrát stává, že jsou podmínky tak dlouhé nebo tak náročné, že je lidé raději bez procházení potvrdí. Automatickým potvrzením souhlasu však může dojít právě ke zneužití osobních údajů nebo údajů o prohlížení.

Graf 15: Pozornost u smluvních podmínek [vlastní zdroj]

67 % respondentů smluvní podmínky nepročítá a 33 % jim věnuje svůj čas a je ochotno si je pročíst. Bohužel v tomto případě není snadné diktovat někomu pročítání předepsaných podmínek, je to velmi zdlouhavé a potvrzení se objevuje na mnoha stránkách, jednalo by se tedy prakticky o nepřetržitou činnost spojenou s využíváním internetu. Je určitě dobré, že alespoň třetina respondentů své soukromé údajů střeží.

Otázka č. 15: Setkali jste se někdy s pojmem GDPR (obecné nařízení o ochraně osobních údajů)?

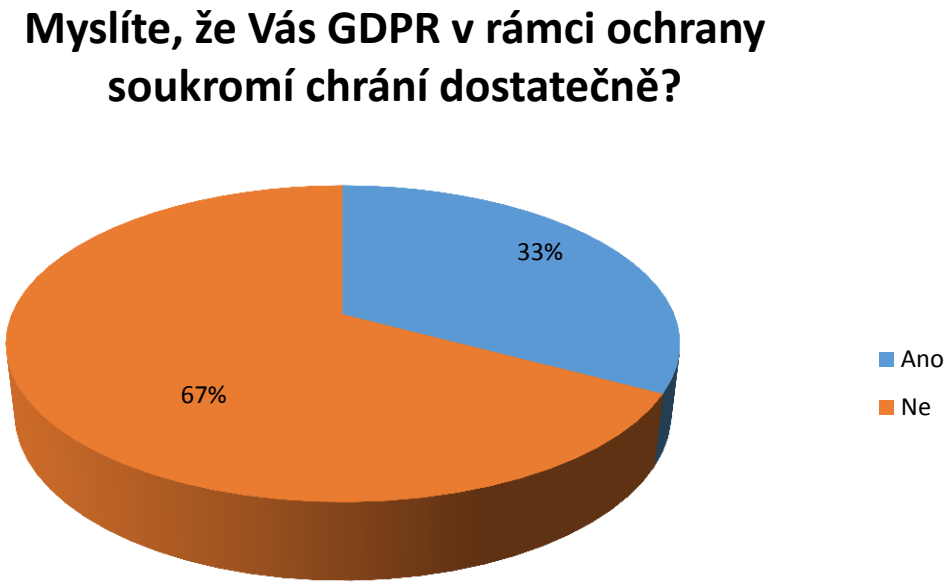
Tato otázka směřovala k informovanosti veřejnosti o nových nařízeních aplikovaných na území České republiky. Nařízení se týká osobních údajů, a proto může být pro prevenci v ochraně soukromí velmi důležité.

Graf 16: Pojem GDPR [vlastní zdroj]

Téměř každý odpovídající se s pojmem GDPR setkal a je tedy možné předpokládat, že si důležitost svých osobních údajů uvědomuje.

Otázka č. 16: Myslíte, že Vás GDPR v rámci ochrany soukromí chrání dostatečně?

Tato otázka je navazující na otázku předchozí a zjišťuje, zda díky GDPR lidé cítí dostatečnou ochranu. Cílem je zjistit, zda by se v této oblasti ochrany údajů dalo něco zlepšit.



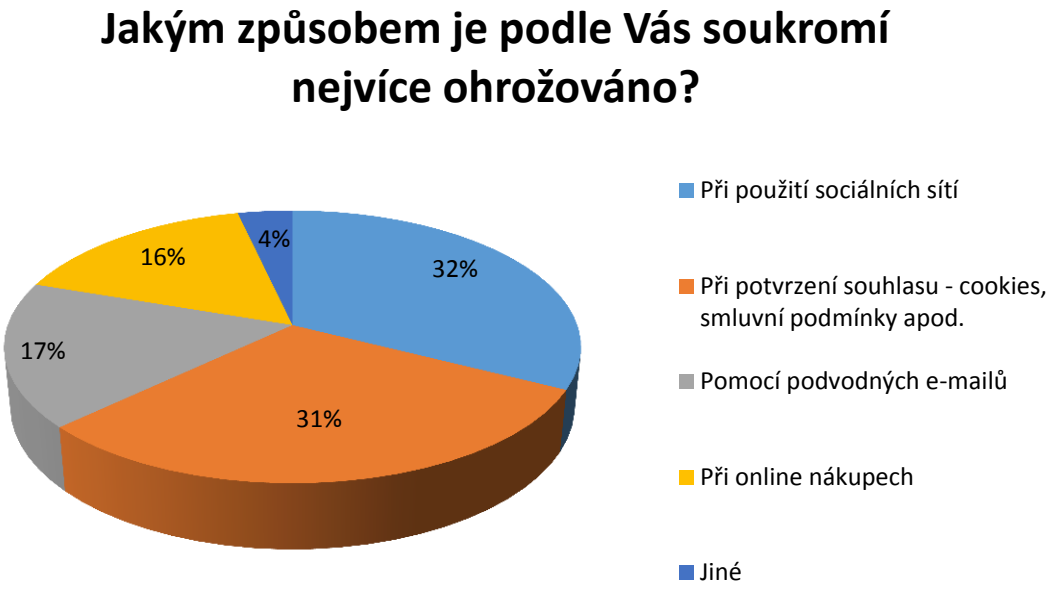
Graf 17: Chrání GDPR soukromí [vlastní zdroj]

Na základě odpovědí je možné usoudit, že pro dvě třetiny respondentů, konkrétně 67 % není GDPR dostatečnou ochranou. Důvodem může být to, že pokud chce osoba využívat nějakou službu nebo produkt, tak k tomu musím udělit souhlas. V podstatě ve všech oblastech společnosti jsme nuceni k předání souhlasu, ale i přestože je možnost výběru, tak existuje vlastně jen jedna možnost vedoucí k pohodlnému životu.

Jistě by bylo vhodné, kdybychom mohli konkrétně zvolit, jaké informace chceme předat a pokud nechceme předat žádné, tak nemůžeme být diskriminováni. Lidé sice vnímají, že se GDPR spolupodílí na ochraně soukromí, ale je k tomu nutné připojit další ochranu, další preventivní opatření, která zamezí úniku informací.

Otázka č. 17: Jakým způsobem je podle Vás soukromí nejvíce ohrožováno?

Cílem této otázky je zjistit, čeho se lidé v rámci ochrany soukromí nejvíce bojí, co pro ně představuje největší hrozbu. Zvoleným hrozbám jsme schopni se poté dále věnovat.

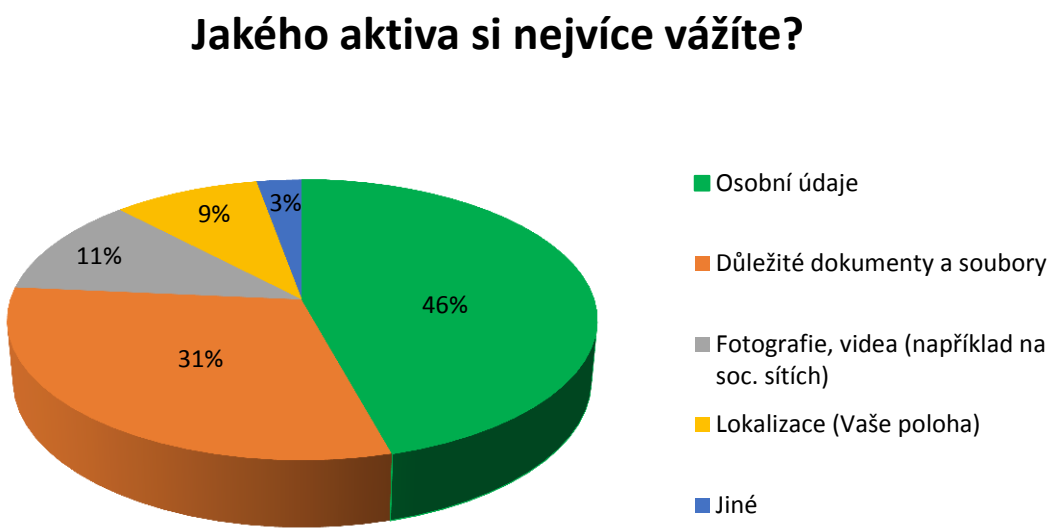


Graf 18: Ohrožení soukromí [vlastní zdroj]

Respondenti mohli v tomto případě volit více možností, přičemž téměř shodně zvolili, že je nejvíce ohrožuje používání sociálních sítí a potvrzování různých souhlasů a podmínek. Je také nutné zmínit, že každou z těchto možností zvolilo více než 100 respondentů. Další téměř třetinu odpovědí tvořilo ohrožení ve formě podvodných e-mailů a online nákupů. V poslední skupině odpovědí: „jiné“, kterou tvořila 4 % odpovědí, se objevovaly nejčastěji souhlasy udělované státu a bankám, nebo aplikace na mobilu.

Otázka č. 18: Jakého aktiva si nejvíce vážíte?

Otázka týkající se vnímaní soukromí a cílem je vyhodnotit jaké aktivum je podle respondentů nejcennější. Na základě vyhodnocení jsme poté schopni se na tato aktiva více zaměřit.



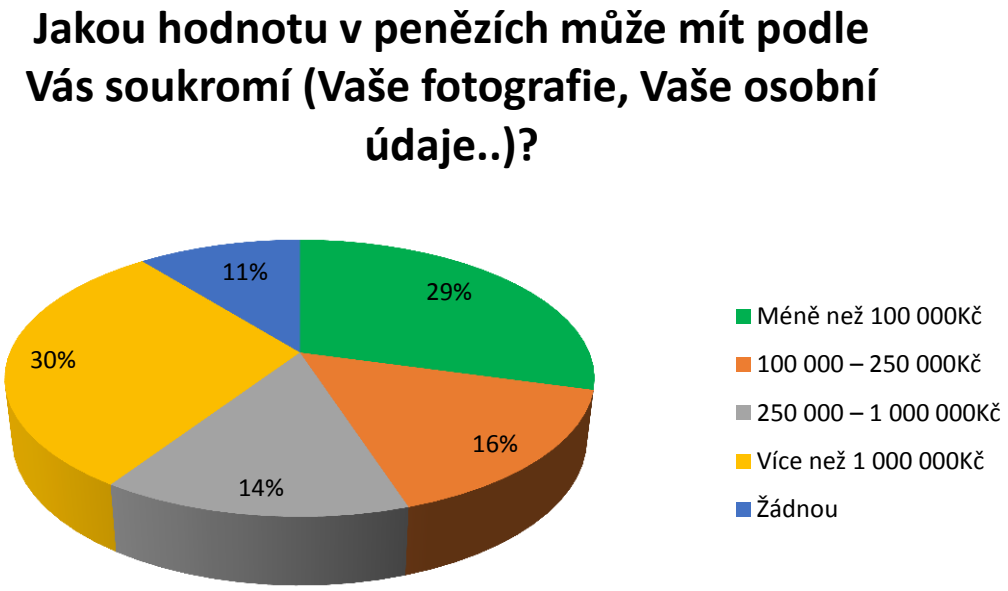
Graf 19: Důležitá aktiva [vlastní zdroj]

Protože účelem bylo vyhodnotit skutečně nejcennější aktivum, tak nebyla možnost zvolit více aktiv, ale pouze jedno. Nejcennějším aktivem se staly osobní údaje a to téměř s polovinou odpovědí, konkrétně 46 %. Tato skutečnost je pochopitelná, protože zneužití osobních údajů dostává poškozené do velkých potíží a zároveň lze říci, že riziko napadení je poměrně vysoké.

Dalším důležitým aktivem byly dokumenty a soubory s 31 %. Okolo 10 % měly také fotografie a videa na sociálních sítích včetně lokalizace. Ve skupině „jiné“, která obsáhla 3 % respondentů, byly nejčastěji odpovědi, které tvrdí, že všechna uvedená aktiva je potřeba chránit a jsou důležitá.

Otázka č. 19: Jakou hodnotu v penězích může mít podle Vás soukromí (Vaše fotografie, Vaše osobní údaje?

Cílem této otázky bylo především zamyšlení respondentů nad aktivy, například uvedenými v předchozí otázce a vyčíslení součtu hodnot těchto aktiv.



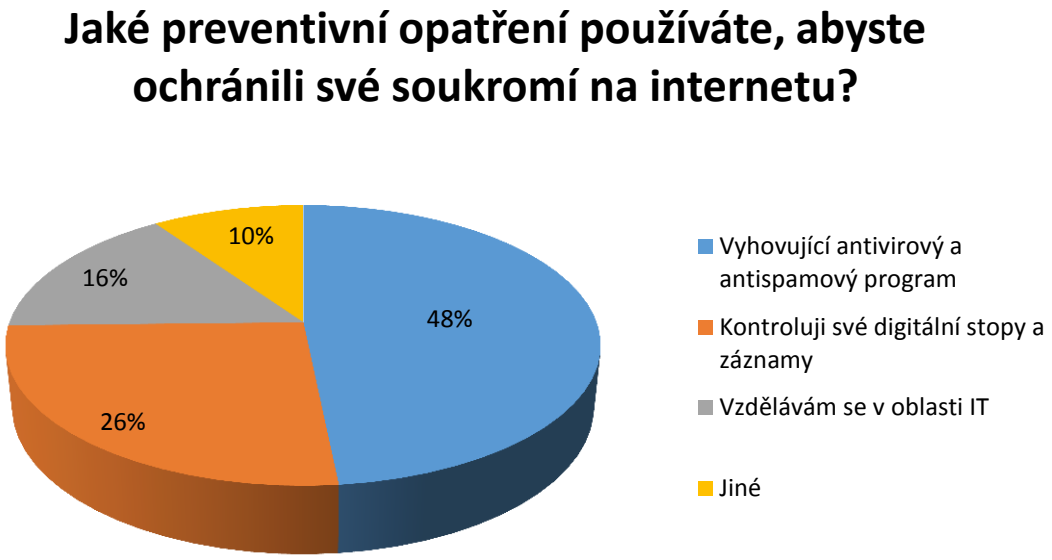
Graf 20: Peněžní hodnota soukromí [vlastní zdroj]

V tomto případě se jedná asi o nejrozmanitější graf. Kde na jedné straně se 30 % stojí odpověď s hodnotou více než 1 000 000Kč a na druhé straně s 29 % stojí odpověď méně než 100 000Kč. Tyto dvě možnosti jsou v podstatě možnosti s nejnižší a nejvyšší peněžní hodnotou a tvoří dvě třetiny hlasů.

Z výsledku lze vyvodit, že skutečně každý vnímá soukromí jinak a i míra financí, kterou by byl ochoten vynaložit na ochranu je různá. Dalším zajímavým výsledkem je, že 11 % respondentů by neobětovalo žádné finanční prostředky k ochraně soukromí. Důležité však je, že většina lidí je ochotna vynaložit jistou část svých financí na preventivní opatření a tím ochránit své soukromí.

Otázka č. 20: Jaké preventivní opatření používáte, abyste ochránili své soukromí na internetu?

Tento typ otázek již spadá do kategorie prevence a cílem je zjistit, co respondenti považují za preventivní opatření a jaké nejčastěji využívají.



Graf 21: Preventivní opatření na internetu [vlastní zdroj]

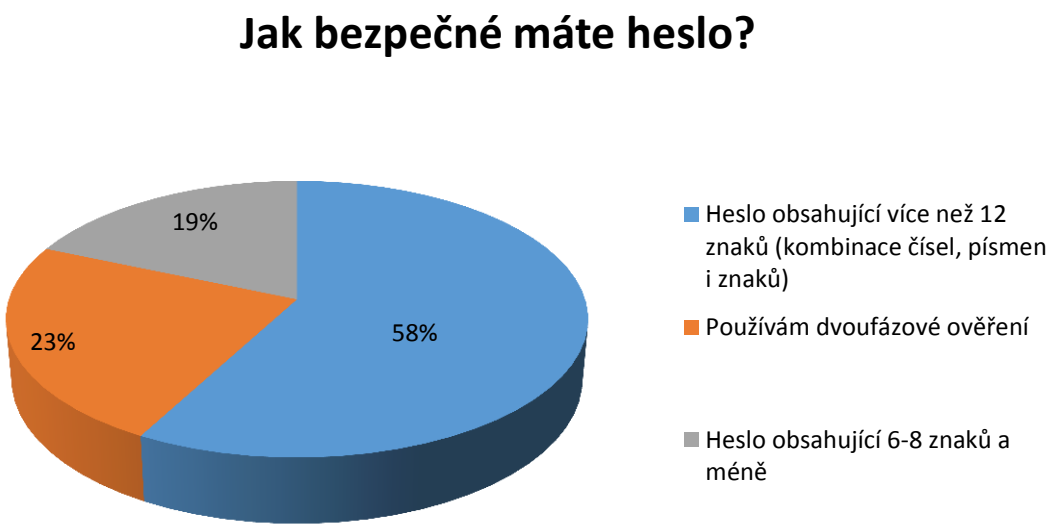
U této otázky bylo možné zvolit více odpovědí. Nejčastěji se objevila odpověď vyhovující antivirový a antispamový program a to v 48 % případů, konkrétně se jednalo o 110 respondentů, kteří tuto možnost zvolili. Kontrola digitálních stop je také velmi účinnou ochranou a proto jí zvolilo 26 % respondentů. Vzdělávání v oblasti IT označilo za vhodnou volbu 16 % respondentů.

Zbylých 10 % respondentů zvolilo vlastní odpověď, mezi nimi se nejčastěji objevovalo silné heslo, minimální sdílení fotografií nebo také správné nastavení prohlížeče (anonymní přístup).

Na základě výsledků z těchto odpovědí a poměrně vysokému počtu textem vypsaných odpovědí, lze říci, že respondenti nad dotazníkem skutečně přemýšlí a preventivní opatření vyjmenovali naprosto správně.

Otázka č. 21: Jak bezpečné máte heslo?

Tato otázka navazuje na předchozí otázku, kde se také objevovala odpověď, že by respondenti využívali k ochraně soukromí jako preventivní opatření silné heslo. Výsledek z předchozí otázky tedy přímo poukazuje na vhodnost této otázky. Cílem je zjistit jakou sílu mají hesla, která respondenti používají a na základě toho aplikovat případná opatření.



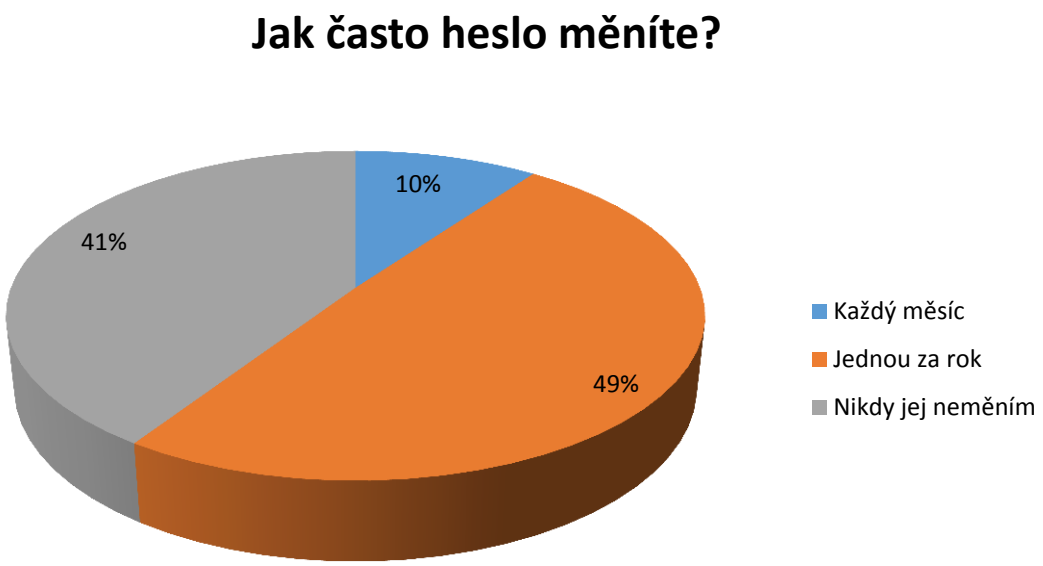
Graf 22: Bezpečnost hesla [vlastní zdroj]

Výsledek odpovědí je velmi uspokojivý, protože 58 % respondentů uvedlo, že používá velmi silné heslo, které může mít velkou úspěšnou v zamezení přístupu k jednotlivým účtům. Dalších 23 % respondentů uvedlo, že používá dvoufázové ověření, což je jistě vhodný způsob ochrany.

V neposlední řadě 19 % respondentů označilo, že má 6-8 místné heslo, což je sice minimální doporučená úroveň ochrany, ale pokud se jedná například pouze o čísla nebo pouze o písmena, nebude složité jej rozšifrovat.

Otázka č. 22: Jak často heslo měníte?

Dalším důležitým aspektem hesel je jejich změna v čase, protože pokud jej necháte dlouho stejné, zvyšuje se tím riziko prolomení. Tato otázka, podobně jako otázka předchozí zjišťuje riziko prolomení hesla a tím zneužití osobních údajů, popřípadě dalších cenností, podle toho o přístup do jaké aplikace by se jednalo.

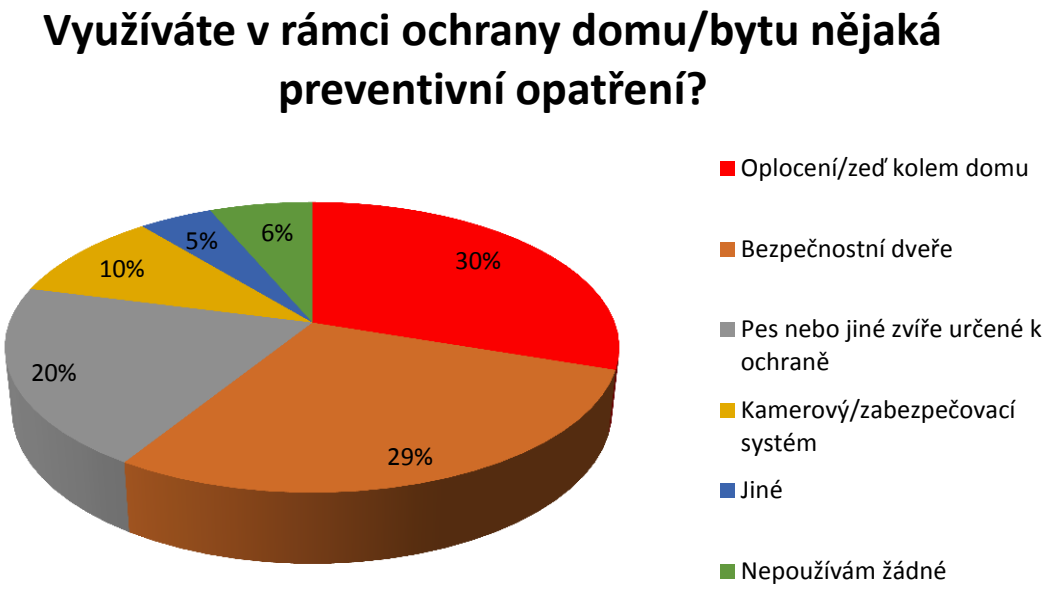


Graf 23: Frekvence změny hesla [vlastní zdroj]

V tomto případě jsou odpovědi velmi znepokojující, protože pouze 10 % odpovídajících si mění heslo každý měsíc. Zbylých 41 % dotazovaných si jej nemění vůbec nebo jen jednou za rok 49 %. V tomto ohledu by bylo možné zajistit preventivní ochranu, například ve formě upozornění na změnu hesla, nebo pokud jde o zapamatování si hesel, tak lze využít nějakou mechanickou pomůcku nebo schránku, kam bude možné hesla uschovat.

Otázka č. 23: Využíváte v rámci ochrany domu/bytu nějaká preventivní opatření?

Tato otázka již přímo poukazuje na to, jaká preventivní opatření lze využít za účelem ochrany soukromí. Zajímá nás především, zda některé z uvedených preventivních opatření respondenti skutečné využívají a případně mohou navrhnout, co je z jejich zkušenosti vhodné. Cílem je zjistit současnou situaci domácností v rámci zajištění preventivní ochrany a to především fyzickou cestou.



Graf 24: Preventivní opatření v rámci ochrany domu nebo bytu [vlastní zdroj]

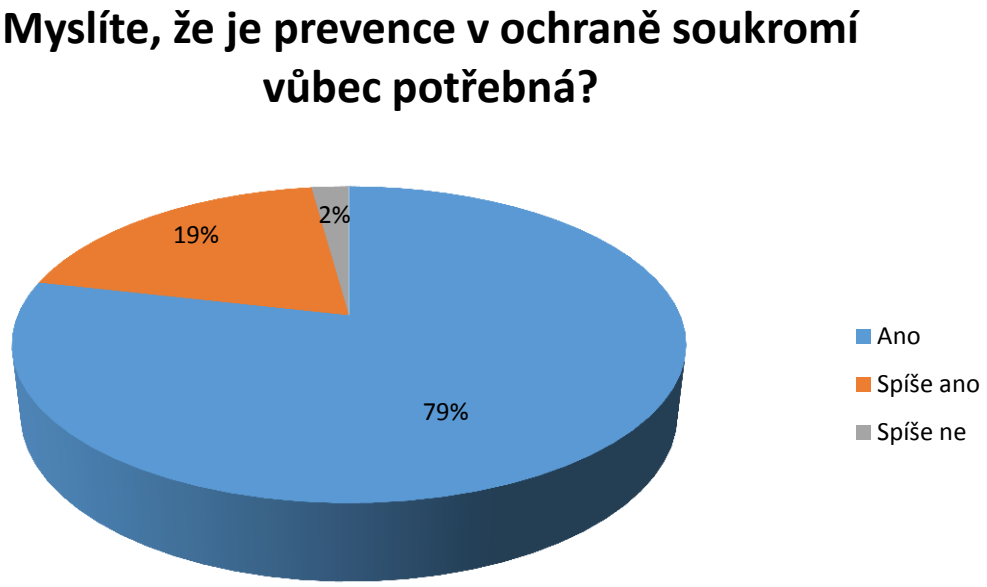
U této otázky bylo možné zvolit více odpovědí. Odpovídající nejčastěji volili možnost bezpečnostních dveří 29 %, ať už z toho důvodu, že například žijí v bytě a jinou ochranu tedy nemohou plně využít nebo z důvodu, že se jim třeba zdá nejdostupnější.

Dále byla nejčastější odpověď s 30 % - oplocení popřípadě zeď, která může mít funkci neprůhlednosti, resp. nepřehlednosti přístupu ke zvolenému objektu. Dalším velmi častým způsobem ochrany je pes, popřípadě jiné zvíře určené k ochraně majetku/soukromí, které má za úkol odstrašit případného pachatele. V neposlední řadě se zde objevovala odpověď, týkající se zabezpečení ve formě kamerového nebo jiného zabezpečovacího systému.

Zhruba 6 % dotazovaných označilo možnost nevyužívání žádných preventivních opatření a zbylých 5 % zmínilo vlastní odpověď, kterou bylo nejčastěji bezpečnostní zámek a v jednom případě dokonce střelná zbraň.

Otázka č. 24: Myslíte, že je prevence v ochraně soukromí vůbec potřebná?

Otázka týkající se vnímání prevence v ochraně soukromí. Cílem bylo zjistit, jak respondenti roli prevence chápou a jestli jí považují za důležitou.



Graf 25: Důležitost prevence v ochraně soukromí [vlastní zdroj]

Celkem 79 % respondentů odpovědělo, že je pro ně prevence v ochraně soukromí důležitá a 19 % odpovědělo, že je pro ně prevence spíše důležitá. Celkem tedy 137 respondentů považuje prevenci v ochraně soukromí za důležitou. Pouhá 2 % dotazovaných nepřisuzuje prevenci v ochraně soukromí žádnou váhu. Toto zjištění je velmi důležité, protože bez něj by závěry této práce mohli být zbytečné a preventivní opatření, která budeme navrhovat, by nemusela být nikomu užitečná.

Otázka č. 25: Vyjmenujte tři klíčová opatření, která z hlediska prevence považujete za klíčové.

Poslední tři otázky dotazníku, tzn. otázky 25. – 27. byly volně položené otázky k zamyšlení, na které bylo možné odpovídat pouze za pomocí vypsání krátké odpovědi. Cílem této otázky bylo zjistit, co respondenti vědí nebo popřípadě zjistili o preventivních opatřeních. Mezi nejčastější odpovědi patřily především: silné heslo, kontrola vyplňování údajů, silný antivirový program, nesdílení fotek a polohy.

Do fyzické části preventivních opatření patřilo především: vhodné dveře a zámek, nebudit zájem veřejnosti, vzdělávání, nenechávat věci bez dozoru. V tabulce č. 6 jsou uvedeny některé odpovědi respondentů.

Tab. 6: Klíčová opatření podle respondentů [vlastní zdroj]

Zajímavé odpovědi a myšlenky respondentů
Dbát na anonymitu, být vždy opatrný, vyhýbat se cizím lidem - nepřidávat např. na fb do přátel, koho neznám osobně, nesdílet s ostatními moc ze svého soukromí.
Nevyplňovat osobní údaje (hesla apod.), neotevírat spamové e-maily, dávat si pozor, kde a co potvrzujeme.
Edukace o důležitosti ochrany soukromí; bdělost a čtení (nenechat se napálit podvodným e-mailem); vytvářet kvalitní hesla.
Neuveřejňovat své osobní a citlivé informace, nenakupovat kartou na pochybných stránkách, neposkytovat intimní fotky neznámým lidem.
Nenechávat věci a údaje bez dozoru, používat omezování soukromí na sítích apod., zamykat dveře, nechlubit se veřejně majetkem.
Informovanost, znalost rizik a možností jejich předcházení, vyhýbat se rizikovým a nedůvěryhodným webům, e-shopům, nabídkám.
Komplikovaná hesla, nedůvěra vůči internetu a cizím lidem, zdravý selský rozum.
Uvědomovat si své soukromí, cítit hodnotu sebe sama.
Opatrnost, kontrola, pozornost.
Neukládat si na počítači údaje k platební kartě, pečlivě si vybírat, kde povolím údaje o poloze, nestahovat soubory na pofidérních stránkách.

Nevyplňovat citlivé údaje na neověřené stránky (např. číslo karty bez šifrovaného připojení), nerozklikávat podezřelé odkazy, používat bezpečná hesla.

Na základě odpovědí zmíněných v tabulce č. 6 je možné potvrdit, že lidé si důležitost svého soukromí uvědomují, jsou schopni o něm přemýšlet a na závěr si i odpovědět formou relevantních preventivních opatření.

Dále je evidentní, že lidé své soukromí často spojují s pohybem na internetu a častokrát vědí, jak snižovat riziko napadení, resp. ztráty soukromí a osobních údajů. V některých z odpovědí uvedených v tabulce č. 6 je možné vypozorovat, že by šli možná respondenti rádi jinou cestou a nechtějí své osobní údaje dávat k dispozici cizím společnostem, ale bohužel jim to dnešní doba ani neumožňuje.

Otázka č. 26: V životech některých známých osobností hraje prevence v ochraně soukromí velkou roli. Proč myslíte, že tomu tak je?

Tato otázka byla malinko zavádějící a měla respondenty přimět k zamyšlení, proč si vlastně celebrity chrání své soukromí a zda by to „obyčejní lidé“ neměli dělat také.

Odpovědí byl v tomto případě nejčastěji stalking, ať už ze strany fanoušků nebo také novinářů. Nicméně důležité také bylo, že někteří odpovídající zmínili, že tato prevence vede také k ochraně ostatních členů rodiny, majetku, obydlí a především zdraví.

Tab. 7: Prevence v ochraně soukromí u známých osobností podle respondentů [vlastní zdroj]

Zajímavé odpovědi a myšlenky respondentů
Rozumí tomu, že osobní data/údaje jsou jejich největším aktivem.
Osobní informace v nesprávných rukou mohou velice ublížit celé rodině, ať už vyhrožováním, vydíráním, napadením apod.
Při narušení soukromí se mohou dostat do skutečného ohrožení, může jim být narušena kariéra, ale také osobní bezpečnost (stalking, vloupání,..).
Kdyby o nich unikla nějaká citlivá informace, rychle by se šířila - protože jsou známí.
Ze stejného důvodu jako u Vás nebo u mě, jen je to u nich ještě znásobeno tím, že se o ně zajímá velké množství lidí.
Protože soukromé údaje známých osobností jsou zpeněžitelné. Útoků na jejich soukromí je tedy

více. Také pravděpodobně nechtějí, aby všechny detaily o jejich životě věděli a rozebírali fanoušci.
Každý chce mať súkromie alebo aspoň isté časti neprístupné svetu.
Bezpečnost jejich i celé rodiny, ochrana majetku, snaha žít osobní život jako "normální" lidé.
Na jejich ukradené identitě se dá dobře vydělat.
Jinak už by nemohli žít normální život. Byli by veřejným majetkem.
Občas si myslíme, že pokud je někdo veřejná osoba, stává se automaticky i majetkem veřejnosti - pomlouváme, rozkazujeme, jsme znechuceni, když naše panenka netančí.
Známé osobnosti a jejich soukromí se dají lehce zneužít, například k propagaci falešných účtů a reklam.
Protože by jinak lidi začali chodit na jejich adresu a obtěžovat je nebo i jejich rodinu. Protože by neměli klid kdykoli by vyšli na veřejnost.
Prevence krádeže identity, stalking, vyhnout se bulvárním článkům, krádež majetku, ohrožení rodiny a blízkých osob.

Řada lidí má pocit, že otázka ochrany soukromí se týká pouze celebrit a veřejně známých osobností, opak je však pravdou. Samozřejmě, že zájem a oči veřejnosti se k těmto lidem upínají daleko častěji, to ale neznamená, že pro běžného člověka by soukromí nemělo být důležité. I přesto, že člověk nemusí mít na svém bankovním účtu velké obnosy peněz, může se stát obětí stalkingu nebo kopírování účtu na sociálních sítích. Krádež financí totiž není jedinou motivací útočníků.

Proto je potřeba zajistit alespoň nutnou část preventivních opatření a nemusí se jednat o finančně náročná opatření. Stačí být obezřetný, pročítat souhlasy se zpracováním osobních údajů, nepředávat nikomu heslo k účtům. Těmito základními pravidly se riziko újmy na osobním soukromí a finanční ztrátě výrazně sníží.

Otázka č. 27: Jakou roli podle Vás soukromí v této době získává a jak na něj, třeba i díky tomuto dotazníku nahlížíte?

Podobně jako u otázky č. 26 bylo důležité uvědomění si důležitosti soukromí a s tím spojených preventivních opatření. Již podle předchozích odpovědí je jasné, že si důležitou roli soukromí většina odpovídajících uvědomuje. Zároveň ale také cítí, že se ze všech stran

někdo snaží jejich soukromí narušit. V rámci odpovědí byl několikrát zmíněn tzv. obchod s informacemi, který neustále zvyšuje svou hodnotu.

Bohužel už může být na některé kroky vedoucí k ochraně soukromí pozdě a část respondentů to ve svých odpovědích také zmínila. Na druhou stranu některé odpovědi obsahují myšlenky o nevyčíslitelné hodnotě soukromí, a proto je nutné pracovat na preventivních opatřeních kvůli zmírnění negativního dopadu na jednotlivá aktiva.

Tab. 8: Role soukromí podle respondentů [vlastní zdroj]

Zajímavé odpovědi a myšlenky respondentů
Soukromí si vážím a v dnešní době si lidé dávají větší pozor ohledně toho, co přidávají na internet.
Lidé si neuvědomují, co vše na sociálních sítích sdílí, jsou dost často naivní a důvěřiví, nemají povědomí o falešných profilech a zprávách, nehlídají si své soukromí.
V dnešní době si většina lidí důležitost soukromí vůbec neuvědomuje, přidává vše na sociální sítě atd.
Obecně je to dnes stále větší vzácnost. Každý mladý člověk sdílí na sociálních sítích i úplné blbosti, jen aby na sebe upoutal pozornost, nebo se vyšvihl před kamarády.
Je to dôležitá vec v živote každého moderného človeka, ktorá je každodenne ohrozovaná a třeba ju chrániť.
Stále stejně - je to privátní prostor, kde mohu být sama sebou, bez obav z interpretací těch, kteří by do něj rádi nahlédli.
Je to něco, co je diskutováno stále více, ale nikdo s tím nic nedělá.
Soukromí je cenná komodita, firmy si kupují informace, aby mohly vhodněji nabízet produkty - zvýšit své zisky apod.
Je to komodita - firmy odkupují informace, aby vhodně nabízely produkty a více prodaly.
Mám pocit, že si lidé začínají více uvědomovat, že za sociální sítě (zadarmo) vlastně platí svými osobními údaji.
Na mladého člověka jsem velký skeptik, raději platím dobírkou, nemám Facebook, bojím se požívat hlasové vyhledávání a podobné věci.
Soukromí je v této době nedoceněné a brzy na to doplatí další generace, díky tomuto dotazníku mám lepší pocit, jsem ráda, že nad tímto tématem nepřemýšlím jen já.
Soukromí je jedna z nejdůležitějších věcí v životě.

Veškeré informace a pohodlnost, které nabízí internet a technologie je po zaplacení pořizovací ceny, dále "financováno" výměnou informací ze svého soukromí, zjištění nákupního chování a následných cílených marketingových kampaní na uživatele technologie.

Lidé si uvědomují důležitost soukromí a nutnou potřebu zavedení preventivních opatření. Velká část dotazovaných byla toho názoru, že v dnešní době nic není zadarmo a už vůbec to neplatí na internetu, kde se v podstatě neplatí penězi, ale právě osobními údaji.

V některých případech však lidé sdílí informace, fotografie a údaje o poloze naprosto dobrovolně, aniž by je k tomu někdo pobízel, resp. mají na výběr, zda tyto údaje na dané webové stránky umístí a skutečně se tak děje. Ve většině případů se jedná o mladší generace, které pochopitelně nad touto problematikou nepřemýšlí, ale preventivním opatřením by mohlo být zavedení jakési osvěty do škol. Forma různých školení podle věkových kategorií, které by děti učila, jak se na internetu chovat.

6 PŘÍPADOVÁ STUDIE - MODEL HYPOTETICKÉHO SOUKROMÍ

V této kapitole bude vytvořen model hypotetického soukromí, odpovídající tří členné rodině, která žije v rodinném domě. Půjde především o označení aktivit jednotlivých členů domácnosti, které by mohly vést k ohrožení. Zároveň bude nutné posoudit bezpečnost místa bydliště a samotnou ochranu objektu.

Je nutné zmínit, že rodina, kterou budeme popisovat, má zájem být chráněná a soukromí je pro jednotlivé členy velmi důležité. Důležitým aspektem může být skutečnost, že narušení soukromí by mohlo vést k finanční ztrátě, ale také ke ztrátě dobrého jména nebo dokonce fyzické újmě jednotlivých členů domácnosti. V další části této kapitoly bude návrh ochrany soukromí a následně vícekriteriální zhodnocení, kterým jednotlivé návrhy ochrany posoudíme.

6.1 Popis referenčního objektu

V rámci modelu hypotetického soukromí budeme popisovat tří členy domácnosti a jejich zvyky a činnosti. Dále bude popsáno umístění bydliště, jeho okolí a rozložení samotného objektu.

6.1.1 Popis domácnosti

Otec

- pracující, jako vedoucí prodeje ojetých automobilů v autosalonu, jež vlastní jeho rodiče, aby mohl tuto práci vykonávat, dokončil středoškolské vzdělání (žádnými dalšími kurzy a vzděláním nedisponuje),

- ke své práci využívá mobilní telefon a počítač, ale tyto k soukromím účelem nepoužívá, osobní mobilní telefon využívá pouze na textové zprávy a volání,

- doma neuchovává žádné peníze, ale má zde cenné papíry, smlouvy o vlastnictví domu a automobilů.

Matka

- pracuje jako pojišťovací specialista, má vystudovanou střední školu se zaměřením na veřejnou správu (žádné další vzdělaní, ani kurzy neabsolvovala),

- ke své práci využívá mobilní telefon i notebook a často pracuje z domova,

- občasně využívá notebook také ke kontrole financí přes internetové bankovnictví a kontrole e-mailů.

Syn

- studuje na základní škole, má 14 let,

- pravidelně využívá mobilní telefon a také notebook, obojí k přístupu na sociální sítě a hraní online her.

Jejich dům v dané lokalitě je odhadován na tržní cenu ve výši 8 milionů Kč. Dále rodina disponuje dvěma auty v celkové hodnotě 2,5 milionu Kč. Oba rodiče dohromady mají čistý měsíční příjem v hodnotě přesahující 100 tisíc Kč.

Na první pohled se může zdát, že se jedná o běžnou rodinu, protože žádný člen nenosí drahé oblečení a v případě matky, ani drahé šperky a doplňky. Jinými slovy, se mezi ostatními snadno ztratí, ale na jejich domě a automobilech, které před ním stojí, je jejich nadprůměrná finanční situace evidentní.

6.1.2 Popis domu a jeho umístění

Obydlí, ve kterém rodina žije je dvoupatrový dům se zahradou s rozlohou okolo 1000 m^2.

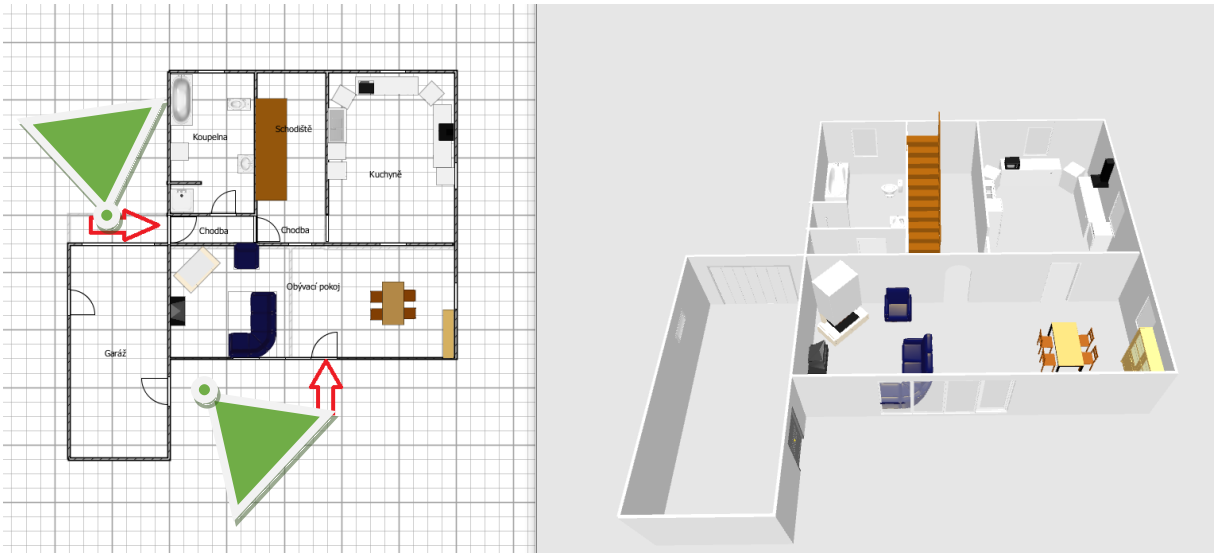
Dům se nachází ve vesnici s názvem Blatec. Tato obec je vzdálená přibližně 10 km od krajského města Olomouc a bydlí v ní okolo 650 obyvatel. V ulici, na niž dům stojí, je šest řadových domů a takovýchto ulic je na místě několik za sebou. K přiblížení umístění domu slouží obrázek č. 5, který zachycuje z leteckého pohledu dům a okolní oblast.

Obr. 5: Letecký pohled na dům a jeho okolí [37]

Z obrázku č. 5 je možné rozpoznat, že dům je na kraji řadové zástavby a obklopují jej dvě silnice, přičemž obě jsou vedlejší a projedou po nich zhruba dvě auta za hodinu. Dále je nutné doplnit, že ze severní a západní strany je dům oplocen betonovou zdí do výšky tří metrů. Z jižní strany, která je společná se sousedem, je dům oplocen 1,8 m vysokým pletivem a stromy a z přední tedy východní strany je 1,2 m vysoký plot z betonových pilířů a dřevěné výplně.

V neposlední řadě je důležité zmínit, že z přední strany vede k domu pojezdová brána a ze severní strany je brána dvoukřídlá, která vede přímo na zahradu. Na závěr je nutno říci, že se na zahradě nachází také kotec se psem. Konkrétně se jedná o plemeno německého ovčáka dospělého vzrůstu.

Pro bližší popis interiéru domu nám poslouží program 3D Sweethome, ve kterém je zpracován nákres obsahující popis jednotlivých místností.

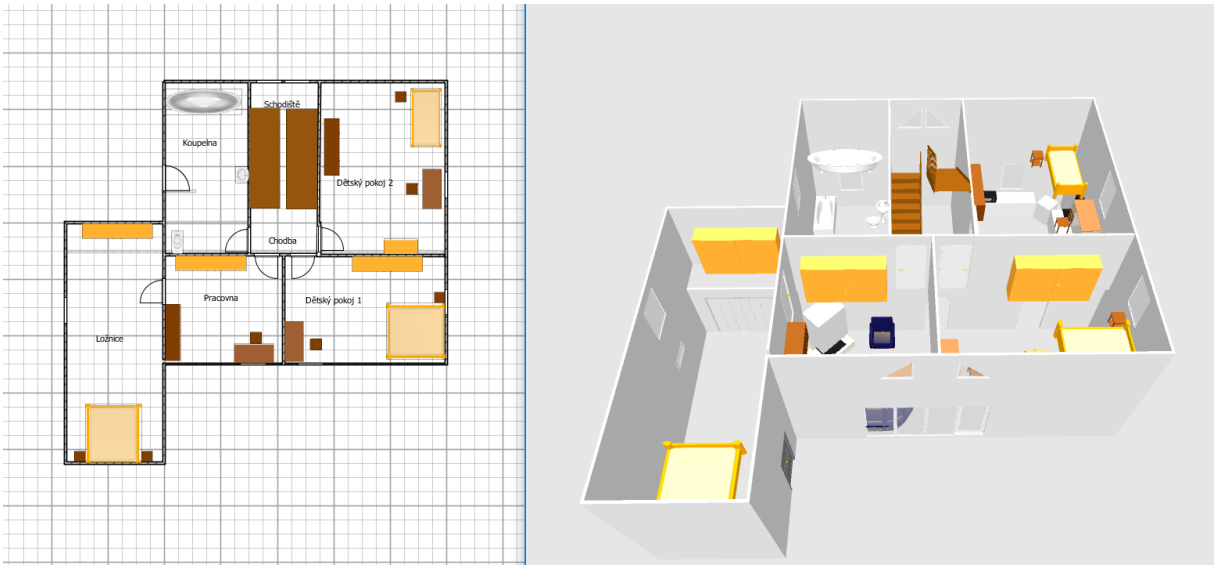


Obr. 6: Půdorys přízemí domu [vlastní zdroj]

Na obrázku č. 6 je možné vidět půdorys přízemí popisovaného domu. V levé části je 2D nákres, který zobrazuje především názvy místností, a červené šipky označují vstupy do domu. Jeden vstup je z východní strany, přes posuvnou bránu a to konkrétně pomocí vchodových dveří. Druhý vstup je ze zahrady přes balkonové dveře s trojitými skly. I když je součástí domu, tak se se samotnými vstupy nachází v přízemí také garáž. Dále je součástí přízemí také koupelna, kuchyně a obývací pokoj.

Ve venkovní části jsou zelenou barvou také označeny spínače, které spínají světla pomocí PIR detektoru. U obou spínačů je dosah snímání 5 metrů a pozorovací úhel 90° a zabírají tím tak celou oblast možného přístupu k objektu. V přední části má světlo tentýž dosah jako spínače, tedy 5 metrů a dosahuje tak ke všem rohům, ze kterých by se mohl případný útočník do objektu vydat, ale v zadní části je dosah světla až 15 m, dosahuje tedy k okrajům pozemku. Podobně jako v přední části domu tedy světlo dosahuje do vzdálenosti a s úhlem pod kterým by byl případný příchod útočníka viditelný.

V pravé části obrázku č. 6 je vidět 3D model jednotlivých místností. Je zde vidět například vybavení těchto místností, což je s větší finanční hodnotou spíše elektronika, například televize a kuchyňské spotřebiče, ale především jsou zde vidět také okna a dveře, tedy eventuální další vstupy do domu a cesty jednotlivými pokoji.



Obr. 7: Půdorys prvního patra domu [vlastní zdroj]

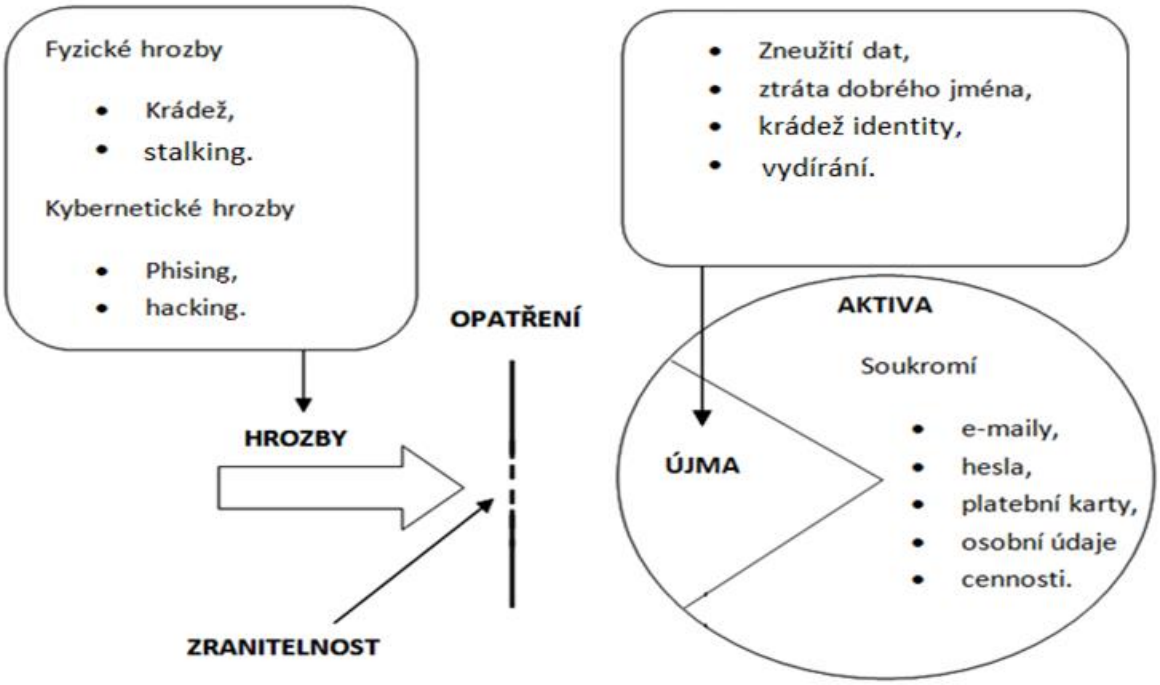
Na obrázku č. 7 je možné vidět půdorys prvního patra domu, kde se po výstupu schodů nacházíme na chodbě, která nás může zavést do dětského pokoje po levé straně nebo do dalšího dětského pokoje přímo naproti schodišti. V těchto místnostech tráví nejvíce času syn a to, jak již bylo zmíněno hrou na notebooku nebo využíváním sociálních sítí.

Vlevo je vstup do druhé koupelny a vedle se nachází vstup do pracovny, kde nejčastěji tráví čas matka, která využívá notebook. Z pracovny je dále vstup do ložnice, kde se mimo jiné nachází skříň se smlouvami a důležitými dokumenty.

V domě není žádný kamerový systém, ani speciální zabezpečení oken. Na druhou stranu mimo automobily, se v domě nenachází nic s větší finanční hodnotou. Nutno podotknout, že důležitá je však v našem případě ochrana soukromí.

6.1.3 Bezpečnostní model

Na obrázku č. 8 je znázorněn bezpečnostní model zaměřený na ochranu osob domácnosti a jejich soukromí. Model zahrnuje nejen aktiva, ale naznačuje také, jaké hrozby mohou domácnost poškozovat.



Obr. 8: Bezpečnostní model [vlastní zdroj]

6.2 Hrozby a rizika referenčního objektu

V následující podkapitole budeme popisovat hrozby, které mohou působit na referenční objekt z pohledu soukromí. Pro jednotlivé hrozby budeme později navrhovat adekvátní preventivní opatření, které by měly vést ke snížení zranitelnosti.

6.2.1 Fyzické hrozby

V rámci prevence v ochraně soukromí, je nutné vyjmenovat hrozby, které mohou působit na model hypotetického soukromí. Nejprve se budeme zabývat hrozbami fyzickými a v další podkapitole budou zmíněny hrozby kybernetické.

Vyloupení domu

Vyloupení domu je nebezpečné ze dvou důvodů. Může dojít ke krádeži cenností, tzn. věcí, které mají nějakou finanční nebo v některých případech i emocionální hodnotu, ale zároveň může dojít ke krádeži informací – různých smluv a dokumentů, ale také zařízení, která mohou tyto informace obsahovat.

Zařízení, která v tomto konkrétním případě mohou být odcizena, jsou notebooky ve druhém patře a to konkrétně v dětském pokoji a pracovně. Cennosti a dokumenty týkající se osobních údajů a informací o rodině jsou také ve druhém patře a to konkrétně v ložnici.

V rámci přístupu na pozemek je pro útočníka nejsnadnější možná cesta přes bránu vedoucí do zahrady nebo přes nižší plot nacházející se v přední části pozemku. Vzhledem k tomu, že cesta z přední části je více využívaná a vede k předním dveřím, které jsou konstrukčně silnější, bude zřejmě pro útočníka snadnější využít zadní a méně přehlednou cestu vedoucí k balkonovým dveřím. Největší riziko ohrožení je tedy přes bránu, která je za objektem v zadní části pozemku.

Krádež dokladů

V objektu se nachází různé smlouvy, ale také rodné listy a pasy. Tyto dokumenty nesou informace o osobních údajích všech členů domácnosti a jejich zneužití by mohlo vést ke ztrátě financí a poškození dobrého jména. Doklady a listiny obsahující identifikační znaky osob jsou jednoznačně určeny k ochraně a jejich zcizení, popřípadě falšování vede ke ztrátě soukromí.

V rámci krádeže dokladů jsou nejznámější případy spojené s půjčováním peněz od různých finančních institucí. Obzvlášť v dnešní době, kde se provádí vše elektronicky, tedy bez osobního kontaktu s bankéřem, který úvěr poskytuje, je žádost o takovouto půjčka otázkou několika minut. Stačí zadat jméno, rodné číslo nebo datum narození a bydliště. V některých případech bankovní instituce požadují zaslat okopírovaný doklad. Poté, co prověří schopnost splácet, je možné částku připsat na účet. Podle některých bankovních portálů, je tímto způsobem možné získat půjčku do 100 tisíc Kč.

Krádež notebooku a jeho zneužití

V této kapitole již bylo zmíněno, že se v objektu nachází dva notebooky. Pomocí krádeže těchto zařízení je možné se dostat k informacím, ať už osobního charakteru, ale také fotografií, které mohou vést i k vydírání nebo ztrátě dobrého jména.

V zařízení bývají velice často uložená hesla a přístupy do různých aplikací, ale také e-mailových schránek. Nebývá vyloučeno, že je možné se dostat také k elektronickému bankovnictví. V rámci modelu hypotetického soukromí je matka přihlášena, jak do databáze klientů se kterými pracuje, tak do osobního e-mailového účtu. Syn je přihlášen k účtu na sociálních sítích. Oba členové domácnosti používají automatické vyplňování přihlašovacích údajů, a proto se k jejich údajům potenciální útočník snadno dostane.

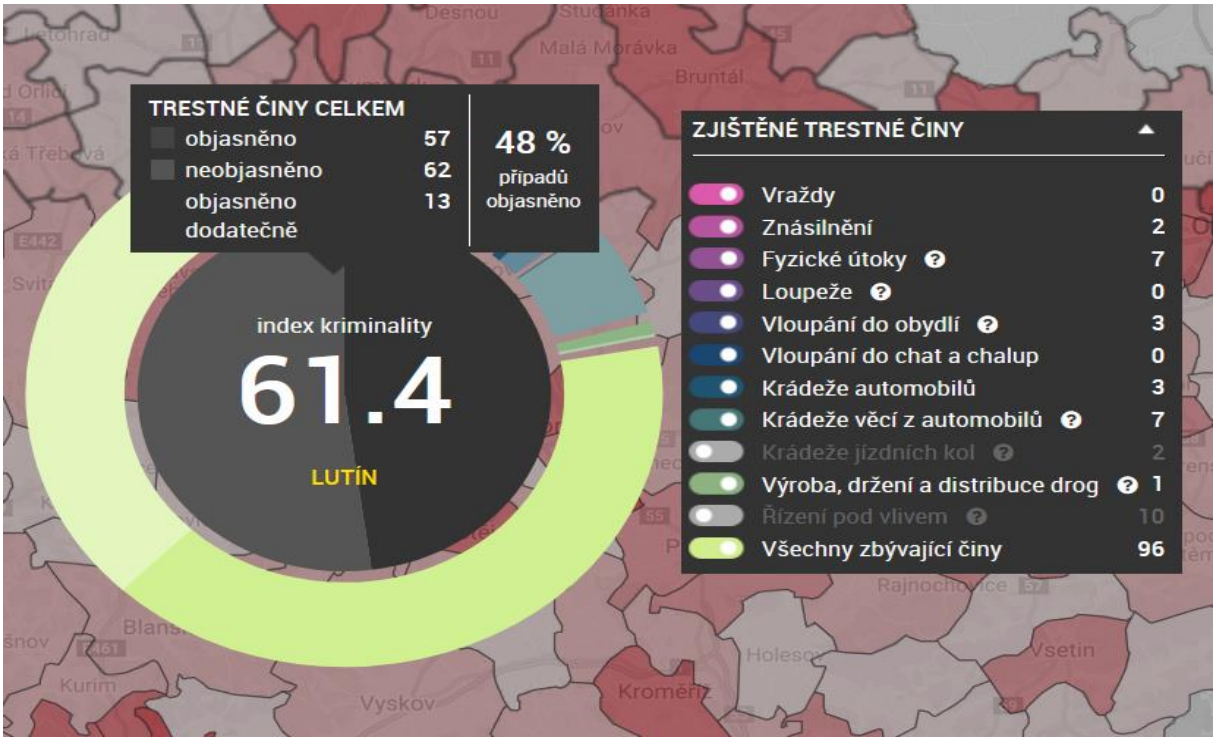
Stalking

U stalkingu se jedná o narušení soukromí, kdy se jeden ze členů rodiny může stát terčem sledování. Nejčastěji je útočníkem osoba, kterou oběť zná a která by z informací mohla mít nějaký prospěch. Často se může jednat o obchodního partnera, bývalou partnerku nebo dokonce kamaráda.

Důležitým aspektem stalkingu se stává to, že útočník poznává denní režim člověka, kterého sleduje a zjistí tak, kam chodí, co dělá a případně jestli mají tyto činnosti a návštěvy nějakou pravidelnost. Může se také stát, že si útočník potenciální oběť fotí a může tak zdokumentovat důležité části soukromí.

U stalkingu se většinou jedná o dlouhodobější záležitost, útočník musí vynaložit čas a úsilí, aby oběť podrobněji poznal. Na základě shromážděných informací dochází k různým výhružkám a případným fyzickým kontaktům. Motivací mohou být peníze, ale také pouze pocit nadvlády nad sledovanou osobou.

V tomto konkrétním případě by mohl mít útočník především finanční motivaci, ale bohužel dochází také k psychické újmě oběti. Nejnáchylnějším členem domácnosti by byl určitě syn. Ten má poměrně pravidelný režim, protože chodí do školy s předepsaným rozvrhem, zároveň je díky nízkému věku fyzicky nejméně zdatný a díky využívání sociálních sítí snadno vysledovatelný. Obrázek č. 9 zobrazuje mapu kriminality, kterou pravidelně upravuje a aktualizuje Policie ČR a je na něm vidět, jaké byly zjištěny trestné činy v okolí obydlí.



Obr. 9: Mapa kriminality - Blatec [27]

Na základě obrázku č. 9 se pokusíme přiblížit situaci týkající se kriminality v místě bydliště. Obec Blatec spadá pod obvodní oddělení obce Lutín. Bohužel umí mapa kriminality vyhodnotit trestné činy pouze na úrovni obvodních oddělení, tzn., nemáme k dispozici data o kriminalitě přímo v námi požadované obci. Zvolené období, ve kterém chceme kriminalitu pozorovat, je od září 2019 do září 2020, tedy přesně jednoho roku.

Celkem bylo za období jednoho roku zaznamenáno 119 trestných činů, z nichž bylo 48 % objasněno. Index kriminality na obrázku č. 9 znamená, kolik bylo trestných činů na 10 tis. obyvatel. Obec Blatec má okolo 650 obyvatel, takže podle přepočtu by to znamenalo, že se za rok staly na území této obce čtyři trestné činy. Lze tedy říci, že je riziko vloupání či krádeže velmi nízké, avšak dojít k němu může.

6.2.2 Kybernetické hrozby

Kybernetické hrozby se budou týkat především syna a matky. Jak již bylo naznačeno v předešlé kapitole, půjde především o ohrožení syna na sociálních sítích a matky, která využívá podobně jako syn ukládání hesel, ale také e-mailového klienta. Nevýhodou může být také využití notebooku k účelům soukromým a zároveň pracovním.

Phishing

V tomto případě bude obětí phishingu především matka, která ke své práci, ale i ve svém soukromí využívá e-mailovou schránku. Do ní jí mohou chodit zprávy s nedůvěryhodným obsahem. Každému člověku někdy takový e-mail může přijít, je však důležité všímat si, kdo zprávu odeslal, jakým písmem a s jakým pravopisem je zpráva napsána.

Phishing může vést k předání informací o bankovních účtech, resp. kreditní kartě nebo internetovému bankovnictví. Cílem útoku je zjištění citlivých dat ze soukromí, je tedy nástrojem k dalšímu zneužití, ať už finančnímu nebo za účelem dalšího vydírání.

Hacking

Pokud je pachatel zdatný v práci s počítačem, může dojít také na hacking. U hackingu může dojít k vážnému zásahu do soukromí a pachatel se může dostat především k fotografiím, heslům, ale také přístupům do různých účtů nebo také internetového bankovnictví.

V tomto případě by mohlo dojít k neoprávněnému vstupu do soukromé i pracovní e-mailové schránky, a také do internetového bankovnictví. Dále k nabourání do sociálního profilu a jeho zneužití a poškození dobrého jméno, jak matky, tak syna.

Kyberstalking

Podobně jako u běžného fyzického stalkingu, dochází u kyberstalkingu ke sledování informací o poloze oběti, sledování fotografií, popřípadě zjišťování jmen blízkých osob, což vede ke spoustě podnětů k vydírání.

U kyberstalkingu se nejčastěji k vyhledání informací o oběti používají sociální sítě. V našem případě je tedy největší hrozbou zneužití sociálního profilu syna, který může mít na svém profilu informace o bydlišti, ale také o místech, která navštěvuje (např. název školy). Dále se na jeho profilu mohou vyskytovat fotografie, které obsahují bližší informace o rozmístění pokojů a předmětů v domě nebo o konkrétním zabezpečení.

Neméně běžnou aktivitou sociálních profilů může být sdílení polohy, tedy informací o aktuální poloze případné sledované osoby. To může vést k fyzickému sledování a tím i k fyzické újmě.

Vydírání

Sdílením informací a fotografií může dojít k tomu, že si pachatel o oběti nashromáždí dostatek podkladů k vydírání. U vydírání je nejčastějším motivem finanční obohacení, ale dochází také k psychické újmě oběti, což může být daleko závažnější. Nátlak, který dokáže pachatel vyvinout, závisí na míře zjištěných informací. Pokud by došlo na informace například o nevěře nebo na informace obsažené v důležitém obchodním dokumentu, tak by u oběti se slabší psychickou odolností mohlo dojít až k myšlenkám na sebevraždu.

U modelu hypotetického soukromí mohou být veřejně dostupné informace o členech domácnosti spíše všeobecného charakteru. Jediná hrozba by mohla plynout pouze z využívání sociálních sítí a zde nasdíleného obsahu.

Krádež identity

Pachatel může shromažďovat informace, které najde na internetu a tím si vytvoří kompletní přehled o osobních údajích oběti. Díky takto nashromážděným údajům může pachatel například požádat o půjčku nebo dokonce vytvořit falešné doklady identity poškozené osoby.

Tyto údaje nebo doklady mohou pachatelé vytvořit, jak již bylo zmíněno k nelegální činnosti. Za účelem obohatit se, ale také se mohou dostat do organizací, kam by se jinak nedostali, například na pracoviště obětí. V tomto případě, může jít konkrétně o infiltraci zpráv a dokumentů, které přichází na pracovní e-mail matky a přes ně se dostat k finančním prostředkům celé rodiny.

6.3 Varianty ochrany referenčního objektu

V této podkapitole jsou zpracovány návrhy opatření ke zlepšení ochrany referenčního objektu z pohledu ochrany soukromí. Vytvoříme dvě varianty zvýšení ochrany, konkrétně se bude jednat o konzervativní a sofistikovanou variantu.

U konzervativní varianty ochrany půjde o elementární návrhy, které povedou ke zvýšení zabezpečení, ale zároveň nebudou příliš nákladné a složité. Budeme se snažit vybírat taková opatření, která budou snadno aplikovatelná.

U sofistikované varianty půjde o cílená opatření, která budou mít vyšší míru ochrany, ale zároveň mohou být nákladnější a složitější může být také jejich udržitelnost a

aplikovatelnost. V závěru obě varianty vyhodnotíme a vybereme tu, která je pro hypotetický model ochrany soukromí vhodnější.

Tabulka č. 9 popisuje jednotlivé hrozby, u kterých jsou uvedena vždy dvě řešení a to v konzervativní a sofistikované variantě. Zároveň je zde uvedena také stávající ochrana modelu hypotetického soukromí.

Tab. 9: Návrhy jednotlivých variant ochrany [vlastní zdroj]

Hrozba	**Stávající ochrana**	**Konzervativní ochrana**	**Sofistikovaná ochrana**
Vyloupení domu	Osvětlení s PIR čidlem.	Maketa kamery.	Poplachový zabezpečovací a tísňový systém, kamerový systém.
Krádež notebooku a jeho zneužiti	Žádná ochrana, bez hesla s automatickým doplněním přihlašovacích údajů.	Umístění na méně dostupných místech, zabezpečení silným heslem.	Zakoupení softwaru na ochranu zařízení, zámek zařízení (mechanický, biometrický)
Stalking	Bez ochrany.	Obezřetnost.	Zastínění oplocení.
Phishing	Běžné užívání, bez ochrany.	Číst důkladně e-maily, nepoužívat neznámý odkaz	Zakoupení softwaru - filtrování nevyžádaných zpráv.
Hacking	Bez hesel, bez ochrany.	Zabezpečení silným heslem, nepřipojovat se k cizím sítím.	Vzdělaní v IT, odborná konzultace k tématu zabezpečení.
Kyber - stalking	Bez kontroly.	Kontrola sdílení fotek a informací.	Konzultace s odborníkem.
Krádež identity	Bez kontroly.	Kontrola zveřejněných údajů.	Konzultace s odborníkem, kontrola digitálních stop.

6.4 Zhodnocení ochrany, výběr varianty

Jednotlivé návrhy jsou porovnány pomocí metody vícekriteriálního hodnocení. Vícekriteriální hodnocení je vhodné, protože je nutné zahrnout důležitost jednotlivých kritérií a zároveň je nutné zvlášť vyhodnotit, jak jsou opatření účinná a jak jsou těmito kritérii ovlivněna. Mezi kritéria, která budou hodnocena, patří nákladnost, udržitelnost a míra zabezpečení.

Tabulka č. 10 vyjadřuje, jakou prioritu kritéria mají. Nejdůležitější je pro náš model míra zabezpečení, protože rodina má jako prioritu ochranu svého soukromí, dále je udržitelnost, tedy jaké úsilí se musí vynaložit, aby mohla daná opatření fungovat a být zavedená. Na závěr je nákladnost, protože finance jsou pro rodinu důležité, ale disponují dostatečnými příjmy, které chtějí primárně využít k ochraně.

Tab. 10: Popis úrovně jednotlivých kritérií [vlastní zdroj]

Číslo	Popis
1.	Míra zabezpečení je silně významnější než udržitelnost.
2.	Udržitelnost je slabě významnější než nákladnost.
3.	Míra zabezpečení je silně významnější než nákladnost.

Pomocí Saatyho matice zapíšeme preference do tabulky a tím vypočítáme jednotlivé váhy předepsaných kritérií.

Tab. 11: Srovnání jednotlivých kritérií [vlastní zdroj]

	Míra zabezpečení	Nákladnost	Udržitelnost	Geom. pr. (G_i)	Váha (v_i)
Míra zabezpečení	1	5	5	2,92	**0,70**
Nákladnost	1/5	1	1/3	0,40	**0,10**
Udržitelnost	1/5	3	1	0,84	**0,20**
∑				**4,17**	**1**

Ke každému návrhu opatření tabulka č. 13 napíšeme, dle tabulky č. 12 hodnotu, která nám bude určovat, jakou mírou, které kritérium na opatření působí. Jednoduše řečeno, jak je které opatření nákladné, udržitelné a jaká je jeho míra zabezpečení.

Tab. 12: Popis úrovně jednotlivých opatření na základě kritérií [vlastní zdroj]

Úroveň	Popis
1	Nízká úroveň zabezpečení, vysoké náklady a těžká udržitelnost
3	Střední úroveň zabezpečení, střední náklady a náročná udržitelnost
5	Vysoká úroveň zabezpečení, nízké náklady a snadná udržitelnost
7	Nejvyšší úroveň zabezpečení, nulové náklady a zanedbatelná udržitelnost

V tabulce č. 13 porovnáme jednotlivá opatření, využitá v rámci konzervativní ochrany. K jednotlivým opatřením uvedeme vždy úroveň podle kritéria a poté také vypočítanou váhu kritérií.

Tab. 13: Ohodnocení opatření v rámci konzervativní ochrany [vlastní zdroj]

Návrh opatření	**Míra zabezpečení**	**Nákladnost**	**Udržitelnost**	**Celkem**
Maketa kamery	1x0,7=0,7	5x0,1=0,5	5x0,2=1	2,2
Umístění na méně dostupných místech, zabezpečení silným heslem	5x0,7=3,5	7x0,1=0,7	3x0,2=0,6	4,8
Obezřetnost	3x0,7=2,1	7x0,1=0,7	1x0,2=0,2	3,0
Číst důkladně e-maily, nepoužívat neznáme odkazy	3x0,7=2,1	7x0,1=0,7	3x0,2=0,6	3,4
Zabezpečení silným heslem, nepřipojovat se k cizím sítím	5x0,7=3,5	7x0,1=0,7	3x0,2=0,6	4,8
Kontrola sdílení fotek a	3x0,7=2,1	7x0,1=0,7	3x0,2=0,6	3,4

informací				
Kontrola zveřejněných údajů	3x0,7=2,1	7x0,1=0,7	3x0,2=0,6	3,4
Součet				**25,0**

V tabulce č. 14 porovnáme jednotlivá opatření, využitá v rámci sofistikované ochrany. K jednotlivým opatřením uvedeme vždy úroveň podle kritéria a poté také váhu kritérií.

Tab. 14: Ohodnocení opatření v rámci sofistikované ochrany[vlastní zdroj]

Návrh opatření	**Míra zabezpečení**	**Nákladnost**	**Udržitelnost**	**Celkem**
Poplachový zabezpečovací a tísňový systém, kamerový systém	7x0,7=4,9	1x0,1=0,1	1x0,2=0,2	5,2
Zakoupení softwaru na ochranu zařízení - anti-theft, zámek zařízení (mechanický, biometrický)	7x0,7=4,9	3x0,1=0,3	1x0,2=0,2	5,4
Zastínění oplocení	5x0,7=3,5	3x0,1=0,3	3x0,2=0,6	4,4
Zakoupení softwaru - filtrování nevyžádaných zpráv	5x0,7=3,5	3x0,1=0,3	3x0,2=0,6	4,4
Vzdělaní v IT, odborná konzultace k tématu zabezpečení	7x0,7=4,9	1x0,1=0,1	1x0,2=0,2	5,2
Konzultace s odborníkem	5x0,7=3,5	1x0,1=0,1	1x0,2=0,2	3,8
Konzultace s odborníkem, kontrola digitálních stop	5x0,7=3,5	1x0,1=0,1	1x0,2=0,2	3,8
Součet				**32,2**

Celkové součty z tabulek č. 13 a č. 14 nám říkají, že sofistikovaná metoda je pro ochranu objektu vhodnější. Jednotlivá preventivní opatření jsou zaměřena především na zabezpečení a vzhledem k tomu, že rodina, kterou chceme chránit, nemusí mít s nákladností a udržitelností přílišné potíže, je metoda sofistikované ochrany lepší variantou. V další kapitole proto budeme podrobněji popisovat preventivní opatření sofistikované ochrany.

7 PREVENTIVNÍ OPATŘENÍ OCHRANY MODELU HYPOTETICKÉHO SOUKROMÍ

V kapitole budou podrobně popsány preventivní opatření ochrany soukromí na základě sofistikované ochrany. Nejprve si rozdělíme opatření podobně jako ve čtvrté kapitole na technická a organizační. A poté budeme specifikovat, jak tato preventivní opatření aplikovat.

7.1 Technická opatření

V této podkapitole se budeme zabývat technickými opatřeními z oblasti prevence, která mají snižovat riziko a dopady v rámci ochrany soukromí.

Technická opatření:

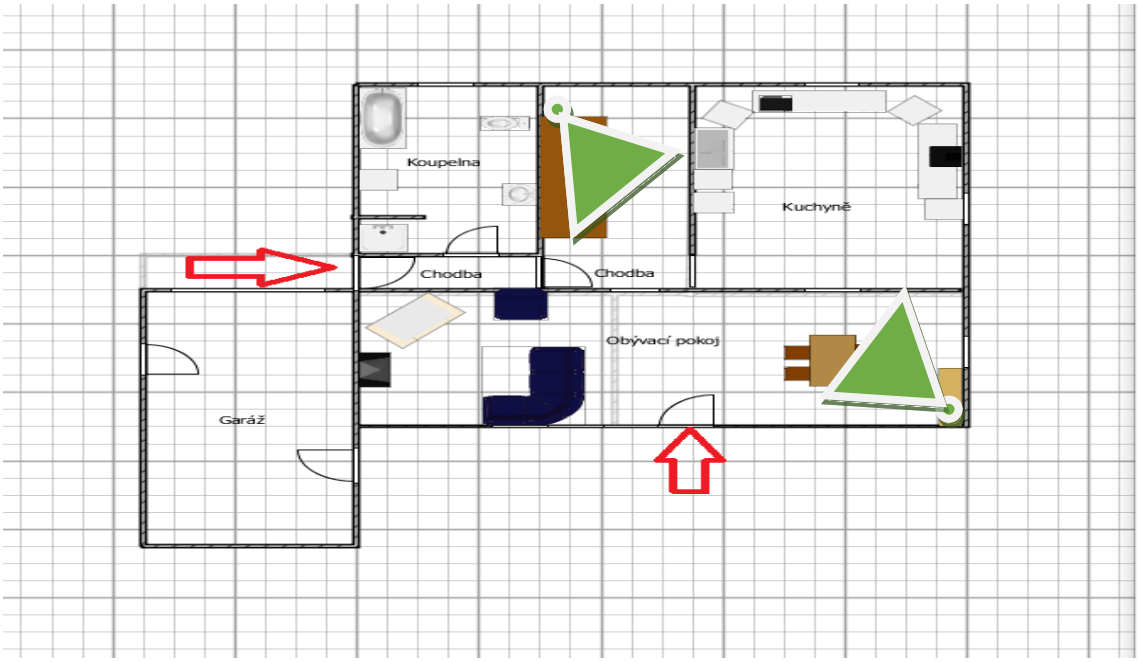
- poplachový zabezpečovací a tísňový systém,
- kamerový systém,
- mechanický zábranný systém,
- zámek proti vniknutí do zařízení,
- software na ochranu počítačových zařízení,
- dvoufázové ověření identity,
- zastínění vnějších prostor obytné zóny,
- zabezpečení cenných dokumentů.

Poplachový zabezpečovací a tísňový systém

Tento systém je určen k detekci přítomnosti, vniknutí nebo pokusu o vniknutí pachatele a následné signalizaci. Tento systém se sestává z ústředny, detektoru narušení a ovládacích periferií (klávesnice, čtečky). Dále jsou součástí také propojovací kabely, ale existují také bezdrátové systémy, ke kterým je však ve většině případů zapotřebí napájení ve formě akumulátorů. A na závěr je součástí signalizační zařízení, které oznamuje narušení bezpečnosti. Důležité je také zmínit, že PZTS je možné připojit na DPPC, což znamená ochranu i v době nepřítomnosti vlastníka [32].

V modelovém případě by bylo vhodné pro pohodlnost uživatelů použít jako ovládací periférii přístupový modul s klávesnicí. Jako detektor narušení by bylo možné použít PIR detektory, díky jejich cenové dostupnosti, snadné instalaci a poměrně přesné detekci. Tato

zařízení by se poté propojila s ústřednou nejspíše pomocí TCP/IP nebo kabelovým spojením [32]. Umístění detektorů narušení u námi navrženého modelového domu je zobrazeno na obrázku č. 10.



Obr. 10: Umístění detektorů [vlastní zdroj]

Na obrázku č. 10 jsou červenými šipkami označeny vstupní dveře do rodinného domu. A zeleně jsou poté označeny detekční charakteristiky PIR detektorů. Při takovém rozložení detektory narušení zaznamenají pohyb především v chodbě, která vede do patra a tedy k notebookům a cenným dokumentům. Druhý detektor, umístěný v obývacím pokoji, poté zaznamená případný vstup do objektu zadními dveřmi.

Konkrétní řešení nám může poskytnout například společnost Jablotron, která nabízí sadu obsahující:

1x JA-101K ústřednu s vestavěným GSM/GPRS komunikátorem,

1xJA-113E sběrnicový přístupový modul s klávesnicí a RFID,

2x JA-110P sběrnicový PIR detektor pohybu,

1x JA-120PB sběrnicový detektor pohybu osob a rozbití skla,

1x JA-111M sběrnicový magnetický detektor otevření,

1x JA-110ST sběrnicový kombinovaný detektor kouře a teploty,

1x JA-110A sběrnicovou sirénu vnitřní,

1x JA -111A BASE-RB sběrnicovou sirénu venkovní,

1x JA-1X1A-C-WH plastový kryt sirény JA-111A, JA-151A - bílý, červený blikač,

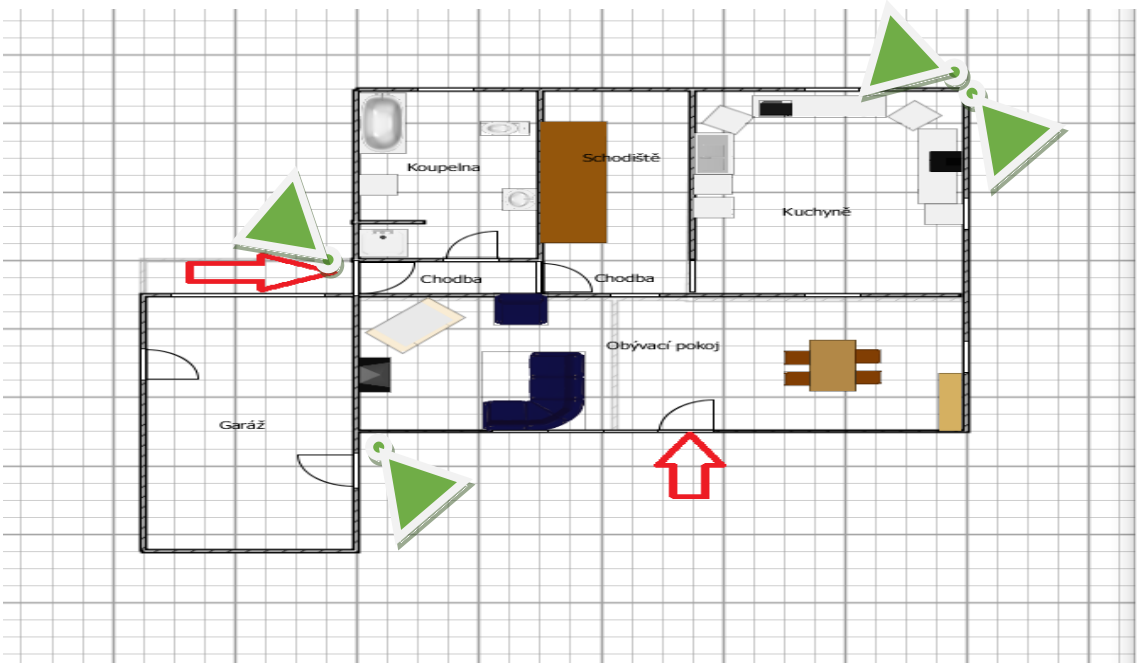
1x SA214-2,6 bezúdržbový akumulátor (12 V / 2,6 Ah) .

Celá sada tedy obsahuje požadované komponenty a navíc je zde také detektor rozbití skla. Sada je v ceně 16 900 Kč a pro námi požadované účely nevyžaduje žádná další doprovodná zařízení [38].

Kamerový systém

Doplňkem poplachových zabezpečovacích a tísňových systémů může být také kamerový systém. Tento systém má za úkol monitorovat požadovaný prostor, v našem případě by se jednalo o snímání okolí domu. Kamerový systém sestává z kamer, záznamového zařízení, přenosových prostředků (kabelů), zobrazovacího zařízení a doplňkového zařízení (nejčastěji softwarové doplňky jako detekce obličeje a další) [32].

Výhodou je, že v dnešní době lze kamerový systém pomocí internetového připojení propojit také s mobilním zařízením a sledovat tak činnosti a případný pohyb v okolí domu v reálném čase. Na obrázku č. 11 je zobrazeno rozmístění kamer u námi navrženého modelu.



Obr. 11: Umístění kamer [vlastní zdroj]

Na obrázku č. 11 jsou červenými šipkami označeny vstupní dveře do objektu. A zeleně jsou poté označeny snímací zóny kamer. Jsou snímány jak prostory ke vstupním dveřím,

tak další strany s přístupem k oknům. Jak již bylo zmíněno, kamerový systém je vhodným preventivním opatřením před neočekávaným vstupem, působí jako nástroj odstrašení a pokud by k narušení bezpečnosti došlo, mohou se záznamy použít také k represi.

Cenová kalkulace navrhované kamerového systému by mohla být od společnosti CP PLUS, která nabízí set:

1x digitální videorekordér CP-UNR-404T1-W,

4x vnější barevná IP kamera 4 Mpix s WIFI CP-UNC-T41l3C-MW,

1x SATA pevný disk HD-2TB WD PURX,

ve výši 21 992 Kč.

Tento set tedy obsahuje námi požadované komponenty v ceně 21 992 Kč, k tomuto setu je však nutné dokoupit také baterie, ke každé z kamer v ceně 606 Kč, celkem tedy za kamerový set + 4ks zdrojů 24 416 Kč. Po propojení je ke kamerám navíc přístup přes webové rozhrání a pohled z kamer je tedy možné sledovat i z mobilního zařízení [39].

Mechanický zábranný systém

Pojem mechanický zábranný systém označuje veškeré prostředky, které mají zabránit vniknutí neoprávněných osob do objektu. Všechny prostředky tohoto typu jsou vždy překonatelné, ale mají za úkol útočníka zpomalit nebo v lepším případě odradit. Do těchto systémů můžeme zařadit například bezpečnostní dveře, mříže nebo ochranné fólie na oknech [32].

Ochranné fólie mohou být poměrně nákladné, ale pro model je vhodné zmínit instalaci bezpečnostních dveří. Tyto dveře totiž disponují vyšším počtem jistících bodů, zároveň mají tuhou kovovou konstrukci, kterou je nesnadné zničit. Důležité také je, aby měly dveře bezpečnostní zámek a vložku chráněnou kaleným krytem, kvůli ochraně proti napadení hrubou silou.

Námi zmíněné dveře ve 3. bezpečnostní třídě s 19-ti jistícími body a požární odolností, včetně bezpečnostní vložky a kování je možné zakoupit například od společnosti NEXT v ceně 39 019 Kč a to i s montáží a dopravou [40].

Zámek proti vniknutí do zařízení

Zámek na zařízení je vždy potřebný i přesto, že se jedná o zařízení, které je využito v domácnosti. Model hypotetického soukromí obsahuje dva notebooky, které je teoreticky možné zcizit a dostat se tak k soukromí uživatelů.

Možností ochrany je klasické psané heslo v různé podobě a délce. Další možností je však také biometrická ochrana zařízení, která lze použít. Mnoho notebooků nabízí přihlášení pomocí otisku prstu. Další možností je kombinace hesla nebo kódu a biometrického zabezpečení.

Software na ochranu počítačových zařízení

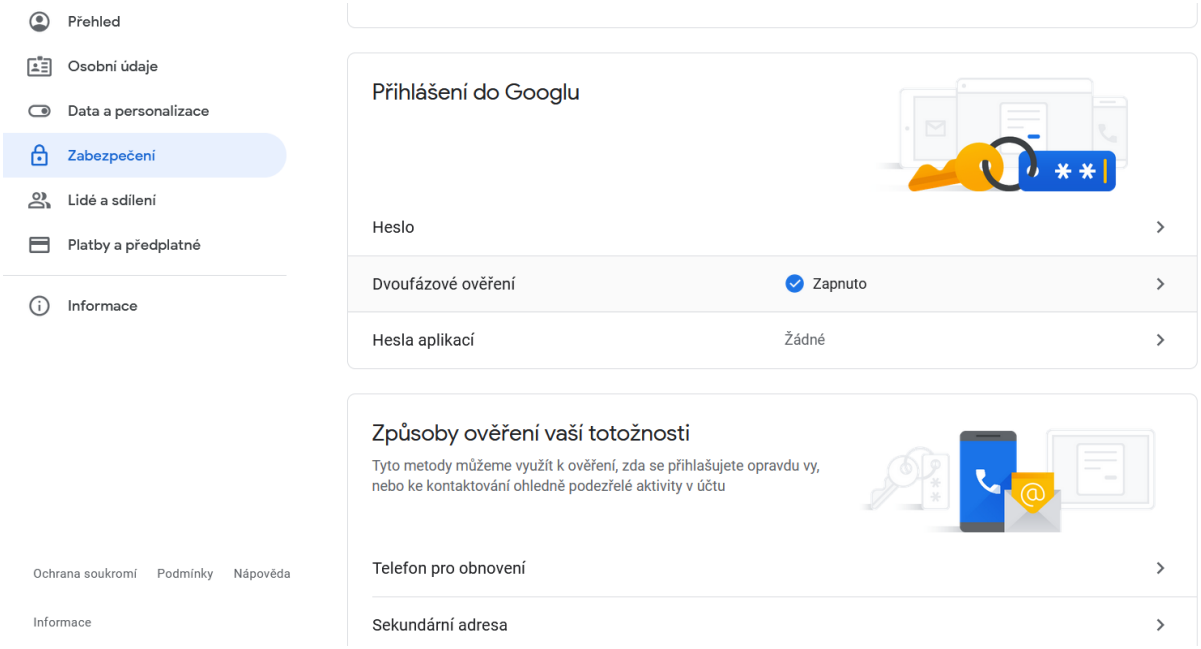
Abychom předešli odcizení, nebo v horším případě měli možnost zařízení snadněji nalézt, mohou k tomu dopomoci specializované softwarové nástroje na ochranu zařízení. Součástí antivirových programů bývají často funkce s názvem anti-theft. Pokud zařízení tuto funkci obsahuje – u notebooku nebo mobilního telefonu, je možné za pomocí anti-theft zjistit například polohu zařízení, fotit obrázky a tím tak zjistit obličej pachatele, odposlouchávat, spustit sirénu nebo zamknout zařízení.

Nejdůležitější je, že je možné touto funkcí smazat obsah zařízení. V rámci ochrany soukromí tak znemožnit přístup k citlivým informacím, fotkám, popřípadě kontaktům a účtům. V lepším případě navíc díky funkci snímání polohy můžeme zařízení s pomocí Policie ČR vystopovat a nakonec tak zařízení zcela ochránit. Jak již bylo zmíněno, tato funkce bývá součástí antivirových programů. Nabízí ji například společnost Avast, ale také NOD32 a další. U některých freewarových programů je za menší příplatek v hodnotě okolo 200 Kč, v jiných případech bývá součástí základního balíčku ochrany, který antivirové softwary nabízí a pohybuje se v cenách okolo 1 200 Kč/rok [41].

Dvoufázové ověření identity

Dvoufázové ověření identity znamená, že nejprve je uživatel nucen zadat při přihlášení k účtu přihlašovací jméno, poté heslo a na základě správně zadaného hesla přijde většinou textová zpráva, která uvádí další kód, který je nutné zadat k přihlášení do účtu.

Základem je při vytváření účtu zvolit dvoufázové ověření a nejčastěji doplnit účet o informaci o svém telefonním čísle, na který budou později chodit ověřovací kódy. Na obrázku č. 12 je možné vidět, jakým způsobem se tato volba v nastavení účtu objevuje u aplikací společnosti Google.



Obr. 12: Volba dvoufázového ověření [42]

V kombinaci se silným heslem se dvoufázové ověření stává jedním ze základních pilířů, které chrání účty. Napomáhá tak chránit soukromí, a pokud by bylo dodrženo i u hypotetického modelu, je téměř jisté, že i při krádeži notebooku se o své soukromí není nutné obávat.

Zastínění vnějších prostor obytné zóny

Zastínění vnějších prostor obytné zóny může znít jako triviální opatření, ale má důležitou roli v ochraně soukromí. Spoustu lidí si neuvědomuje, že pokud nechá případného útočníka nahlédnout na zahradu, popřípadě přímo do domu, dává jim tím informace o zabezpečení. Možnost prohlédnout si cesty vhodné ke vstupu do obydlí, popřípadě ukázat přímo umístění důležitých a cenných předmětů.

Pokud budeme chtít toto preventivní opatření aplikovat v rámci modelu, tak především v rámci předního dřevěného oplocení, kterým je možné vidět do části zahrady a ke vstupním dveřím. Oplocení je dostatečně vysoké na to, aby přes něj nebylo vidět. Ale je nutné zastínit viditelnost skrze dřevěné plaňky. Tímto se zajistí soukromí pro činnosti na zahradě a případný útočník nebude mít možnost pozorovat cenné předměty, vchody/východy a pohyb lidí. Zastínění lze provést stínícím úpletem, který má 90 % neprůhlednění nebo jiným materiálem, který je k tomu určen. Samozřejmě by bylo možné nechat na místě vyrůst dřeviny, které by výhled znemožnili, ale to by trvalo mnohem déle.

Proto zvolíme stínící úplet od společnosti Pilecký, který se nabízí ve výšce 180 cm a bude snadné jej připevnit ke stávajícímu dřevěnému plotu. Cena za 25 m roli je 1 985 Kč a my budeme v modelovém případě potřebovat dvě, protože dřevěný plot má délku 40 m. Celkem tedy 3 970 Kč za 50 bm stínící tkaniny výšky 180 cm s 90 % stínivostí [43].

Zabezpečení cenných dokumentů

Zabezpečení cenných dokumentů je myšleno především jako uložení dokumentů do bezpečné schránky, tedy trezoru. Jde o ochranu, která zabraňuje nejen zneužití osobních údajů, které se často na takových dokumentech nachází, ale také může jít o ochranu například před požárem.

V rámci modelu hypotetického soukromí budeme chtít ochránit především běžné dokumenty, jako pojistné smlouvy, smlouvy o vlastnictví domu nebo auta, popřípadě jiných movitých statků, které rodina vlastní. Jelikož dům nedisponuje žádnou dostatečně silnou zdí, do které by bylo možné trezor ukotvit natrvalo, bude nutné použít volně stojící ohnivzdorný trezor, který lze ukotvit do podlahy. Umístění by bylo vhodné ve druhém patře rodinného domu a nejlépe v ložnici, která je nejméně dostupná. Konkrétně je možné jej umístit, buď za dveře v místě kam se dveře otvírají, takže nebude trezor na očích při vstupu do pokoje, nebo do skříně, kterou by bylo nutné patřičně upravit, aby šel trezor otevírat.

Zvolíme jednodušší variantu za dveře tak, aby byla k dokumentům pohodlnější dostupnost a trezor nezabíral místo ve skříni. Velikostně a cenově by mohl být vhodný trezor od výrobce Rottner, protože má 490x450x360mm, tudíž se nám snadno za dveře schová, zároveň je ohnivzdorný a má vysokou odolnost proti odvrtání, zároveň je vhodný pro uložení různých dokumentů. Cena takového trezoru je 13 490 Kč [44].

7.2 Organizační opatření

V této podkapitole se budeme zabývat organizačními opatřeními z oblasti prevence, která mají snižovat riziko a dopady v rámci ochrany soukromí.

Organizační opatření:

- vzdělání v oblasti IT a kybernetické bezpečnosti,
- outsourcing pro správu údajů na veřejných portálech,
- kontrola digitálních stop.

Vzdělání v oblasti IT a kybernetické bezpečnosti

Do organizačních opatření patří vzdělání v oblasti IT a kybernetické bezpečnosti, které může všeobecně napomoci bezpečnějšímu užívání IT zařízení. Obezřetnějšímu zakládání účtů, chování na sociálních sítích, popřípadě udělování souhlasů a poskytování různých osobních údajů.

Forma vzdělání záleží na finančních a časových možnostech dané osoby. Samozřejmě ideální je komplexní vzdělání ve formě například vysoké školy, zaměřené na bezpečnost a informatiku. V tomto případě je jasné, že pracující rodiče nejsou z časových důvodů schopni studovat vysokou školu při svých zaměstnáních, takže by se jednalo spíše o vzdělání formou online kurzu. Například společnost GOPAS (www.gopas.cz) nabízí kurz „Ochrany dat a soukromí pro běžné uživatele“, který se přímo na požadované zabezpečení a prevenci v ochraně zaměřuje. Tento kurz je na dva dny a stojí 9 000 Kč [45].

Důležité je, že díky těmto kurzům může například rodič zadávat různá omezení navštěvování stránek pro dítě, dále kontrolovat jeho činnost a mít větší a podrobnější přehled o fungování a využívání elektronických zařízení dítětem. Na tyto činnosti sice není nutné žádný kurz absolvovat a při větší vůli je možné se je naučit samostatně a bez pomoci. Na druhou stranu za pomoci zkušeného lektora se rodič může dobrat rychleji výsledkům a mít zabezpečení na vyšší úrovni.

Outsourcing pro správu údajů na veřejných portálech

Tímto preventivním opatřením je myšleno najmout si společnost nebo odborníka, který bude dohlížet na činnost a údaje, které sdílíme na sociálních sítích. Jde nám především o to, aby se na internetu neobjevoval obsah, který by mohl přílišně odhalovat naše soukromí.

V podstatě by nám šlo o kontrolu stávajících zveřejněných údajů a poté průběžnou kontrolu na měsíční bázi, která by zahrnovala kontrolu postupů a sdílení dat. Takové řešení by mohla poskytnout například společnost NGSS, která se zabývá bezpečností na internetu a má zkušenosti s analýzou rizik, právními normami a postupech při zajišťování bezpečnosti [46].

Bohužel nebylo možné služby nacenit, protože požadavky jsou velmi specifické a nacenění je individuální, ale na webovém portálu, který nabízel přímo správu dat na sociálních sítích, byla uvedena cena 8 000 Kč při prvotní kontrole a měsíční poplatek za správu 1 000 Kč.

Kontrola digitálních stop

Podobně jako u outsourcingu pro správu údajů jsme schopni si na kontrolu digitálních stop najmout odborníka, který zajistí, aby se po internetu neobjevovaly informace o soukromí dotyčné osoby. Jde tedy především o zajištění údajů, fotografií a informací, které mohou být spojeny s naší osobou. Bohužel zveřejněné informace ve většině případů nelze smazat, ale je možné alespoň zakrýt cesty, které k těmto informacím mohou vést.

S tímto řešením by nám mohla pomoci společnost Alpha solutions, která nabízí školení v oblasti IT a zabývá se zabezpečením dat. Zároveň tato společnost nabízí dekódování šifrovaných dat, což znamená, že by nám mohla poradit i v oblasti zajištění dat v zařízeních a případně s autentizací [47].

7.3 Shrnutí navrhovaných řešení

Na základě návrhů, které jsme v této kapitole uvedli, jsme schopni stanovit, jaká by byla celková cena doporučených opatření. Poté budeme schopni vyhodnotit, jakým způsobem bude model hypotetického soukromí chráněn.

Tab. 15: Souhrn nákladů na aplikaci navrhovaných opatření [vlastní zdroj]

Technická opatření	**Cena**
PZTS Jablotron	16 900Kč
Kamerový systém CP PLUS	24 416Kč
Bezpečnostní dveře NEXT	39 019Kč
Softwarová ochrana NOD32	1 209Kč
Zastínění vnějších prostor Pilecký	3 970Kč
Zabezpečení cenných dokumentů (trezor) Rottner	13 490Kč
Organizační opatření	
Kurz: „Ochrana dat a soukromí“	9 000Kč
Správa dat na sociálních sítích	8 000Kč + 1 000Kč/měsíc
CELKEM	**116 004Kč (+ 12 000Kč/rok)**

Pomocí navrhovaných preventivních opatření jsme schopni soukromí chránit proti vnějšímu vniknutí. Díky zastínění zahrady potenciální útočník neuvidí, co se na zahradě děje a kde se nachází případné vstupy a další bezpečnostní zařízení. Pokud by se dostal útočník na zahradu tak jej zachytí kamery, které jej mohou také částečně odradit. U vstupu se útočník setká s bezpečnostními dveřmi, které díky vyšší bezpečnostní třídě a bezpečnostní vložce není snadné překonat a pokud už by se dostal do objektu, tak na jeho neoprávněný příchod upozorní siréna, která je součástí navrhované PZTS.

Uvnitř objektu nám šlo především o ochranu soukromí, takže cenné dokumenty jsou v bezpečí trezoru v nejvzdálenější místnosti od vstupu do domu, a zařízení, ve kterém mohou být soukromá data je zabezpečená heslem a navíc je v zařízení nainstalován tzv. anti-theft software. Pokud jde o kybernetickou bezpečnost, tak sdílení dat a celkově bezpečnost na internetu je zajištěna částečně antivirovou ochranou a zároveň je pravidelně kontrolována odbornou firmou, která je specializovaná na tento druh bezpečnosti.

ZÁVĚR

Práce se zabývá problematikou prevence v ochraně soukromí. V první kapitole bylo vyspecifikováno, co je to prevence. Dále bylo popsáno rozdělení prevence z pohledu teorie bezpečnosti na primární a sekundární prevenci. Ke každému druhu prevence byly poté uvedeny příklady z praxe, z důvodu lepšího pochopení dané problematiky.

Dále bylo analyzováno, co je to soukromí a jak je na něj právně nahlíženo. Ochrana soukromí je právně zajišťována především občanským zákoníkem, Listinou základních práv a svobod a trestním zákoníkem. Ochrana osobních údajů je navíc také podpořena nařízením GDPR. Pro přehlednější orientaci a popis soukromí byly vypsány jednotlivé části soukromí, jako jsou osobní údaje, hesla, cenné dokumenty a další. V poslední části druhé kapitoly bylo také popsáno, jakým způsobem se hodnota soukromí s rozvojem technologií vyvíjí a jak také vzniká rozdíl mezi hodnotou soukromí a majetku.

Součástí práce byla také analýza hrozeb, které ohrožují soukromí. Na základě této analýzy byl vyhotoven soubor preventivních opatření a u těchto preventivních opatření byla následně zhodnocena účinnost pomocí párového srovnání.

Praktická část práce se zabývala analýzou dotazníkového šetření, které pokládalo otázky z oblasti hrozeb, vnímaní soukromí a preventivních opatření. Odpovědi respondentů ukázaly, že lidé jsou si vědomi ohrožení soukromí a v mnoha ohledech považují svá aktiva za nedostatečně chráněná. Zároveň byly v této části práce uvedeny volné odpovědi respondentů na otázky o roli soukromí v této technologické době a byla zde také vyjmenována klíčová preventivní opatření z pohledu respondentů. Odpovědi z těchto otázek, lze považovat za velmi užitečné, především při budoucím konání a tvorbě preventivních opatření.

Další část praktické části práce obsahovala model hypotetického soukromí, odpovídající tří členné rodině, která žije v rodinném domě. Tato rodina, měla zájem být chráněna a motivací byla především ochrana soukromí a finančních prostředků. V další části této kapitoly byly také návrhy ochrany soukromí a následně vícekriteriální zhodnocení, kterým jsme jednotlivé návrhy preventivní ochrany posoudili. Dále byl vhodnější návrh ochrany založený na preventivních opatřeních rozpracován a zhodnocen. Zvolený návrh může sloužit jako návod, sloužící ke zvýšení ochrany soukromí.

SEZNAM POUŽITÉ LITERATURY

[1] LUKÁŠ, Luděk. *Teorie bezpečnosti I*. Zlín: Radim Bačuvčík - VeRBuM, 2017. ISBN 978-80-87500-89-7.

[2] LUKÁŠ, Luděk, ed. *Sborník 3. ročníku mezinárodního workshopu SECULIN 2018: role prevence v zajištění bezpečnosti na lokální úrovni: 10. - 11. října 2018, Kopánky*. Ve Zlíně: Univerzita Tomáše Bati, Fakulta aplikované informatiky, 2018. ISBN 978-80-7454-809-3.

[3] ZEMAN, Petr, ed. *Česká bezpečnostní terminologie: výklad základních pojmů*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2002. ISBN 80-210-3037-2.

[4] MESÁROŠ, Marián, Miroslav KELEMEN a Stanislav KRIŽOVSKÝ. *Teória bezpečnosti*. Košice. VŠBM v Košiciach, 2011. ISBN 978-80-89282-61-6.

[5] Soukromí. *Úřad pro ochranu osobních údajů* [online]. Praha, 2013 [cit. 2020-11-21]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=4414

[6] FERENSTEIN, Greg. *The Age of Optimists* [online]. 2015 [cit. 2021-02-25]. Dostupné z: https://medium.com/the-ferenstein-wire/the-birth-and-death-of-privacy-3-000-years-of-history-in-50-images-614c26059e

[7] MATES, Pavel. Ochrana soukromí ve správním právu. Praha: Linde, 2004. 307 s. ISBN 80-7201-458-7.

[8] VALOUŠEK, Martin, Pavel MATES, Eva FIALOVÁ, et al. Ochrana osobnosti, soukromí a osobních údajů. Praha: Leges, 2019. Praktik. ISBN 978-80-7502-346-9.

[9] Moderní úprava tradičního a vyzkoušeného. *Nový občanský zákoník* [online]. [cit. 2021-02-25]. Dostupné z: http://obcanskyzakonik.justice.cz/index.php/obecna-cast/obecne

[10] Zákon č. 89/2012 Sb. *Zákony pro lidi* [online]. Praha, 2012 [cit. 2021-02-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-89/zneni-20200701

[11] Listina základních práv a svobod. *Poslanecká sněmovna parlamentu České republiky* [online]. [cit. 2021-02-25]. Dostupné z: https://www.psp.cz/docs/laws/listina.html

[12]Trestní legislativa. *Justice.cz* [online]. [cit. 2021-02-25]. Dostupné z: https://justice.cz/web/msp/trestni-legislativa1

[13] Zákon č. 40/2009 Sb. *Zákony pro lidi* [online].Praha, 2009 [cit. 2021-02-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[14] Co je GDPR. *Ministerstvo vnitra České republiky* [online]. [cit. 2021-02-25]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx

[15] ŠALAMON, Tomáš. *Připravte se na GDPR* [online]. 2017 [cit. 2021-02-25]. Dostupné z: https://web.archive.org/web/20171222051432/https://www.incomaker.com/cs/blog/pripravte-se-na-gdpr-l-osobni-udaje-jsou-vsude

[16] Základní pojmy v GDPR. *Ministerstvo vnitra České republiky* [online]. [cit. 2021-02-25]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/zakladni-pojmy-v-gdpr.aspx

[17] ALLEN, Christopher. The four kinds of privacy. *Life with Alacrity* [online]. 2015 [cit. 2021-02-25]. Dostupné z: http://www.lifewithalacrity.com/2015/04/the-four-kinds-of-privacy.html

[18] Phishing. *ESET* [online]. [cit. 2021-02-25]. Dostupné z: https://www.eset.com/cz/phishing/

[19] Mýty a fakta o bezkontaktním placení. *Měšec* [online]. 2013 [cit. 2021-02-25]. Dostupné z: https://www.mesec.cz/clanky/myty-a-fakta-o-bezkontaktnim-placeni/

[20] NISSENBAUM, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press. Stanford, California, 2009. ISBN 9780804772891.

[21] Jak Google využívá soubory cookies. *Ochrana soukromí a smluvní podmínky* [online]. 2013 [cit. 2021-02-25]. Dostupné z: https://policies.google.com/technologies/cookies?hl=c

[22] Jednotlivé druhy kyberkriminality. *Policie České republiky* [online]. [cit. 2021-02-25]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

[23] Google maže fotky nahých celebrit. Hrozí mu totiž soud. *Aktuálně* [online]. [cit. 2021-02-25]. Dostupné z: https://magazin.aktualne.cz/celebrity/google-hacker-nahe-fotky-jennifer-lawrence/r~bb52b2f44d5811e48afe002590604f2e/

[24] Analýza rizik: identifikace hrozeb. *Clever and smart* [online]. [cit. 2021-02-25]. Dostupné z: https://www.cleverandsmart.cz/analyza-rizik-identifikace-hrozeb/

[25] Z nákupního vozíku zmizel batoh. *Policie České republiky* [online]. [cit. 2021-02-25]. Dostupné z: https://www.policie.cz/clanek/z-nakupniho-voziku-zmizel-batoh.aspx

[26] Platil nalezenou kartou. *Policie České republiky* [online]. [cit. 2021-02-25]. Dostupné z: https://www.policie.cz/clanek/krajske-reditelstvi-olomouckeho-kraje-zpravodajstvi-platil-nalezenou-kartou.aspx

[27] Mapa kriminality. *Policie České republiky* [online]. [cit. 2021-02-25]. Dostupné z: https://kriminalita.policie.cz/

[28] Téměř čtvrtina Čechů se setkala s phishingovým útokem Mapa kriminality. *AVAST* [online]. [cit. 2021-02-25]. Dostupné z: https://press.avast.com/cs-sk/temer-ctvrtina-cechu-se-setkala-s-phishingovym-utokem

[29] Hacker. *AVAST* [online]. [cit. 2021-02-25]. Dostupné z: https://www.avast.com/cs-cz/c-hacker

[30] Kyberkriminalita. *Policie České republiky* [online]. [cit. 2021-02-25]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[31] Falešní nápadníci. *Policie České republiky* [online]. [cit. 2021-02-25]. Dostupné z: https://www.policie.cz/clanek/falesni-napadnici.aspx

[32] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 9788087500057.

[33] Privacy predictions for 2021. *Secure list* [online]. [cit. 2021-02-25]. Dostupné z: https://securelist.com/privacy-predictions-for-2021/100311/

[34] ČERNÝ, Michal. *Digitální stopy* [online]. 2011, 19. 9. 2011 [cit. 2021-02-25]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/sociotechnika/312-digitalni-stopy

[35] Antispamová ochrana. *ESET smart security* [online]. [cit. 2021-02-25]. Dostupné z: https://help.eset.com/essp/12/cs-CZ/idh_config_smon_main.html

[36] Co je firewall? *ESET* [online]. [cit. 2021-02-25]. Dostupné z: https://www.eset.com/cz/firewall/

[37] Mapa - Olomouc. In: *Mapy.cz* [online]. [cit. 2021-02-27]. Dostupné z: https://en.mapy.cz/letecka

[38] *Sada zabezpečovacího systému Jablotron 100* [online]. [cit. 2021-04-14]. Dostupné z: https://www.hlidejsimajetek.cz/sbernicove-dratove-sady-zabezpecovacich-systemu-jablotron/sada-zabezpecovaciho-systemu-jablotron-100-pro-rd-3-1-sbernicova-varianta

[39] *Kamerový set IP-10* [online]. [cit. 2021-04-14]. Dostupné z: https://www.jabloshop.cz/kamerovy-set-ip-10-3mpix

[40] *Orientační cena bezpečnostních protipožárních vchodových dveří pro byt a dům* [online]. [cit. 2021-04-14]. Dostupné z: https://www.next.cz/bezpecnostni-vchodove-dvere-cena

[41] *Základní antivirová ochrana* [online]. [cit. 2021-04-14]. Dostupné z: https://www.eset.com/cz/domacnosti/antivirus/?from=cz_google&utm_source=cz_google&utm_medium=ppc&utm_campaign=be31&utm_content=eset_nod32&utm_term=brand&gclid=EAIaIQobChMIycrb2rP27wIViuF3Ch3wzQlWEAAYASAAEgLxA_D_BwE

[42] *Nastavení účtu google* [online]. [cit. 2021-04-14]. Dostupné z: https://myaccount.google.com/

[43] *Stínící úplet zelený* [online]. [cit. 2021-04-14]. Dostupné z: https://www.ploty-pletivo-oploceni.cz/stinici-uplet-zeleny-vyska-180-cm-role-25-m-90-znepruhledneni

[44] *Ohnivzdorný trezor FireHERO 50 EN-1* [online]. [cit. 2021-04-14]. Dostupné z: https://www.trezor.cz/trezory/ohnivzdorny-trezor-firehero-50-detail.html

[45] *Ochrana dat a soukromí pro běžné uživatele* [online]. [cit. 2021-04-14]. Dostupné z: https://www.gopas.cz/Kurzy/Katalog-kurzu/IT-bezpecnost-a-Hacking/IT-bezpecnost-a-Hacking/Ochrana-dat-a-soukromi-pro-bezne-uzivatele-GOC51.aspx

[46] *Kybernetická bezpečnost na internetu a zákon* [online]. [cit. 2021-04-14]. Dostupné z: https://www.ngss.cz/

[47] *Spolehlivý dodavatel IT řešení* [online]. [cit. 2021-04-14]. Dostupné z: https://alphasolutions.cz/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

DPPC Dohledové a poplachové přijímací centrum

EU European Union

FB Facebook

GDPR General data regulation protection

GPRS General packet radio service

GSM Groupe spécial mobile

IP Internet protocol

IT Information technology

NFC Near field communication

PIR Passive infrared detektor

PZTS Poplachový zabezpečovací a tísňový systém

RFID Radio frequency identification

SMS Short message service

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ