Zneužití identity osob jako nový typ bezpečnostní hrozby

Bc. Aneta Pernicová

Diplomová práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Aneta Pernicová**
Osobní číslo:	**A18311**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Zneužití identity osob jako nový typ bezpečnostní hrozby**
Téma práce anglicky:	**Identity Abuse as a New Type of Security Threat**

Zásady pro vypracování

1. Analyzujte, co je identita, jaké je její obsahové a právní vymezení. Specifikujte, které informace tvoří identitu osoby.
2. Pojednejte o kybernetické bezpečnosti. Identifikujte bezpečnostní hrozby, které jsou založeny na zneužití identity.
3. Specifikujte zranitelnosti, které umožňují vznik narušení bezpečnosti, spojených se zneužitím identity.
4. Zpracujte a analyzujte případové studie vybraných způsobů zneužití identity. Popište příslušné scénáře narušení bezpečnosti. Identifikujte a analyzujte bezpečnostní problémy, spojené se zneužitím identity.
5. Navrhněte opatření, která budou znemožňovat nebo alespoň omezovat zneužití identity.

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

Seznam doporučené literatury:

1. RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Praha: Grada, 2008. Profesionál. ISBN 978-80-247-2365-5.
2. LUKÁŠ, Luděk. Teorie bezpečnosti I. Zlín: Radim Bačuvčík – VeRBuM, 2017. ISBN 978-80-87500-89-7.
3. POŽÁR, Josef. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.
4. DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. Brno: M. Drahanský, 2011. ISBN 978-80-254-8979-6.
5. KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.
6. Online identity theft. Paris: OECD, c2009. ISBN 978-92-64-05658-9.
7. KAMBERG, Mary-Lane. Digital identity: your reputation online. New York, NY: Rosen Publishing, 2019. ISBN 978-15-08-18460-7.
8. NOONAN, Harold W. Personal identity. Second edition. London: Routledge. ISBN 0-203-42835-8.

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

Datum zadání diplomové práce: **9. prosince 2019**
Termín odevzdání diplomové práce: **29. května 2020**

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Milan Navrátil, Ph.D.
ředitel ústavu

Ve Zlíně dne 9. prosince 2019

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/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- 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/bakalářské 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 11.08.2020

Aneta Pernicová, v. r.
podpis diplomanta

ABSTRAKT

Tato diplomová práce se zabývá stanovením bezpečnostních problémů souvisejících se zneužitím vybraných identit, které uživatel využívá při vystupování v síti internet. Jedná se o identitu elektronickou, digitální a bankovní. K jednotlivým identitám byly definovány jejich zranitelnosti. Pro přiblížení problematiky bylo zanalyzováno 5 vybraných případových studií, které se zneužitím vybraných identit souvisely. Na základě těchto znalostí je v poslední části uveden obecný, i konkrétní souhrn opatření pro jednotlivé identity, který vede uživatele k maximální možné ochraně těchto identit.

Klíčová slova: identita, eIdentita, zneužití, bezpečnost, zranitelnost, opatření

ABSTRACT

This diploma thesis is focused on determinating security issues associated with abuse of chosen identities, which are used by users when performing on the Internet. The chosen identities are electronic, digital and banking. For these individual identities have been defined their vulnerabilities. To approach the issue, 5 selected case studies were analyzed, which were somehow related to the abuse of selected identities. Then, based on the gained knowledge, is in the last part given the general and the specific summary of precautions for the individual identities, which leads users to the maximum possible protection of these identities.

Keywords: identity, eIdentity, abuse, security, vulnerability, precaution

Touto cestou bych chtěla poděkovat především vedoucímu mé diplomové práce doc. Ing. Luďkovi Lukášovi, CSc. za cenné rady, odborné vedení a přínosné konzultace po celou dobu řešení práce.

Chtěla bych také poděkovat své rodině a blízkým přátelům za trpělivost a podporu nejen při zpracovávání této práce, ale také po celou dobu studia.

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

OBSAH

ÚVOD

S neustále se rozvíjejícími technologiemi rostou také možnosti, jak mohou uživatelé využívat svou identitu prostřednictvím sítě Internet. Přináší to s sebou spoustu výhod, avšak mnozí uživatelé ještě stále nejsou dostatečně obezřetní, a tak dochází ke krádežím či zneužití jejich identit. Jestliže se nejedná o identity chráněné legislativou, útočníci, kteří identitu své oběti zcizili, nemusí být nikdy potrestáni.

Problematika krádeže či zneužití přihlašovacích, nebo osobních údajů, které identitu člověka dotváří je velice důležitá, jelikož je často spojována nejen s poškozením finančním, ale také s možným poškozením pověsti oběti. Při dodržení určitých opatření, lze ale krádežím či zneužití uživatelových identit zabránit, nebo útočníkům jejich snahy o krádež či zneužití ztížit, případně minimalizovat následky, které z toho pro poškozeného uživatele plynou. Zranitelnosti vybraných identit, bezpečnostní problémy, jejich následky a opatření, jak jim zabránit rozebírá tato práce.

Cílem diplomové práce bylo seznámit se obecně s tím, jak je možné chápat identitu člověka, co ji vytváří, a jak se k identitě člověka staví legislativa České republiky. Identita člověka byla rozdělena na jednotlivé typy. Z těchto typů byly následně vybrány takové, které uživatelé využívají při vystupování v síti Internet. Jedná se o identitu elektronickou, digitální a bankovní.

Pro přiblížení problematiky bylo zanalyzováno pět vybraných případových studií, které se zneužitím identity souvisely. Poznatky vyplývající z této analýzy byly poté využity pro vytvoření souhrnu opatření. Tento souhrn opatření slouží jako návod pro uživatele, jak co nejvíce ochránit jednotlivé vybrané typy identit před zneužitím, případně jak minimalizovat škody, které byly zneužitím identity způsobeny.

I. TEORETICKÁ ČÁST

1 CO JE IDENTITA

Pojem „identita“, nebo také „totožnost“, pochází z latinského slova *identitas*, které je odvozeno od slova *idem* – stejný. Jestliže srovnáváme dva objekty, které se nám zdají stejné (mohli bychom je zaměnit) můžeme o nich tvrdit, že jsou stejné neboli identické. [1]

V tomto případě je řeč o obecné identitě, která problematiku popisuje jako zkoumání a porovnávání znaků věcí (objektů) mezi sebou, nebo s nimi samotnými. [1]

Při posuzování totožnosti dvou objektů je třeba brát v potaz jak jejich slovní popis, tak i jejich obsah. Například, my můžeme říct, že vůz stojící před domem, je náš automobil. Kdežto náhodný kolemjdoucí prohlásí, že se jedná o červené osobní vozidlo. Oba myslíme ten stejný vůz stojící před domem, ale každý jej můžeme popsat odlišně.

Na druhou stranu, my řekneme, že vůz stojící před domem, je náš automobil a myslíme tím náš červený osobní vůz. Náš soused může říct totéž – tedy, že vůz stojící před domem, je jeho automobil, přestože myslí svůj žlutý sportovní vůz. Jedná se tedy o dva různé objekty, se stejným popisem.

Z příkladu popsaného výše tedy vyplývá, že důležitější než subjektivní popis vlastností objektu jednotlivců, jsou takové vlastnosti objektu, které jsou s ním fyzicky spojeny a nemění se v závislosti s pohledy různých jednotlivců. [1]

Můžeme tedy prohlásit, že „každý objekt je identický sám se sebou“. [1]

V návaznosti na toto prohlášení se můžeme zamyslet také nad pojmy kvalitativní a číselná identita. [2]

Kolem sebe totiž můžeme vidět i případy, kdy dva objekty porovnávané vedle sebe jsou od sebe jen těžko rozlišitelné, případně od sebe nejsou rozlišitelné vůbec. Například, koupíme-li si v pekárně deset rohlíků, které uložíme do papírového sáčku. Pokud se na ně podíváme, vidíme deset naprosto totožných kusů pečiva. Jestliže jeden z nich vytáhneme a vrátíme zase zpátky, jen těžko budeme hádat, který z nich jsme před tím vytáhli. V tomto případě lze říct, že se jedná o identitu kvalitativní, protože všechny kusy sdílejí naprosto stejné vlastnosti – kvality. Oproti tomu, se v tomto případě nejedná o jednu a tutéž věc, přestože k jejich popsání lze použít naprosto stejný popis. Je to deset kusů pečiva, z nichž každý existuje nezávisle na druhých. Tuto situaci tedy můžeme nazvat jako číselnou identitu. [2]

Neplatí to ale pouze pro objekty. Z hlediska kvalitativní nebo číselné identity můžeme porovnávat také osoby.

1.1 Identita osoby

Identitu osoby můžeme zjednodušeně popsat jako to, co člověka definuje, jak vypadá, to, kým je. Problematika identity člověka je ale mnohem komplikovanější.

Když mluvíme o lidech, jako o živočišném druhu, mají všichni stejné znaky, např.: dolní končetiny, horní končetiny, k dorozumívání používají geograficky a historicky dané jazyky, učí se pozorováním, přemýšlejí apod. Všechny tyto posuzované vlastnosti spadají spíše do kategorie kvalitativní identity. Stejně tak, pokud se o někom vyjadřujeme, že je například „fotbalový hráč“. Ten samý člověk totiž může pro někoho jiného být také otcem, nebo „dobrovolným hasičem“. Záleží, při jaké okolnosti danou osobu popisujeme. Co je ale pro všechny lidské bytosti rozhodující, jsou vlastnosti z pohledu identity číselné neboli kvantitativní. Ta totiž činí ze dvou stejně vypadajících jedinců (kvalitativní identita), dvě jedinečné osobnosti – jednovaječná dvojčata sice vypadají stejně, ale jsou to dva odlišní lidé s odlišnými charakterovými vlastnostmi. [3, 4]

Při rozboru něčí identity tedy musíme brát v potaz nejen, jak daná osoba vypadá, je důležité zahrnout také charakterové vlastnosti, vlastnosti psychické, vrozené či získané. Identitu člověka doplňuje také to, jak vnímá sám sebe, protože identitu dotváří také vzpomínky, schopnosti a zkušenosti. [1, 2]

Je důležité také zmínit, že osobní identita člověka se za dobu jeho života neustále vyvíjí a přetváří. To je důvod, proč může být mnohdy obtížné poznat například kamarády z dětství, které potkáme po tom, co uplynou dvě desetiletí. Mohou se změnit jak jejich fyzické rysy (vrásky v obličeji, barva vlasů, postava), tak i rysy psychické (záliby, názory). Tudíž i když se vlastnosti či rysy mění, je to stále ten stejný člověk. [2, 4]

Z toho tedy vyplývá, že každý člověk je jedinečný – totožný pouze sám se sebou, a může definovat sám sebe v různých situacích odlišně. Může o sobě tvrdit, že je homosexuál, zároveň je také umělcem a v jiné situaci zase prohlásí, že je ateista. Všechna tato prohlášení, spolu s ostatními rysy jeho osobnosti (ať už fyzickými nebo psychickými) definují jen a pouze jeho identitu. [1]

1.2 Čím je tvořena identita

Obecně je problematika definice identity osoby velice komplexní. Lze na ni ale nahlížet z několika typů:

- tělesná identita (nebo také identita biologická) – je taková identita, která je viditelná na první pohled. Jedná se o identitu, která nám byla přidělena geneticky (zděděním/získáním) naším DNA, bez našeho vědomí. [1, 5]
- psychologická identita – vědomí duševně zdravého člověka – ví kým je, registruje změny časové i prostorové, které se kolem něj nebo i jemu odehrávají. Přestože je běžné, že během života se lidské vědomí mění a vyvíjí, uvědomujeme si sami sebe – svou osobnost. Za psychologickou identitou stojí lidský mozek, který tuto identitu ukládá. V dnešní době může být spjatý pouze s jedním lidským tělem, se kterým dohromady tvoří podstatnou část identity člověka. Je velice důležité, aby každý svůj mozek chránil, jelikož při nějakém jeho poškození může dojít ke ztrátě paměti, která může vést k výrazným změnám osobnosti – tím pádem i ke změně identity. [1, 5]
- fyzická identita – stejně jako identita psychologická, se váže k mozku člověka. Vychází z toho, že lidský mozek se skládá ze dvou hemisfér – levé a pravé. Levá hemisféra se stará převážně o pohyb pravých končetin či očí – pravé strany těla obecně. Pravá hemisféra má na starosti ovládání levé části těla. Zároveň má levá část za úkol ovládání jazykových a matematických schopností dospělého člověka, pravá hemisféra dominuje poznávání tvarů a vzorů nebo hudebních melodií. Ovšem obě hemisféry jsou schopné zvládat všechny výše vyjmenované činnosti, avšak ty, kterým nedominují, zvládají pouze na úrovni malého dítěte. Principem tohoto pohledu na identitu je, že levá hemisféra jednoho mozku, by nedokázala fungovat s pravou hemisférou mozku jiného. [5]
- filosofická identita – definuje osobu z pohledu jejího bytí a myšlení. [1]
- sociální identita – řadí člověka podle jeho vlastností, projevů, zvyků či chování do některé sociální skupiny lidí, kteří se vyznačují stejnými charakteristikami – geografické, jazykové, etnické apod.
- vzpomínková identita – je založena na tvrzení, že osobu dotváří její vzpomínky – to, co zažila, kde byla, s kým, jak dlouho, co viděla, koho viděla apod. Do tohoto pohledu nezapadají vzpomínky faktické, jako třeba, kdy člověk musí navštívit rodinu, co má jít nakoupit. Problémem je, že lidé zapomínají a mění se (vyvíjí). Ve vzpomínkách na událost, která se odehrála před dvaceti lety, jsme to sice my, fotografie to mohou dokázat, avšak za dvacet let se naše osobnost změnila natolik,

že s osobou na fotografii již nemusíme mít jinak nic společného než jen, že „jsme to prostě my“. [5]

- pracovní identita – člověka definuje z pohledu toho, čím se živí. Popisuje ho jako kolegu, odborníka na specifickou činnost. Svými schopnostmi přináší finanční výnos svému zaměstnavateli, který následně může své zaměstnance finančně ohodnotit ve formě platu. Tato identita tvoří velkou část osobnosti člověka, jelikož tvoří poměrně dlouhý interval jeho života.
- právní identita – pro člověka velice důležitá. Váže se k osobním dokladům vydaným ve státě, ve kterém člověk získal občanství, a jimiž se před státem a jeho institucemi prokazuje. Právní identita je chráněna legislativou státu.
- digitální identita – poslední, a pro tuto práci nejdůležitější pohled na identitu člověka. Vztahuje se k době informačních technologií a čím dál větší dostupnosti sítě internet. Definuje uživatele podle jeho chování na internetu, často se k ní vážou přihlašovací údaje (uživatelské jméno a heslo), které jsou ekvivalentem osobních dokladů, jelikož pomocí nich uživatel prokazuje svou totožnost před portály, na kterých má uživatel svůj uživatelský účet vytvořený. Na internetu může jednomu člověku náležet hned několik digitálních identit, dle portálů, na kterých se nachází. V době sociálních sítí mohou mít lidé nekonečně mnoho digitálních identit i v rámci jedné sociální sítě. Podrobnějším rozborem této identity se zabývá kapitola 2.

Identitu lze chápat i z mnoha dalších typů, pohledů či kritérií. Pro uvedení do problematiky a účely této práce však stačí výše uvedené.

1.2.1 Zneužitelné identity

Je potřeba si uvědomit, že pokud dojde ke zneužití identity, může to mít pro majitele identity negativní následky. Nemusí se jednat jen o finanční poškození. Může dojít také k psychické újmě v podobě poškození reputace majitele identity. Různé instituce mohou majitele zneužité identity poté považovat za nedůvěryhodného, vztahy mezi majitelem zneužité identity a přáteli či rodinou mohou být ohroženy.

Výše uvedené identity mají různé úrovně zneužitelnosti – některé identity lze zneužít snadno, některé hůř, a některé, jako takové, nelze zneužít samostatně. Z teoretického hlediska lze ale nějakým způsobem zneužít jakoukoliv identitu. Ne všechny identity jsou ale pro potenciálního útočníka zajímavé – nezíská finanční obnos, nepoškodí reputaci své oběti apod. Záleží na záměru, s jakým se útočník připravuje identitu oběti zcizit.

Následující identity s sebou nesou největší riziko zneužití:

- tělesná identita,
- sociální identita,
- vzpomínková identita (v kombinaci s tělesnou identitou),
- právní identita,
- digitální identita.

1.2.1.1 Zneužitelnost tělesné identity

Jednou z nejsnadněji zneužitelných identit je identita tělesná. Je viditelná na první pohled, potenciální útočník nemusí cílovou osobu znát nijak důvěrně. Stačí k tomu například fotografie, nebo pouhý pohled. Styl oblékání, rysy v obličeji či vlasy lze v dnešní době celkem spolehlivě napodobit.

Útočník, který zcizil pouze tělesnou identitu své oběti, tzn. vypadá přesně jako ona, nejspíš neošálí rodinu či přátele, protože se jako oběť nechová a pravděpodobně ani nemluví. Může ale obelstít například bezpečnostní kamery v podniku, kde se chystá spáchat trestný čin. Případně může vystupovat prostřednictvím fotek, jako majitel útočníkem zcizené identity, na sociálních sítích. V obojím případě dojde k poškození pověsti oběti a ochraně identity útočníka, pokud nedojde k objasnění situace – že byla zcizena identita osoby.

1.2.1.2 Zneužitelnost sociální identity

Sociální identita může být také poměrně snadno zneužitelná. Nestačí pro to ale pouze fotografie. Potenciální útočník musí cílovou osobu již chvíli sledovat. Vypozorovat její vzorce chování, návyky, vlastnosti a další povahové rysy. Tato identita se ale významně vztahuje k identitě tělesné. Zneužití samotné sociální identity mnoho „užitku“ nepřinese. Pokud je ale zneužita zároveň s identitou tělesnou, lze se již poměrně důvěryhodně vydávat za někoho jiného.

Pokud tedy budeme uvažovat, že útočník zároveň s identitou sociální zneužije i identitu tělesnou, může kromě obelstění bezpečnostních kamer, obelstít také rodinu či přátele oběti. Může se tak dostat k citlivějším informacím oběti, od rodiny či přátel si vypůjčit různé peněžní částky. A stejně jako v předchozím případě u tělesné identity, může poškodit reputaci oběti.

1.2.1.3 Zneužitelnost vzpomínkové identity

Zneužitelná může být také identita vzpomínková, avšak pokud se jedná o kombinaci také s identitou tělesnou. Vzpomínky jednoznačně dotváří osobnost člověka a některé vzpomínky jsou typické pro konkrétního jedince. Pokud ale útočník zneužije pouze vzpomínkovou identitu, je pro okolí více než rozeznatelný a lze snadno rozeznat zneužití, jelikož útočník cílovou osobu nemusí připomínat ani vzdáleně. Pokud ale zneužije jak tělesnou, sociální i vzpomínkovou, rozeznat podvrh již není tak jednoduché.

Vzpomínková identita víceméně dotváří identitu tělesnou a sociální – pokud útočník zneužije všechny tyto identity najednou, působí tak důvěryhodněji, jako majitel jím zcizené identity. Může ji tedy použít stejně jako identitu tělesnou a sociální.

1.2.1.4 Zneužitelnost právní identity

Pro zneužití právní identity musí mít pachatel k dispozici osobní doklady svojí oběti. Jelikož je právní identita chráněna legislativou, lze její zneužití trestně stíhat, tudíž pachatel, který se dopustí činu zneužití právní identity pomocí osobních dokladů, může následkem toho, být potrestán vězením a zápisem do svého trestního rejstříku, který může podstatně ovlivnit jeho budoucnost (např. při hledání zaměstnání po skončení trestu).

V případě, že se útočníkovi podaří získat osobní doklady svojí oběti, může tak například vyzvedávat zásilky, které mu nepatří (patří jeho oběti – tomu, komu osobní doklady patří), jelikož některé doručovací společnosti požadují při vyzvedávání pouze občanský průkaz. S doklady oběti se může pokusit jednat na různých úřadech či bankovních institucí jménem jeho oběti. Mnohdy totiž fotografie na dokladech nekontrolují, případně může útočník vymyslet způsob, jak se z toho, že se fotografii na dokladu nepodobná vymluvit.

1.2.1.5 Zneužitelnost digitální identity

Pro dnešní dobu ale největší riziko zneužitelnosti představuje digitální identita, které je také především věnována tato práce.

Dnešní doba, kdy má přístup k internetu téměř každý, ať už prostřednictvím stolního počítače, notebooku či mobilního telefonu, nabízí komukoliv nespočet možností, jak si svou digitální identitu budovat. Spousta uživatelů si ale již neuvědomuje, jaké riziko s sebou nese každý uživatelský účet, a každý příspěvek, který pomocí něj zveřejní. V současnosti již existují velice rafinované metody, jak získat osobní informace uživatele, a jak tyto osobní informace využít k přístupu k jeho dalším uživatelským účtům.

Pokud si uživatel pečlivě nechrání své osobní informace, která dává nejen na sociální sítě, ale celkově na jakékoliv místo přes síť Internet, jeho identita může být velice snadno zneužita. Ať už se jedná o fotografie, citlivé údaje jako je adresa bydliště nebo rodné číslo, či uživatelské jméno a heslo k některému ze svých účtů.
Obecně je doporučováno takové informace, které má uživatel zájem ochránit (zabránit zneužití), do sítě Internet vůbec nevkládat (ne všechny portály požadují při registraci vložení např. jména a příjmení). Výjimku představují takové digitální identity, které jsou v kombinaci s identitou právní (elektronická identita, bankovní identita).
Všechny tyto informace mohou být potenciálními útočníky zneužity – pro přístup k financím (internetové bankovnictví), k sociálním sítím, e-mailovým schránkám atd.

1.3 Identita z pohledu práva

Identita je z pohledu práva chráněna v následující legislativě:

- zákon č. 89/2012 Sb. Občanský zákoník,
- zákon č. 110/2019 Sb. Zákon o zpracování osobních údajů,
- zákon č. 40/2009 Sb. Trestní zákoník,
- zákon č. 262/2006 Sb. Zákoník práce.

V této podkapitole bude převážně čerpáno ze zákona č. 89/2012 Sb., občanský zákoník (dále jen občanský zákoník), který pojednává právě o osobnosti člověka a ochraně informací, spojenými s osobností člověka.

V rámci této diplomové práce je pozornost zaměřena pouze na osoby fyzické, tedy na jednotlivce, o kterých pojednává občanský zákoník – hlava II – Osoby, díl 2 – Fyzické osoby. [6]

Identita je tedy analyzována pouze z pohledu práva České republiky.

Jak je ve výše uvedené části občanského zákoníku definováno (oddíl 1 – Obecná ustanovení, § 23), u člověka vzniká právní osobnost narozením, a zaniká až smrtí (důkaz smrti je také definován v občanském zákoníku – hlava II – Osoby, díl 2 – Fyzické osoby, oddíl 1- důkaz smrti). [6]

Podstatnou část z hlediska definice právní identity člověka tvoří v občanském zákoníku hlava II – Osoby, díl 2 – Fyzické osoby, oddíl 6 – Osobnost člověka. Následující řádky rozebírají vybrané pododdíly tohoto oddílu, relevantní k obsahu této diplomové práce. [6]

Pododdíl 1 – Obecná ustanovení – § 81 – vymezuje ochranu osobnosti člověka i jeho přirozená práva bez ohledu na souhlas či nesouhlas s jeho svobodným rozhodnutím žít podle svého. Uvádí také ochranu života a důstojnosti člověka, „*jeho zdraví a právo žít v příznivém životním prostředí, jeho vážnost, čest, soukromí a jeho projevy osobní povahy*“. [6]

Pododdíl 1 – Obecná ustanovení – § 82 – dává člověku právo na odstranění následků a upuštění od neoprávněného zásahu v případě, že byla dotčena jeho osobnost. V druhém článku se myslí také na to, že domáhat se ochrany osobnosti člověka může po jeho smrti také jakákoliv jeho blízká osoba. [6]

Pododdíl 2 – Podoba a soukromí – § 84 – k tomu, aby mohla být jakkoliv zachycena podoba člověka, za účelem zjištění jeho totožnosti, musí příslušná osoba dát svůj souhlas. [6]

Pododdíl 2 – Podoba a soukromí - § 85 – bez souhlasu dané osoby, nesmí být šířena jeho podoba. [6]

Pododdíl 2 – Podoba a soukromí - § 87 – v případě, že někdo svolil k šíření některého rysu svojí osobnosti (podoba, zvukový nebo obrazový záznam, jiné projevy jeho osobnosti), má právo na to, aby svolení odvolal, nezávisle na tom, zda jej poskytl na dobu určitou či neurčitou. [6]

Ne vždy je ale potřeba poskytovat souhlas k šíření nebo jinému použití některých osobnostních rysů. Pojednávají o tom následující paragrafy:

- § 88 – podobizna, obrazový či zvukový záznam jsou pořízeny nebo použity „*k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob nebo se použijí na základě zákona k úřednímu účelu či v případě, že někdo veřejně vystoupí v záležitosti veřejného zájmu.“* [6]
- § 89 - podobiznu, obrazový či zvukový záznam je možné také bez souhlasu pořídit k vědeckému či uměleckému účelu, nebo pro tiskové, rozhlasové, televizní a podobné vysílání. [6]

Dle § 90, je zásah do soukromí člověka možný, pouze přiměřeným způsobem, a nesmí být v rozporu s oprávněnými zájmy člověka. [6]

Podstatným dílem rozebírá identitu člověka pododdíl 3 občanského zákoníku – Právo na duševní a tělesnou integritu. [6]

Hned první paragraf (§ 91) v tomto pododdílu určuje nedotknutelnost člověka. V dalším paragrafu (§ 92) také uvádí, že smrtí lidské tělo neztrácí právní ochranu. Je zakázáno

nakládat s lidskými ostatky způsobem, jenž by se dal považovat jako nedůstojný vzhledem k zemřelému. [6]

Pododdíl 3 – Zásah do integrity – jedná se o obsáhlou část pododdílu 3 vymezující okolnosti, za kterých, kdo a jak má právo na zásah do integrity člověka. Jedná se o paragrafy 93-103. [6]

U žádného z výše uvedených paragrafů, se nejedná o jejich přesné znění. Přesné znění všech paragrafů je možné dohledat v zákoně č. 89/2012 Sb. – Občanský zákoník.

Identita člověka je tedy občanským zákoníkem velice dobře chráněna. Z občanského zákoníku vyplývá, že právo nakládat se svou identitou má pouze ten, komu patří, a může s ní být zacházeno další osobou jen v případě, že k tomu dá její majitel souhlas. Ošetřeny jsou také výjimky, dle kterých majitel identity nemusí poskytnou svůj souhlas k šíření některých částí jeho identity. Kromě identity tělesné (fyzické), se v občanském zákoníku myslí také na psychickou stránku identity a soukromí člověka.

1.3.1 Prokázání identity

Každý stát, především v zájmu svojí bezpečnosti i bezpečnosti občanů, vyžaduje od svých, ale i cizích (příchozích – občanů jiného státu) občanů, nějakým způsobem prokázání jejich totožnosti. Dělají tak na základě některého z dokladů, které jim byly oficiálně vystaveny některým z oprávněných úřadů jejich vlasti.

Doklady o osobní identitě člověka jsou vydávány státní evidencí – matrikou, jenž je definována v zákonu č. 301/2000 Sb. – část první – Matriky, jméno a příjmení, hlava I – Matrika, Díl 1. [7]

Úplně prvním dokladem totožnosti člověka se stává rodný list, který je vystavován na základě zápisu do knihy narození, kam se dle § 14, definovaného v zákonu č. 301/2000 Sb. – část první – Matriky, jméno a příjmení, hlava I – Matrika, Díl 2 – Zápisy narození, uzavření manželství, vzniku partnerství a úmrtí – Kniha narození zapisuje:

- jméno (jména) a příjmení dítěte,
- den, měsíc a rok narození dítěte,
- rodné číslo, místo narození a pohlaví dítěte,
- jméno, popřípadě jména, příjmení, popřípadě rodná příjmení, data a místa narození, rodná čísla, státní občanství a místo trvalého pobytu rodičů,

- datum zápisu a podpis matrikáře (definici matrikáře popisuje zákon č. 301/2000 Sb. – část první – Matriky, jméno a příjmení, hlava I – Matrika, Díl 1, § 9 – Matrikář). [7]

Podrobnosti o zápisu do knihy narození (kdy se uvádí či neuvádí určité informace, doklady, které musí osoba oznamující narození dítěte předložit atp.), jsou stanoveny ve výše zmíněném dílu výše zmíněného zákona v paragrafech 14-19. [7]

Informace o tom, co musí obsahovat rodný list, jsou uvedeny v paragrafu 29. Jedná se o stejné údaje, které musí obsahovat kniha narození. [7]

Osoby, které nedosáhly 15 let, svou identitu prokazují svým rodným listem.

Při dovršení 15 let věku musí osoby vlastnit občanský průkaz, který při prokazování identity nahradí rodný list. [8]

Podmínky vydání občanského průkazu jsou uvedeny v zákoně č. 328/1999 Sb., část druhá – Vydávání občanských průkazů a potvrzení o občanském průkazu, hlava I – Podmínky a postup při vydávání občanských průkazů, § 4 a § 4a – Vydávání občanského průkazu. [8]

Podrobnosti o tom, kdo je povinen vlastnit občanský průkaz, udává zákon č. 328/1999 Sb., část první – Základní ustanovení, § 2 – Občanský průkaz. [8]

Ze stejné části zákona je také § 3, který stanovuje veškeré náležitosti, jež musí občanský průkaz obsahovat. Jsou to:

- digitální zpracování podoby občana (fotografie),
- podpis občana,
- jméno (jména), příjmení, pohlaví, státní občanství, datum, místo a okres narození, rodné číslo, adresa místa trvalého pobytu, včetně označení tohoto údaje jako adresy úřadu, je-li takto označen v evidenci obyvatel, a rodinný stav nebo registrované partnerství,
- datum skončení platnosti, číslo a datum vydání občanského průkazu a označení úřadu, který jej vydal,
- strojově čitelné údaje:
    - do strojově čitelné zóny jsou zapisovány tyto údaje (v tomto pořadí): kód dokladu, kód vydávajícího státu, číslo dokladu, kontrolní číslice, datum narození, kontrolní číslice, pohlaví, datum platnosti, kontrolní číslice, státní

občanství, celková kontrolní číslice, příjmení, jméno, popřípadě jména občana; kontrolní číslice a celková kontrolní číslice jsou číselným vyjádřením vybraných údajů ve strojově čitelné zóně,

- 2D kód: číslo občanského průkazu. (2D kód = dvoudimenzionální čárový kód s vysokou informační hodnotou a schopností detekce a oprav při jeho porušení,
- elektronický čip. [8]

Podrobnosti o uvedených informacích na občanském průkazu, občanských průkazech pro občany narozených v jiné zemi nebo co musí/může obsahovat elektronický čip jsou uvedený v plném znění paragrafu 3 ve výše zmíněném zákoně.

Pokud je tedy osoba požádána k prokázání totožnosti (právní identity), činí tak na základě občanského průkazu, případně jiného dokladu, který je spojen výhradně s údaji dotyčné osoby – například řidičský průkaz nebo cestovní pas – tyto doklady jsou dotyčné osobě vydávány mimo jiné po předložení občanského průkazu.

1.4 Identifikace

Úzce souvisí s prokazováním totožnosti – viz podkapitola 1.3.1 Prokázání identity, jelikož se jedná o zjištění či vyhodnocení totožnosti ve smyslu existence osoby či porovnávání s osobou jinou. [1]

Identifikace je rozhodovací proces, který má za úkol porovnat shodné nebo odlišné vlastnosti objektů. Nemusíme identifikovat pouze osoby, lze porovnávat i různé objekty. Důležité je, aby tento rozhodovací proces měl konečný počet rozhodovacích kroků, zkrátka aby šlo usoudit, že rozhodovací proces je u konce. [1]

Důležitým faktorem také je, že identifikace je podmíněna reálnou potřebou. Pokud se jedná o hledanou osobu, za dobu jejího pohřešování se mohla změnit délka jejich vlasů, což může znesnadnit její nalezení, avšak pokud jiné důkazy jasně hovoří, že dotyčná osoba je skutečně ta hledaná, délka vlasů nehraje žádnou roli. [1]

Osoby lze identifikovat ze dvou pohledů – vnější identifikace a vnitřní identifikace. [1]

1.4.1 Vnější identifikace osoby

Souvisí s identifikací takových lidských vlastností či charakteristik, které můžeme vzájemně porovnávat mezi sebou, díky své jedinečnosti a neopakovatelnosti. Mají zároveň

dostatečnou vypovídající schopnost a jsou přijatelné jak pro specialisty, tak i pro laickou veřejnost. [1]

Jedním z největších aspektů při vnější identifikaci, jsou biologické rysy člověka. K vnější identifikaci osoby také slouží charakteristiky, které byly osobě přiděleny uměle, nebo si je dobrovolně osvojila. Jedná se především o:

- jméno a příjmení,
- osobní doklady,
- identifikační čísla a karty,
- identifikační karty a čipy,
- biočipy. [1]

1.4.2 Vnitřní identifikace osoby

Vnitřní identifikace osoby, nebo také sebeidentifikace, je založena na tom, že osoba se může sebeztotožňovat také s různými politickými ideami, původem, jazykem, vyznávaným náboženstvím, etnickou příslušností apod. Osoba se ale může sebeztotožňovat i s jinou osobou – dokáže se vcítit do jeho situace, nebo do jeho pozice. [1]

1.5 Shrnutí

Z pohledu identičnosti, lze tedy zkoumat nejen osoby, ale také předměty, objekty, zvířata či rostliny. Identita člověka je ale tvořena i dalšími částmi identity, které však neživé objekty postrádají, jako je jeho chování v různých kruzích společnosti, jeho povahové rysy nebo vlastnosti, jenž můžeme v omezené míře pozorovat také u zvířat.

Záleží také na tom, z jakého úhlu identitu pozorujeme. Je potřeba vždy posoudit konkrétní situaci a vyhodnotit, zda je pro nás důležitější pohled kvalitativní, nebo kvantitativní.

Všechny dílčí identity člověka ale mají tu nevýhodu, že je možné je zneužít. Ať se jedná o jakoukoliv, všechny součásti naší identity je třeba chránit, jelikož ztráta téměř každé části představuje různý stupeň nebezpečí.

Nejen pro tyto případy jsou ve sbírce zákonů státu jasně definovány údaje, které slouží k identifikaci jedince z právního hlediska.

V současné době informačních technologií a především internetu, představuje nejdůležitější článek digitální identita, na kterou se primárně zaměřuje tato práce.

2 KYBERNETICKÁ BEZPEČNOST

Tato kapitola se bude zabývat otázkou kybernetické bezpečnosti, ochrany osobních údajů a identitami člověka v kyberprostoru.

Kybernetická bezpečnost je podle Jiráska definována jako *„souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.“* [9]

Název pochází z anglického Cyber Security a v současné době neodmyslitelně patří k informačním technologií. Nebyla však vždy jejich nezbytnou součástí. Své místo si v tomto oboru získávala postupně s rozvojem, a tím pádem i s potřebou, uchovávat data elektronicky. Jejím hlavním úkolem je chránit veškerá data, informace a majetek před kybernetickými útoky (zničení, ztráta, zneužití, krádež). [10, 11]

K tomu, aby byla spolehlivě ochráněna data uživatelů, je potřeba, aby se dostatečné ochrany dostalo také systémům, sítím a programům, ve kterých se data nachází, nebo s nimi jinak pracují. [10]

Ať je snaha sebevětší, ochrana nikdy nemůže být naprosto dokonalá. Kybernetickou bezpečnost totiž velice ovlivňuje lidský faktor, jeho zájmy a chybovost. Uživatelé by měli perfektně ovládat zásady ochrany dat a dalších principů, jako je informovanost o nebezpečných e-mailových přílohách, zabezpečení svých účtů dostatečně silnými hesly nebo pravidelném zálohování svých dat. [10]

Dalším podstatným článkem kybernetické bezpečnosti jsou postupy, které je potřeba dodržet ať už při aktivní ochraně před útoky, tak i v situaci, kdy již k útoku došlo a následné obnově dat/systému. Z pohledu organizace je velice důležité, aby měla připravené scénáře, které pokryjí takovéto situace, a tudíž všichni zaměstnanci (nebo zaměstnanci, od kterých to situace vyžaduje) mají jasné pokyny, jak postupovat. [10]

Poslední, neméně významnou, složkou kybernetické bezpečnosti jsou dostupné technologie, kterými uživatelé mohou ochránit svoje data. Jedná se především o softwarová řešení jako je správné nastavení firewallu či antivirové programy apod. Mnohem větší ochrany dosáhneme, když kromě koncového počítače zabezpečíme proti útokům celou lokální počítačovou síť na úrovni routeru. [10]

Pokud to tedy shrneme, kybernetická bezpečnost se skládá ze tří nejdůležitějších složek:

- lidský faktor,

- postupy v případě, že došlo útoku,
- dostupné technologie. [10]

Bezpečnostní technologie musí jít neustále dopředu spolu s tím, že v době moderních technologií je snaha veškeré dokumentace, informace, data vést pouze v elektronické podobě. Spolu s nimi jdou ale také útočníci, kteří se svými útoky snaží dostávat ještě o krok napřed a být tak hůře odhalitelní. Nehrozí ale pouze zneužití dat, spolu s tím je také velkou hrozbou odcizení financí z bankovního účtu, či právě zneužití identity.

2.1 Kybernetická bezpečnost v ČR

Česká republika jako stát, dle webu cybersecurity.cz, poprvé přijala opatření na celostátní úrovni v oblasti kybernetické bezpečnosti 15. března 2010, kdy bylo schváleno usnesení vlády č. 205, které pojednává o řešení problematiky kybernetické bezpečnosti. Institutem zodpovědným za tuto oblast bylo stanoveno Ministerstvo vnitra České republiky. [11]

O rok později, 19. října 2011, tuto roli převzal Národní bezpečnostní úřad. 1. srpna 2017 potom vzniká Národní úřad pro kybernetickou a informační bezpečnost – NÚKIB. Podkladem k tomu byl nově novelizovaný zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Tento zákon je v souladu se zákony Evropské unie a pojednává o bezpečnosti sítí elektronických komunikací a informačních systémů. Udává práva a povinnosti subjektů, kteří spadají do kyberprostoru České republiky. [11]

Každý ze subjektů, spadající do kybernetického prostoru České republiky ale může mít v rámci svého, uzavřeného, kyberprostoru ještě i vlastní pravidla, která ale nesmí být v rozporu z výše zmíněným zákonem o kybernetické bezpečnosti. [11]

2.2 GDPR

Jedná se o „*Obecné nařízení na ochranu osobních údajů*“ (z anglického General Data Protection Regulation – GDPR), které bylo v dubnu 2016 schváleno Evropským parlamentem a Radou Evropské unie, a v květnu 2018 vzešlo v platnost plošně ve všech státech Evropské unie. *„Nařízení Evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)“*(dále jen „nařízení“), si dává za cíl zvýšit ochranu osobních dat občanů

členských států. Nařízení upravuje pravomoci Úřadu pro ochranu osobních údajů, který problematiku ochrany osobních dat zastřešuje. [12, 13]

V první části je definováno, z jakých důvodů toto nařízení vzniklo a proč je důležité jeho zavedení a dodržování, co je hlavním účelem, uvádí související úpravu platnosti směrnice 95/46/ES nebo pojednává o důležitosti rovnocennosti zpracovávání údajů ve všech státech EU. [13]

Hlavní cílem tohoto nařízení je především ochránit osobní údaje fyzických osob. Ty jsou v nařízení definovány jako: *„všechny informace, dle kterých lze danou fyzickou osobu identifikovat. Kromě jména do těchto informací zahrnuje také např. identifikační číslo, síťový identifikátor, nebo i různé části identit, které nařízení označuje jako identitu fyzickou, fyziologickou, genetickou, psychickou, ekonomickou, kulturní a společenskou.“* [13]

V souvislosti s ochranou údajů se v nařízení pojednává také o nakládání s nimi neboli o jejich zpracovávání. Za zpracovávání se považuje shromažďování, zaznamenání, uspořádání, strukturování, ukládání, přizpůsobení, pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření, seřazení, zkombinování, omezení, vymazání nebo zničení. [13]

Nařízení specifikuje také určité role. Jsou jimi správce a zpracovatel. Správcem může být jakákoliv fyzická či právnická osoba či jakýkoliv jiný subjekt, který udává, z jakého důvodu a jakými prostředky jsou osobní údaje zpracovávány. Správci pro zpracovávání osobních údajů využívají tzv. zpracovatele. Zpracovatelem může být opět jakýkoliv subjekt. [13]

Nařízení definuje také „příjemce“ a „třetí stranu“. Jak příjemcem, tak třetí stranou může být také libovolný subjekt, který ale nemá roli subjektu údajů, správce, zpracovatele ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů. Třetí straně tedy mohou být osobní údaje poskytnuty, stejně tak, jako příjemci, avšak nesmí být jimi využity pro další zpracovávání. [13]

Za správnost a korektnost zpracovaných osobních údajů odpovídá správce, který to zároveň musí být schopen doložit. V jaké formě a za jakým účelem mohou být osobní údaje zpracovávány, je uvedeno v kapitole II, článku 5 a 6. [13]

Osoba, jejíž osobní údaje jsou předmětem zpracování, je v nařízení označována jako subjekt údajů. Subjekt údajů nemusí vždy poskytnout souhlas se zpracováním svých osobních údajů. Pokud jej ale poskytne, musí jej udělit výslovně/písemně a správce musí být schopný tento souhlas dohledat, a prokázat tak, že osobní údaje zpracovává vždy se souhlasem subjektu

údajů. Subjekt údajů může, dle nařízení, svůj souhlas kdykoliv odvolat stejně snadno, jako svůj souhlas poskytnul. Za dítě, které je mladší 16 let poskytuje souhlas se zpracováním jeho osobních údajů osoba, která nese rodičovskou zodpovědnost k dítěti. [13]

Z pohledu nařízení, existuje skupina zvláštních kategorií osobních údajů, jejichž zpracovávání je zakázáno. Tyto údaje však smí být zpracovány, pokud:

- byl udělen výslovný souhlas s jejich zpracováním,
- to bylo z právního hlediska nezbytné,
- na tom závisí ochrana životně důležitých zájmů subjektu údajů,
- údaje zveřejní sám subjekt údajů,
- je zpracování důležité pro účely archivace.

Jedná se o tyto kategorie osobních údajů:

- rasový/etnický původ,
- politické názory,
- náboženské vyznání,
- filozofické přesvědčení,
- členství v odborech,
- genetické údaje,
- biometrické údaje,
- údaje o zdravotním stavu,
- údaje o sexuálním životě či sexuální orientaci. [14]

Jakmile subjekt údajů poskytne své osobní informace ke zpracování, může se poté domáhat opravy nepřesných osobních údajů, ale také úplného vymazání osobních údajů. Podmínky pro vymazání osobních údajů jsou uvedeny v kapitole III, oddíle 3, článku 17. [13]

V kapitole IV, oddíle 1, jsou v článcích 24 až 31 upřesněny odpovědnosti správců a zpracovatelů, stanoveny pravidla zastupování zástupců správců a zpracovatelů mimo Evropskou Unii, a ukládá povinnost správcům vést záznamy o zpracování osobních údajů. [13]

Oddíl 2, nacházející se ve stejné kapitole, se zabývá zabezpečením osobních údajů. Správce i zpracovatel jsou povinni provést vhodná technická a organizační opatření, pro zajištění takové úrovně zabezpečení, která odpovídá danému riziku. Zpracovávané osobní údaje musí být v zašifrované podobě. Důraz je kladen také na důvěrnost, integritu, dostupnost systémů, a také na schopnost obnovy v případě, že dojde k fyzickým či technickým problémům. Opatření musí být pravidelně testována, aby bylo možné posoudit jejich účinnost a efektivitu. [13]

Nařízení také ukládá zpracovateli povinnost neprodleně ohlásit správci jakékoliv narušení bezpečnosti osobních údajů, a to nejpozději 72 hodin po tom, co se o narušení bezpečnosti dozvěděl. Ohlášení musí také splňovat určité požadavky, které jsou sepsány v kapitole IV, oddíle 2, článku 33. [13]

Zbytek nařízení rozebírá nakládání s osobními údaji, pokud jsou předávána do třetích zemí nebo mezinárodních organizací, nezávislé dozorové úřady, které dohlíží na dodržování tohoto nařízení. Také definuje vztahy mezi dozorovými úřady. [13]

Dále potom definuje právní ochranu pro subjekt údajů, odpovědnost a sankce, vymezuje zvláštní situace, při nichž dochází ke zpracování, akty v přenesené pravomoci a prováděné akty, a nakonec závěrečná ustanovení. [13]

2.3 Elektronická identita

Pojem „elektronická identita“ se v České republice začal hojně skloňovat v červenci 2018, kdy (podle nového zákona č. 250/2017 Sb., o elektronické identifikaci, který odpovídá nařízení eIDAS, a novely zákona č. 328/1999 Sb., o občanských průkazech) se začaly do nových občanských průkazů implementovat kontaktní elektronické čipy. Takto vybavené občanské průkazy slouží především jako prostředek k jednoznačné identifikaci občana při přístupu na webové portály státní správy. Elektronický čip totiž nese stejné informace o majiteli, jako jsou uvedeny na jeho občanském průkazu. [15, 16]

Obr. 1. Zadní strana občanského průkazu s elektronickým čipem [17]

Aby bylo možné čip používat a byla zajištěna maximální možná bezpečnost a důvěryhodnost při přístupu, je potřeba na příslušném úřadě čip aktivovat a vytvořit k němu dva kódy o délce 4 až 10 číslic. Kódy jsou označovány jako IOK (= identifikační osobní kód) a DOK (= deblokační osobní kód) sloužící stejně, jako je tomu u PINu a PUKu u SIM karet mobilních telefonů. Shodně také dochází k zablokování čipu, je-li třikrát chybně zadán IOK. Pokud se desetkrát zadáním DOKu nepodaří čip odblokovat, je nutné navštívit příslušný úřad. [16, 18]

Pokud tedy uživatel má čip na svém občanském průkazu aktivní, zná svůj IOK a DOK a disponuje čtečkou karet, může pro přístup k online službám státní správy využívat svou elektronickou identitu. [16]

2.3.1 eIDAS

V souvislosti s elektronickou identitou je vhodné vysvětlit i zkratku „eIDAS“, která s ní úzce souvisí. Je tak označováno „*nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES*“. Toto nařízení stanovuje okolnosti a podmínky, za kterých je možné elektronickou identifikaci považovat za bezpečnou a důvěryhodnou s ohledem na přístup k portálům a službám státní správy. Aby nebylo o důvěryhodnosti elektronické identifikace pochyb, je nutné k ní využít kvalifikovaného systému elektronické identifikace, jenž může být poskytován buď státními orgány, nebo subjekty, kterým byla Ministerstvem vnitra udělena akreditace pro provoz takového systému. [19]

Nařízení eIDAS se zabývá také problematikou elektronických podpisů, pečetí a časových razítek. [19]

2.3.2 Potvrzení identity osobním certifikátem

Elektronický čip na občanském průkazu může sloužit také jako úložiště osobních certifikátů, které jsou určeny k elektronickému podpisu. I ty totiž mohou definovat identitu člověka, například při elektronickém podepisování elektronických dokumentů. Takový podpis zcela nahrazuje podpis vlastnoruční. Aby bylo zajištěno maximální bezpečnosti a důvěryhodnosti, uživatel si nejprve musí zažádat u některého z poskytovatelů certifikačních služeb (certifikační autority) o osobní, nejlépe kvalifikovaný, certifikát (kvalifikované certifikáty jsou přesně definovány zákonem a lze je tedy použít pro komunikaci se státními orgány). Pomocí webu si vygeneruje žádost, do které vyplní své osobní údaje – jméno a příjmení, bydliště, případně další informace (například akademické tituly či generační označení), s žádostí uloženou na nějakém přenosném médiu (například flash disk) se dostaví na některou z poboček registrační autority, kde předá žádost ke zpracování operátorovi registrační autority. Před zpracováním žádosti se uživatel nejprve musí prokázat dvěma doklady totožnosti (běžně občanský průkaz spolu s řidičským průkazem nebo cestovním pasem). Jakmile je žádost zpracována, uživatel podepíše smlouvu o převzetí certifikátu, a certifikát je mu následně doručen na e-mailovou adresu, kterou zadal při vyplňování žádosti. Tyto certifikáty nejsou zdarma, jejich ceny se u různých certifikačních autorit liší. [20]

Princip ověřování elektronických podpisů vytvořené pomocí certifikátů spočívá v asymetrické kryptografii (pár klíčů – veřejný a soukromý klíč). Samotný podpis totiž nevzniká certifikátem jako takovým. Dokument je podepsán klíčem soukromým a pro ověření pravosti podpisu se používá klíč veřejný, který bývá většinou součástí podpisu – každý, pro koho je dokument určen tedy dostává náš veřejný klíč, který je v páru s klíčem soukromým, který se naopak nesmí dostat k nikomu jinému, než k tomu, komu patří. Veřejný klíč je uveden v certifikátu, který obsahuje také autoritu, která certifikát vydala, a to jsou právě ty informace, které zaručují, že elektronický podpis provedla osoba, která je uvedena v certifikátu, jelikož dokazuje, že ta stejná osoba drží také soukromý klíč. [20, 21]

Jestliže uživatel nevlastní občanský průkaz obsahující elektronický čip, má možnost certifikát uložit na libovolnou podporovanou kartu s elektronickým čipem, případně si klíč i certifikát uložit přímo do počítače. [20]

Certifikáty jsou vydávány vždy na konkrétní dobu (z pravidla 1 rok). Pokud se blíží konec jeho platnosti, uživatel jej musí obnovit. Musí tak učinit, pokud je původní certifikát stále platný, jelikož žádost o následný certifikát musí být podepsána soukromým klíčem prvotního certifikátu. [20]

2.4 Digitální identita

Někdy se používá také výraz online či virtuální identita. Jedná se o totožnost, kterou si člověk utváří svým vystupováním na internetové síti. Pro její získání stačí alespoň jednou do této sítě vstoupit, jelikož do utváření digitální identity spadají také webové stránky, které uživatel navštěvuje (jeho historie prohlížení), služby, které na internetu využívá (internetové bankovnictví, e-mail), přihlašovací údaje, jako je přihlašovací jméno (nickname) a heslo, k portálům, které navštěvuje (sledování videí/filmů/seriálů, internetové obchody – e-shopy) nebo jaké nástroje k tomu používá (internetový prohlížeč, počítač, mobilní telefon). [22, 23]

Podstatnou část digitální identity člověka tvoří v dnešní době také sociální sítě, které jsou mocným nástrojem pro vykonstruování takové digitální identity, která je pro uživatele žádoucí. Zveřejněním jen vybraných informací o své skutečné osobě a nahráváním různě upravených a naaranžovaných fotografií potom uživatel může získat naprosto odlišnou identitu oproti jeho identitě v reálném světě. To samozřejmě není v rozporu s tím, že lze na sociálních sítích vybudovat svoji digitální identitu totožnou s tím, kým opravdu je. Existují i sociální sítě speciálně pro sdílení pracovních profilů (pracovních identit), a jejich uživatelé jsou jako potenciální zaměstnanci pro budoucí zaměstnavatele viditelnější. Můžou si na takovém profilu vést například svůj životopis, nebo sdílet odborné články související s jejich profesí. [22, 25]

Sociálních sítí je navíc mnoho, takže si uživatel může vybudovat na každé síti identity odlišné, nebo založením nového profilu a poskytnutím opět jen vybraných informací vytvořit další identitu v rámci jedné sociální sítě, které je ale odlišná od té původní. Tato situace již hraničí s identitou falešnou. V tomto případě se ale o falešnou identitu nejedná, jelikož uživatel mající na sociální síti více identit se tím nesnaží nikoho poškodit. [24, 25]

Stejně jako ve skutečném světě se prokazujeme občanským průkazem, na internetové síti, nejen na té sociální, musíme prokázat, že daná digitální identita je opravdu naše. Většinou se tak děje zadáním přihlašovacích údajů jako je přihlašovací jméno a heslo. Přihlašovacím jménem se většinou rozumí:

- přezdívka, kterou si uživatel sám vymyslel, a která byla k dispozici (nepoužívá ji už někdo jiný),
- e-mail – jedinečný identifikátor – nemůže existovat více shodných e-mailových schránek,
- identifikační číslo (klientské – např. u elektronického bankovnictví),
- případně jiný identifikátor, pro daný portál typický. [22]

V kombinaci s přihlašovacím jménem je nutné zvolit také heslo, které musí splňovat určité parametry a neměl by ho znát nikdo jiný kromě uživatele samého. [22]

2.5 Bankovní identita

Bankovní identita spadá do kategorie právní identity a můžeme ji obecně pojmout jako souhrn informací, které nás definují před bankou, u které máme založený bankovní účet. Zpravidla je to jméno a příjmení, rodné číslo, trvalé bydliště, e-mail a telefonní číslo, dále potom klientské číslo, které nám bylo přiděleno právě založením účtu. Jako alternativa slouží unikátní uživatelské jméno, které si volí uživatel společně s heslem k účtu. Po založení účtu může uživatele definovat také číslo jeho kreditní karty, která se vždy vztahuje ke konkrétnímu účtu a její číslo je jedinečné. Některé banky umožňují potvrzení identity PIN kódem nebo otiskem prstu přes mobilní aplikaci, ověření hlasem nebo osobním certifikátem uloženým na kartě. Způsoby ověření se mezi bankovními subjekty liší, důležité je, aby banka měla tolik důvěryhodných osobních informací, aby mohla jednotlivé uživatele jednoznačně identifikovat. [26, 27]

V roce 2019 se v České republice začal ve spojení s bankovní identitou objevovat výraz „BankID“, což by měl být systém, který by umožňoval majitelům bankovních účtů přistupovat na portály služeb státní správy či soukromého sektoru na základě ověření identity pomocí internetového bankovnictví. [28]

Ještě téhož roku Česká bankovní asociace představila projekt nazvaný „SONIA“, který bude mít za úkol právě ověřování totožnosti občanů pomocí svého internetového bankovnictví při jednání nejen se státními úřady, ale také soukromými subjekty, do kterého spadá i například podepisování oficiálních dokumentů přes internet. Projekt si získal podporu jak státu, tak i všech bankovních subjektů patřících do České bankovní asociace. Podstatná je také integrita se všemi již existujícími státními službami s ohledem na legislativu. Projekt by se měl dostat do provozu v roce 2021. [29, 30]

2.6 Falešná identita

Je ekvivalentem toho, když se na základě zcizených dokladů člověk vydává za někoho jiného. V internetovém prostředí se však uživatel vydává za někoho jiného zcizením jeho přihlašovacích údajů k danému portálu/službě/webové stránce atd. [31]

Zneužití digitální identity ohrožuje nejen uživatele, kterému zcizená identita patří, ale také uživatele, kteří v domnění, že danou osobu znají, mohou prozradit citlivé, či snadno zneužitelné informace a tím ohrozit i svou digitální identitu. [31]

Falešná identita většinou vzniká s cílem poškodit toho, komu identita patří. Ať už se jedná o jeho pověst, vztahy nebo finance. Způsobů, jak útočník – uživatel, který se záměrně snaží dostat k digitální identitě jiného uživatele – může falešnou identitu získat je několik. Tím úplně nejjednodušším je, že potenciální oběť se svými citlivými či přístupovými údaji zachází neopatrně a poskytne je svým nezodpovědným jednáním. Například je útočníkovi přímo sdělí po dotázání nebo je zveřejní někde v rámci svého profilu. Útočník pak nemusí vyvinout vůbec žádnou námahu pro získání falešné identity. V dnešní době jsou ale uživatelé čím dál obezřetnější a své údaje si chrání. [31, 32]

2.7 Bezpečnostní hrozby založené na zneužití identity

Jestliže se budeme držet stále kybernetické bezpečnosti a identit existujících v rámci internetového prostředí, v současné době jsou již uživatelé velice obezřetní při zadávání citlivých informací na internet. S obezřetností uživatelů ale také roste sofistikovanost způsobů získávání zmíněných údajů, jelikož již není tak snadné tyto údaje získat od uživatelů přímo. Útočníci začali využívat automatizované útoky, které mají právě za cíl získání dat uživatelů, nebo je finančně, či jinak, poškodit. Těmto útokům se říká anglicky „Advanced Persistant Threats“ nebo ve zkratce APT, což v doslovném překladu znamená „pokročilé trvalé hrozby“. Je jich několik druhů. [10]

2.7.1 Phishing

Za tímto výrazem se skrývá automatické rozesílání podvodných e-mailů. Vychází z podobnosti mezi rybařením (v českém překladu) a způsobem, jakým útočníci data od svých obětí získávají. Nejdříve rozešlou podvodné zprávy, a čekají, která z potenciálních obětí na tuto zprávu nějakým způsobem zareaguje (chytí se, podobně jako se ryby chytnou na nahozenou návnadu). Zpráva se většinou tváří, že byla odeslána například z banky uživatele a často vyžaduje kliknutí na přiložený odkaz, který vede na podvodnou stránku, a následné

zadání přihlašovacích údajů uživatele do internetového bankovnictví. Pokud tak uživatel učiní, útočníci tak získají jeho přístupové údaje a mohou již snadno provádět transakce pod účtem své oběti, čímž dochází ke krádeži nejen jeho identity, ale také jeho financí. [10,32]

Útočníci využívají phishing několika technikami:

- pharming – v češtině někdy označováno jako „farmaření“. Spočívá v zachycení komunikace mezi uživatelem a serverem (například serverem banky uživatele) a přesměrování komunikace v procesu přihlašování (po zadání přihlašovacích údajů a odeslání požadavku o přihlášení), na IP adresu podvrženou útočníky. Ti takto získají uživatelské jméno a heslo uživatele – to jim umožní se za uživatele vydávat a zcizit mu tak jeho identitu. [32]
- MITM – zkratka anglického „Man-in-the-middle“. Jedná se o útok, kde se útočník stane prostředníkem mezi uživatelem a cílovým zařízením (například serverem), a může tak zachytávat a případně měnit veškerá data plynoucí jak od uživatele, tak i cílového zařízení bez toho, aniž by bylo možné jej odhalit. Takto tedy útočník může buď odchytit veškeré přihlašovací údaje, kterými se uživatel přihlašuje ke svým digitálním identitám bez toho, aniž by si toho uživatel všimnul. Nebo může komunikaci od uživatele zachytávat (získávat jeho informace) a přesvědčit jej, že komunikuje se správným cílovým zařízením. Ve skutečnosti však uživatel komunikuje s útočníkem. Může pak být zneužita jakákoliv digitální identita uživatele. [32]
- SMiShing – tato technika je založena na principu vymáhání citlivých dat od uživatelů přes mobilní telefony pomocí rozesílání SMS zpráv. Obsah zpráv většinou obsahuje sdělení, že uživatel je přihlášen k odběru některé ze služeb společnosti, za kterou se útočníci vydávají, nebo za libovolnou důvěryhodnou společnost. Pokud uživatel svůj odběr nezruší, bude mu služba účtována vymyšlenou částkou například za den, týden, měsíc atd. Uživatel pak v domnění, že toto předplatné ruší následuje webovou stránku jejíž odkaz je ve zprávě přiložen, zadá požadované údaje a tím je přímo poskytne útočníkům, kteří je pak mohou využít ke zcizení identity oběti. [32]
- vishing – využívá k útoku VoIP protokol (Voice over Internet Protocol), který je využíván pro hovory přes internetové spojení. Útočníci buď rozešlou podvodný e-mail, vydávající se za některou důvěryhodnou společnost, obsahující telefonní číslo, na které má uživatel zavolat. Po zavolání chtějí útočníci z nějakého důvodu po

uživateli, aby sdělil citlivé informace, nebo volají potenciálním obětem „naslepo“. Uživatel tedy sdělí přihlašovací údaje ke svojí identitě přímo útočníkům, pro které již není problém jeho identitu zneužít. [32]

- spam – nevyžádaná hromadná elektronická pošta, je rozesílána naslepo na náhodně vybrané e-mailové adresy. Tento typ podvodu již není tak efektivní, jelikož většinou obsahuje nabídku služeb, která by mohla uživatele zajímat a přinutit ho tak ke kliknutí na přiložený odkaz. Ten ale vede na podvrženou webovou stránku, kde by přihlášením uživatel poskytnul přihlašovací údaje útočníkům. Vůči spamům jsou již ale uživatelé velice nedůvěřiví a přistupují k nim obezřetně. Někteří poskytovatelé e-mailových služeb již zvládnou potenciální spamy filtrovat na základě společných charakteristik typických pro tuto metodu, a přesunout je rovnou do stejnojmenné složky. [32]

2.7.2 Malware

Tento typ škodlivého software se do počítače uživatele může dostat například kliknutím na nebezpečný odkaz, návštěvou nedůvěryhodného webu, stažením infikované e-mailové přílohy apod. Může v sobě nést téměř jakýkoliv škodlivý software. Ke zneužití identity může být například využít tak, že v sobě ponese tzv. keylogger, který dokáže zachytávat stisknuté klávesy na klávesnici uživatele, a tím útočníkům poskytnout přihlašovací jména a hesla uživatelů. Kromě zcizení identity může být také jeho cílem například poškození dat v počítači. [10, 32]

2.7.3 Social Engeneering

Jedná se o metodu, která využívá nejrůznějších triků, aby přiměla uživatele otevřít podvodný odkaz, navštívit infikovaný web, zadat své přihlašovací údaje pod důvěryhodnou záminkou, stažení podvodné aplikace apod. Pokud se útočníkům povede uživatele ošálit, snadno získají přístup k jeho účtům a tím získají také jeho digitální identitu. [10]

Tento způsob útoku pracuje s lidskými emocemi. Útočníci se často snaží ve svých obětech vyvolat například strach, chamtivost nebo zvědavost. Oběti potom pod nátlakem těchto emocí útočníkům poskytnou informace, o které si požádali. [33]

Příkladem může být například útočníky rozeslaný podvodný e-mail nebo telefonát. Svým obětem se v něm představí jako bankéř či investor s výhodnou investiční nabídkou. Stačí pouze, aby uživatel zaslal požadované informace k jeho bankovnímu účtu a o zbytek se

postará sám bankéř/investor. Útočníci většinou zmíní, jakou částku uživatel musí vložit (např. 1 000,- Kč), a jakou částku „za pomoci této výhodné investice“ získá (např. 100 000,- Kč). Pro přesvědčení uživatele často uvedou „pravdivý případ“, kterého byli svědkem (např. „Jeden můj klient vložil 500,- Kč a za měsíc se mu tato investice proměnila v 50 000,- Kč). [33]

Dalším příkladem, ve kterém hraje hlavní roli lidská zvědavost. Útočníci, kteří takto chtějí cílit na své oběti, se zajímají o to, co se děje ve světě. Mohou pak využít touhu po informacích a nedávnou tragickou událost k zacílení svých obětí. Rozešlou e-mailovou zprávu, která uvádí, že obsahuje přílohu s nově uniklými, dosud nikde nezveřejněnými, informace právě o této tragické události. V příloze se ale místo těchto informací nachází malware, který si tak oběti dobrovolně do svých zařízení nainstalují. [33]

2.8 Shrnutí

Kybernetická bezpečnost je v dnešní době velice důležitým pojmem nejen pro organizace a jejich počítačové sítě. Povědomí by měli mít i běžní uživatelé pohybující se po síti Internet. Současné technologie již dokážou zajistit poměrně spolehlivou ochranu před ztrátou či zneužitím dat. Nejsou to ale jen technologie, do kybernetické bezpečnosti spadá také lidský faktor, který chybovost může podstatně ovlivnit.

Kybernetická bezpečnost je natolik důležitým článkem, že jsou opatření přijímána plošně, pro celý stát, a nejen v České republice je na její zkoumání a zajištění zřízen speciální úřad. Evropská unie, jíž je Česká republika součástí, se problematikou ochrany osobních údajů v kyberprostoru také zabývá, vydala proto nařízení GDPR, kde nařizuje, jak se s osobními údaji, které lidé poskytnou pro zpracování má či nesmí zacházet.

Internet poskytuje svým dnešním uživatelům mnoho způsobů, jak v jeho prostorech vystupovat. Uživatelé tak získávají různé identity, a nemusí se jednat pouze o identity na sociálních sítích. Jedná se také o „oficiální“ elektronické identity, které zastupují občany v kyberprostoru naprosto shodně, jako při osobním setkání (například na úřadech). Z jejich zneužití tedy plynou právní důsledky.

Při nekonečných možnostech, které internet poskytuje, ale musí všichni uživatelé dbát pravidel bezpečného vystupování na internetu a prozíravě sledovat, zda se nestal obětí kybernetického útoku, jelikož vystupovat online jako někdo jiný je mnohem jednodušší než v realitě. Zároveň je potřeba pečlivě chránit veškerá data, která do sítě uživatel vypustí, protože útoky na získání dat uživatelů jsou velice časté a čím dál sofistikovanější.

3 ZRANITELNOSTI UMOŽŇUJÍCÍ ZNEUŽITÍ IDENTITY

Zranitelností obecně se rozumí slabé místo zkoumaného objektu – taková vlastnost objektu, která když je překonána, může dojít, za působení hrozby, k narušení bezpečnosti, případně ke vzniku újmy. [34]

Pokud se budeme držet kybernetické bezpečnosti, jedná se například o takové místo v software (neošetřená část kódu), které může být využito útočníky k útoku. Útočníci tato místa využívají ke vkládání tzv. exploitů. Mohou to být různé příkazy, části kódu apod. které mají za cíl uživateli škodit. Uživatel při otevírání důvěryhodné aplikace netuší, že obsahuje exploit, a nemusí vědět ani o tom, že se na pozadí jeho počítače děje něco, co mu škodí. To se však odvíjí od chování exploitu a záměru útočníků. [35]

Obecně, pokud se takto zaměříme na zranitelnosti, tedy slabá místa identit, spojená s kybernetickou bezpečností, můžeme se na ně dívat ze dvou úhlů. Z pohledu uživatele, a z pohledu toho, komu uživatel svá data poskytnul. Aby se zamezilo zneužití slabých míst třetí osobou, musí být aplikována bezpečnostní opatření na obou stranách. [34]

3.1 Možnosti autentizace

Podstatnou část problematiky zranitelností umožňujících zneužití identity tvoří proces autentizace. Jedná se o postup, kterým se uživatel ověřuje, že je opravdu majitelem daného účtu. Nedostatečné zabezpečení autentizace je primární zranitelností, které souvisí se všemi typy identit, jež jsou zmíněny v kapitole 3.2.

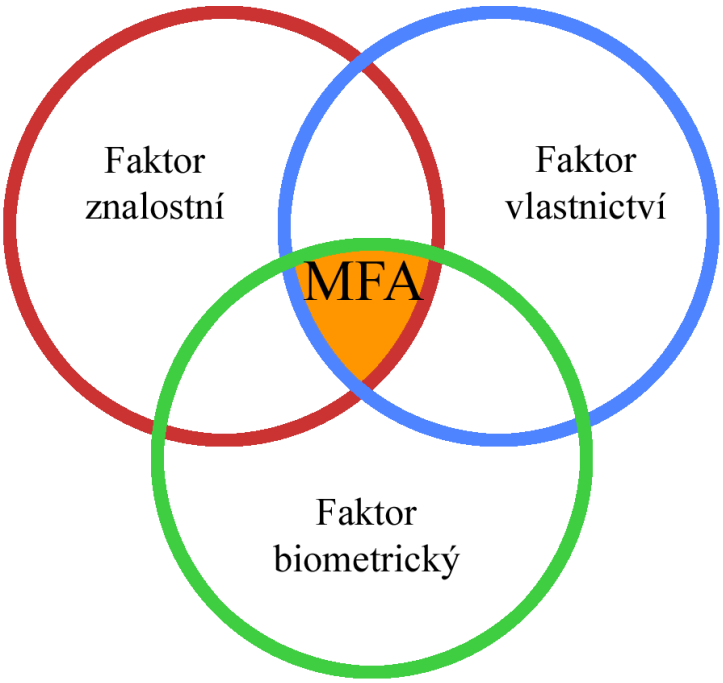
Možnosti autentizace můžeme rozdělit podle následujících faktorů:

- faktor znalostní – zakládá se na znalostech uživatele – heslo, PIN kód apod.,
- faktor vlastnictví – je omezen věcmi, které uživatel vlastní – doklady, platební kartu, mobilní telefon apod.,
- faktor biometrický – souvisí se samotnými rysy uživatele – otisk prstu, rozpoznání obličeje apod. [36]

Možnosti autentizace, na základě zmíněných faktorů, můžeme rozdělit na tři hlavní:

- pouze jménem a heslem (jednofaktorová autentizace) – základní způsob autentizace, uživatel si pamatuje pouze přihlašovací jméno, a k němu odpovídající heslo,

- dvou-faktorová autentizace – k ověření se používají dva faktory – většinou se jedná o vlastnický a znalostní faktor – uživatelské jméno a heslo (znalostní faktor) v kombinaci např. se SMS kódem či mobilní aplikací, ke kterým uživatel využije svůj mobilní telefon (vlastnický faktor),
- vícefaktorová autentizace – v angličtině označována jako MFA – Multi Factor Autentification. Přidává autentizaci na bezpečnosti, jelikož spoléhá na všechny tři faktory – k uživatelskému jménu a heslu, ověřovacímu kódu ve formě SMS, či mobilní aplikace do procesu vstupuje ještě ověření např. pomocí otisku prstu, či jiného biometrického rysu (biometrický faktor). [36]



Obr. 2. Vícefaktorová autentizace – Vennův diagram [36]

3.2 Zranitelnosti jednotlivých typů identit

Jelikož, jak již bylo zmíněno v předchozích kapitolách, lidé mohou mít více identit a podstata těchto identit se v různých případech liší, také zranitelnosti jednotlivých identit jsou odlišné. Tato podkapitola se bude zabývat zranitelnostmi identit vyjmenovaných v kapitole 2.

3.2.1 Zranitelnosti elektronické identity

Elektronická identita je úzce spojena s občanským průkazem osoby, konkrétně s elektronickým čipem, který je do občanského průkazu vložen, a na kterém jsou uloženy osobní informace uživatele.

Největší zranitelností této identity je ztráta občanského průkazu, protože právě ten musí mít uživatel fyzicky u sebe pro přihlášení k portálu veřejné správy. To, že dojde ke ztrátě občanského průkazu, ale neznamená, že dojde také ke zneužití identity. Proces autentizace totiž kromě občanského průkazu vyžaduje také znalost kódů IOK, případně DOK. Pokud by se tedy o přihlášení pokoušel někdo, kdo tyto kódy nezná, musel by se pokusit je uhodnout. Může tak učinit pomocí speciálního software na prolomování hesel, nebo namátkou zkoušet kombinace čísel (například datum/rok narození, nebo jiné kombinace, které by mohly mít pro vlastníka občanského průkazu nějaký význam). Hádání kódu IOK je ale omezeno počtem pokusů na 3. Pokud se nepovede zadat správný kód ani potřetí, dojde k zablokování a jediné východisko je, zadat správný DOK kód. Na jeho zadání má uživatel 10 pokusů. Poté již musí následovat návštěva příslušného úřadu, a to je pro toho, kdo se snaží identitu zneužít nepřípustné. [37]

Druhou nezanedbatelnou zranitelností této identity je zapomenutí kódu IOK. Pro zajištění největší možné bezpečnosti, se nedoporučuje tento kód kamkoliv zapisovat. Jakmile je kód někde zvěčněn (papír, počítač, mobilní telefon), zvyšuje se tím riziko, že se k němu dostane neoprávněná osoba a může ho využít ke zneužití identity vlastníka. Pokud se neoprávněná osoba dostane také fyzicky k občanskému průkazu, je potom zneužití identity vlastníka velmi jednoduché. [37]

Související, ne však tak kritickou, zranitelností je zapomenutí kódu DOK. Kritickou zranitelností se stane v případě, že uživatel zapomene také kód IOK, nebo třikrát zadá tento kód špatně. Pokud desetkrát netrefí správnou kombinaci, nezbývá uživateli nic jiného než navštívit příslušný úřad. Jestliže se neoprávněná osoba dostane pouze ke kódu DOK, pravděpodobně bude muset uhodnout i IOK, aby mohla být identita vlastníka zneužita. [37]

3.2.1.1 Zranitelnosti elektronické identity související s osobními certifikáty

S elektronickou identitou souvisí také osobní certifikáty používané pro elektronický podpis. Abychom mohli stanovit zranitelnosti, je potřeba rozdělit úložiště certifikátů, jelikož obecně se dá rozdělit na dva hlavní typy:

- interní úložiště certifikátů – takové úložiště, které je k dispozici neustále (systémové úložiště certifikátů Microsoft Windows, úložiště certifikátů různých internetových prohlížečů atd.),
- externí úložiště certifikátů – tato úložiště je možné odebrat a připojit, když je třeba (čipové karty, USB tokeny apod.). [20]

Pokud máme osobní certifikát spolu s privátním klíčem uložený v interním úložišti certifikátů, obecně lze říct, že toto úložiště je méně bezpečné než to externí. Certifikáty, jejichž privátní klíč je generován do systémového úložiště certifikátů Microsoft Windows, lze totiž snadno exportovat, a při exportu certifikátu povolit i export privátního klíče. V praxi to znamená, že byť certifikát patří pouze jedné konkrétní osobě, může jej používat na několika různých zařízeních, pokud si exportovaný certifikát s klíčem na různá zařízení naimportuje. Jakmile je certifikát s klíčem jednou exportován (je uložen do souboru s příponou .pfx), může snadno dojít k jeho šíření. Nemusí ani dojít ke kybernetickému útoku. Stačí, když majitel zařízení (notebook, počítač) zapůjčí další osobě. Po návratu zařízení si majitel ani nemusí být vědom toho, že byly jeho certifikáty i s klíči zcizeny. Překážkou k použití takto získaného certifikátu s klíčem je heslo pro ochranu privátního klíče. Pokud se totiž uživatel rozhodne k exportu i privátního klíče, povinnou součástí je zadání hesla, které je při importu vyžadováno, aby se co nejvíce zamezilo jeho zneužití. Pokud tedy export provádí vlastník certifikátu, měl by nastavit takové heslo, které nebude snadno prolomitelné. [20]

Ukládání privátního klíče na externí úložiště certifikátů vylučuje jeho export na úložiště interní (platí pouze pro privátní klíč – ne pro certifikát – bez privátního klíče nelze certifikát využít pro podepisování). Zranitelností, stejně jako u všech přenosných médií, je skutečnost, že může být ztraceno, nebo odcizeno. Pro přístup k těmto médiím je potřeba zadávat kód PIN. Pokud dojde k blokaci, pak je třeba znát i kód PUK (obdobné jako IOK a DOK u elektronického občanského průkazu). [20]

3.2.2 Zranitelnosti digitální identity

Digitální identitu si uživatelé drží ve většině případů pouze uživatelským jménem a heslem, v některých případech i telefonním číslem. Zatímco přihlašovací jméno (v mnoha případech jedinečný identifikátor) je viditelné, často pod ním uživatel na daném portále/síti/službě vystupuje, heslo je primárně to, co drží účet zabezpečený proti neoprávněným uživatelům. [25]

Za nejpodstatnější zranitelnost digitální identity, můžeme s jistotou považovat slabé heslo. Tímto pojmem se rozumí snadno prolomitelné nebo uhodnutelné heslo. V současnosti již drtivá většina sociálních sítí, e-shopů, různě zaměřených portálů a ostatních webů, které umožňují založení uživatelského účtů, požaduje po uživatelích hesla splňující jimi definované parametry. Většinou jsou to požadavky na:

- délku hesla – udává minimální délku hesla – např. minimálně 8 znaků,
- vložení číslic a symbolů – symboly se myslí např. vykřičník, uvozovky nebo procento,
- velká a malá písmena – většinou je vyžadována jejich kombinace. [38]

Čím složitější heslo je, tím hůře a déle bude trvat útočníkovi, ať už manuálně zkoušením, nebo pomocí softwaru, než heslo prolomí. Mnohdy stačí prolomit jen jedno heslo (například k e-mailové adrese) a díky synchronizaci tím útočník získá přístup i k dalším službám, které se k této e-mailové adrese vztahují.

Často je také po zadání hesla po uživateli vyžadováno odpovědět na několik kontrolních otázek. Jejich nevýhodou je, že pokud se k účtu dostane osoba, která vlastníka zná, je velice pravděpodobné, že zná také odpovědi na kontrolní otázky, jelikož se většinou jedná o otázky související s vlastníkem účtu (oblíbený film/seriál, rodné příjmení matky apod.). Pokud se k účtu uživatele dostane někdo, kdo jej osobně nezná, odpověď na tyto otázky může nalézt také na sociálních sítích – konkrétně na profilech majitele účtu. Uživatelé si často neuvědomují/nepamatují, jaké otázky a odpovědi si při zakládání účtu zvolili a nevědomě odpovědi na tyto otázky zveřejní. [25]

Platí také pravidlo, že hesla k účtům by se neměla zaznamenávat ani na papír, ani kamkoliv do počítače či do mobilu. Heslo kdekoliv viditelně napsané představuje nebezpečí pro zneužití druhou osobou.

V dnešní době chytrých telefonů můžeme za zranitelnost považovat také jeho ztrátu. Spousta uživatelů si již zvykla, že ve svém chytrém telefonu mohou mít synchronizované všechny uživatelské účty, které potřebují/využívají. Ať už se jedná o různé sociální sítě, e-mailové schránky, aplikace internetových obchodů a dalších účtů. U mobilních zařízení se většinou klade důraz na jednoduchost a rychlost použití. Proto si mnoho aplikací dokáže heslo zapamatovat, a již ho po uživateli nevyžaduje, pokud to není nastaveno jinak. Z toho důvodu je potřeba heslo nastavit i přímo na mobilním telefonu. Může se jednat o číselný kód, slovní heslo, nebo znak (spojení bodů na displeji jedním tahem). Moderní chytré telefony, pro zvýšení bezpečnosti, v sobě mají zabudovanou čtečku otisku prstů. Výhodou je, že otisk

prstu je téměř nemožné zfalšovat, tudíž by se mohlo zdát, že je to ideální způsob, jak svůj mobilní telefon ochránit. Avšak tyto čtečky nejsou neomylné a často otisk prstu není možné identifikovat (mastné, znečištěné prsty, úraz apod.). Z toho důvodu se při vložení otisku prstu požaduje po uživateli ještě heslo, někdy označované taky jako PIN kód. Jedná se většinou o šestimístný číselný kód a ten už je pro potenciálního útočníka mnohem lépe zjistitelný. Na uhodnutí kódu má také jen omezený počet pokusů, pokud jej vyčerpá, dojde k zablokování zařízení. Pokud se mu ale povede zařízení odemknout, získá tak přístup ke všem uloženým účtům uživatele a může se tak za něj bez problémů vydávat na sociálních sítích, číst a odesílat zprávy, čerpat různé služby, nebo i nakupovat na kreditní kartu majitele zařízení. [39]

To, co platí pro chytré mobilní telefony, můžeme vztáhnout i na notebooky – i ty mohou být ztraceny, vzhledem k tomu, že jsou přenosné.

Lze sem zařadit také prodej zařízení, ve kterém má uživatel uložené své přihlašovací údaje. I při vymazání či navrácení zařízení do továrního nastavení, je možné smazaná data obnovit.

Jako zranitelnost můžeme považovat také důvěřivost uživatele. Objevují se případy, že uživatel v dobrém úmyslu vyzradí své heslo kamarádovi, příteli apod., který jej později (například po konfliktu) zneužije buď ke zjištění osobních informací, přístupových hesel nebo získání požadovaných fotografií/videí. [40]

3.2.3 Zranitelnosti bankovní identity

Nejzávažnější zranitelností bankovní identity je ztráta platební karty, která se k bankovní identitě neodmyslitelně váže. Dojde-li ke ztrátě platební karty, nálezce toho může velice jednoduše zneužít. Není-li nastaveno jinak, u současných platebních karet lze bezkontaktně a bez nutnosti zadat PIN kód zaplatit částku až do výše 500,- Kč za transakci. Pokud nálezce platební kartu najde, může ji využít hned na několik transakcí, pokud se každá transakce vejde do limitu 500,- Kč.

Za neméně závažnou zranitelnost lze považovat vyzrazení PIN kódu k platební kartě. Při každém zadávání PIN kódu na terminálu (ať už u bankomatu nebo při platbě např. v obchodech) hrozí, že někdo stojící v blízkosti majitele platební karty, podle pohybu prstu/ruky po klávesnici zjistí zadávaný PIN kód. Majitel karty ale může doplatit také na svou důvěřivost a blízké osobě PIN kód prozradit. Blízká osoba potom může využít nestřeženého okamžiku, platební kartu si od majitele „vypůjčit“ a využít jeho finančních prostředků. [41]

Zranitelností platební karty je také možnost ji okopírovat a spolu s ní jde ruku v ruce neobezřetný uživatel. Útočníci této kombinace dokážou efektivně využít pomocí takzvaného skimmingu. Jedná se o podvodnou techniku, kdy útočníci pomocí speciálního zařízení vloženého do bankomatu zkopírují magnetický proužek platební karty, který pak použijí pro odčerpání peněz přes internetové bankovnictví nebo pro výběr peněz z bankomatu. [41]

I u bankovní identity tvoří poměrně velkou část zranitelnosti také možnost ztráty chytrého mobilního telefonu. Většina bankovních subjektů již nabízí pro větší pohodlí klientů své mobilní aplikace, pomocí kterých mohou snadno provádět bankovní transakce. Přestože aplikace bývají velice dobře zabezpečeny před potenciálním zneužitím, pokud se útočníkovi dostane do rukou přímo zařízení, které má uložené potřebné údaje, pravděpodobnost, že tyto údaje budou zneužity je poměrně vysoká. [27, 39]

Jako poslední je ještě vhodné zmínit zranitelnost vztahující se k přihlašovacím údajům do internetového bankovnictví. Funguje zde ještě ověření pomocí jednorázového přihlašovacího SMS kódu, který je uživateli zaslán na mobilní telefon po zadání platného klientského čísla/uživatelského jména a hesla, pro co největší zajištění bezpečnosti. Jistá míra zranitelnosti tu ale je. Pro zadání hesla k bankovnímu účtu se vztahují stejná pravidla, tj. aby heslo splňovalo konkrétní požadované parametry určené bankou. I klientské číslo/uživatelské jméno by si měl uživatel pečlivě střežit, jelikož při zakládání účtu (ať již na pobočce, nebo při zakládání účtu online, které je již umožněno některými bankami), je uživateli klientské číslo/uživatelské jméno doručeno buď na papíře, nebo v elektronické formě (např. na e-mailovou adresu. Banky mají v současné době spoustu metod zabezpečení, aby možnost zneužití účtů svých klientu minimalizovat na minimum. [27]

Zranitelnost se skrývá také pod možností, že si uživatel zapíše potřebné údaje pro přihlášení někam na papír, do počítače nebo mobilního telefonu. Hrozí potom, že se údaje dostanou k neoprávněnému uživateli, který se potom bude moci velice snadno vydávat za majitele účtu.

3.3 Shrnutí

Zranitelnosti se ve větší či menší míře objevují u všech zmíněných identit. Nestačí jim ale předcházet pouze z pohledu uživatele, který svoje data poskytuje. Musí jim předcházet také ten, kdo data uživatelů zpracovává.

Proto, aby bylo možné svoji identitu vůči někomu prokazovat, je potřeba využití autentizace a autorizace. Autentizace se odvíjí od různých faktorů a může být buď kombinací všech existujících faktorů, nebo jen některých, případně využívat jen jeden faktor.

Za společně zranitelnosti, které všechny zmíněné identity sdílí můžeme obecně považovat:

- zapomětlivost uživatele,
- nedostatečné hlídání věcí uživatele (občanský průkaz, čipová karta, chytrý telefon atd.),
- neopatrné zacházení se zařízeními, ve/na kterých má uživatel uloženy své přihlašovací údaje.

II. PRAKTICKÁ ČÁST

4 PŘÍPADOVÉ STUDIE SOUVISEJÍCÍ SE ZNEUŽITÍM IDENTITY

Tato kapitola popisuje 5 případových studií, všechny související se zneužitím identity. Jelikož ke zneužití identity může docházet různými způsoby, pro účely této práce jsou jednotlivé případy rozděleny do pěti kategorií, do kterých každá případová studie spadá.
Kategorie případových studií:

- zneužití identity blízké osoby oběti s cílem získání přístupu k finančním prostředkům – případová studie č. 1,
- krádež osobních údajů oběti – případová studie č. 2,
- zneužití identity společnosti – případová studie č. 3,
- únik osobních údajů společnosti působící v České republice – případová studie č. 4,
- únik osobních údajů společnosti působící celosvětově – případová studie č. 5.

U případových studí č. 4 a 5 se nejedná přímo o zneužití identity, ale o potenciální možnost, že ke zneužití identity dojde, a to i přesto, že uživatel (majitel přihlašovacích údajů), udělá vše pro to, aby nebyly údaje zcizeny jeho nedbalostí.

4.1 Případová studie č. 1 – zneužití identity blízké osoby oběti

Případ pochází z Olomouckého kraje a informovala o něm Policie ČR na svém webu www.policie.cz.

Incident se odehrál 15. července 2015 v podvečer, kdy neznámý pachatel kontaktoval devatenáctiletou ženu z Prostějova. Zcizil přitom identitu jednomu z jejích kamarádů tím, že prolomil heslo k jeho účtu na sociální síti Facebook. Pod záštitou identity kamaráda požádal ženu o půjčku finančního obnosu ve výši 40 Kč. Žena žádost přijala a pachateli sdělila potvrzovací kódy ke svému bankovnímu účtu, pro ověření bezhotovostního převodu. Pachatel využil tyto informace k odcizení celkem 40 tisíc korun. [42]

4.1.1 Bezpečnostní problémy

Ke zmíněnému případu jsou vázány tyto bezpečnostní problémy:

- uživatel někomu vyzradí své přihlašovací údaje k internetovému bankovnictví – stejně jako u přihlašovacích údajů ke všem svým uživatelským účtům, i u přihlašovacích údajů k internetovému bankovnictví platí, že je uživatel nesmí

nikomu jinému sdělit, ani člověku, kterému důvěřuje nejvíce (partner/partnerka, rodiče, …).

- někdo prolomí uživatelovo heslo k internetovému bankovnictví – uživatelé poměrně často volí hesla jednoduchá, jednoslovná, volí slova, která jsou spojena s jejich osobou (oblíbený seriál, jméno domácího mazlíčka, …), a tím potenciálním útočníkům velice zjednodušují práci při snaze o prolomení hesla.
- někdo prolomí uživatelovo heslo na některý z jeho uživatelských účtů – v tomto případě se myslí konkrétně sociální sítě, pomocí kterých se lze po prolomení hesla vydávat snadno za někoho jiného. Problém je opět vázán na nedostatečnou sílu hesla.
- uživatel někomu vyzradí údaje na jeho platební kartě – ať už z důvěřivosti, nebo omylem, může dojít ke zcizení finančních prostředků majitele platební karty.

4.1.2 Příčiny

Pravděpodobně hlavním spouštěčem narušení bezpečnosti bylo nedostatečné zabezpečení uživatelského účtu na sociální síti Facebook ženina kamaráda, kterému bylo jeho heslo prolomeno. Pokud by totiž k prolomení hesla nedošlo, pachatel by neměl identitu důvěryhodné osoby jako prostředek k tomu, jak získat od důvěřivé ženy údaje potřebné pro získání přístupu k jejímu bankovnímu účtu.

Pokud by ale žena byla dostatečně obezřetná a dbala na pravidlo „nikdy nikomu nesdělovat přihlašovací údaje k bankovním/uživatelským/jiným účtům“, k narušení bezpečnosti by také dojít nemuselo, jelikož by její zdánlivý kamarád, za kterého pachatel vystupoval, neměl k jejímu účtu přístup. Jestliže by i přesto chtěla zdánlivému kamarádovi finanční částku půjčit, měla by sama mít kontrolu nad tím, do jaké výše finanční částku poskytne.

4.1.3 Následky

Důsledkem neopatrného jednání ženy jí byla způsobena finanční škoda prostřednictvím odčerpání finančních prostředků z jejího bankovního účtu, pro potřeby pachatele. Ve zprávě o narušení bezpečnosti bylo uvedeno, že pachatel z bankovního účtu oběti odčerpal přesně 40 000,- Kč.

Za škodu můžeme také považovat tu, kterou pachatel způsobil majiteli účtu na sociální síti Facebook, tím že, mu tento účet odcizil. Jelikož pachatel za muže vystupoval a následně finančně poškodil mužovu kamarádku, mohla žena ke svému kamarádovi ztratit důvěru

v domnění, že právě on jí finanční obnos zcizil. Mohla tuto skutečnost také sdělit své rodině či známým a poškodit tak mužovu pověst ještě víc.

Také není známo, zda pachatel mužovi jeho účet na sociální síti navrátil. Pokud pachatel změnil heslo k účtu a muž si musel vytvořit účet nový, můžeme i tuto skutečnost brát v potaz jako škodu.

4.1.4 Opatření

Pokud by všechny zúčastněné osoby dodržely následující opatření, nedošlo by k žádnému negativnímu dopadu:

- dodržovat zásady silného hesla (kamarád poškozené) – více jak 8 znaků, použity speciální znaky, čísla, různě velká písmena.
- nikdy nikomu nesdělovat přihlašovací údaje (poškozená) – ať už se jedná o profily na různých webech nebo internetové bankovnictví, přihlašovací údaje by měl vždy znát pouze jejich majitel, i kdyby v jeho okolí byl někdo, v koho by měl maximální důvěru.
- nikdy nikomu nesdělovat potvrzovací kódy, které uživateli přijdou ve formě SMS – většinou při potvrzení bankovní transakce online, je třeba transakci potvrdit ověřovacím kódem, který banka svému zákazníkovi zasílá na mobilní telefon ve formě SMS. Jestliže někdo žádá o jeho zaslání bez toho, aniž by uživatel věděl, o jakou transakci se jedná, je pravděpodobné, že někdo získal přístupové údaje k bankovnímu účtu uživatele a zasláním potvrzovacího kódu pachateli dáváme souhlas se zneužitím našich finančních prostředků. Při potvrzování plateb online figuruje telefonní číslo jako součást identity majitele bankovního účtu, ke kterému se toto číslo vztahuje.

4.2 Případová studie č. 2 – krádež a zneužití osobních údajů

O případu informovala Policie ČR na svém webu, řešili ho kriminalisté v Jablonci nad Nisou.

Třicetiletý muž 31. ledna 2018 uzavřel úvěrovou smlouvu přes internet na osobní údaje své matky, za kterou se vydával. Smlouvu opatřil elektronickým podpisem a vyčerpal celkovou částku 119 689,- Kč.

Znovu poté, 27. února 2018, se muž u jiné společnosti opět vydával za svoji matku, při uzavírání další úvěrové smlouvy. Tentokrát zneužil její osobní doklady a uvedl nepravdivé

údaje. Úvěr využil ke koupi nového mobilního telefonu a společnosti způsobil škodu ve výši 24 492,- Kč. Splátky, ke kterým se v rámci obou uzavřených smluv zavázal, pravidelně neuhrazoval.
Byl obviněn ze spáchání trestného činu úvěrový podvod, hrozí mu až pět let odnětí svobody. [43]

4.2.1 Bezpečnostní problémy

Uvedený případ je rozsáhlý, a proto bezpečnostních problémů s ním spojených je více. V případu figuruje také výraz elektronický podpis, kterým je pravděpodobně myšlen elektronický podpis pomocí certifikátu. Budou tedy zkoumány bezpečnostní problémy s ním spojeny:

- certifikát pro elektronický podpis je uložen na zařízení, ke kterému má přístup více osob – certifikáty mohou být uloženy v úložišti operačního systému, webových prohlížečů, čipových kartách, občanských průkazem s čipem, speciálních tokenech (většinou USB). Pokud k některému úložišti má přístup i někdo další, než je majitel certifikátu, představuje tato situace bezpečnostní problém, jelikož tento certifikát může být bez vědomí majitele zneužit. Při uložení certifikátu na čipovou kartu/token/občanský průkaz s čipem je od uživatele vyžadován PIN kód, takže takto uložený certifikát je znatelně menším bezpečnostním problémem (to, že má uživatel přístup k čipové kartě/tokenu/občanskému průkazu s čipem ještě neznamená, že zná PIN kód, pokud není některé z médií připojeno k zařízení jako je počítač/notebook, a uživatel, který PIN kód zná a je tedy majitelem certifikátu, nepřikázal, aby se PIN na tomto zařízení pamatoval, potom již není třeba pro podpis PIN kód zadávat).
- povolen export certifikátu i s klíčem – tento bezpečnostní problém se vyskytuje především u certifikátů uložených v operačních systémech. Při instalaci certifikátu do zařízení jako je počítač či notebook je potřeba také myslet na to, zda uživatel bude potřebovat používat certifikát pro podpis také na jiném zařízení. Certifikáty mají určitou platnost a po dobu této platnosti je potřeba zvážit, zda je možné, že se zařízení, na kterém má uživatel certifikát nainstalovaný poškodí. Pokud totiž dojde k tomu, že jediné zařízení, na kterém má uživatel certifikát i s privátním klíčem nainstalovaný, přestane fungovat, uživatel tak přijde o možnost použít svůj elektronický podpis. Mít exportovaný pouze certifikát pro vytvoření podpisu totiž nestačí, a export certifikátu i s klíči představuje riziko. Proto je vždy potřeba zvážit

nutnost exportu, a povolení exportu certifikátu i s klíčem. Při exportu certifikátu i s klíčem je vyžadováno heslo pro import certifikátu s privátním klíčem – tohle heslo je nutné vytvořit co nejsilnější, aby se minimalizovalo riziko, že jej někdo prolomí a získá tak certifikát majitele.

- uživatel někomu zapůjčí zařízení, na kterém má nainstalovaný svůj certifikát s privátním klíčem – samotné zapůjčení takového zařízení (počítač/notebook/mobilní telefon) je potřeba vždy zvážit, o to více pokud na něm má uživatel uložen svůj certifikát s privátními klíči.
- majitel ztratí své osobní doklady – tento bezpečnostní problém se týká této případové studie spíše okrajově. V případě ztráty například peněženky, ve které majitel své doklady uchovává, není příliš složité pro nepoctivého nálezce tyto doklady zneužít. Při zřizování některých produktů některých bankovních subjektů, často stačí kopie dvou osobních dokladů, a lze si například sjednat půjčku, nebo v případě této případové studie úvěr, na člověka, jemuž doklady náleží.
- majitel nechá své doklady bez dozoru – tento případ dokazuje, že i ve zdánlivém bezpečí vlastního domova je potřeba své doklady pečlivě chránit i před členy domácnosti.

4.2.2 Příčiny

Ve zprávě není uvedeno, jak je možné, že pachatel mohl vytvořit elektronický podpis své matky. Mohl se k němu dostat:

- vypůjčením matčina zařízení, na kterém měla uložen certifikát s privátním klíčem (počítač/notebook),
- exportováním certifikátu včetně privátního klíče z matčina zařízení a zkopírováním do svého zařízení, pokud byl export certifikátu včetně privátního klíče povolen.
- certifikát včetně privátního klíče byl uložen na občanském průkazu s elektronickým čipem.

Matka tedy především dostatečně neochránila svůj certifikát pro elektronický podpis. V každém případě muselo dojít buď k zapůjčení zařízení, k distribuci certifikátu včetně privátního klíče na jiná zařízení, nebo stačilo pouze získat občanský průkaz s elektronickým čipem.

Stejně tak, jako nezabezpečila svůj certifikát před neoprávněnými uživateli, nezabezpečila ani svoje osobní doklady, jelikož k nim pachatel měl přístup, a bez jejího vědomí je zneužil.

4.2.3 Následky

Protože pachatel, syn poškozené ženy, vystupoval pod identitou své matky, byly úvěry připsány na její jméno, tudíž ona se stala v očích úvěrových společností dlužníkem, který není schopen plnit sjednané závazky. To by v budoucnu mohlo znemožnit ženě poskytnutí úvěru od těchto společností.
Poškozeny byly také společnosti, které pachateli úvěry poskytly. Ve zprávě se píše, že jim byla způsobena škoda téměř 150 000,- Kč.
Případ velmi dobře prokazuje, jak je důležité si chránit identifikační data nejen virtuálně, pro vystupování na internetu, ale také fyzicky naše doklady.

4.2.4 Opatření

Následuje výčet opatření, která kdyby byla dodržována, mohla by zabránit narušení bezpečnosti:

- certifikát včetně privátního klíče ukládat výhradně na zařízení, ke kterým má přístup pouze jeho majitel – jestliže je privátní klíč certifikátu uložen do operačního systému (v počítači/notebooku), měl by být ukládán pouze do zařízení, která má ve své správě majitel certifikátu. Tato zařízení by měla být chráněna dostatečně silným heslem.
- zařízení, na kterém je certifikát včetně privátního klíče uložen, nepůjčovat bez dozoru majitele – nezáleží na tom, o jaké zařízení se jedná. Pokud je na něm uložen certifikát s privátním klíčem majitele, neměl by jej nikomu půjčovat, aby nedošlo ke zneužití majitelova podpisu. Pokud majitel přesto zařízení zapůjčí, měl by mít dohled na tím, jak s ním dotyčný nakládá.
- pokud je certifikát včetně privátního klíče uložen na čipové kartě/tokenu, měl by jej majitel uchovávat na dobře zabezpečeném místě – majitel by měl zajistit, aby k zařízení neměl nikdo jiný přístup (nejlépe zamknout např. do šuplíku nebo do trezoru, případně zajistit, že bude mít zařízení vždy u sebe a maximálně zajistit, aby nedošlo k jeho ztrátě či zcizení).
- jestliže je certifikát s privátním klíčem uložen na čipové kartě, majitel by měl zvolit dostatečně silný PIN kód – nevztahují se na něj stejná pravidla jako na heslo. PIN kód jsou zpravidla pouze číslice, a minimální délka je podmíněna nastavením čipu

karty. PIN kód by neměla být posloupnost za sebou jdoucích stejných čísel, jejich kombinace by měla být různá a neměla by souviset s ničím, co majitele definuje (např. datum narození, rodné číslo atd.).

- pečlivě zvážit, zda je nutné certifikát s privátním klíčem zálohovat, a zda povolit jeho export – obecně platí, že zálohovat soubory, dokumenty atd. je potřeba. Pokud se ale jedná o certifikáty včetně privátních klíčů, je třeba zvážit, zda majitel je schopen poskytnout jeho záloze dostatečnou ochranu před zneužitím. Záloha by vždy měla být opatřena dostatečně silným heslem, a měla by být uložena na bezpečném místě (externí/flash disk nejlépe někde uzamčený).
- oskenované kopie/fotografie svých osobních údajů uchovávat na bezpečném místě – pro nákup nejrůznějších bankovních produktů většinou dostačují kopie dvou osobních dokladů, proto pokud majitel vlastní elektronickou verzi svých dokladů, měl by je mít uložené na bezpečném místě v počítači/notebooku, nebo na externím/flash disku, uloženém na bezpečném místě.
- i ve zdánlivém bezpečí domova doklady uchovávat na skrytém místě – přestože se to může zdát zbytečné, měl by majitel osobní doklady střežit i před členy domácnosti – právě to vyplívá z této případové studie (za předpokladu, že pachatel i jeho matka žili ve společné domácnosti).

4.3 Případová studie č. 3 – zneužití identity společnosti

Třetí případ se objevil na webu www.protiseti.cz, kde redakce zmíněného webu informovala 5. února 2012, o zcizení jejich facebookové stránky.

Dle webu, měla stránka na Facebooku s názvem „Proti módní šedi v českých ulicích!“ 21 443 fanoušků, kteří díky ní mohli sdílet nejen příspěvky o módě, ale mohli se také zveřejnit jako začínající umělci, nebo pomocí stránky najít ztracené psy, brigády či podnájem. Správci na stránce také denně zveřejňovali zajímavosti ze zahraničí nebo různých koutů kultury.

K incidentu došlo 4. února 2012, neznámý útočník se dostal k přístupovým údajům správců stránky. Nejprve změnil profilovou fotku stránky na fotku polonahého exotického domorodce a na stránce se začaly objevovat vulgární příspěvky s drogovou tématikou. Zároveň upravil přístupová práva tak, aby k ní již původní správci neměli přístup. Poté se útočník snažil vzbudit dojem, že stránka byla opět navrácena původním majitelům tím, že

zveřejňoval příspěvky o „zažehnání krize“. Mezitím už ale majitelé stránky založili jinou stránku, kde o incidentu své fanoušky informovali. [44]

4.3.1 Bezpečnostní problémy

Bezpečnostních problémů spojených s tímto konkrétním případem může být několik:

- heslo pro přístup k administraci facebookové stránky bylo příliš slabé – hesla, která se skládají např. ze snadno uhodnutelných slov, nebo jsou příliš krátká, je většinou možné uhodnout i bez použití speciálního software. V dnešní době není ani velkým problémem software na prolomování hesel sehnat.
- heslo zahlédne/zaslechne neoprávněná osoba – nevýhoda silných hesel tkví v tom, že jsou hůře zapamatovatelná. Z případu můžeme usoudit, že správců stránky bylo více než jeden. Pokud si některý z nich heslo někam zapsal, ať již na papír či do počítače nebo mobilního telefonu, dochází ke zvýšení šance, že heslo někdo zneužije. Problém může nastat také ve chvíli, kdy jeden ze správců heslo zapomene, například zatelefonuje správci jinému a ten mu heslo prozradí. Zde nastává opět problém, že heslo bude zaslechnuto neoprávněnou osobou.
- správce nechá uložené heslo v prohlížeči zařízení, které pro správu stránky používá – může tak dojít ke zcizení stránky bez toho, aniž by útočník heslo znal. Všechny webové prohlížeče si již umí pamatovat přihlašovací údaje uživatelů. Uživatelům to tak zrychluje a zjednodušuje přístup ke všem svým uživatelským účtům, ale také to představuje značné riziko při ztrátě zařízení s takto uloženými hesly. Zařízení je vždy potřeba chránit silnými hesly, aby v případě ztráty maximálně ztížili prolomení hesla a tím pádem i ztížili přístup k uživatelským účtům s uloženými hesly.
- správce nechá bez dozoru zařízení, na kterém je přihlášen k účtu stránky – pokud uživatel odchází od zařízení, ke kterému je přihlášen na některém ze svých účtů, měl by toto zařízení vždy uzamknout, nebo se ze všech účtů odhlásit.
- správce se pro administraci stránky přihlásil na vypůjčeném zařízení – některá zařízení totiž uživatele po ukončení aplikace/webového prohlížeče neodhlásí, to znamená, že zůstane přihlášen poslední uživatel, dokud účet někdo neodhlásí.

V tomto konkrétním případě není známo, jak se útočník k přístupu k účtu dostal. Mohl to být kterýkoliv z výše uvedených.

4.3.2 Příčiny

U této případové studie není jasné, jak pachatel získal přístup k administraci stránky. Mohl využít kteréhokoliv bezpečnostního problému zmíněného v předchozí podkapitole 4.3.1.

4.3.3 Následky

Přestože důsledkem incidentu nebyla žádná materiální, nebo finanční škoda, výrazně utrpěla image zmíněné facebookové stránky, a tím pádem i image jejích zakladatelů. Stránku s počtem uživatelů v desetitisících její majitelé budovali několik let, a v důsledku tohoto incidentu ji museli pachateli přenechat a začít budovat stránku novou. Ne všichni sledují dění kolem sebe, nemuselo by jim dojít, že stránka byla zcizena. Jednání útočníka mohlo zanechat negativní pocit u dřívějších fanoušků stránky, kteří již důvěru k původním majitelům neobnoví.

4.3.4 Opatření

Jelikož zde není jasné, jak k incidentu došlo, je třeba definovat opatření proti všem bezpečnostním problémům zmíněných v kapitole 4.3.1. Lze jim zabránit, nebo alespoň minimalizovat pravděpodobnost jejich výskytu následujícími způsoby:

- zvolit dostatečně silné heslo pro přístup k administraci stránky – při volbě hesla je vždy důležité dbát na dostatečnou sílu hesla – speciální znaky, velká/malá písmena, číslice, délka hesla.
- heslo nikam nezapisovat, diktovat co nejvíce diskrétně – hesla ke svým účtům by si uživatel nikdy neměl zapisovat do zařízení, ze kterého se k účtům přihlašuje. Špatnou volbou je též napsat si heslo na papír. Také by jej nikdy neměl nikomu diktovat nebo posílat přes sociální sítě. Pokud nelze jinak než heslo nadiktovat, musí být dodržena maximální obezřetnost a kontrola, že se v blízkosti nenachází neoprávněná osoba. V úvahu také připadá poslat heslo například přes elektronickou poštu pouze zašifrovaně.
- neukládat heslo ve webových prohlížečích zařízení, nebo přímo někam do zařízení – přestože uložení hesla zrychluje a zjednodušuje přístup, uživatel by své přihlašovací údaje do prohlížeče ukládat neměl. Minimálně ne do zařízení, která jsou náchylná k tomu, že je uživatel ztratí (např. mobilní telefon, popř. notebook).
- nenechávat zařízení, na kterém je uživatel přihlášen bez dozoru – zařízení na kterém je uživatel přihlášen k některému ze svých uživatelských účtů, by nikdy nemělo

zůstat bez dozoru. Pokud se uživatel od zařízení musí vzdálit, měl by toto zařízení vždy uzamknout silným heslem.

- při přihlášení z vypůjčeného zařízení vymazat přihlašovací údaje – vždy před tím, než uživatel vypůjčené zařízení vrátí, musí zkontrolovat, že jeho přihlašovací údaje v zařízení nezůstaly uložené a z předtím používané aplikace/webového prohlížeče se odhlásit.

4.4 Případová studie č. 4 – únik údajů o klientech Mall.cz

Úřad pro ochranu osobních údajů informoval 19. října 2017 o kontrole, kterou zahájil na začátku října, společnosti Mall.cz.
Impulzem pro kontrolu společnosti byl hackerský útok, který probíhal v období od 31. prosince 2014 do srpna 2017, a při kterém se útočníci dostali přesně k 735 956 údajům klientů společnosti. Jednalo se o tyto údaje:

- jméno,
- příjmení,
- e-mailová adresa,
- heslo uživatelského účtu,
- telefon.

Po útoku došlo k zveřejnění získaných dat na serveru Uložto.cz.
Úřad po prozkoumání případu udělil společnosti Internet Mall, a. s. pokutu ve výši 1,5 milionu korun. [45]

4.4.1 Bezpečnostní problémy

Veškeré bezpečnostní problémy související s touto případovou studií, se týkají především zabezpečení databáze před neoprávněným přístupem:

- databáze je nedostatečně ochráněna před vstupem neoprávněných uživatelů – databázové systémy většinou dokážou řešit přístupy uživatelů prostřednictvím rozdělených rolí na základě přihlašování uživatelským jménem a heslem. Pokud takto přístupy omezeny nejsou, může dojít k neoprávněnému přístupu. Přístupy uživatelů k databázi lze řešit také např. pravidly pro IP adresy (např. lze rozdělit pravidla pro uživatele přistupující k databázi z firemní sítě a pro ty, kteří k ní přistupují ze sítě veřejné).

- správce databáze používal pro přístup k databázi slabé heslo – útočníci využili přihlašovacích údajů správce, které získali buď prolomením nedostatečně silného hesla, nebo přihlašovací údaje získali např. odposloucháváním komunikace, správce si heslo někam zapsal a útočníci jej získali atd.
- soubor obsahující databázi, nebo záloha ostré databáze se nenachází na bezpečném místě – pokud lze k některému z těchto souborů získat přístup prostřednictvím internetové sítě, podstatně se zvyšuje riziko úniku, a tím pádem i možnost zneužití, databázových dat. Stejně tak pokud se soubory nachází například na externím disku a ten se fyzicky nenachází na bezpečném místě (nijak nezabezpečená budova, nezamknutá místnost, …).
- síťová komunikace mezi klientem a serverem je nezašifrovaná – pokud se data, která jsou přenášena od klienta na server, a naopak posílají nezašifrovaná, je možné, že potenciální útočník může tuto komunikaci odposlouchávat, či pozměňovat posílaná data.
- data, především hesla, se do databáze ukládají v nezašifrované podobě – i přesto, že můžeme co nejlépe omezit přístupová pravidla k databázi, riziko, že se k nim dostane neoprávněná osoba, existuje stále.
- k zašifrování dat se používá zastaralá kryptografická funkce – myšlena je především kryptografická (šifrovací) funkce MD5 (Message Digest 5), která vytváří kontrolní součty o délce 32 znaků (128 bitů) ze vstupních dat. V současné době se již objevil nespočet kolizí, které značily nedostatečnou bezpečnost tohoto algoritmu, a ani jeho dešifrování již není nemožné [46].
- SQL injection – jeden z nejčastějších útoků, jehož úkolem je umožnit útočníkovi spravovat databázi tak, jak zrovna potřebuje. SQL injection je možné provádět tam, kde aplikace žádá po uživateli zadání přihlašovacích údajů. Útočník ale místo korektních přihlašovacích údajů do pole pro uživatelské jméno a heslo zapíše řetězec příkazů jazyka SQL, a pokud databáze proti těmto útokům není ošetřena, může útočník docílit toho, že nejen že do databáze získá přístup, ale bude ji moci také spravovat (přidávat, mazat, upravovat). Tím tedy získá přístup ke všem uživatelským datům uložených v databázi. [47]
- některý ze zaměstnanců útočníkům přístup k databázi poskytnul, případně ji sám zveřejnil – mohlo dojít k tomu, že některý ze zaměstnanců mohl útočníku databázi

přímo poskytnout, případně ji zveřejnil sám např. z nenávisti k zaměstnavateli, z pomsty či za vidinou zisku (mohl databázi útočníkům prodat za finanční částku).

4.4.2 Příčiny

Proč přesně k úniku dat došlo, společnost nezveřejnila. Mohl hrát roli tedy jakýkoliv bezpečnostní problém vyjmenovaný v předchozí podkapitole s číslem 4.4.1, nebo i jiný sled událostí.

4.4.3 Následky

Nejpodstatnějším důsledkem celého incidentu bylo zveřejnění 736 956 osobních informací o zákaznících společnosti, tudíž přestože sami zákazníci byli ke svým přihlašovacím údajům obezřetní a dbali všech bezpečnostních opatření, dostaly se jejich přihlašovací údaje k neoprávněným osobám, které je mohly využít libovolným způsobem.

Někteří uživatelé také používají stejné přihlašovací údaje pro více svých uživatelských účtů. Tím, že útočníci odhalili, jaké přihlašovací údaje používají pro jeden ze svých účtů, mohli se pokusit dostat se pod těmito přihlašovacími údaji také na jiné portály, kde by vybraní uživatelé mohli mít své uživatelské účty.

Neznámý uživatel, ať už to byl sám útočník, či jiný uživatel, jenž měl k získané databázi přístup, poté uložil získaná data na server www.uloz.to. Tam k nim měl přístup každý s patřičným odkazem, nebo věděl, jak daný soubor vyhledat, než administrátoři serveru uloz.to tento soubor odstranili.

Tudíž kdokoliv mohl získat jakékoliv přihlašovací údaje na uživatelské účty pro internetový obchod Mall.cz a tím poškozené uživatele o účty připravit, nebo poškodit jejich důvěryhodnost nekorektním jednáním při používání jejich účtu. Tím se ale také objevila poměrně obsáhlá sbírka zaručeně existujících e-mailových adres, kterou mohl kdokoliv snadno využít pro marketingové účely, phishingové a jiné útoky, nebo rozesílání spamových zpráv.

Jelikož se jednalo, nebo stále i jedná, o vysoce sledovanou kauzu, mohl tento incident také zapříčinit to, že stávající uživatelé, či uživatelé potenciální ke společnosti ztratí důvěru. Zákazníci stávající přestanou služby zmíněného internetového obchodu využívat, a potenciální zákazníci raději zvolí alternativu.

4.4.4 Opatření

Aby se co nejvíce minimalizovala pravděpodobnost, že v budoucnu dojde k dalšímu úniku dat, nebo se úniku dokonce zabránilo, měla by být dodržena následující opatření:

- dbát a pečlivě rozdělit práva administrátorů pro přístup k databázi – pokud možno co nejvíce minimalizovat počet administrátorů, kteří můžou databázi spravovat.
- správci databáze by měli volit co nejsilnější hesla pro přístup k databázi – platí stejná pravidla jako u hesel uživatelských účtu – dostatečná délka hesla, velká/malá písmena, speciální znaky a číslice. Heslo by nemělo být tvořeno existujícími slovy, nemělo by se používat pro přístup k jiným účtům atd.
- databáze samotná, i její záloha, je uložena fyzicky na zabezpečeném místě – zamknutá místnost, do které mají přístup jen oprávnění uživatelé, zálohy databáze na jiném místě, než je databáze ostrá. Pokud je na přenosném médiu, toto médium uchovávat také v zamknuté místnosti, popřípadě na jiném místě, které lze opatřit zámkem (přihrádky ve stole, sejf, …).
- ke komunikaci mezi klientem a serverem vždy používat šifrovanou komunikaci – takovou komunikaci obstarávají protokoly, které šifrovanou komunikaci umožňují (SSL/TLS, HTTPS).
- data v databázi ukládat vždy zašifrovaná – pro zašifrování nepoužívat algoritmus MD5, který je již v dnešní době nedostačující. Zvolit jinou alternativu jako je například kryptografický algoritmus SHA1 obohacený o tzv. kryptografickou sůl (jakýkoliv libovolný řetězec znaků). Samotný algoritmus SHA1 už v dnešní době také přestává být dostačující. Přidáním kryptografické soli lze útočníkovi podstatně znesnadnit dešifrování dat v databázi. Nelze tím však dešifrování znemožnit. Postup pro přidání kryptografické soli je pro všechny data v databázi stejný (např. SHA1 hash hesla zřetězený s kryptografickou solí, který dá dohromady posloupnost znaků), a tak útočník může přijít na to, jak je sůl využívána, jelikož na to existuje pravidlo. Bylo by vhodné využívat delší hashovací funkce jako je např. SHA256 nebo SHA512. Jejich nevýhodou může ale mnohdy být, že jejich výpočet zabere více času, avšak i přesto by správci měli sledovat vývoj šifrovacích (hashovacích) algoritmů a vždy ten, který se již stává zastaralým průběžně nahrazovat bezpečnějšími variantami.

- chránit databázi proti SQL injection – nejbezpečnějším způsobem, jak se proti těmto útokům chránit jsou tzv. parametrizované dotazy (prepared statements).
- pokud již došlo k úniku dat, vynutit resetování hesel všech zákazníků – zákazníky poté o úniku informovat, a zdůraznit, že musí zadat hesla nová. [47, 48]

4.5 Případová studie č. 5 – únik dat uživatelů z Dropboxu

V polovině roku 2012, jak uvádí server www.haveibeenpwned.com, došlo k útoku na cloudové úložiště Dropbox. Útočníci se dostali a následně zveřejnili přesně 68 648 009 účtů zákazníků společnosti. Zveřejněny byly e-mailové adresy a k nim i hesla. Většina hesel byla zašifrovaná hashovacím bezpečnějším algoritmem BCrypt. Zbytek byl zašifrován způsobem SHA1 v kombinaci s kryptografickou solí. [49]

4.5.1 Bezpečnostní problémy

Bezpečnostní problémy vázané k této případové studii jsou velice podobné, jako tomu bylo u předchozí případové studie č. 4.

- databáze je nedostatečně ochráněna před vstupem neoprávněných uživatelů – tento bezpečnostní problém samozřejmě souvisí s touto případovou studií, dle dostupných informací ale není zcela relevantní.
- správce databáze používal pro přístup k databázi slabé heslo – tento problém je vždy potřeba brát v potaz, jelikož jak tento případ dokazuje, přestože fyzická i softwarová bezpečnost databáze nikdy zcela nezamezí chybě lidského faktoru, který za stav bezpečnosti zodpovídá.
- soubor obsahující databázi, nebo záloha ostré databáze, se nenachází na bezpečném místě – platí stejně jako u předchozího bodu. I přes maximální možnou fyzickou i softwarovou ochranu vždy záleží také na lidském faktoru (například oprávněná osoba, jinak splňující všechny bezpečnostní předpisy, zapomene zamknout místnost, kde se databáze nachází apod.).
- síťová komunikace mezi klientem a serverem je nezašifrovaná – nezašifrovanou komunikaci může útočník odposlouchávat.
- SQL injection – viz případová studie č. 4., podkapitola 4.4.1.

- některý ze zaměstnanců útočníkům přístup k databázi poskytl, případně ji sám zveřejnil – ani u tohoto případu nelze tento scénář, popsaný u předchozí případové studie, vyloučit.

4.5.2 Příčiny

Začátkem celého incidentu bylo, podle oficiálního blogu Dropboxu, zcizení hesla zaměstnance útočníky. Heslo, které zaměstnanec používal pro své různé uživatelské účty na internetu, používal také ke svému účtu právě na Dropboxu, kde si uchovával pracovní dokumenty. Se znalostí tohoto hesla se potom útočníci dostali nejen k databázi přihlašovacích údajů uživatelů, ale také k seznamu e-mailových adres (které měl zaměstnanec uložené právě v jednom z pracovních dokumentů nacházejícím se na Dropboxu), které poté využili k rozesílání spamu (nevyžádané pošty) na tyto adresy. [50]

4.5.3 Následky

Následkem bylo zveřejnění přihlašovacích údajů uživatelů Dropboxu, a to konkrétně 68 648 009. Oproti předchozí případové studii, se však většina hesel na internetu nacházela v zašifrované podobě. Dropbox přiznal, že několik málo uživatelských účtů bylo zcizeno, ostatní zašifrované údaje se útočníkům prolomit nepodařilo. To však neznamená, že by k jejich prolomení, od jejich zveřejnění až po vynucený reset hesel uživatelů, nemohlo dojít. Hesla byla sice uložena šifrovaně, e-mailové adresy podle dostupných informací nikoliv, takže přesto, že díky šifrovaným heslům nebyly příliš ohroženy uživatelské účty na Dropboxu, mohly být zneužity e-mailové adresy uživatelů pro zasílání marketingových zpráv, phishingové a jiné útoky, či rozesílání spamů (nevyžádané pošty), ke kterému v rámci úniku souboru se seznamem e-mailových adres, již došlo.

Únik představuje také možnost, že se útočníci získanými přihlašovacími údaji pokusí přihlásit i na jiných portálech, kde by vytipovaní uživatelé mohli mít svůj uživatelský účet, a zneužít tak jejich osobní údaje i na jiném místě.

Některé následky se také shodují s předchozí případovou studií jako třeba ztráta důvěry v cloudové úložiště Dropbox jak stávajícími, tak potenciálními zákazníky, a stejně tak mohlo dojít k poškození pověsti uživatelů, kterým byly uživatelské účty zcizeny, a pod jejichž jmény útočníci mohli nekorektně vystupovat.

4.5.4 Opatření

Opatření, která z popsané případové studie vyplývají nejvíce, jsou:

- správci databáze, a všichni uživatelé by měli volit co nejsilnější hesla – dodržovat dostatečnou délku hesla, speciální znaky, malá/velká písmena, číslice, heslo by nemělo obsahovat existující slova, a především pro každý účet používat jiné heslo.
- pro šifrování dat používat vždy dostatečně bezpečný algoritmus – začínají se objevovat případy, kdy hashovací algoritmus sha1 již přestává být dostačující. Uvádí se, že hesla, která byla v tomto případě dešifrována, byla šifrována práce funkcí sha1 společně s kryptografickou solí.

Jako další lze uvést také všechna opatření z předchozí podkapitoly 4.4.4, která platí i v tomto případě.

4.6 Shrnutí

Přestože přístup k internetové sítí má v dnešní době téměř každý, ne všichni si ale chrání informace, které na internet dává. Stále se objevují případy, kdy byla zneužita identita oběti, spojená nejen se sociálními sítěmi. Nemusí se jednat pouze o identity jednotlivých uživatelů. Zneužití identity se může týkat také společností, organizací, spolků apod. a důsledkem je poškození jejich pověsti.

Uživatelé mají možnost provádět elektronicky, prostřednictvím svých digitálních identit, čím dál více úkonů, především bankovních služeb. Proto je potřeba, aby každý, kdo využívá své digitální identity, dbal na jejich ochranu. Často totiž dochází, společně se zneužitím identity, taky k finanční újmě poškozeného.

Pokud uživatel dbá všech opatření, aby útočníkům co nejvíce ztížil, případně znemožnil, zneužití svých identit, stále ještě musí brát zřetel na to, na jaké portály své údaje vkládá. V minulosti došlo k hackerským útokům, jejichž následky byly úniky obrovských objemů dat uživatelů. I ti, kteří nejen přihlašovací údaje uživatelů schraňují by měli maximálně zabezpečit, aby k únikům dat nedocházelo. V případě selhání jsou totiž ohroženy identity všech uživatelů portálu.

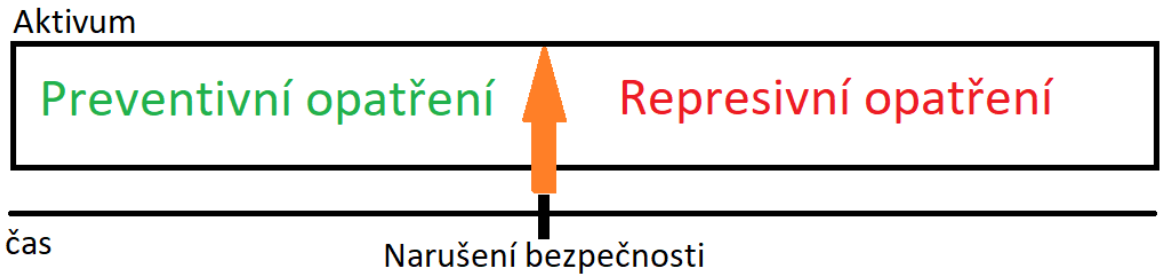
5 NÁVRHY OPATŘENÍ PROTI ZNEUŽITÍ IDENTITY

Tato kapitola bude věnována opatřením, která se vážou k jednotlivým identitám zmíněným v kapitole 2, tzn.:

- elektronická identita,
- digitální identita,
- bankovní identita.

Opatření pro každou identitu budou rozdělena na:

- preventivní = opatření, která mají za cíl předcházet nežádoucím jevům, chránit před nimi, snižovat pravděpodobnost, že k nim dojde,
- represivní = tato opatření začínají působit v momentě, kdy nežádoucí jevy začnou poškozovat aktivum (objekt, který opatření chrání), a jejich cílem je minimalizovat škody, které nežádoucí jevy způsobí.



Obr. 3. Preventivní vs. represivní opatření

5.1 Opatření proti zneužití elektronické identity

Jelikož elektronická identita úzce souvisí s občanskými průkazy (nebo jinými zařízeními, v případě kvalifikovaných certifikátů) s elektronickým čipem, budou opatření zaměřena hlavně na ochranu tohoto zařízení s elektronickým čipem a na zacházení s ním.

5.1.1 Preventivní opatření

Následují preventivní opatření proti zneužití elektronické identity:

- nenechávat občanský průkaz s elektronickým čipem bez dozoru – nechávat své doklady bez dozoru, není dobré ani v prostoru vlastního domova, kde se můžeme domnívat, že jsou naprosto v bezpečí. Především je ale velice nebezpečné nechávat je bez dozoru kdekoliv mimo domov. Je důležité mít neustále přehled, kde se doklady

nachází, a v nejlepším případě je mít kdykoliv po ruce na místě, kde nemůže dojít k jejich zcizení, ztrátě nebo okopírování.

- ukládat eOP (i další doklady) doma na bezpečném místě – nejlépe mít na doklady vyhrazené místo – např. zamknuté v přihrádce, ve skříňce (klíč samozřejmě také schovat na skrytém místě, popř. jej nosit neustále u sebe). Pokud není možnost doklady někam zamknout, ukládat je na hůře přístupném, nebo na nepředvídatelném místě, kde by doklady či jiné cennosti potenciální zloděj nehledal.
- stejná opatření, uvedená v předchozích dvou bodech, se vztahují také pro vlastnění zařízení, na kterém má jejich majitel uloženy své kvalifikované osobní certifikáty – karty s elektronickým čipem, USB tokeny či jiné bezpečné uložiště.
- eOP, ani jiné zařízení s osobními údaji či osobními certifikáty nikdy nikomu nepůjčovat – údaje a osobní certifikáty pro elektronický podpis (dále jen certifikáty) patří vždy jen jejich majiteli, a tudíž pouze ten by je měl využívat. Pokud se ale najde případ, kdy majitel svůj eOP nebo zařízení se svými certifikáty někomu zapůjčí, měl by dohlédnout na to, jak je s nimi zacházeno a mít je neustále pod dozorem.
- při volbě kódů, ať už k eOP pro elektronický čip (IOK, DOK), nebo kódů pro podepisování osobními certifikáty (PIN, PUK u čipových karet a eOP + QPIN u eOP) zvolit dostatečnou délku, a pokud možno náhodnou posloupnost číslic, která nijak nesouvisí s majitelem – délka je většinou u všech zmíněných kódů omezena jak minimálním (u eOP IOK, DOK 4 znaky), tak i maximálním (u eOP IOK, DOK 10 znaků) počtem znaků (minimální i maximální hranice pro různé kódy se u různých čipových karet liší). Kódy by tedy měly být delší než minimální povolený počet znaků (pokud možno zvolit maximální délku), a číslice by měly být co nejnáhodnější. Zvolit tedy např. kód IOK, který bude vypadat takto: „1111“ a k němu kód DOK: „1234“ je technicky možné, ale z bezpečnostního hlediska naprosto vyloučené.
- žádný z kódů, zmíněných v předchozím bodě, nikam nezapisovat – a to ani na papír, ani do počítače, notebooku nebo mobilního telefonu. U papíru, notebooku nebo telefonu může dojít ke ztrátě či zcizení, které představuje pro potenciálního nálezce příležitost. Kódy zapsané v některém ze zařízení, které má přístup k internetu, může být napadnuto útočníky, a ti je potom mohou využít ve svůj prospěch. Jestliže si ale uživatel z důvodu zapomětlivosti nebo pro pocit jistoty, že kódy nezapomene, kódy někam potřebuje zapsat, měl by to udělat na papír, který je uložený například

v zamykatelné přihrádce, či ve skříňce. Rozhodně by je neměl zapsat k dalším kódům/heslům, které již někde používá, raději by každé heslo/kód měl zapsat na jiný papír/jiné místo a už vůbec neuvádět, k čemu kódy patří.

- kódy nikomu nesdělovat – přestože se může zdát, že bez toho, aniž by útočník měl eOP majitele fyzicky u sebe, nemůže znalost těchto kódů využít. Tyto kódy by měl znát jen jejich vlastník.

Pokud je uživatel také vlastníkem certifikátů, jejichž klíče má uloženy v úložišti operačního systému (MS Windows) svého zařízení, platí pro něj následující opatření:

- zařízení nikomu nepůjčovat – certifikáty patří vždy jednomu majiteli, a jsou vázány k zařízení, na kterém jsou vygenerovány klíče. Jestliže se uživatel rozhodne zařízení, na kterém má uloženy klíče ke svým certifikátům, někomu zapůjčit, měl by dohlížet na to, že jeho certifikáty nejsou zneužity, případně do zařízení (počítače, notebooku) vytvořit účet pro hosty a tomuto účtu omezit oprávnění. Dbát při tom na to, aby privátní klíče byly generovány pro správný účet, a certifikát instalovat pouze pro tohoto uživatele.

- důkladně zvážit, zda je potřeba certifikáty včetně privátního klíče zálohovat – záloha dat a souborů je velice důležitá obzvlášť pokud uživatel nechce přijít o své důležité dokumenty. V případě certifikátů včetně privátního klíče (dále jen certifikátů) je ale otázka zálohy komplikovanější. Pokud totiž uživatel svůj certifikát vyexportuje, vznikne mu tím soubor obsahující jak jeho certifikát, tak i privátní klíč. Tento soubor může být nainstalován i do jiného zařízení než do toho, který patří majiteli certifikátu. Jakmile existuje jedna záloha, mohou nezodpovědným chováním vzniknout i další kopie a uživatel tak může ztratit kontrolu nad tím, kde všude již jsou jeho certifikáty nainstalovány. Jestliže se ale na problém podíváme z druhé strany, mít zálohu svých certifikátů má i své výhody. Pokud si například vygenerujeme pár klíčů do notebooku, a notebook přestane fungovat, bez zálohy certifikátu jsme o něj nenávratně přišli, a jediný způsob, jak získat nový je projít celým procesem vydání certifikátu znovu a znovu za prvotní certifikát zaplatit (následné certifikáty, které jsou obnovou certifikátů prvotních, bývají zpravidla levnější).

- jestliže se uživatel rozhodne pro zálohu (export) svého certifikátu, měl by ji uložit na bezpečné místo, a zvolit dostatečně silné heslo pro její instalaci – za bezpečné místo můžeme považovat flash/externí disk, který má uživatel dobře uložený a chráněný.

Není vhodné zálohu ukládat pouze do zařízení, ve kterém již jsou uloženy klíče k certifikátu, právě kvůli možné poruše zařízení, kvůli které by uživatel přišel nejen o certifikáty, ale také o jejich zálohy. Při vytváření exportu v OS Windows je po uživateli požadované heslo pro ochranu privátního klíče. Platí zde stejné zásady pro heslo, jako kdekoliv jinde (více v kapitole 5.4).

- heslo k privátnímu klíči (souboru se zálohou) nikam nezapisovat – platí stejné podmínky jako u přístupových kódů k čipové kartě/eOP. Pokud si je uživatel chce či potřebuje někam zapsat, měl by to udělat na papír na bezpečném místě, mimo ostatní zapsaná hesla a nezmiňovat, k čemu se heslo váže.

5.1.2 Represivní opatření

Tato opatření zafungují až v případě, že selžou opatření preventivní, tzn. jsou to opatření po tom, co již nějakým způsobem došlo k možnému zneužití elektronické identity a nedošlo k velkým škodám. Do takových opatření můžeme zařadit:

- v případě ztráty eOP (nebo dokladů obecně) neprodleně provést blokaci čipu a navštívit jakýkoliv úřad obce s rozšířenou působností – nemusí se jednat o úřad, který daný doklad vydal, ani to nemusí být úřad ve městě, kde má uživatel trvalé bydliště.
- pokud uživateli někdo zcizí jeho eOP (nebo jakýkoliv jiný doklad), může to kromě libovolného úřadu obce s rozšířenou působností, ohlásit také na Policii ČR.
- majitel certifikátu by měl vždy znát (nebo být schopen dohledat) minimálně sériové číslo svého certifikátu a heslo pro zneplatnění – jestliže dojde ke ztrátě nebo zcizení zařízení, na kterém má uživatel uložené své osobní certifikáty (čipová karta, eOP, notebook atd.), měl by uživatel neprodleně zažádat o jeho zneplatnění. Způsobů, jak to může provést je několik, vždy záleží na konkrétní autoritě, která službu poskytuje. Může to být například přes webový formulář, pomocí e-mailu, osobně na některé z poboček registrační autority, nebo fyzicky dopisem. Nejrychlejší a nejpřístupnější způsob je pravděpodobně pomocí webového formuláře. Zneplatnění certifikátu je nevratná akce, po zneplatnění již není možné certifikát obnovit tak, aby byl opět platný, jelikož zneplatněný certifikát je vzápětí uložen na seznam zneplatněných certifikátů (CRL – Certificate Revocation List).

5.2 Opatření proti zneužití digitální identity

Digitální identita, je oproti předchozí, elektronické identitě, rozsáhlejší pojem, jelikož v sobě zahrnuje všechny identity, na všech možných sociálních sítích a webových portálech, zkrátka všechny weby, které uživateli dovolí zaregistrovat si profil.

5.2.1 Preventivní opatření

Pro maximální možné zabezpečení digitální identity, je potřeba dodržovat následující preventivní opatření:

- před registrací profilu na některém webovém portále si ověřit jeho důvěryhodnost – nejlépe z jiného zdroje než z portálu samotného – recenze na internetu nebo od přátel, zkrátka si zjistit, že údaje neposkytujeme podvodníkům.
- vždy volit silné heslo – ne všechny portály mají požadavky na formát hesla. Přestože to portál nevyžaduje, uživatel by měl vždy uvážlivě volit délku i obsah hesla. Více k volbě hesla v kapitole 5.4.
- heslo si nikam nezapisovat – nejlépe ani na papír, ani do některého ze zařízení, které má přístup k internetu. Jestliže si uživatel zapíše heslo například do notebooku nebo do mobilního telefonu s přístupem na internet, hrozí, že se stane obětí hackerského útoku a útočníci takto získají přístup nejen k uloženým heslům, ale také poměrně snadno zjistí, k jakým účtům hesla patří obzvláště pokud si uživatel své přihlašovací údaje ukládá do webového prohlížeče. Může také dojít ke ztrátě nebo zcizení zařízení, a jestliže má uživatel v zařízení uložené jak přihlašovací údaje, tak heslo je pro potenciálního nálezce velice snadné zneužít identitu majitele zařízení. Pokud si uživatel z nějakého důvodu potřebuje hesla někam zapisovat, měl by to dělat na papír, který je uložený na místě, které není viditelné a pokud možno jde zamknout (zamykací přihrádka/skříňka). Zároveň by se měl vyhnout tomu, aby hesla psal na stejné místo, a aby si k heslům nezapsal i přihlašovací jména, která k heslům patří.
- zařízení, ze kterých na svoje uživatelské účty uživatel přistupuje opatřit bezpečným heslem, či je jinak zabezpečit proti neoprávněnému přístupu – hesla opět musí splňovat určité požadavky, aby bylo možné je požadovat za bezpečné (viz kapitola 5.4). Dnešní notebooky a mobilní zařízení jsou již opatřena čtečkou otisku prstů, které se dají považovat za bezpečnou metodu, jak ochránit své zařízení proti neoprávněnému přístupu. Většinou ale kromě otisku prstu volí uživatel také

bezpečnostní heslo, které zadává v případě, že čtečka nedokáže z nějakého důvodu (např. rozmočené, zamazané nebo i zpocené prsty, či nečistota na čtečce) otisk prstu rozpoznat. Proto by uživatel neměl volbu tohoto hesla zanedbat a opět zvolit heslo silné. Kromě otisku prstu dnes některé chytré telefony dokážou uživatele rozpoznat podle obličeje. I zde ale platí, že pokud rozpoznání obličeje selže (make-up, špatné osvětlení atd.), měl by uživatel zvolit i silné heslo.

- nikomu nesdělovat své přihlašovací údaje – ani lidem, kterým naprosto důvěřujeme. Čím více lidí přihlašovací údaje zná, tím větší je pravděpodobnost, že se najde mezi nimi někdo, kdo toho zneužije. Přihlašovací údaje by měl znát vždy jen jejich majitel.
- před tím, než uživatel zapůjčí někomu zařízení, které používá pro přístup kde svým uživatelským účtům, by se měl přesvědčit, že je ze všech účtů odhlášen – případně mít zařízení pod dozorem, zatímco ho někdo jiný používá a kontrolovat, že nedochází ke zneužití.
- pokud se uživatel přihlašuje ke svým účtům z vypůjčeného zařízení, před tím, než zařízení vrátí, by se měl přesvědčit, že je ze všech svých účtů odhlášen, a že heslo nezůstalo v zařízení uloženo.

5.2.2 Represivní opatření

Jestliže dojde k selhání některého preventivního opatření zmíněného výše, stále tu jsou následující opatření, která mohou pomoci ke zmírnění škod:

- na svůj uživatelský profil nedávat zneužitelné informace – jestli si již uživatel založil profil na některém webovém portále, měl by se důkladně zamyslet, jaké informace na svém profilu o sobě uvede. Například zvážit, zda uvést veřejně svoji e-mailovou adresu nebo telefonní číslo, kontrolovat fotografie vkládané na profil, jestli v pozadí uživatel omylem nezvěčnil třeba přihlašovací údaje napsané na papíře apod.
- pokud dojde ke ztrátě zařízení, kde uživatel má uloženy své přihlašovací údaje, neprodleně změnit hesla k uživatelským účtům – potenciální nálezce by se mohl zachovat nečestně a uživateli jeho účty zneužít.
- jestliže dojde k odcizení účtu útočníky, pokusit se získat účet zpět obnovou/změnou hesla – jakmile ale útočníci účet odcizí, není jisté, že přístup k účtu bude možný. Je to nicméně první věc, kterou by v tomto případě měl uživatel zkusit.

- jestliže se uživateli nepodaří získat účet zpět obnovou hesla, měl by tuto skutečnost (že mu byl účet zcizen a nedaří se mu jej získat zpět) okamžitě nahlásit správcům webového portálu, pod který účet spadá – na webových stránkách mají jeho správci většinou uvedeny kontakty pro uživatele – e-mailovou adresu, telefonní číslo, případně adresu sídla.
- po zcizení jeho uživatelského účtu by uživatel také neměl zapomenout na své přátele, a o této situaci je informovat – útočníci by totiž přístup k účtu uživatele mohli využít k poškození jeho přátel, případně poškození pověsti samotného uživatele.

5.3 Opatření proti zneužití bankovní identity

Bankovní identitu v současné době používá snad každý, kdo splňuje podmínky pro založení bankovního účtu. Dnešní technologie potom dovolují uživateli spravovat jeho bankovní účty (kterých může mít i více než jeden) z pohodlí domova prostřednictvím internetového bankovnictví. Některé banky mají k dispozici i mobilní aplikace, které uživateli umožňují své účty spravovat odkudkoliv z mobilního telefonu. Přestože se na tyto systémy kladou velké nároky, co se bezpečného přístupu týče, stále ještě nejsou naprosto bezpečné a bez dodržování několika opatření může dojít k incidentu zneužití identity uživatele.

5.3.1 Preventivní opatření

Proti zcizení bankovní identity se uživatel může bránit následujícími opatřeními, které budou rozděleny na opatření pro internetové bankovnictví, a opatření pro používání platební karty na internetu.

5.3.1.1 Preventivní opatření pro internetové bankovnictví

Nejdříve tedy opatření, která je třeba dodržovat při používání internetového bankovnictví:

- základem je opět nastavení silného hesla, v tomto případě, k internetovému bankovnictví – dodržet doporučenou délku hesla, střídání znaků, velká/malá písmena atd.
- přihlašovací údaje k internetovému bankovnictví nikdy nikomu nesdělovat – pokud by někdo další získal přístup k internetovému bankovnictví uživatele, nepoškodil by pouze jeho identitu, pravděpodobně by došlo také ke krádeži finančních prostředků, které bankovnímu účtu a také uživateli náleží.

- pokud uživatel obdrží na svoje telefonní číslo potvrzovací kód pro přihlášení do jeho internetového bankovnictví, nikomu ho nesdělovat a okamžitě si do internetového bankovnictví změnit heslo – přihlašování do internetového bankovnictví je většinou dvoufázové – nejdříve musí uživatel zadat přihlašovací jméno a heslo, poté mu na mobilní telefon na telefonní číslo, které zadal přijde formou SMS zprávy potvrzovací kód, který musí pro dokončení přístupu zadat. Skutečnost, že uživateli tento potvrzovací kód přišel bez toho, aniž by se on sám nesnažil do svého internetového bankovnictví přihlásit, by jej měla donutit zbystřit, jelikož se velice pravděpodobně o přístup pokouší někdo jiný.
- také platí, že přihlašovací údaje k internetovému bankovnictví nikam nezapisovat – a pokud si uživatel, z nějakého důvodu, potřebuje údaje někam zapsat, měl by si zapsat pouze heslo. Neměl by ale zmiňovat k čemu patří, a měl by ho zapsat na papír, který je uložen na bezpečném, nebo těžce dohledatelném místě.
- po dokončení používání internetového bankovnictví, se okamžitě odhlásit – většina systémů využívaných jako internetové bankovnictví již má nastaveno, že po několika minutách (zpravidla krátká doba – 3 minuty, 5 minut) neaktivity uživatele samy odhlásí. Doporučeno je ale nečekat na uplynutí této doby, a odhlásit se ihned po provedení poslední akce v systému.
- do internetového bankovnictví přistupovat pouze ze zařízení, na kterém je nainstalovaný antivirový software – antivirový software dokáže často rozpoznat, zda odkaz webového portálu pro přístup do internetového bankovnictví není povržený. To znamená. že se uživatel opravdu přihlašuje do internetového bankovnictví a nejedná se například o podvod, kde se uživatel pomocí podvodného odkazu dostane na webovou stránku útočníků. Taková stránka vypadá naprosto shodně s tou původní, avšak po stisknutí tlačítka pro přihlášení odešle uživatelovi údaje přímo útočníkům. Antivirový program také chrání uživatele před přístupem na podezřelé webové stránky a zmenšuje tak riziko, že si uživatel přístupem na nebezpečnou webovou stránku stáhne do počítače nějaký malware či počítačový vir, jehož následkem by mohlo být získání přihlašovacích údajů uživatele.
- pro maximální bezpečnost, by měl uživatel přistupovat do svého internetového bankovnictví přes VPN (Virtual Private Network – Virtuální Soukromá Síť). Zajištění bezpečné, šifrované, komunikace prostřednictvím VPN není zdarma, avšak

po zakoupení (platba je většinou měsíčně) má uživatel jistotu, že veškeré jeho aktivity na internetu jsou zabezpečené, zašifrované, z venku nejsou sledovatelné, a především jsou skryté za „falešnou“ IP adresu, přes kterou uživatelovo zařízení nelze dohledat.

5.3.1.2 Preventivní opatření pro používání platební karty na internetu

Stejně tak, jako může být bankovní identita definována údaji pro internetové bankovnictvím, může být definována také platební kartou, která se k bankovnímu účtu uživatele váže. Platí pro ni následující opatření:

- nikdy nikomu nesdělovat údaje o platební kartě – na platební kartě se nachází tyto údaje: číslo platební karty, platnost od (již jen na některých platebních kartách), platnost do, jméno držitele a trojmístný ověřovací kód (kód CVV/CVC), pro platbu na internetu platební kartou je potřeba znát tři z nich: číslo platební karty, platnost do a ověřovací kód na zadní straně karty.
- údaje uvedené na platební kartě nikam jinam nezapisovat – platí i pro PIN kód, který ale pro internetové transakce není potřeba. Údaje nezapisovat ani na papír, ani do jakéhokoliv zařízení. Pokud uživatel potřebuje údaje o kartě, může se podívat přímo na ni. Zapsáním na papír zbytečně zvyšuje riziko, že se k údajům dostane někdo další. Stejně tak je to se zapsáním údajů ke kartě do počítače či jiného zařízení. Útočníci by se tak mohli dostat k údajům o platební kartě bez toho, aniž by museli čekat, než je uživatel sám zadá při provádění transakce.
- platební kartu nikomu nepůjčovat – mimo zneužití prostřednictvím internetu by mohlo dojít také ke zneužití v kamenných obchodech, nebo bankomatu, pokud by osoba, které byla karta zapůjčena, znala či uhodla také PIN kód. V kamenných obchodech lze navíc kartou platit bezkontaktně bez zadání PIN kódu zpravidla do výše částky 500,- Kč.
- platební kartu mít neustále uloženou na bezpečném místě – ať doma, nebo pokud ji má uživatel u sebe, zatímco je mimo domov, stejně tak jako tomu je v případě osobních dokladů.
- neukládat svou platební kartu ke svému profilu na různých portálech – v rámci zjednodušení používání služeb pro uživatele, často portály nabízí možnost uložení platební karty k profilu uživatele, aby pro případ budoucích plateb nemusel údaje o

platební kartě zadávat znovu. Pokud se ale útočníci dostanou k profilu uživatele, je v ohrožení také jeho platební karta. Mnohdy po uložení platební karty není zobrazeno celé její číslo, ale třeba jen poslední 4 číslice. I to je ale o celé 4 číslice víc, než by měl kdokoliv, kromě majitele znát. Nejbezpečnější je kartu nikam na webu neukládat, a dát si tu práci s vyplněním všech položek při každé transakci.

5.3.2 Represivní opatření

Represivní opatření budou, stejně jako preventivní opatření, rozdělena na represivní opatření pro internetové bankovnictví a represivní opatření pro používání platební karty na internetu.

5.3.2.1 Represivní opatření pro internetové bankovnictví

Tato část je věnována represivním opatřením pro internetové bankovnictví:

- jestliže uživatel zjistí, že byly jeho přihlašovací údaje zcizeny, měl by se okamžitě pokusit získat svůj účet zpět změnou/obnovou hesla – není ale zaručeno, že mu to bude umožněno, protože útočníci mohli pozměnit nastavení tak, aby tomu zamezili.
- pokud se mu nepodaří heslo obnovit/změnit, měl by uživatel okamžitě zavolat bance, u které má účet zřízen – operátor poté uživateli poradí, jak jeho konkrétní problém řešit.

5.3.2.2 Represivní opatření pro používání platební karty na internetu

Níže jsou uvedena represivní opatření pro používání platební karty na internetu:

- stejně tak nikomu nesdělovat potvrzovací kód, který přijde uživateli na mobilní telefon ve formě SMS – pokud totiž uživatel tento kód obdrží bez toho, aniž by sám neprováděl nějakou transakci, došlo ke zneužití jeho platební karty, a jediné co schází pro dokončení transakce je právě zmíněný kód. Pokud ho uživatel nikomu nesdělí, tomu, kdo platební údaje zneužil, nezbývá než potvrzovací kód uhodnout a transakci tak dokončit. Bez potvrzovacího kódu transakci nelze dokončit.
- pokud dojde ke ztrátě karty, nebo ke zneužití údajů karty, okamžitě kartu zablokovat – kartu může uživatel zablokovat většinou přímo ve svém internetovém bankovnictví, nebo přes telefonní číslo své banky.

5.4 Obecná opatření proti zneužití identity

Tato závěrečná kapitola bude zahrnovat základní opatření a tipy, společné pro všechny identity, které pomáhají identitu chránit. Stejně jako předchozí opatření pro jednotlivé identity, i tyto opatření budou rozdělena na preventivní, a represivní.

5.4.1 Preventivní opatření

Tato preventivní opatření se obecně vážou ke všem druhům identity:

- všechny karty, či jiná úložná zařízení uchovávat za jakýchkoliv okolností na bezpečném místě, které je chráněno před přístupem neoprávněných osob,
- vždy pečlivě zvážit jakékoliv půjčování zařízení, ze kterého se někdy uživatel přihlašoval k některému ze svých uživatelských účtů – především se zamyslet, zda uživatel není ještě k některému ze svých účtů na zařízení přihlášen, a zda tak nemůže dojít ke zneužití jeho identity,
- dodržovat zásadu silného hesla, případně přístupových kódů,
- přihlašovací údaje/hesla/kódy nikdy nikomu nesdělovat,
- přihlašovací údaje si nikam nezapisovat,
- vždy ověřovat důvěryhodnost portálu, ke kterému se přihlašujeme,
- počítač/notebook/chytrý telefon (zařízení, ze kterých se ke svým uživatelským účtům přihlašujeme) vždy opatřit dostatečně silným heslem, případně používat ověření pomocí biometrie (otisk prstu nejčastěji),
- po ukončení práce s uživatelským účtem, se vždy odhlásit,
- pokud to portál dovoluje, používat dvoufázové ověřování (zadání hesla, následně ověřovacího kódu zaslaného pomocí SMS na telefonní číslo uživatele),
- na zařízení, ze kterého se přihlašujeme ke svým uživatelským účtům, mít vždy nainstalovaný antivirový software,
- neotevírat podezřelé e-mailové zprávy či jejich přílohy (aby nedošlo k zanesení malware do počítače/notebooku/mobilního telefonu),
- využívat VPN.

5.4.1.1 Zásady bezpečného hesla

Tato podkapitola bude věnována pravidlům, která by měla být splněna pokaždé, když uživatel volí heslo ke svému uživatelskému účtu:

- délka hesla – každý portál vyžaduje jinou minimální délku hesla. Jistou míru bezpečnosti již poskytne heslo v délce 10 znaků, které je ještě poměrně snadno zapamatovatelné, musí ale splňovat i další požadavky zmíněné níž,
- heslo musí obsahovat velká a malá písmena – nejlépe náhodně se objevující v celé délce hesla,
- heslo musí obsahovat číslice – stejně tak jako v předchozím bodě by se měly objevovat náhodně v celé délce hesla,
- heslo by mělo obsahovat české znaky – myšleny jsou znaky jako č, ř, ž atd. nejlépe také ve velkých i malých variantách. Problémem mohou být zahraniční (nebo i české) portály, které tyto znaky nemusí podporovat,
- heslo by mělo obsahovat speciální znaky – jsou jimi myšleny znaky jako například ?, _, -, „“ atd. Opět se u některých portálů může stát, že tyto znaky nebudou podporovány.
- používat různá hesla pro různé uživatelské účty – především u hesel k internetovému bankovnictví, e-mailové schránky, elektronických peněženek (například PayPal), účtům k herním knihovnám (například Steam, Uplay atd.), zkrátka k účtům pro uživatele důležitým.
- pravidelně hesla měnit – preventivně je dobré jednou za čas heslo změnit.

Příklad silného hesla: pŘ1ckL4d-5!lnéH0h3SlA
Příklady slabého hesla: aaa, 1234, heslo

Pro zajištění maximální bezpečnosti a udržení přehledu všech hesel, jsou k dispozici speciální programy označované jako „správci hesel“. Tyto programy nejen že ukládají hesla, často obsahují také generátor silných hesel, vícefázové ověřovaní, nabízí také automatické vyplnění přihlašovacích údajů uživatele na jeho uživatelské účty, a spoustu dalších funkčností, ze kterých si každý uživatel může vybrat ty, které budou nejvíce odpovídat jeho představám.

Zpravidla jsou tyto programy na bázi předplatného (měsíčně, ročně), najdou se ale také spolehlivé, bezplatné verze.

Web vpnMentor sestavil žebříček 10 nejlepších bezpečných správců hesel pro rok 2020, a tady je 5 nejlepších z nich:

1. Dashlane
2. Keeper
3. LastPass
4. 1Password
5. RoboForm

Všichni zmínění správci hesel jsou k dispozici pro všechny nejpoužívanější operační systémy: Windows, macOS, iOS, Android, Linux, a pro získání jejich plnohodnotných verzí je potřeba si je zakoupit. Většina z nich je dostupná také v bezplatné verzi, avšak s omezením některých funkčností (počet zařízení, velikost uložiště atp.). [51]

V kategorii plně bezplatných správců hesel stojí rozhodně za zmínku KeePass Password Safe. Jedná se o bezplatný správce hesel, který uživatelé dostanou v plné verzi a zdarma. Pro mnohé může být velkou výhodou i to, že je open source tzn. jeho vývojáři dávají k dispozici zdrojový kód programu, takže si každý může zkontrolovat, jak je jejich program napsán (naprogramován). Stojí na principu databáze, kam si uživatel svá hesla ukládá. Pro přístup k nim stačí uživateli znát jedno hlavní heslo (pro otevření programu). Zároveň jsou k němu doplňky, kterými uživatel může rozšířit jeho funkčnost, podle toho, co zrovna potřebuje. [52]

5.4.1.2 Různé priority pro různé identity

Za předpokladu, že uživateli nevadí pamatovat si vícero přihlašovacích údajů, může si všechny své identity označit prioritou, podle toho, jak moc je ochrana těchto identit důležitá (jak moc velkou škodu by uživateli způsobilo jejich zcizení).

Na začátku takového opatření stojí založení několika e-mailových adres, jelikož podmínkou pro založení uživatelského účtu na většině portálů je zadání e-mailové adresy. Spousta portálů nabízí založení e-mailové adresy zdarma, takže jich uživatel může mít klidně desítky – pro každou identitu jiná e-mailová adresa. Takové řešení je ale velice nepraktické, protože uživatel může snadno ztratit přehled o tom, která adresa patří ke kterému uživatelskému účtu, a u každého poskytovatele musí být e-mailová adresa jedinečná, takže se může stát, že

názvy e-mailových adres se budou naprosto lišit (myšlena je hlavně část e-mailové adresy nacházející se před zavináčem – část za zavináčem je většinou pevně daná možnostmi, které nabízí poskytovatel: @gmail.cz pro Google, @seznam.cz či @email.cz pro Seznam, @centrum.cz pro Centrum atp.).

Nejvhodnější způsob zakládání e-mailových adres je vytvořit si vždy e-mailovou adresu, pokud zároveň se založením nového uživatelského účtu vznikne nový stupeň priority.

Stupně priority pro potřeby této práce budeme značit:

- I. – největší priorita – nejdůležitější identita, která uživateli náleží, její zcizení či ztráta by měla největší dopad na uživatele (po finanční, psychické i zákonné stránce).
- II. – střední priorita – ztrátou či zcizením této identity by nedošlo k finančnímu či zákonnému poškození uživatele, mělo by ale dopad na jeho psychiku, protože by mohla být poškozena jeho pověst.
- III. – nejnižší priorita – ztráta či zcizení takto označené identity uživatele nijak nepoškodí, o nic nepřijde.

Samozřejmě není nutné si priority takto jasně definovat. Podstatou je, aby měl uživatel jasno v tom, jak moc důležité pro něj jeho různé identity jsou a uměl rozlišit mezi identitami, jejichž zcizení či ztráta jej mohou vážně poškodit, a těmi, jejichž zcizení či ztráta pro něj nic neznamená. Je přitom potřeba brát zřetel na to, jaké osobní informace budou s novým uživatelským účtem (novou identitou) svázané. Pokud tedy bude mít uživatel ke svému uživatelskému účtu přiřazenou například platební kartu (e-shopy, klienti pro nákup a hraní počítačových her apod.), měl by tomuto účtu dát nejvyšší prioritu.

Příklad:

Uživatel má pouze jednu e-mailovou adresu, kterou primárně využívá pro komunikaci s rodinou a přáteli, uvedl ji také jako kontaktní adresu pro banku, ve které má zřízený svůj bankovní účet. Je to tedy e-mailová adresa, která je pro uživatele nejdůležitější, jelikož patří k jeho identitě před bankovním subjektem, rodinou, přáteli a vážou se k ní velice citlivé informace o uživateli. Může si tedy tuto adresu označit prioritou nejvyšší úrovně, a používat ji jen pro stejně tak důležité identity, či pro komunikaci např. se státními orgány, bankovními či podobnými institucemi.

Tento stejný uživatel se rozhodne, že si založí profil na některé z mnoha sociálních sítí. Tím si vytvoří identitu novou, není pro něj tolik podstatná, protože není vázaná s jeho občanským průkazem, a u bankovních subjektů se touto identitou neprokazuje. Navíc tím dá možnost komukoliv z celého světa tuto jeho identitu vyhledat. Nechce, aby tato jeho identita byla

spojena s jeho bankovním účtem, ale chce tuto identitu budovat, přidávat fotografie, komentovat příspěvky ostatních. Vytvoří si tedy další kategorii s o něco menší prioritou, a založí si novou e-mailovou adresu, kterou bude uvádět vždy při vytváření profilu i na dalších sociálních sítích.

Zálibou zmíněného uživatele je úprava a vylepšování svého automobilu. Rady s různými problémy při modifikacích vozidla hledá na tematických diskuzích či různých fórech. Nikdo před ním do diskuze nevložil stejný problém, a odpověď na svou otázku tedy nenašel. Rozhodne se, že se pomocí příspěvku do diskuze zeptá ostatních automobilových nadšenců sám. Pro přispívání do diskuze si ale na fóru musí založit uživatelský profil. Jediné, co portál vyžaduje, je nickname (přihlašovací jméno), e-mailová adresa a samozřejmě heslo. Uživatel ví, že tuto identitu moc často využívat nebude a vytváří si ji jen aby mohl vložit svůj dotaz. Nepotřebuje tedy, aby tato jeho identita byla svázaná s ničím, co by jej mohlo identifikovat. Pokud by na portále došlo k úniku e-mailových adres či hesel, jediné, co by ztratil je jeho uživatelský účet, který v budoucnu plánoval pouze pro přidání případného dotazu, či okomentování dotazu někoho jiného. Na jeho pověsti na tomto portále mu nezáleží. Pokud by mu účet někdo zcizil, mohl by si založit nový bez větších ztrát. Vzniká mu tedy další stupeň priority, pro který si vytvoří e-mailovou adresu.

Takový systém je přínosem obzvláště v případě, že dojde například k úniku e-mailů (často využívané jako přihlašovací jména) a hesel k uživatelským účtům. Uživatelské účty spadající do priority nejvyšší úrovně se nachází pouze v systémech ověřených institucí (vládní portály, bankovní systémy atd.) a tudíž pravděpodobnost, že dojde k úniku dat je minimální, a uživatel může mít jistotu, že pokud by i přesto k úniku došlo, bude následující postup v souladu se zákonem a způsobená újma mu bude nahrazena.

Například u sociálních sítí již tuto jistotu mít uživatel zdaleka nemůže, jelikož sociální sítě působí většinou celosvětově tzn. napříč legislativami všech států, ve kterých je dovoleno sociální síť využívat. Širší oblast působení znamená více aktivních uživatelů, větší povědomí, a více lidí, kteří mají zájem o získání údajů těchto uživatelů. Pokud tedy dojde k úniku e-mailových adres a uživatel využívá systém různých priorit pro různé identity, v ohrožení jsou, za předpokladu dodržení zásad dostatečně silného hesla, pouze účty, které mají stejnou prioritu a využívají tak stejný e-mail. Není ohrožena bankovní identita uživatele, tzn. jeho finance, ani jeho pravá identita, související s jeho občanským průkazem, kterým se uživatel prokazuje před státem.

Podobně může také postupovat v případě volby hesel. K e-mailovým adresám, by měl volit vždy hesla stejně silná (každé heslo samozřejmě odlišné). U uživatelských účtů může podle

priority na síle hesla ubírat. Pro největší prioritu heslo splňující všechny zásady bezpečného hesla, pro nejnižší prioritu již například heslo nemusí být velmi dlouhé, nemusí obsahovat speciální znaky apod. Do jisté míry by ale každé heslo mělo být považováno za bezpečné (tzn. mělo by obsahovat minimálně 2 zásady silného hesla – např. malá/velká písmena + číslice).

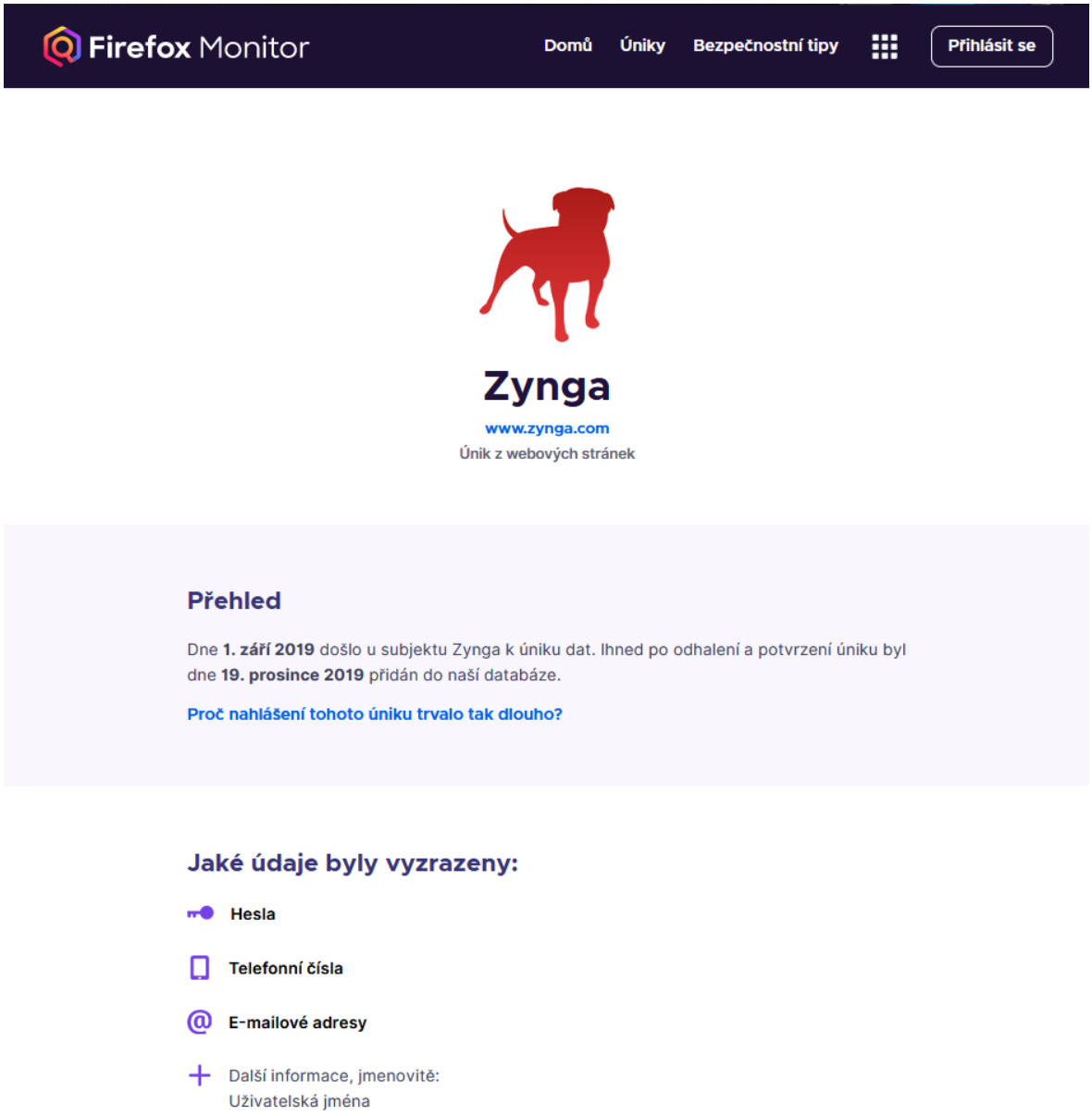
5.4.2 Represivní opatření

Následující represivní opatření můžeme vztáhnout ke všem druhům identity:

- zcizení identity (přihlašovacích/přístupových údajů k identitě) vždy okamžitě bez prodlení ohlásit autoritě, která za správu těchto údajů zodpovídá,
- po zjištění krádeže identity se okamžitě pokusit získat zpět přístup obnovením/změnou hesla,
- informovat o zcizení identity své přátele/známé, kterých by se tento incident mohl dotknout.

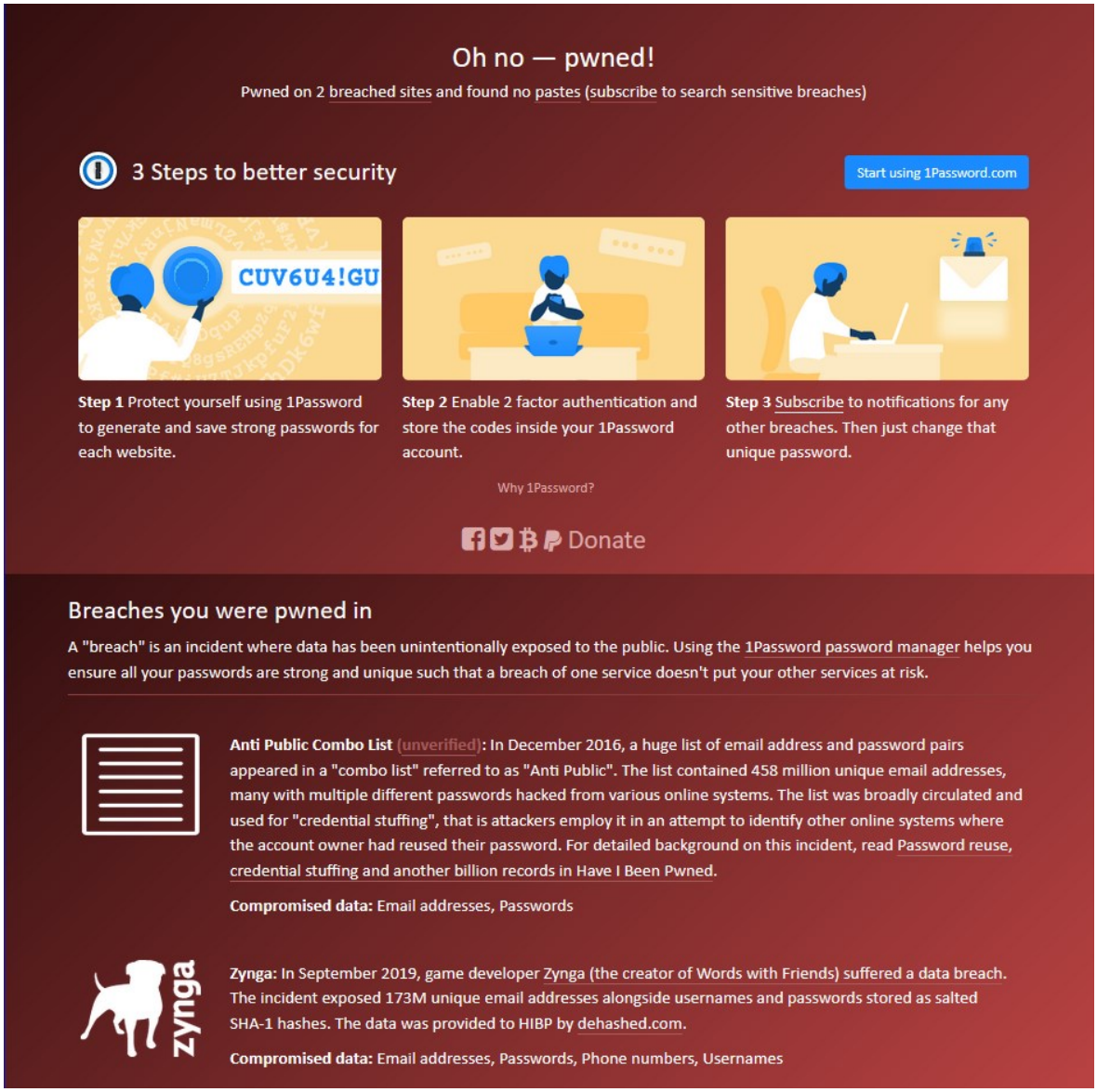
5.4.2.1 Kontrola úniku e-mailové adresy

Pokud má uživatel podezření, že se jeho e-mailová adresa, či jiné přihlašovací údaje, staly cílem úniku dat, v současné době existuje několik webových stránek, kde si tuto skutečnost může uživatel vždy pro konkrétní e-mailovou adresu. Uživatel zadá požadovaný údaj (většinou e-mailovou adresu) do příslušného políčka a počká na výsledek. Ten potom ukáže, zda se tento údaj objevil někde mezi známými úniky dat. Pokud ne, znamená to, že se uživatelovi údaje nenacházely nikde v databázích, u kterých došlo k úniku. Pokud ano, většinou se uživateli také zobrazí, ke kterému portálu se daný únik vázal, a zobrazí se mu jaké údaje konkrétně unikly (e-mailové adresy, telefonní čísla, hesla atd.).



Obr. 4. Detail o úniku dat, který je uživateli zobrazen, jestliže byla jeho e-mailová adresa v databázi známých úniků dat – Firefox Monitor [53]

Každá webová stránka pro ověření má jinou databázi, ve které úniky vyhledává, takže se výsledky mohou na jednotlivých webových stránkách lišit.



Obr. 5. Detail o úniku dat, který je uživateli zobrazen, jestliže byla jeho e-mailová adresa v databázi známých úniků dat – Have I Been Pwnd? [54]

Pokud uživatel zjistí, že se některý z jeho účtů nacházel v databázi úniků, měl by reagovat změnou hesla.

Zde je příklad tří webových stránek, na kterých lze zjistit, zda se údaje uživatele nestaly předmětem úniku dat:

https://haveibeenpwned.com/

https://monitor.firefox.com/

https://leakedsource.ru/

ZÁVĚR

Cílem této diplomové práce bylo pojednat o zneužití identity člověka jako o novém druhu bezpečnostní hrozby. Práce je zaměřena především na ochranu identit, pod kterými uživatelé vystupují v síti Internet. Nejdříve bylo třeba definovat, co to identita je, jak může být vnímána, jak ji vnímá legislativa České republiky a jak může být zneužita.

Identita člověka je zákonem velice dobře chráněna, bylo tedy potřeba se na ni podívat také z právního hlediska. Jak z pohledu ochrany identity obecně, tak i z pohledu ochrany osobních dat, které uživatelé mohou poskytnout jiným subjektům pro jejich zpracování. Zpracovávání osobních údajů se musí řídit nařízením GDPR, které platí v celé Evropské unii.

Všechny typy identit mají také své zranitelnosti, které mohou být útočníky zneužity. Tato diplomová práce byla zaměřena na identitu elektronickou, digitální a bankovní, jelikož zrovna to jsou identity, které v současnosti začíná využívat čím dál více uživatelů. Mnozí si ale neuvědomují, že s těmito identitami jsou spojené také jejich zranitelnosti. Tyto zranitelnosti byly definovány, společně s bezpečnostní problémy, které z nich vyplývají, aby bylo možné stanovit vhodná opatření.

Dále byla provedena analýza pěti vybraných případů, ke kterým došlo v posledních deseti letech, a souvisely se zneužitím osobních údajů, jenž se k identitě člověka vážou. Tři z nich se týkaly zneužití osobních údajů jednotlivce, dvě velkého úniku dat, který byl následkem hackerského útoku, a při kterém byla zveřejněna uživatelská jména a hesla, takže mohlo dojít k jejich zneužití.

Ze znalostí a poznatků, které vyplynuly z analýzy případových studií byl následně vytvořen jak souhrn opatření pro jednotlivé vybrané typy identit, tak i obecný souhrn opatření. Tento souhrn opatření slouží jako návod pro uživatele, jak nejlépe ochránit své identity, případně jak postupovat, když zjistí, že mu některá z vybraných identit byla odcizena.

SEZNAM POUŽITÉ LITERATURY

[1] RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. ISBN 978-80-247-2365-5.

[2] KIND, Amy. *Persons and personal identity*. Malden, MA: Polity, 2015. ISBN 978-0-7456-5431-7.

[3] GARRETT, Brian. *Personal identity and self-consciousness*. New York: Routledge, 1998. ISBN 04-151-6573-3.

[4] DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. [Brno: M. Drahanský], 2011. ISBN 978-80-254-8979-6.

[5] NOONAN, Harold W. *Personal identity*. Second edition. London: Routledge. ISBN 0-203-42835-8.

[6] ČESKÁ REPUBLIKA. Zákon č. 89 ze dne 3. února 2012 občanský zákoník. In: Sbírka zákonů České republiky. 2012, částka 33. Dostupný také z: *https://www.zakonyprolidi.cz/cs/2012-89*

[7] ČESKÁ REPUBLIKA. Zákon č. 301 ze dne 2. srpna 2000 o matrikách, jménu a příjmení a o změně některých souvisejících zákonů. In: Sbírka zákonů České republiky. 2000, částka 85. Dostupný také z: https://www.zakonyprolidi.cz/cs/2000-301

[8] ČESKÁ REPUBLIKA. Zákon č. 328 ze dne 30. listopadu 1999 o občanských průkazech. In: Sbírka zákonů České republiky. 1999, částka 107. Dostupný také z: https://www.zakonyprolidi.cz/cs/1999-328

[9] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978–80–7251–397–0.

[10] What Is Cybersecurity? *Cisco* [online]. [cit. 2020-02-16]. Dostupné z: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

[11] Kybernetická bezpečnost (Cyber Security). *CyberSecurity.cz: Kybernetická bezpečnost a obrana* [online]. CyberSecurity.cz, 2018, 1. 11. 2017 [cit. 2020-02-16]. Dostupné z: https://www.cybersecurity.cz/basic.html

[12] Co je GDPR a jak bude aplikováno v Česku. *GDPR: Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2020-02-16]. Dostupné z: https://www.gdpr.cz/gdpr/co-je-gdpr/

[13] EVROPSKÁ UNIE. Nařízení Evropského parlamentu a rady (EU) č. 679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Dostupný také z: *https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679&from=EN*

[14] Co považuje GDPR za osobní údaje. *GDPR: Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2020-02-16]. Dostupné z: https://www.gdpr.cz/gdpr/osobni-udaje/

[15] eObčanka: Začátek digitalizace v ČR. *Portál veřejné správy: Na úřad přes internet* [online]. Ministerstvo vnitra, 2018 [cit. 2020-02-16]. Dostupné z: https://portal.gov.cz/eobcanka/o-projektu

[16] eObčanka: Začátek digitalizace v ČR: eObčanka. *Portál veřejné správy* [online]. Ministerstvo vnitra, 2018 [cit. 2020-02-16]. Dostupné z: https://portal.gov.cz/eobcanka

[17] Nové občanské průkazy s čipem vydávané v ČR. *Velvyslanectví České republiky v Canbeře* [online]. MZV ČR, 2020, 31. 08. 2018 [cit. 2020-08-02]. Dostupné z: https://www.mzv.cz/canberra/cz/konz_a_viz_info/nove_obcanske_prukazy_s_cipem_vydavane_v$1325.html?action=setMonth&year=2020&month=9&day=1

[18] Aktivace čipu. *Portál veřejné správy: Na úřad přes internet* [online]. Ministerstvo vnitra, 2018 [cit. 2020-02-16]. Dostupné z: https://portal.gov.cz/eobcanka/aktivace-cipu

[19] Služby vytvářející důvěru a elektronická identifikace. *Ministerstvo vnitra České republiky* [online]. Ministerstvo vnitra České republiky, 2019 [cit. 2020-02-16]. Dostupné z: https://www.mvcr.cz/clanek/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace.aspx

[20] PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, c2011. CZ.NIC. ISBN 978-80-904248-3-8.

[21] POŽÁR, Josef. *Základy teorie informační bezpečnosti*. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8. Dostupné také z: http://www.digitalniknihovna.cz/mzk/uuid/uuid:b38af330-77b3-11e9-8cea-005056827e52

[22] KAMBERG, Mary-Lane. *Digital identity: your reputation online*. New York, NY: Rosen Publishing, [2019]. ISBN 978-15-08-18460-7.

[23] Mějte pod kontrolou svou virtuální identitu. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, 2013 [cit. 2020-02-20]. Dostupné z: https://www.uoou.cz/mejte-pod-kontrolou-svou-virtualni-identitu/ds-5603

[24] SEARGEANT, Philip a Caroline TAGG. *The language of social media: identity and community on the Internet*. Houndmills, Basingstoke, Hampshire: Palgrave Macmillan, 2014. ISBN 978-113-7029-300.

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

[26] ČSOB Identita: Bankovní identita od ČSOB. *ČSOB* [online]. 2020 [cit. 2020-02-20]. Dostupné z: https://www.csob.cz/portal/csob/csob-identita

[27] Bankovní IDentita. *Česká spořitelna* [online]. Česká spořitelna, 2020 [cit. 2020-02-20]. Dostupné z: https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/bankovni-identita

[28] Návrh zákona upravující podmínky pro vznik bankovní identity. *Epravo.cz* [online]. EPRAVO, 2020, 16. ledna 2020 [cit. 2020-02-20]. Dostupné z: https://www.epravo.cz/top/clanky/navrh-zakona-upravujici-podminky-pro-vznik-bankovni-identity-110488.html

[29] O projektu. *Epravo.cz* [online]. ČBA, 2019 [cit. 2020-02-20]. Dostupné z: https://www.bankovni-identita.cz/o-projektu

[30] *Bankovní identita* [online]. 2020 [cit. 2020-02-21]. Dostupné z: https://www.bankovni-identita.cz/

[31] Falešná identita (False Identity). *Management Mania* [online]. ManagementMania.com, 2016 [cit. 2020-02-20]. Dostupné z: https://managementmania.com/cs/falesna-identita

[32] *Online identity theft*. Paris: OECD, c2009. ISBN 978-92-64-05658-9.

[33] Examples of Social Engineering: 9 examples of Social Engineering Attacks. *Terranova Security* [online]. Terranova Worldwide Corporation, 2020, 07. 10. 2019 [cit. 2020-08-01]. Dostupné z: https://terranovasecurity.com/examples-of-social-engineering-attacks/

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

[35] Vulnerabilities, Exploits, and Threats: Defining three key terms in cybersecurity. *Rapid7* [online]. Rapid7 [cit. 2020-03-14]. Dostupné z: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/

[36] Bezpečnostní politika hesel a vícefaktorová autentizace. *System OnLine: S přehledem ve světě informačních technilogií* [online]. CCB, 2020, 01.11.2016 [cit. 2020-06-14]. Dostupné z: https://www.systemonline.cz/it-security/bezpecnostni-politika-hesel-a-vicefaktorova-autentizace.htm

[37] Nejčastější dotazy. *eObčanka: Začátek digitalizace v ČR* [online]. Ministerstvo vnitra, 2018 [cit. 2020-03-15]. Dostupné z: https://portal.gov.cz/eobcanka/nejcastejsi-dotazy

[38] Vytvoření silného hesla a jeho vlastnosti. *Bezpečný internet.cz* [online]. [cit. 2020-03-15]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/hesla/vytvoreni-silneho-hesla.aspx

[39] První pomoc při ztrátě mobilu: zachovejte chladnou hlavu a řiďte se těmito radami. *Digitální pevnost* [online]. Digitální pevnost, 2018, 15.10.2019 [cit. 2020-03-15]. Dostupné z: https://www.digitalnipevnost.cz/zpravodaj/detail/prvni-pomoc-pri-ztrate-mobilu

[40] Policie České republiky – KŘP Jihomoravského kraje: Prozrazení hesla je jí nevyplatilo. *Policie České republiky: Pomáhat a chránit* [online]. Policie ČR, 2019, 12.12.2019 [cit. 2020-03-15]. Dostupné z: https://www.policie.cz/clanek/prozrazeni-hesla-se-ji-nevyplatilo.aspx

[41] Policie České republiky – KŘP Jihomoravského kraje: Pozor na zneužití platební karty. *Policie České republiky: Pomáhat a chránit* [online]. Policie ČR, 2019, 07.03.2012 [cit. 2020-03-15]. Dostupné z: https://www.policie.cz/clanek/pozor-na-zneuziti-platebni-karty.aspx

[42] Policie České republiky – KŘP Olomouckého kraje: Prolomení hesla na sociální síti. *Policie České republiky: Pomáhat a chránit* [online]. Policie ČR, 2019, 17. 7. 2015 [cit. 2020-05-03]. Dostupné z: https://www.policie.cz/clanek/krajske-reditelstvi-olomouckeho-kraje-zpravodajstvi-prolomeni-hesla-na-socialni-siti.aspx

[43] Policie České republiky – KŘP Libereckého kraje: Na svoji matku si půjčil téměř sto padesát tisíc. *Policie České republiky: Pomáhat a chránit* [online]. Policie ČR, 2019, 24. 8. 2018 [cit. 2020-05-03]. Dostupné z: https://www.policie.cz/clanek/na-svoji-matku-si-pujcil-temer-sto-padesat-tisic.aspx

[44] Jak ukrást facebook? Snadno a rychle! *Protišedi.cz: O zlato nejde, jde o to co z něj vyrobit* [online]. Praha: Protišedi, 2020, 05. 02. 2012 [cit. 2020-05-03]. Dostupné z: http://archiv.protisedi.cz/article/jak-ukrast-facebook-snadno-rychle

[45] Úřad udělil společnosti Internet Mall, a.s. pokutu 1,5 milionu korun. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů, 2013, 03. 10. 2018 [cit. 2020-05-03]. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=31959&n=urad%2Dudelil%2Dspolecnosti%2Dinternet%2Dmall%2Da%2Ds%2Dpokutu%2D1%2D5%2Dmilionu%2Dkorun

[46] *Md5() Encrypt & Decrypt* [online]. 2020 [cit. 2020-05-03]. Dostupné z: https://md5decrypt.net/en/

[47] SQL Injection. *W3schools.com: The world's largest web developer site* [online]. Refsnes Data, 2020 [cit. 2020-05-03]. Dostupné z: https://www.w3schools.com/sql/sql_injection.asp

[48] Obrana proti útoku SQL injection v PHP. *ITnetwork.cz: Největší česká IT akademie* [online]. itnetwork.cz, 2020 [cit. 2020-05-03]. Dostupné z: https://www.itnetwork.cz/php/bezpecnost/tutorial-bezpecnost-v-php-utok-sql-injection-a-obrana

[49] Pwned websites: Breached websites that have been loaded into Have I been Pwned. *';--have i been pwned?: Check if you have an account that has been compromised in a data breach* [online]. 2020 [cit. 2020-05-03]. Dostupné z: https://haveibeenpwned.com/PwnedWebsites#Dropbox

[50] Security update and new features. *Work in progress* [online]. Dropbox, 2020, 31. 07. 2012 [cit. 2020-05-03]. Dostupné z: https://blog.dropbox.com/topics/company/security-update-new-features

[51] 10 nejlepších bezpečných správců hesel roku 2020. *VpnMentor* [online]. vpnMentor, 2020 [cit. 2020-05-24]. Dostupné z: https://cs.vpnmentor.com/blog/nejlepsich-bezpecnych-spravcu-hesel/

[52] *KeePass: Password Safe* [online]. Dominik Reichl, 2020 [cit. 2020-05-24]. Dostupné z: https://keepass.info/

[53] *Firefox Monitor* [online]. 2020 [cit. 2020-05-24]. Dostupné z: https://monitor.firefox.com/

[54] *';--have i been pwned?* [online]. 2020 [cit. 2020-05-24]. Dostupné z: https://haveibeenpwned.com/

SEZNAM OBRÁZKŮ