Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Ochrana dat a rizika bezpečnostních incidentů

Kateřina Mackovíková

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Kateřina Mackovíková

Informatika

Název práce

Ochrana dat a rizika bezpečnostních incidentů

Název anglicky

Data protection and security threats

Cíle práce

Cílem práce je představit metody zabezpečení informačních technologií a zohlednit současné trendy v této oblasti. Budou uvedeny příklady nejčastějších chyb uživatelů, bezpečnostních incidentů a budou navrženy možnosti jejich prevence. To vše bude demonstrováno na příkladu konkrétního uživatele informačních systémů.

Dílčím cílem práce bude definovat pojmy z oblasti informačních a komunikačních technologií, vztahující se k řešené problematice, charakterizovat druhy bezpečnostních hrozeb a zohlednit aktuální témata, která mají na problematiku bezpečnosti ICT vliv (např. General Data Protection Regulation). V poslední části práce budou zhodnoceny získané závěry a navržena odpovídající doporučení.

Metodika

V teoretické části práce budou definovány nejdůležitější pojmy zkoumané problematiky, budou uvedeny oblasti využití informačních technologií a definována základní rizika, s nimi spojená. Dále bude tato část pojednávat o způsobech, jakými mohou uživatelé těmto rizikům předcházet a zabezpečit tak systémy, které využívají.

V další části bude práce zaměřena na dílčí problematiky, které oblast ICT ovliňují; v současné době především na nařízení GDPR, které vstupuje v účinnost.

V praktické části práce budou demonstrována bezpečnostní rizika na příkladu běžného uživatele ICT, bude analyzována kvalita zabezpečení jednotlivých využívaných oblastí a rizikovost chování uživatele. U zjištěných nedostatků budou navržena odpovídající doporučení.

Poslední část práce poskytne závěry ze zkoumané problematiky a navržená doporučení.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

data, informace, bezpečnostní opatření, ICT, přístupová hesla, autentizace, autorizace, uživatelské účty, internet

---

Doporučené zdroje informací

DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

ERICKSON, Jon. Hacking: umění exploitace. 2., upr. a dopl. vyd. Přeložil Jan POKORNÝ. Brno: Zoner Press, 2009. Encyklopedie Zoner Press. ISBN 978-80-7413-022-9.

HILL, David G. Data protection: governance, risk management, and compliance. Boca Raton, FL: Taylor & Francis, c2009. ISBN 1439806926.

HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 5. aktualiz. vyd. Brno: Computer Press, 2011, 303 s. ISBN 9788025131763.

HUNT, Craig. TCP/IP network administration. Beijing: O'Reilly & Associates, 2002. ISBN 0-596-00297-1.

SZOR, Peter. Počítačové viry: analýza útoku a obrana. Brno: Zoner Press, 2006. Encyklopedie Zoner Press. ISBN 80-86815-04-8.

Předběžný termín obhajoby

2018/19 LS – PEF

Vedoucí práce

Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 28. 6. 2018

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2018

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 28. 03. 2019

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Ochrana dat a rizika bezpečnostních incidentů" jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 28.03.2019 _____

Poděkování

Ráda bych touto cestou poděkovala Ing. Jiřímu Vaňkovi, Ph.D. za čas, který mi věnoval, cenné připomínky a vedení mé diplomové práce. Dále bych ráda poděkovala Michalu Špačkovi a Janu Javorkovi, kteří mi poskytli podporu a hodnotné informace a podělili se se mnou o své zkušenosti z oblasti bezpečnosti informačních technologií. Poslední poděkování patří mým spolužákům za vzájemnou podporu během studia.

Ochrana dat a rizika bezpečnostních incidentů

Abstrakt

Práce se zabývá vybranými aspekty ochrany dat a riziky bezpečnostních incidentů v oblasti informačních technologií.

Nejprve definuje základní relevantní pojmy, spojené s touto problematikou, včetně zahrnutí právního hlediska. Zde je obsaženo také relativně nové Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation).

V praktické části práce probíhá testování vybraných oblastí informační bezpečnosti, k čemuž je základním podkladem rozsáhlé dotazníkové šetření. Tento úsek se zabývá pohledem uživatelů informačních technologií, nicméně zároveň reflektuje, jakým způsobem se pohled uživatele prolíná s pohledem firem (poskytovatelů služeb). Z šetření vyplynula významná rizika spojená s bezpečností uživatelských hesel.

Následně je vytvořena testovací webová stránka, která umožňuje prokázat triviálnost prolomení uživatelských hesel, pokud jsou k jejich zabezpečení voleny slabé nástroje.

Dalším krokem je zohlednit riziko bezpečnostních incidentů z pohledu poskytovatelů služeb. V rámci participace na projektu, který mapuje, jakým způsobem firmy zacházejí s uživatelskými hesly, proběhlo oslovení těchto firem a vyhodnocení získaných informací.

Tato šetření umožnila vyvodit příslušná doporučení a závěry.

Klíčová slova: data, informace, bezpečnostní opatření, ICT, přístupová hesla, autentizace, autorizace, uživatelské účty, internet

Data protection and security threats

Abstract

The thesis is dedicated on specific aspects of data protection and security threats in field of information technologies.

Initially there is defined basic relevant terminology related to the topic, including legal aspects such as General data protection regulation, among others.

Following section is focused on practical testing of specific elements of information security. As the basic analytical tool was conducted an extensive questionnaire survey, providing information from the point of view of information technologies users. At the same time there is reflected the fact of significant relation between information technologies users and companies (service providers), handling all the data. Extracted data proved risks of high importance in field of handling passwords.

In next step there is implemented test web page which helps to show simplicity of passwords cracking in case of using inappropriate password storage tools.

To link user point of view with service providers attitude there is introduced a real project which reflects important facts. Based on documented communication with companies was obtained information about the way in which companies are storing user data.

These procedures allowed to make objective recommendations and conclusions.

Keywords: data, information, security measures, ICT, passwords, authentication, authorization, user accounts, internet

Obsah

1 Úvod ... 11

2 Cíl práce a metodika ... 13
2.1 Cíl práce ... 13
2.2 Metodika ... 13

3 Teoretická východiska ... 14
3.1 Základní pojmy ... 14
3.2 Informační bezpečnost ... 23
3.3 Bezpečnostní hrozby ... 27
3.4 Nejčastější chyby ... 31
3.5 Technologie ... 33
3.6 Nástroje ... 35
3.7 Hodnocení rizik v oblasti ochrany dat ... 45
3.8 Právní aspekty ICT ... 48

4 Vlastní práce ... 52
4.1 Pohled uživatele ... 54
4.1.1 Dotazníkové šetření ... 55
4.1.2 Implementace webové stránky k demonstraci útoku na hesla ... 60
4.2 Pohled poskytovatele služeb ... 66

5 Výsledky a diskuse ... 71
5.1 Doporučení uživatelům ... 72
5.2 Doporučení poskytovatelům služeb ... 74
5.3 Diskuse ... 75

6 Závěr ... 77

7 Seznam použitých zdrojů ... 78

8 Přílohy ... 82

Seznam obrázků

Obrázek 1 Princip Certificate Transparency 44
Obrázek 2 Dotazníkové šetření – výběrová a nevýběrová chyba 47

Seznam tabulek

Tabulka 1 Nejčastěji používaná hesla v letech 2013-2018 54
Tabulka 2 Způsob ukládání uživatelských hesel – reakce poskytovatelů služeb 68

1 Úvod

Bezpečnost informačních systémů je vzhledem k neuvěřitelně rychlému a stále pokračujícímu vývoji informačních technologií neustále diskutovaným tématem. Oblast ICT je zároveň velmi široká a zasahuje do života jednotlivců i firem. Běžně využíváme počítače, mobilní telefony, tablety, platební terminály, navigace a mnoho dalších zařízení, která do této oblasti spadají a život bez nich si již nelze představit.

V dnešní době je každý člověk zdrojem neuvěřitelného množství dat a informací, které je s pomocí informačních systémů mnohdy velmi snadné získat. Krásným příkladem je současná forma on-line marketingu, kdy se stačí podívat cíleně na webové stránky produktu, který nás zrovna zajímá (ať už se jedná o letenky, obuv, elektroniku nebo cokoliv jiného) a vzápětí se nám reklama na tento produkt objeví prakticky na každé komerční stránce, kterou otevřeme. V tomto případě se jedná o tzv. personalizovanou inzerci.

I přes nesporný přínos informačních technologií do každodenního života je třeba brát zřetel na jejich rizika, především cíleně mířené útoky, zahrnuté pod pojmem kyberkriminalita.

Přestože společnosti a instituce se většinou snaží o maximální zabezpečení svých sítí a aplikací, často se podaří ho obejít, protože i vývoj malware a dalších ohrožujících činitelů jde ruku v ruce kupředu.

Běžní uživatelé, kteří často fungují na cloudových účtech, e-mailových klientech a mnoha hravých aplikacích, se většinou o kvalitní zabezpečení těchto služeb zajímají výrazně méně a rizika si ani příliš neuvědomují. Přitom stačí ponechat například notebook nebo mobilní telefon bez požadavku na přístupové heslo a při jejich odcizení je možné přijít o velmi citlivá data. Mnoho z nás je již trvale přihlášeno na e-mailové účty a různé aplikace a cizí osoby se tak mohou dostat jak ke kontaktům, tak i dalším údajům, fotografiím, heslům. A toto je jen zlomkový příklad možných rizik.

Neznamená to ale, že možností zabezpečení je málo a že je třeba propadat panice. Samozřejmě ne vždy je to dostačující, ale často by pomohlo udělat si přehled o možnostech

a dodržovat alespoň základní bezpečnostní zásady. Zároveň jsou někdy zvoleny zbytečně složité cesty tam, kde je možno postupovat jednodušším způsobem.

V rámci práce bude demonstrován příklad, jakým uživatel využívá informační technologie, v jakých oblastech může dojít k pochybení a ohrožení bezpečnosti dat a informací. Budou také testovány hypotézy, související s tímto tématem a v rámci výsledků šetření budou vyvozena doporučení, jak odvozeným rizikům zabránit.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je představit metody zabezpečení informačních technologií a zohlednit současné trendy v této oblasti. Budou uvedeny příklady nejčastějších chyb uživatelů, bezpečnostních incidentů a budou navrženy možnosti jejich prevence. To vše bude demonstrováno na příkladu konkrétního uživatele informačních systémů.

Dílčím cílem práce bude definovat pojmy z oblasti informačních a komunikačních technologií, vztahující se k řešené problematice, charakterizovat druhy bezpečnostních hrozeb a zohlednit aktuální témata, která mají na problematiku bezpečnosti ICT vliv (např. General Data Protection Regulation). V poslední části práce budou zhodnoceny získané závěry a navržena odpovídající doporučení.

2.2 Metodika

V teoretické části práce budou definovány nejdůležitější pojmy zkoumané problematiky, budou uvedeny oblasti využití informačních technologií a definována základní rizika, s nimi spojená. Dále bude tato část pojednávat o způsobech, jakými mohou uživatelé těmto rizikům předcházet a zabezpečit tak systémy, které využívají.

V další části bude práce zaměřena na dílčí problematiky, které oblast ICT ovlivňují; v současné době především na nařízení GDPR, které vstupuje v účinnost.

V praktické části práce budou demonstrována bezpečnostní rizika na příkladu běžného uživatele ICT, bude analyzována kvalita zabezpečení jednotlivých využívaných oblastí a rizikovost chování uživatele. U zjištěných nedostatků budou navržena odpovídající doporučení.

Poslední část práce poskytne závěry ze zkoumané problematiky a navržená doporučení.

3 Teoretická východiska

Následující kapitola se věnuje vysvětlení základních pojmů, které budou obsaženy v rámci diplomové práce a charakterizování jednotlivých technologií a druhů bezpečnostních hrozeb. Slouží také ke zmapování problematiky, související s bezpečnostními incidenty. Vzhledem k účelu a rozsahu této práce není možné obsáhnout kompletní terminologii z oblasti informačních systémů. Tu je možné nalézt ve specializovaných slovnících.

Odborná literatura zařazuje mezi jednu z nejcitlivějších oblastí problematiku uživatelských hesel. Z této informace následně vychází praktická část práce, která je zaměřena na hesla.

3.1 Základní pojmy

V této podkapitole je definována řada základních pojmů, které souvisejí se zpracovávaným tématem. Vysvětlení další relevantní terminologie bude obsaženo v podkapitolách následujících.

Ochrana dat

Současné zdroje používají slovní spojení „ochrana dat“ především v souvislosti s novou regulací Obecné nařízení pro ochranu osobních údajů. Není se čemu divit, neboť toto nařízení ovlivňuje celou řadu oblastí a dotýká se, respektive upravuje, především způsob nakládání s osobními údaji, které jsou zpracovávány obrovským množstvím institucí a firem. Nicméně na ochranu dat by mělo být pohlíženo ve výrazně širším kontextu. (1)

Data jsou často chápána jako kapitál, jehož ztráta nebo možné zneužití může znamenat i přímé ohrožení chodu firmy nebo dokonce její krach. Zároveň nejen firemní, ale i osobní údaje jsou permanentně vystaveny různým rizikům. Problematika ochrany dat pojímá i tato rizika a nástroje, jak se proti nim chránit. V souvislosti s informačními technologiemi se jedná o velmi relevantní pojem. (2) (3) (4)

Uvádí se, že průměrná finanční ztráta malého a středního podniku (SMB) způsobená únikem dat dosáhla v roce 2018 částky 120 000 dolarů (okolo 2 660 000 Kč). Dále se uvádí, že je to o 36 % více než v předcházejícím roce (88 000 dolarů), kdy se velké firmy v případě úniku dat musejí v průměru vypořádat se ztrátou 1,23 milionu dolarů (přes 27 milionů Kč). Oproti roku 2017 tak v případě hackerského útoku musejí vynaložit o 24 % více finančních prostředků. (5)

Kyberkriminalita

Kriminalita, nazývaná nejdříve počítačová, nyní pak kybernetická kopíruje technické vlastnosti i uživatelské možnosti počítačů, počítačových sítí, resp. celého kyberprostoru. Ze všeho nejdříve se počítače staly předmětem klasických kriminálních útoků, směřujících proti nim, coby věcem movitým – krádeže, poškozování cizí věci atd. Později se jednání pachatelů posunulo směrem k neoprávněnému užívání. Následovaly útoky na data počítači zpracovávaná, a přes podvody se tento druh kriminality posunul až k dnešnímu stavu, kdy skutkových podstat spojených s počítači a počítačovými sítěmi je možné nalézt v současném trestním zákoníku celou řadu a kdy variabilita jednání pachatelů v kyberprostoru je značná a neustále se rozšiřuje. (6)

Kyberkriminalita může být namířena proti počítačům, jejich hardwaru, softwaru, datům, sítím, nebo v ní vystupuje počítač jen jako nástroj páchání trestného činu, případně jsou počítačová síť a k ní připojená zařízení prostředím, ve kterém se trestná činnost odehrává. Obtížnost sledovaní projevů kyberkriminality mimo jine spočívá i v tom, že se uvedené jednání odehrává v prostředí, které je objektivně pouze obtížně vnímatelné. Dění v kyberprostoru je možné sledovat pouze za pomoci jiného počítače. (7)

Kybernetická bezpečnostní událost

Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací. (8)

Kybernetický bezpečnostní incident

Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události. (8)

Kybernetický útok

Je možné ho definovat jako jakékoli protiprávní jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby. Tato jednání nemusí mít vždy podobu trestného činu, podstatné je, že narušují běžný způsob života poškozeného. Kybernetický útok může být dokonán, stejně jako může být ve stádiu přípravy či pokusu. (7 str. 55)

Počítačová síť

Jedná se o soubor počítačů spolu s komunikační infrastrukturou (komunikační linky, technické vybavení, programové vybavení a konfigurační údaje), jejímž prostřednictvím si (počítače) mohou vzájemně posílat a sdílet data. (9 str. 73)

Internet

Komplexní a globální počítačovou sítí pak je Internet, který je také označován jako „Síť sítí“.

Technicky se jedná o decentralizovanou, celosvětovou distribuovanou počítačovou síť složenou z jednotlivých menších sítí navzájem spojených pomocí protokolů TCP/IP. (7 str. 69)

Internet Protocol

Pracuje v síťové vrstvě soustavy TCP/IP. Od nadřazených protokolů transportní vrstvy obdrží datové segmenty s požadavkem na odeslání. K segmentům připojí vlastní hlavičku a vytvoří IP datagram. V IP hlavičce je především IP adresa příjemce a odesílatele, což předznamenává hlavní poslání protokolu: doručení jednotlivých datagramů k příjemci – provádí tedy adresování a směrování datagramů mezi počítači.

IP protokol je nespojovaný (před zahájením výměny dat nevytváří relaci) a nespolehlivý (předání paketů na místo určení není kontrolováno). Paket IP se tedy může ztratit, být doručen mimo pořadí, zdvojen nebo zpožděn. Protokol IP neobsahuje prostředky pro zotavení z chyb tohoto typu. To vše má zajistit nadřízená transportní vrstva – protokol TCP. (10 stránky 58, 59)

IPv4

Jedná se o první, masově rozšířenou a v současnosti stále nejrozšířenější verzi Internet protokolu. IPv4 používá 32bitové adresy, které jsou zapsány dekadicky po jednotlivých oktetech (osmicích bitů). Veřejná adresa v rámci IPv4 je tvořena čtveřicí čísel, vždy od sebe oddělených tečkou, přičemž hodnota každého z nich nepřesahuje 255. IP adresa tedy může mít podobu například takovéhoto číselného řetězce: 195.113.149.160, či 64.233.168.99 apod. Číselný řetězec IP adresy: 302.233.8.158, či 64.233.168.299 v tomto provedeni je nesmyslný a není se možné jeho prostřednictvím přihlásit do sítě Internet. (7 stránky 74, 75)

IPv6

IPv6 je novým protokolem, který by měl vyřešit problémy související s nedostatkem veřejných IP adres. IP adresa verze 6 má délku 128 bitů, které jsou zapsány hexadecimálně (např. 2001:0:5ef5:79fd:386a:e7:4dee:fb51). U IPv6 je odstraněna potřeba použití překladu síťových adres. IPv6 obsahuje celkem 2 128 adres. (7 str. 75)

Webový prohlížeč (web browser, prohlížeč, klient)

Webový prohlížeč je další aplikací, která standardně předává informace o uživateli a jeho počítačovém systému, počítačovému systému (serveru) navštívené stránky. Tento server pak v rámci dotazu od klienta zjistí například referer (což je stránka ze které uživatel přichází), používaný webový prohlížeč a operační systém (včetně přesné verze), cookies, flash cookies, historie, cache aj. (7 str. 139)

Vzhledem k tomu, že webové prohlížeče (např. Interet Explorer a Firefox) realizují stranu klienta http, jsou v rámci aplikace Web výrazy prohlížeč a klient zaměnitelné. (11 str. 97)

Request for comment (RFC)

Používá se pro označení řady standardů popisujících Internetové protokoly, systémy a další věci související s fungováním internetu. Například RFC 5321 popisuje protokol SMTP pro výměnu a zpracování elektronické pošty. (9 str. 99)

Cookie

Na webu se používá bezstavový protokol http, který si sám o sobě neumí žádné informace z HTTP dotazů nebo odpovědí zapamatovat. Složitější webové stránky ale paměť potřebují, a tak vznikly takzvané cookies (RFC 2109), které jsou součástí http dotazů i odpovědí a slouží k ukládání jednoduchých informací. Cookies mají různou životnost – některé se vztahují jen ke konkrétní relaci a zaniknou s ukončením webového prohlížeče, jiné si prohlížeč ukládá na disk a zapomíná až po určené době. (Na Windows 9x se cookies obvykle ukládají do adresáře %windir%\Cookies, na novějších Windows do %userprofile%\Cookies.) Manipulací s cookies může útočník změnit uživatelovu online identitu nebo získat citlivé informace.

Cookies lze získat a odeslat například odposlechem sítě, nějakým podvodem uživatele nebo zneužitím bezpečnostní díry webového prohlížeče. (12 str. 456)

Trvalé cookies soubory jsou uloženy na disku a svým tvůrcům umožňují sledovat konkrétního uživatele a jeho návštěvy daného webu, uživateli dovolují nastavit vlastní téma webu.

Dočasné cookies soubory jsou uloženy v RAM paměti a po uzavření prohlížeče jsou smazány. Proto některé aplikace vyžadují od uživatele, aby po odhlášení uzavřel prohlížeč. Takové řešení se spoléhá na uživatele, což v konečném důsledku snižuje bezpečnost.

Správné odhlášení funguje na principu, že aplikace změní nastavení času cookies souborů a prohlížeč je vzhledem k času, který je z minulosti, zničí. (13 str. 275)

HTTP server neuchovává informace o uživateli, to znamená, že je to bezstavový protokol. To zjednodušuje návrh serveru a umožňuje vývojářům vyvíjet vysoce výkonné webové servery, které mohou obsloužit tisíce paralelních TCP spojení. Pro webovou stránku je však často potřebné identifikovat uživatele. Buď proto, že server chce uživatelům omezit přístup, nebo proto, že chce nabízet obsah v závislosti na identitě uživatele. Pro tyto účely používá protokol HTTP cookies. Cookies, definované ve specifikaci [RFC 6265], umožňují webům sledovat činnost uživatele. Většina hlavních komerčních webů v dnešní době používá cookies. (11 str. 104)

Cookies tedy lze použít k identifikaci uživatele. Když uživatel navštíví stránky poprvé, může poskytnout identifikaci uživatele (případně své jméno). Během dalších relací předává prohlížeč serveru záhlaví cookie, čímž se uživatel na serveru identifikuje. Cookies lze tedy použít k vytvoření uživatelské relace nad prostým protokolem http. Když se uživatel například přihlásí k aplikaci webového e-mailu (například Hotmail), prohlížeč odešle na server informaci cookie, která serveru umožní identifikovat uživatele v průběhu celé relace s aplikací.
Přestože soubory cookie uživatelům často zjednodušují nakupování na internetu, jsou kontroverzní, protože je lze také považovat za narušení soukromí. Pomocí kombinace cookies a informací dodaných uživatelem může web shromáždit mnoho informací o uživateli a potenciálně tyto informace prodat třetí straně. (11 str. 105)

ISO/OSI

K tomu, aby bylo možno přenášet data mezi jednotlivými počítačovými systémy, byl definován model ISO/OSI jako referenční komunikační model. Tento model rozděluje komunikaci do sedmi vzájemně propojených vrstev. Tento model je zařazen do ISO/IEC 7498-1:1994 [v ČR: ČSN EN ISO/IEC 7498-1 (369614). Informační technologie – Propojení otevřených systémů – Základní referenční model – Základní model (ISO 7498-1:1994).]. (7 str. 70)

TCP/IP

Spadá pod síťové architektury. Podobně jako referenční model ISO/OSI vychází z představy, že by měl být uspořádán do úhledné hierarchické struktury vrstev. Proto

se někdy mluví o síťových architekturách jako o vrstvových. ISO/OSI se skládá ze 7 vrstev, kdežto TCP/IP má pouze 4. (14 str. 607)

PAN (Personal Area Network)

Jedná se o malou privátní síť, která zpravidla slouží pro potřeby jednotlivce či domácnosti. V rámci této sítě dochází typicky k propojení jednotlivých počítačových systémů (mobilní telefon, PDA, laptop aj.) typicky za pomoci Bluetooth, IrDA, WiFi, ZigBee. PAN sítě se v současnosti značně rozšiřují a zapojují do své struktury čím dál více zařízení. Příkladem fungovaní PAN sítě je komunikace jednotlivých technologií v domácnosti například s mobilním telefonem či počítačem, a to v rámci propojení těchto systémů do Internetu věcí (IoT) či Internetu všeho (IoE). (7 str. 68)

LAN (Local Area Network)

Označení pro počítačovou síť, rozléhající se na relativně malé geografické oblasti. Používá se pro propojení prvků v rámci místnosti, budovy, skupin budov, v rámci domácnosti nebo podnikové sítě. Nejčastějším způsobem zapojení je pomocí technologií Ethernet a Wi-Fi. K propojení cílových uzlů se v této síti používají aktivní a pasivní prvky, nejčastěji switche a routery. Jednotlivé prvky jsou propojeny kroucenou dvojlinkou, koaxiálním kabelem, optickým vláknem nebo bezdrátově. V těchto sítích jsou dosahovány vysoké přenosové rychlosti, v řádech Gb/s. (15)

WiFi (Wireless Fidelity)

Je nutné odlišit označení 802.11 a zkratku WiFi. Číselné označení je číslem standardu mezinárodní organizace IEEE, většinou se používá verze 802.11b. WiFi je označení, které uděluje asociace WECA (Wireless Ethernet Compatibility Alliance) produktům, které splňují všechny požadavky normy. Řada prodejců a některé literární prameny tyto pojmy směšuje či zaměňuje. WiFi sítě se řadí do sítí bezdrátových, které jsou hojně využívány na mnoha veřejných prostranstvích a jejichž výrazným rizikem je snadná odposlechnutelnost. Připojit se k nim může kdokoliv s patřičně vybaveným počítačem a vzhledem k absenci opatření k zabránění odposlechů může útočník získat

citlivé informace a dokonce s provozem na dané síti i manipulovat. (16 stránky 114, 115)

Přístupový bod (access point, AP)

V podstatě jsou AP huby, z nichž se rozvádí signál. Vlastní provedení se liší u jednotlivých výrobců, do hubů mohou být integrovány funkce mostu nebo routeru (nejčastěji pro sdílené připojení internetu). Mnoho výrobců nabízí napájení AP bodu pomocí kroucené dvojlinky, jíž je bod připojen k pevné síti. K přístupovému bodu (na obtížně dostupném místě) se tak nemusí táhnout dvě vedení. Přístupový bod a jeho protějšky – klientské adaptéry pracují pouze tehdy, pokud mezi nimi není žádná překážka – mezi AP a počítači umístěnými v bezdrátové síti musí být přímá viditelnost. Proto jsou přístupové body k nalezení v nejvyšších částech místností. (10 str. 40)

SSID

SSID: (Service Set ID) – je názvem Access Pointu, pod nímž jej uvidí všichni klienti, kteří se dostanou do jeho dosahu. SSID je tak logickým identifikátorem určité bezdrátové podsítě. Může být nastaven manuálně na stanici, nebo informaci o SSID přístupový bod pravidelně vysílá, či může být vysílání SSID vypnuto a klient se na SSID sám dotáže (probe). (10 str. 41)

MAN (Metropolitan Area Network)

Jedná se o síť, která propojuje LAN sítě v městské zástavbě. Síť MAN spojuje jednotlivé uzly v řádech jednotek až desítek kilometrů. Někteří autoři řadí tuto síť do sítí WAN. (7 str. 68)

WAN (Wide Area Network)

Ty se skládají z více vzájemně propojených sítí LAN. Jejich spojování se provádí speciálními linkami či bezdrátově. Rozlehlost sítí může být různá, od sítí městských či firemních (firma s pobočkami ve více městech, zemích či kontinentech), až po nejznámější celosvětovou síť – Internet. (10 str. 9)

Privátní síť

Využívá privátní IP adresy. Privátní adresy jsou používány v rámci sítě LAN (domácí, podnikové aj.). Pokud privátní síť potřebuje připojení k Internetu (přes přidělené veřejné IP adresy), musí používat překlad síťových adres (NAT), nebo proxy server. Privátní sítě se využívají zejména z důvodu nedostatečného množství veřejných IP adres ve verzi Ipv4. (7 str. 69)

Veřejná síť

Je otevřena nejširší veřejnosti, které nabízí své služby spočívající v přenosu dat. Uživatelem takovéto sítě se skutečně může stát kdokoli, kdo o to má zájem a je ochoten za to zaplatit, resp. přistoupit na podmínky toho, kdo takovouto síť provozuje. Provozovatelem přitom bývá takový subjekt, který svou datovou sám nepoužívá - vlastní ji a provozuje především proto, aby její služby mohl poskytovat na komerční bázi jiným subjektům. (17)

Virtuální privátní síť (VPN – Virtual Private Network)

VPN je mechanismus (nebo metoda) umožňující propojení počítačových systémů prostřednictvím nedůvěryhodné (např. veřejné) počítačové sítě tak, že propojené počítačové systémy mezi sebou budou moci komunikovat, jako by byly propojeny v rámci důvěryhodné (uzavřené privátní) sítě. Tyto počítačové systémy ověřují svoji totožnost (např. pomoci certifikátů, hesla aj.) a po vzájemné autentizaci je komunikace mezi těmito privátně propojenými počítači šifrována. (7 str. 69)

Typy VPN podle typu spojení:

Site-to-Site VPN spojuje dvě (nebo více) sítí dohromady, většinou centrálu a pobočky, používají se speciální síťová zařízení (VPN koncentrátor, firewall, router, server), která slouží jako VPN gateway a naváží mezi sebou VPN spojení (příchozí komunikaci rozbalí a do sítě posílají standardně, odchozí zapouzdří do VPN tunelu), uživatelské stanice pak nepotřebují VPN klienta, často používané protokoly/typy jsou IPsec VPN a MPLS VPN. (18)

Remote Access VPN připojuje klienty do lokální sítě, klienti musí mít nainstalován speciální software neboli VPN klienta, na straně privátní sítě se nachází opět specializované síťové zařízení. (18)

3.2 Informační bezpečnost

Jedná se o multidisciplinární obor, usilující o komplexní pohled na problematiku ochrany informací během jejich vzniku, zpracování, ukládání, přenosu a likvidace. Je tak možné chápat odvětví, zabývající se snižováním rizik, vztahujících se k fenoménu informací a navrhující opatření, vztahující se k příslušným organizačním, řídícím, metodickým, technickým, právním a dalším otázkám, které s touto problematikou souvisí. Někdy je možné se setkávat s podstatně omezenějším chápáním daného pojmu, jako úzké disciplíny, týkající se výhradně bezpečnosti informačních a komunikačních technologií. (19 str. 1)

Pojem „Informační bezpečnost“ v sobě zahrnuje komplexní systémový přístup při zajištění ochrany informací v celém jejich životním cyklu, tj. ochranu odpovídajících technologických, programových i organizačních komponent IS a informací, které jsou v nich uchovávány, zpracovávány a přenášeny. Do takto formulované informační bezpečnosti pak spadá i komunikační bezpečnost, tj. ochrana informace přenášené mezi výpočetními prostředky (počítači, servery apod.), fyzická bezpečnost, tj. ochrana před přírodními hrozbami i hrozbami způsobenými lidským faktorem a personální bezpečnost, tj. ochrana před zaměstnanci podniku. (6 str. 10)

Bezpečnost uživatelských hesel

V dnešní době existuje nespočet webů, na kterých si uživatelé zakládají účty za různým účelem. Většinou se jedná o nákup zboží, komunikaci prostřednictvím sociálních sítí, sdílení koníčků, nahrávání dokumentů a videí, online bankovnictví apod. Jsou to citlivé údaje, mnoho z nich je používáno několikanásobně, mezi různými službami, a často jsou vytvořené způsobem, který není bezpečný. Hesla k účtům mnoho lidí tvoří tak, že jsou spojena přímo s jejich osobou, např. použitím roku narození, jmen potomků, domácích mazlíčků, zdrobnělin nebo jejich přezdívek.

Případně jsou hesla naprosto triviální, ve stylu 1234, admin, test, heslo, název webových stránek a podobně. Bezpečnost hesla navíc bohužel nikdy nezávisí jen na jeho majiteli ale také na dalších stranách, které s hesly pracují. V odborné literatuře se uvádí, že právě problematika hesel ve spojení s používanými internetovými protokoly http(s) je jednou z nejohroženějších oblastí.
Z pohledu uživatele je současný stav vyhodnocen v rámci praktické části práce.

Podle doporučení z odborné literatury musí uživatelé dodržovat následující **nejdůležitější povinnosti při práci s hesly:**

1. Hesla nesmí být jakýmkoliv způsobem sdělena jiné osobě.
2. Hesla nesmí být nikde poznamenána a musí se udržovat v tajnosti.
3. Nesmí být, jakkoliv umožněno jiné osobě seznámit se s heslem.
4. Jako hesla nesmí být použita jména blízkých osob, zvířat a další slova, která mohou být odhadnuta ze znalosti držitele hesla, nebo neobsahovalo po sobě jdoucí stejné.
5. Heslo musí být dostatečně silné, tak aby se nedalo jednoduše strojově nebo ručně prolomit (kombinace velkých a malých písmen a číslic, délka alespoň 10 znaků) a mělo by být pravidelně měněno v závislosti rizicích spojených s prolomením.
6. Hesla nesmí být zaznamenána na papíře nebo v obdobné podobě (výjimku tvoří bezpečné uložení administrátorských hesel pro případ havárií).

Hesla se musí změnit v případě jakéhokoliv náznaku možného kompromitování systému nebo hesla. Plnění těchto požadavků nelze nechat na samotných uživatelích, je nutno implementovat do informačních systémů řešení, které bude řádnou správu hesel vynucovat. (6 str. 27)

Bezpečnostní politika

(1) Na úrovni organizace základní dokument, který vymezuje strukturu bezpečnostního rizika, odpovědnost za ochranu informací v organizaci, úroveň ochrany informací. (2) Na úrovni systému soubor pravidel a praktik, které specifikují

nebo regulují, jak systém (nebo organizace) poskytuje bezpečnostní služby, aby chránil citlivé nebo kritické zdroje systému. (9 str. 26)

Mohlo by se zdát, že pojmy informační bezpečnost a bezpečnostní politika jsou spojeny primárně s podnikatelskou činností firem a že jednotlivců ve smyslu běžných uživatelů se zase tolik netýkají. Takto úzce by ale neměly být chápány. Uživatelé i firmy čelí téměř totožným rizikům a tyto dvě roviny se velmi těsně prolínají (už jen proto, že firmy jsou seskupením jednotlivců a vždy hraje vysokou roli lidský faktor).

Nicméně pravdou je, že jednotlivci pro své osobní užívání technologií nemají obvykle k dispozici stejné nástroje bezpečnostní politiky (nebo ne v takovém rozsahu).

Bezpečností politika obsahuje celou řadu oblastí:

- **Fyzická bezpečnost** – tzn. místo, kde se data fyzicky skladují, zda je toto místo vyhovující z pohledu fyzického přístupu k zařízením pro ukládání a zpracování dat a zda je zajištěno z pohledu požárního zabezpečení, poruch či přírodních pohrom.

- **Zálohování a archivace dat** – zálohování je určeno k uchovávání operativních dat umožňujících rychlou obnovu v případě nějakého incidentu, archivace je zase důležitá k uchování historických dat pro možné (často zákonem stanovené) dohledávání informací.

- **Zabezpečení před viry a malwarem** – základní opatření, které ochraňuje podnikové informační prostředky před útoky zvenčí a narušením bezpečnosti dat, zajištění před krádeží dat – opatření zabraňující tomu, aby data nemohla podnik žádným způsobem opustit, případně aby v případě krádeže mohla být jakkoli zneužita.

- **Řízení pohybu dat** – stanovení obecného řízení pohybu dat v podniku, tedy kategorizace dat, manipulace s nimi, sledování jejich pohybu, autorizace přístupu k nim apod.

- **Monitoring uživatelů a procesů** – nastavení systému informujícího o tom, co pracovníci dělají s podnikovými prostředky a daty s možností zpětné kontroly a nastavení firemní politiky.

- **Patch management** – pravidelné aktualizace softwarového vybavení, které udržují podnikové systémy zabezpečené proti nejnovějším hrozbám.

- **Konfigurační databáze** – jakmile je organizace trochu větší, přestává mít přehled o nastaveních všech svých zařízení, je proto třeba mít systém pro řízení změn a vše ukládat do konfigurační databáze.

- **Školení uživatelů** – ať již to vyžadují normy, nebo ne, je důležité informovat uživatele o důvodech existence bezpečnostních pravidel a způsobech jejich dodržování.

- **Externí přístup k datům** – pravidla pro přístup do podnikové sítě z nepodnikových zařízení, z domácí kanceláře, vzdálené kanceláře, na cestách apod., k vybraným datům ze zvolených zařízení.

- **Periodické kontroly a audit** – každá informační infrastruktura potřebuje čas od času pravidelnou (a pokud možno) nezávislou kontrolu svého zabezpečení, protože útoky hackerů jsou stále vynalézavější, a obrana tak musí být neustále vylepšována. (20)

3.3 Bezpečnostní hrozby

Firmy a klíčová infrastruktura čelí napříč časem s vývojem technologií stále většímu množství bezpečnostních hrozeb. V současné době je vyšší dostupnost nástrojů, šifrovacích a anonymizačních platebních systémů a vzdáleně ovladatelných prvků, které potenciální útočníci mohou zneužít.

Za případné bezpečnostní katastrofy ve firmách nenese odpovědnost pouze IT oddělení. I management a další lidé by měli být zapojeni do prevence bezpečnostních rizik. Útočníci jsou sofistikovaní a jsou většinou o krok napřed před běžnými uživateli technologií. Je jich víc, mají více času a často pracují v etablovaných skupinách nebo je dokonce sponzorují státy. Informace získávají například i z pracovních inzerátů firem a sociálních sítí. Proto je potřeba neustále dělat kybernetická cvičení, simulace útoků, a hlavně zvyšovat povědomí zaměstnanců o tom, jaké následky může mít nepozornost a rizikové chování. Management by měl jít příkladem. (21)

Níže jsou uvedeny nejčastější bezpečnostní hrozby.

Hacking / cracking

Neoprávněný průnik do konkrétního informačního systému, provedený zvnějšku, zpravidla ze vzdáleného počítače. Samotný průnik je podmínkou pro další neautorizovanou činnost v rámci cílového systému. Pachatelé se zpravidla nepřipojují k objektu útoku (počítači) přímo, ale přes jeden i více internetových serverů v různých částech světa. Cílem takového postupu je podstatné snížení možnosti identifikace skutečného umístění počítače, který byl při útoku užit. Po spáchání činu na cílovém počítači je často možno zjistit pouze internetovou adresu předchozího počítače, k němuž byl pachatel připojen (a do kterého učinil popsaný zásah). Jednotlivé případy takových incidentů se liší zejména co se týče jejich motivace (vzrušení, zábava, msta, zvědavost, hmotný zisk). Samotný pojem „hacking“ bývá (zpravidla, ale nikoli výlučně) spojován s jinou než zištnou (či nezvratně ničivou) motivací; pojem „cracking“ bývá naopak užíván právě v případech, jejichž cílem je počitatelný zisk (respektive jejichž výsledkem je nevratná škoda).

Phishing („rhybaření“, „házení udic“)

Podstatou metody, usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtu apod. za účelem jejich následného zneužití (výběr hotovosti z konta, neoprávněný přístup k datům atd.), je vytvoření podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmíněné údaje z uživatele vylákat. Zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele. Muže jít například o padělaný dotaz banky, jejíchž služeb uživatel využívá, se žádostí o zaslání čísla úctu a PIN pro kontrolu (použití dialogového okna, předstírajícího, že je oknem banky - tzv. spoofing). Tímto způsobem se snaží přistupující osoby přesvědčit, že jsou na známé adrese, jejímuž zabezpečení důvěřují (stránky elektronických obchodů atd.). Tak bývají rovněž velice často zcizována například čísla kreditních karet a jejich PIN. Prvním případem pokusu o uplatnění phishingu v prostředí bankovní sféry České republiky se v březnu 2006 stala Citybank. V březnu 2008 kulminovala masivní kampaň, obsahující prvky phishingu, zaměřená na klienty České spořitelny a. s.

Nevyžádaná pošta (spam)

Nevyžádané, v prostředí elektronické pošty masově šířené sdělení. Jako každá elektronická zpráva, i spam v sobě může nést, a často také nese, další hrozby (crimeware, spyware atd.). Častým jevem je například nevyžádaná instalace poštovního klientu, který spam (a mnohdy nejenom jej) rozešle na všechny adresy elektronické pošty, které nalezne v počítači nebo i v celém konkrétním informačním systému. Konkrétní uživatel či organizace se tak stávají nedobrovolnými rozesílateli spamu, který, vzhledem k tomu, že přichází z pohledu dalších adresátů z důvěryhodných zdrojů, nemusí být odfiltrován jejich antispamovými prostředky. (19)

Spam obsahující kriminální či jiný podvodný obsah je označován jako **scam** (z anglického „scam“ – podvod, švindl). Scamy tvoří v současnosti podstatnou část spamu a jejich účelem je, typicky za použití sociálního inženýrství získat důvěru uživatele a donutit ho vykonat požadované úkony (např. otevření přílohy e-mailu, navštívení zobrazeného URL aj.). Mezi scam je možné zařadit i phishing, malware,

419, hoax, podvodné loterie a nabídky, dárcovský scam, Cold-call Scam, Facebookový like scam aj. (7 str. 235)

Poměrně nově jsou scamy oblíbené také u mobilních aplikací, kde mohou sázet na nepozornost uživatele. S využitím několika vyskakovacích oken, kde např. dvě z nich slouží pro výběr funkcí aplikace, ale třetí, stejně designované okno ale s jiným obsahem již slouží k potvrzení platby za službu, o které se předpokládalo, že je bezplatná. (22)

Malware (škodlivý software)
Souhrnný pojem pro jakýkoli software, který při svém spuštění zahájí činnost ke škodě systému, ve kterém se nachází. Jeho vnější projevy mohou reagovat na konkrétní naprogramovanou spouštěcí událost (např. na okamžik, kdy oprávněný uživatel otevře zprávu v rámci elektronické pošty). Může se jednat například o:

- **Infoware** muže být specifikován jako aplikace pro informatickou podporu klasických bojových akcí, respektive jako soubor aktivit, které slouží k ochraně, vytěžení, poškození, potlačení nebo zničení informací nebo informačních zdrojů, s cílem dosáhnout významné výhody v boji nebo vítězství nad konkrétním protivníkem. Pojem infoware nelze zaměňovat s termínem infowar, tj. informační válka.

- **Spyware** (špionážní software) jsou programy, skrytě monitorující chování oprávněného uživatele počítače nebo systému. Svá zjištění tyto programy průběžně (např. při každém spuštění) zasílají subjektu, který program vytvořil, respektive distribuoval. Takové programy jsou často na cílový počítač nainstalovány spolu s jiným programem (utilita, počítacová hra), s jehož funkcí však nesouvisí.

- **Vir** (virus) je podmnožina malware. Parazitující soubor, který se připojí k určitým programům nebo systémovým oblastem, které pozmění. Může se nekontrolovatelně rozšiřovat, nebo po svém spuštění zahájit destrukční

proceduru (poškození, změnu či zničení dat, degradaci funkce operačního systému, stahování dalšího malware atd.). Existují viry, které mohou zároveň plnit funkci trojského koně a (nebo) vytvářet tzv. „zadní vrátka“ do napadeného systému. Počátek šíření počítačového viru může být distribuován v prostoru ohnisek vytvořených na již kompromitovaných (zavirovaných) počítacích, což nesmírně urychluje celý proces šíření infekce.

- **Červ** (worm) je podmnožina malware. Autonomní program, schopný vytvářet své kopie, které rozesílá do dalších počítačových systému (sítí), kde vyvíjí další činnost, pro kterou byl naprogramován. Často slouží ke hledání bezpečnostních skulin v systémech nebo v poštovních programech.

- **Trojské koně, keyloggery** jsou podmnožinou malware. Programy, implantované do systému bez vědomí oprávněného uživatele, monitorující specifické činnosti, o které projevuje útočník zájem. Zaznamenávají např. znaky které oprávněný uživatel stiskl na klávesnici (zejm. hesla) nebo stránky, které navštívil. Tyto údaje předávají útočníku k dalšímu zpracování. Ten tak může získat přístupové informace k webovým stránkám, bankovním účtům nebo kontům elektronické pošty. Může se jednat i o textový editor, který zároveň ukládá text, který byl jeho prostřednictvím napsán, do skryté části systému, odkud může být vyzdvižen autorem trojského koně. Trojské koně často instaluje nevědomky sám oprávněný uživatel, když instaluje z internetu nebo zdarma distribuovaných CD jiné programy, se kterými jsou však tyto trojské koně spojeny (např. hry či servisní programy – utility).

- **Přesměrovávače** (re-dial, „pharming crimeware“) jsou podmnožinou malware. Programy, jejichž úkolem je přesměrovat uživatele na určité stránky namísto těch, které původně hodlal navštívit. Na takových stránkách dochází k instalaci dalšího crimeware (viru), nebo touto cestou dojde ke značnému zvýšení poplatku za připojení k internetu (prostřednictvím telefonních linek se zvýšeným tarifem).

- **Logické bomby** (logical bombs) jsou podmnožinou malware. Programy, které se tajně vkládají do aplikací nebo operačního systému, kde za předem určených podmínek provádějí destruktivní aktivity. Předem specifikovanou podmínkou startující logickou bombu může být například konkrétní datum (výročí určité události – viz např. „Virus 17. listopad“). (19)

3.4 Nejčastější chyby

Níže jsou uvedeny nejčastější chyby, která podle odborných zdrojů ohrožují bezpečnost ICT a nezřídka vedou ke vzniku bezpečnostních incidentů.

Špatně nastavená/zvolená přístupová hesla

Uživatelé často používají slabá a lehce uhodnutelná hesla. Heslo by mělo být rozumně složité a unikátní. Pro každé přístupové místo bychom měli mít jiné heslo, což je mnohdy také ignorováno ze strany uživatelů. Heslo by se mělo volit snadno zapamatovatelné, ale neuhodnutelné pomocí tzv. slovníkového útoku. Nicméně v dnešní době bohužel není rizikem jen nevhodně volená forma hesel, ale přicházejí také rizika z druhé strany. Záleží zároveň na způsobu, jakým je s hesly zacházeno zpracovateli těchto dat, kteří je mají k dispozici (tj. například jakým způsobem je ukládají do databází, zda mají k údajům přístup jen oprávněné osoby apod.)

Absence antivirů a bezpečnostních programů

Absence pravidelně aktualizovaného antivirového a bezpečnostních programů je dalším častým problémem firem i jednotlivců. Ti zpravidla neaktualizují software pravidelně, případně nemají nastavenou vhodnou konfiguraci.

Podcenění zálohování

Uživatele lze rozdělit do dvou skupin – na uživatele, kteří již přišli o svá data a na ty, kteří o svá data zatím nepřišli. Data lze zálohovat manuálně, případně automaticky. Zálohování chrání před ztrátou dat při poruše hardwaru, nechtěném smazání, ale

i v případě kybernetického útoku. Jsou stále oblíbenější útoky pomocí takzvaného ransomware, který může firmě znepřístupnit data a způsobit jí tak velké finanční ztráty. Podcenění zálohování tedy může ohrozit dokonce i samotnou její existenci.

Podcenění školení zaměstnanců

Bezpečnostní problémy vznikají nejčastěji po chybách uživatelů. Ve společnosti by se měla provádět pravidelná školení s cílem seznámit zaměstnance se základními bezpečnostními prvky, které se využívající ve společnosti. Zaměstnanci by měli být varování, aby ignorovali veškeré emaily, webové stránky a soubory od neznámých odesílatelů, jedná se o nejčastější způsob infiltrace podnikové sítě počítačovým virem či jiným škodlivým software.

Zanedbání aktualizace software

Veškerý software by měl být pravidelně aktualizován. Uživatelé si zpravidla vystačí s jednou verzí programu, kterou aktualizují pouze při aktualizaci jednotlivých funkcí a takto používaný software může být starý i několik let. Bezpečnostní záplaty uživatele zpravidla nenutí software aktualizovat, čehož využívají útočníci. Absence aktualizací může znamenat vysoké riziko už jen z toho důvodu, že poskytovatelé daného software v průběhu času nástroj zdokonalují, včetně odstraňování chyb (tzv. „bugů“), které mohou způsobit bezpečnostní incident a napadnutelnost systému.

Špatná bezpečnostní politika

Bezpečnost v organizaci je tak silná, jako její nejslabší článek. Při tvorbě bezpečnostní politiky je třeba dbát na bezpečnost jako celek, nikoliv zabezpečovat pouze jednotlivá místa. Zároveň i jednotlivci se potýkají s hrozbami a měli by dodržovat základní bezpečnostní doporučení (nezanechávat přístroje s otevřeným přihlášením, nesdělovat svá přístupová hesla, nepřihlašovat se do služeb prostřednictvím nedůvěryhodných webových stránek, zálohovat své údaje na bezpečném úložišti apod.).

Nezabezpečený přístup do firemní sítě – pro přístup do podnikové sítě z míst mimo tuto síť by měla být komunikace vždy zabezpečena. V opačném případě by mohl

útočník odposlechnout komunikaci zasílanou skrz nezabezpečený kanál a získat přístup k datům, která mohou být klíčová pro danou společnost.
(23) (24) (25)

3.5 Technologie

Z pohledu bezpečnosti zpracovávaných informací plyne nutnost řešit na úrovni technologií zejména následující požadavky:

- Autentičnost, dostupnost a integritu zpracovávaných informací v podnikovém informačním systému (zajištění oprávněného přístupu, problematika neodmítnutelnosti činností uživatelů systému, zabezpečené uložení).
- Základní nástroje a metody správy systému ochrany informací.
- Systém autentizace – např. elektronický podpis a jeho využití, PKI, certifikační autority.
- Kryptografické prostředky.
- Právní aspekty, normotvorné a legislativní úpravy.

Ale z pohledu zajištění systému bezpečnosti informací je třeba řešit technologické komponenty ve shodě s navrhovanými bezpečnostními procesy a s možnostmi a schopnostmi lidí (uživatelů i odborného personálu). (6 str. 18)

Níže jsou uvedeny vybrané technologie, které úzce souvisí s oblastí ochrany dat.

Hypertext Transfer Protocol (Secure) – HTTP(S)
HyperText Transfer Protocol slouží pro přenos HTML souborů. Samotné HTML stránky jsou tvořeny většinou texty a nějakou grafikou, není tedy nějaký zvláštní důvod k jejich ochraně. Vzhledem k rozšířenosti klientů pro prohlížení HTML souborů (složité označení pro internetový prohlížeč) se této platformy využívá k řadě citlivých aplikací.

Jako příklad může posloužit přístup k e-mailové schránce přes webové rozhraní, webová podoba firemního informačního systému nebo dokonce aplikace

internetového bankovnictví. V takových případech je samozřejmě velmi žádoucí, aby byl přenos dat protokolem HTTP vhodným způsobem zabezpečen. V základní podobě jsou data přenášena v otevřené podobě, všechna hesla a uživatelská jména jsou tedy snadno odposlechnutelná.

K zabezpečení přístupu na webové stránky se používá speciální vrstva – protokol SSL. Takto zabezpečený web je označován jako HTTPS, prohlížeče signalizují zabezpečené stránky například symbolem zámku ve stavovém řádku. (16 str. 108)

SSL/TLS

SSL (Secure Socket Layer) je speciální vrstva, která byla pro potřeby šifrování vložena mezi transportní a aplikační vrstvu protokolové sady TCP/IP. Vložená vrstva obsahuje prostředky, které umožňují šifrovat a dešifrovat zprávy, manipulovat s digitálními certifikáty a výtahy zpráv. Její služby využívají zvolené aplikační protokoly, tj. třeba http, ftp, nntp apod., přičemž takové protokoly se pak označují shodným jménem doplněným písmenem „s“, tedy https, ftps, nntps apod. (26 str. 390)

SSL a TLS jsou generické termíny pro sadu odvětvových standardů umožňujících aplikacím vytvářet zabezpečené komunikační relace v nechráněné síti, jako např. v síti Internet. Protokol SSL se vyvinul a byl nahrazen protokolem TLS. Protokol TLS je přesnější termín, zde se však používá termín protokol SSL/TLS, aby se udrželo spojení s termínem protokol SSL, který zůstává vestavěný v existujících aplikačních rozhraních, dokumentaci a konfiguraci.

Verze specifikace protokolu SSL nebo TLS identifikuje relativní úroveň poskytovaného zabezpečení. Neexistují žádné verze specifikace protokolu SSL, které by se měly v současnosti používat. Pouze jedna verze protokolu TLS je povolena za účelem zajištění kompatibility zabezpečení v některých odvětvích. (27)

Firewall

Firewall je sada opatření (hardwarových, softwarových či personálních), která mají za cíl propojit dvě nebo více sítí s různou úrovní důvěryhodnosti tak, že sníží (předem definovaná) rizika, vyplývající pro chráněné sítě z tohoto propojení.

Technologie používané při tvorbě firewallu můžeme rozdělit do několika skupin. Jako vše, ani firewally nejsou čistě teoretická záležitost, reálný firewall tedy různě kombinuje několik popsaných technik. Nutno přitom poznamenat, že firewall může být jak softwarových program běžící na vyhrazeném počítač, tak hardwarové zařízení, zapojené mezi chráněnou sítí a internetem. Základní technologie jsou tři:

- jednoduchý IP filtr,
- stavový IP filtr,
- proxy.

(16 stránky 116, 117)

Proxy

Jedná se o program určený pro jeden konkrétní protokol, který filtruje pakety podle toho, která aplikace a na kterém portu s nimi pracuje. V praxi tak může mít jeden program přístup například k portu 110 (POP3 – stahování pošty), zatímco pro všechny ostatní programy je tento pot tabu. (16 str. 118)

3.6 Nástroje

Řešení bezpečnosti musí zahrnout všechny možné přístupy ke zpracovávaným informacím, a to jak z interního prostředí, tak i z vnějších sítí. Součástí bezpečnostního perimetru je celá řada bezpečnostních nástrojů, které zajišťují bezpečný přístup k informacím.

Ověřování (autentizace)

Autentizace je proces, který určuje osobu uživatele, jaké má oprávnění k přístupu k aplikacím, do informačního systému aj. Pro kontrolu a audit autentizačních procesů jsou v informačních systémech implementovány systémy řízení oprávněného přístupu (např. Active Directory v prostředí MS Windows). (6 str. 25)

Ověřování (autentizace) koncového bodu je proces, kdy jeden subjekt prokazuje totožnost jinému subjektu přes počítačovou síť. Například uživatel prokazuje svou identitu e-mailovému serveru. (11 str. 538)

Vícefaktorová autentizace

Odborníci v oblasti bezpečnosti odkazují na nezbytnost minimálního použití dvou forem ověřování, tj. dvoufaktorové autentizace. Dvoufaktorová autentizace je doporučena pro řízení přístupu již ke standardním informačním systémům nebo pro vzdálený přístup k těmto systémům, neboť tímto způsobem je eliminována zranitelnost informačních systémů v případech využívání autentizace typu „jméno, heslo“.

Tradiční faktory ověřování je možné rozdělit následovně:

- něco, co oprávněný uživatel zná, například heslo;
- něco, co oprávněný uživatel má, například symbol;
- něco, čím oprávněný uživatel je, například biometrické charakteristiky;
- kde se oprávněný uživatel nachází, například pomocí globálních satelitů pro určování polohy.

Klientská softwarová řešení mohou též využívat dalších nástrojů, jako jsou „tokeny" nebo "certifikáty", které jednoznačně identifikují jak vlastníka příslušné pracovní stanice (např. osobního počítače), tak i samotné fyzické zařízení. Toto SW řešení umožňuje řešit úskalí vzdáleného přístupu, kdy je ověřeno, že daný oprávněný uživatel přistupuje do systému z fyzického zařízení, které je deklarováno a je tak možné kontrolovat oprávnění k vzdálenému přístupu k systému i v rozsáhlých sítích. V každém případě by organizace a podniky měly využívat dvoufaktorovou autentizaci pro přístup do systému, protože jednoduché uživatelské ID a hesla neposkytují dostatečnou záruku, že nedošlo k přístupu neoprávněných osob, zejména při nedostatečné správě hesel. (6 str. 26)

Autorizace

Funkce autorizace umožňuje správcům systému omezit některé speciální oprávnění na určité role nebo funkce, které zaměstnanci vykonávají v rámci organizace. S využitím autorizace je tak řešeno strukturování oprávnění jednotlivých uživatelů informačního systému.

Příkladem jsou systémy s jednotlivými aplikacemi, ve kterých jsou odděleny typy povinností a pravomocí dle dané role jednotlivých uživatelů. Modelově se může jednat o personál, který má přístup k citlivým informacím (jako je například mzda).

Správa účtů slouží jak k auditu, a tak i kontrole využití zdrojů. Z pohledu auditu je důležité mít dobré znalosti o tom, kdo přistupuje k různým zdrojům v rámci podniku a mít přehled o činnosti uživatelů. Tento přístup spadá do „dobré praxe“, vyžadované při revizi protokolů kritických systémů (nejenom), aby bylo zajištěno, že k nim mají přístup pouze oprávnění uživatelé.
Správa účtů je těsně spojena s autorizací, kdy základem je pravidelná kontrola uživatelů, kteří mají přístup do vyhrazených oblastí, jako je datové centrum podniku apod. Navíc je nutnou podmínkou při vytváření prostředí, kde lze zajistit dohledání záznamů o činnostech s příslušnými informacemi (daty, elektronickými dokumenty) v celém jejich životním cyklu. (6 stránky 27, 28)

Kryptologie

Vědecká disciplína, věnující se ochraně dat před neoprávněným čtením se jmenuje kryptologie. Rozděluje se na dvě části:

- Kryptografie – věnuje se kódování a šifrování dat.
- Kryptoanalýza – má za hlavní náplň analýzu algoritmů a zašifrovaných dat. (16 str. 4)

Kryptografie

Kryptografické techniky umožňují odesílateli maskovat data, takže útočník nemůže ze zachycených dat získat informace. Příjemce musí být ovšem schopen obnovit původní data z maskovaných dat.

Stojí za zmínku, že u mnoha moderních kryptografických systémů, včetně těch, které se používají na internetu, jsou samotné šifrovací techniky známé (publikované a standardizované) a jsou k dispozici všem (například RFC 1321; RFC 3447; RFC 2420; NIST 2001), a to i potencionálním útočníkům. Je zřejmé, že pokud každý zná způsob kódování dat, pak musí existovat nějaká tajná informace, která útočníkovi zabraňuje dešifrovat přenášená data. A pro tento účel existují klíče. (11 str. 520)

Šifrování

Příkladem je situace, kdy osoba č. 1 poskytuje jako vstup do šifrovacího algoritmu řetězec čísel nebo znaků, který se označuje jako klíč K. Šifrovací algoritmus převezme klíč a zprávu v holém textu m jako vstup a vytvoří šifrovaný text jako výstup. Zápis Ka(m) vyjadřuje šifrovaný text (šifrovaný pomocí klíče K) z prostého textu zprávy m. Aktuální šifrovací algoritmus, který používá klíč K bude zřejmý z kontextu. Podobně platí, že osoba č. 2 poskytne klíč Kb dešifrovacímu algoritmu, který převezme šifrovaný text a její klíč jako vstup a vytvoří původní prostý text jako výstup. To znamená, že když osoba č. 2 obdrží šifrovanou zprávu Ka(m), dešifruje ji pomocí výpočtu Kb(Ka(m)) = m. V systémech symetrických klíčů jsou klíče obou osob identické a tajné. V systémech veřejných klíčů se používá dvojice klíčů. Jeden z klíčů zná jak osoba č. 1, tak osoba č. 2 (ve skutečnosti jej zná celý svět). Druhý klíč zná pouze buď osoba č. 1, nebo osoba č. 2 (ale ne oba účastníci komunikace). (11 str. 521)

Šifrovací algoritmus

Algoritmus, který se snaží utajit data jejich zašifrováním. K této činnosti používá nějaké tajemství, to je většinou nazýváno šifrovacím klíčem. Více lidí tak může používat jeden šifrovací algoritmus, každý ovšem musí mít k šifrování i dešifrování dat jiný klíč. (16 str. 23)

Blokové šifry

V současné době existuje celá řada populárních blokových šifer, včetně DES (zkratka za Data Encryption Standard), 3DES a AES (zkratka za Advanced Encryption Standard). Každý z těchto algoritmů používá řetězec bitů jako klíč. Například DES používá 64bitové bloky s 56bitovým klíčem. AES používá 128 bitové bloky a může pracovat s klíči o délce až 128, 192 a 256 bitů. Klíč algoritmu určuje specifickou „minitabulku“ mapování a permutací v rámci vnitřní struktury algoritmu. Případný útok „hrubou silou“ na každou z těchto šifer by musel procházet všechny klíče a na každý klíč použít dešifrovací algoritmus. (11 str. 524)

Kódovací algoritmus

Algoritmus se stejnou funkcí – snaží se chránit data před neoprávněným přečtením. Do procesu ale nevstupuje žádné tajemství, o utajení se stará vlastní algoritmus. Je samozřejmé, že pokud bude stejný algoritmus sdílet více lidí, budou si moci navzájem prohlížet chráněná data. Do této skupiny spadají například cizí jazyky – text přeložený do esperanta je srozumitelný jen lidem, kteří tímto jazykem hovoří. Zařadit sem můžeme i různé kódové knihy – obě komunikující strany vlastní slovník slov a jejich překladu do kódu. (16 str. 24)

Kryptografické hašovací funkce

Hašovací funkce má vstup m a vypočítává řetězec H s pevnou velikostí (m), známý jako hash. Tuto definici splňuje internetový kontrolní součet. K získání následující další vlastnosti je nezbytná kryptografická hašovací funkce:
Je výpočetně nemožné najít nějaké dvě různé zprávy x a y takové, že H(x) = H(y)

Jinými slovy tato vlastnost znamená, že pro útočníka je výpočetně nemožné nahradit zprávu chráněnou hašovací funkcí jinou zprávou. Tudíž pokud (m, H(m)) jsou zpráva a hash zprávy vytvořené odesílatelem, pak útočník nemůže padělat obsah jiné zprávy y, který má stejnou hodnotu hash jako původní zpráva. (11 str. 531)

MD5 a SHA algoritmy

U MD5 byly nalezeny chyby v návrhu, které snižují jeho bezpečnost, takže mnozí tvůrci přechází na SHA algoritmy. Je vhodné podotknout, že SHA1 byl rovněž označen za slabší a doporučeno je používat algoritmy SHA2 (SHA256, SHA512 atd.). Útočníky zvýhodňuje také skutečnost, že MD5, SHA1, SHA2 a podobné algoritmy jsou určené pro rychlý výpočet hashe u velkých vstupních souborů. U MD5 dokáže poměrně běžný server počítat hashe rychlostí větší než 300 MB za sekundu. To znamená, že např. kombinace malých písmen a číslic o délce 6 znaků může ověřit za zhruba 40 sekund. (28)

Je dobré zmínit, co je označováno za nevhodný algoritmus. Jsou to všechny MD5, SHA-1, SHA-2, SHA-3, a to v jakékoliv variantě. Je bezpředmětné, zda s použitím saltu („solí“), nebo bez něj, zda jsou „zesílené“ pomocí několika stovek tisíc iterací, nebo má funkce jen jedno volání. Na ukládání hesel by se měla použít některá z těchto funkcí: Argon2 (varianta Argon2id nebo Argon2i), bcrypt, scrypt, nebo PBKDF2. Ty jsou relativně pomalé, takže pro útočníky na hesla je časově i finančně náročné je odkrýt. (29)

Hash

Mnohem lepší variantou je ukládání hesla v podobě hashe – „otisku“, který je výsledkem speciální matematické funkce. Obecně tyto funkce pracují tak, že berou vstupní data a k nim vrací řetězec, který má některé specifické vlastnosti: 1. pro stejná vstupní data je stejný, 2. má konstantní délku, 3. drobná změna vstupních dat vyvolá velkou změnu ve výsledku, 4. je prakticky nemožné nalézt různá vstupní data se stejným hashem a 5. z výsledného řetězce je v praxi nemožné rekonstruovat původní text. (28)

Sůl (salt)

Čím delší heslo, tím víc času je zapotřebí na výpočet hashů možných kombinací. Tabulku pro čtyřznaková hesla je možné spočítat během pár sekund, pro pětiznaková už to bude pár minut, a časová náročnost roste s délkou hesla. Ideální možností by bylo donutit uživatele, aby používali alespoň patnáctiznaková hesla se speciálními znaky,

ale takový systém by jen těžko uspěl. Proto se sahá k metodě solení (salt), kdy ke „standardně dlouhým“ heslům na serveru je přidán dlouhý řetězec. Hash je pak počítán např. pro 40 znaků – a pro tak dlouhé řetězce je vytváření rainbow tables ze všech možných kombinací téměř nemožné. (28)

Variabilní sůl

Namísto konstantního dlouhého řetězce se používá konstantní dlouhý řetězec a k němu ještě náhodná kombinace znaků. Tu je možné uložit pro každého uživatele do databáze v otevřeném textu. Nezáleží na tom, že útočník bude tuhle náhodnou část znát; jde o to, že by musel pro každého uživatele budovat znovu vlastní sadu tabulek, což by bylo časově velmi náročné. (28)

Algoritmus Bcrypt

Bcrypt kromě hesla a salt řetězce pracuje ještě s parametrem „cost“, kterým lze ovlivnit náročnost výpočtu hashe. Tím je možné nastavit algoritmus tak, že výpočet hashe bude trvat třeba sekundu – u přihlášení uživatele ani při registraci to nepředstavuje větší problém, ovšem pro výpočet „rainbow tables“ je třeba tisícinásobně pomalejší algoritmus výrazným faktorem. Počítat tabulky týden je únosné, ovšem počítat je devatenáct let již většinu útočníků téměř jistě odradí. (28)

PBKDF2

Jedná se o kryptografickou funkci, která generuje klíč o požadované délce z hesla zadaného uživatelem a soli libovolné délky, a to opakovaným voláním pseudonáhodné funkce. Jejím výstupem je hash o určité délce. Vzhledem k tomu, že hesla zadávaná uživateli jsou zpravidla slabá, doporučuje se používat sůl o minimální délce 128 bitů a provádět alespoň 1000 iterací. Je ale možné provádět i 10.000 nebo 100.000 iterací, vše záleží jen na výkonnosti hardware. (30)

Scrypt

Scrypt je funkcí, která kromě počtu iterací používá i konfigurovatelné množství paměti, což představuje omezení pro útočníka snažícího se paralelně prolomit více hesel najednou. (31)

Logování

Logování označuje činnost, při níž systém vytváří logy. Jedná se o sběr událostí, kdy log shromažďuje data za účelem jejich analýzy. Příkladem může být server access log, v němž webový server uchovává informace o přijatých požadavcích ze strany klienta. Sledování logů je jedním z účinných nástrojů pro detekci podezřelých událostí na serveru a umožňuje předejít některým hrozbám. Servery jsou stále častěji předmětem útoku „botů“, kteří hledají slabá místa a většinou se pokoušejí hádat oblíbené kombinace jméno / heslo. Protože četnost pokusů bývá vysoká vzhledem ke strojovému zkoušení, logy tyto činnosti zaznamenají a jsou snadno pozorovatelné. Vhodné je následně využít některý z nástrojů, který pročítá autentizační log a hledá v něm neúspěšné pokusy o přihlášení. Podle nastavených metrik pak pomocí IP tabulek může blokovat přístupy z příslušné IP adresy na stanovenou dobu. Výhodou je, že takové blokování proběhne už na síťové úrovni a agresivní „boti“ přestanou server zatěžovat. (32) (33)

Etický hacking

Je činnost vykonávaná takzvanými bílými klobouky (White hats). To jsou hackeři, kteří uskutečňují své průniky do systému za využití bezpečnostních slabin za účelem odhalení nedostatků a vytvoření mechanismu a bariér, které by tyto útoky měly znemožnit. Jsou často zaměstnanci či externími spolupracovníky renomovaných společností podnikajících v oblasti informačních technologií. Ti průnikem do systému nezpůsobují uživatelům škodu, ale naopak upozorňují na bezpečnostní chyby. (7)

Kritické myšlení

Nekritický přístup k informacím, které "počítač napíše" je velice nebezpečný, protože uživatel může být velmi snadno podveden. Dá se říci, že je na tomto principu založen dnes také trend v narušování bezpečnosti IT – phishing. Přestože se o této hrozbě mluví stále častěji, je mezi uživateli počítačů spousta lidí, kteří si myslí, že to, co uvidí v televizi, uslyší v rádiu, přečtou v novinách a najdou na Google, musí být zaručeně pravda.

Žádné antispamy, proxy servery, firewally a další sofistikované technologie nenahradí zdravý rozum. Navíc je potřeba počítat s tím, že z principu jsou podvodníci před výrobci ochranných technologií vždy o krok napřed, takže zdravý rozum je jedinou možností, jak zabránit bezpečnostnímu incidentu. Proto by se novým trendem měla stát široká osvěta v oblasti IT bezpečnosti. (34 str. 138)

Certifikační autorita

Spojení veřejného klíče s určitým subjektem obvykle provádí certifikační autorita (CA), jejímž úkolem je ověřovat totožnost a vydávat certifikáty. CA má následující úkoly:

- CA ověřuje, zda subjekt (člověk, router atd.) je ten, kdo říká, že je. Neexistují žádné nařízené postupy, jak provádět certifikaci. Při jednání s certifikační autoritou je třeba věřit, že CA vykonává přísné ověřování identity. Pokud například útočník mohl zajít do pochybné CA a jednoduše oznámit „Já jsem osoba A“ a získat certifikáty spojené s identitou osoby A, pak by veřejným klíčům certifikovaným pochybnou CA nikdo příliš nedůvěřoval. Na druhé straně, někdo může (nebo také nemusí) být ochotnější důvěřovat certifikační autoritě, která je součástí federálního nebo státního programu. Identitě spojené s veřejným klíčem je možné věřit jen do té míry, do jaké je možné důvěřovat certifikační autoritě a jejím technikám ověřování identity.

- Jakmile CA ověří identitu subjektu, vytvoří certifikát, který spojuje veřejný klíč subjektu s jeho identitou. Certifikát obsahuje veřejný klíč a globálně jedinečné identifikační údaje o vlastníkovi veřejného klíče (například lidské jméno nebo IP adresu). Certifikát je digitálně podepsán certifikační identitou. (11 str. 537)

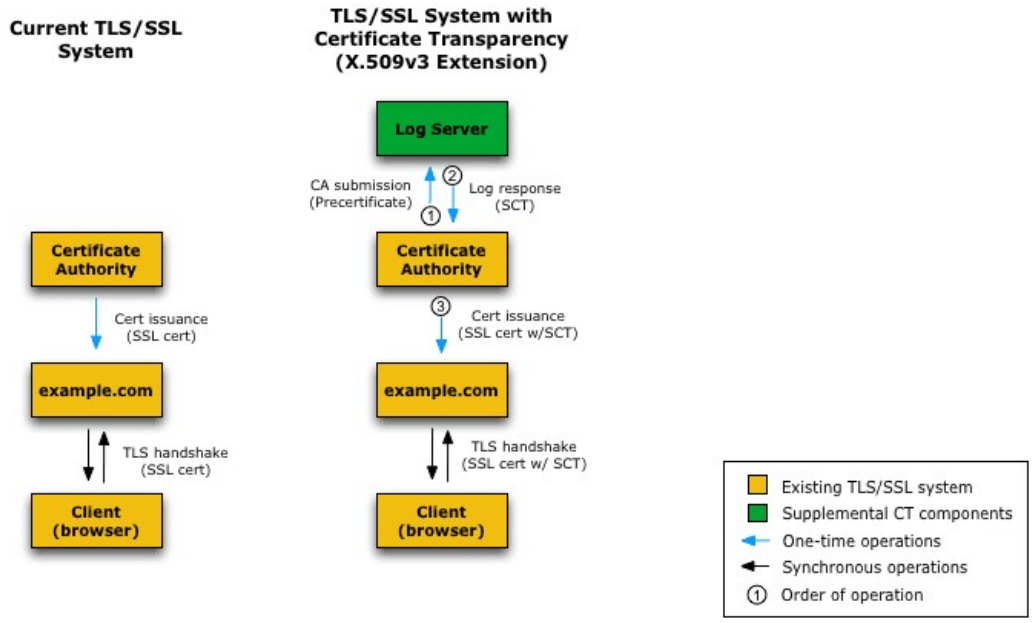
Certificate Transparency

Certificate Transparency je popsán v RFC 6962 a jedná se o veřejné logy, do kterých může kdokoliv přidávat certifikáty vydané uznávanými autoritami. Jednotlivé záznamy jsou ukládány v Merklově hashovém stromu, takže není možné je nepozorovaně měnit či odstraňovat.

Logy dnes provozuje desítka organizací a další přibývají. Je možné v nich vyhledávat pomocí různých nástrojů, například na webu crt.sh. Princip spočívá v tom, že sledovat obsah logů může kdokoliv, v první řadě by to ale měli dělat majitelé domén, kteří chtějí ohlídat, že žádná autorita nevystavila neoprávněně certifikát na jejich doménová jména.
Neexistuje totiž úplně pevná vazba mezi doménou a autoritou, tudíž teoreticky může na jakoukoliv doménu vystavit platný certifikát libovolná autorita. (35)

Na obrázku níže je popsán rozdíl mezi běžným fungováním certifikátů a zavedením Certificate Transparency.

Obrázek 1 Princip Certificate Transparency



Zdroj: http://www.certificate-transparency.org/how-ct-works

3.7 Hodnocení rizik v oblasti ochrany dat

Firmy si uvědomují možné závažné problémy, které by mohly mít, pokud by si svá digitální aktiva dostatečně nechránily. Počítají s významnými investicemi do bezpečnostních řešení i kvalifikovaných specialistů. Tlak na vedení společností směrem k uvolnění zdrojů pro řízení IT bezpečnosti navíc umocňují zprávy o ztrátě dat způsobených zaměstnanci nebo zranitelností webové aplikace. (36)
Řada společností volí jako jednu z metod zkoumání oblasti ICT a hodnocení bezpečnostních rizik dotazníkové šetření. (37) (38) (39)

Dotazníkový průzkum
Dotazníkové šetření je účinným nástrojem, jak analyzovat skutečnosti, které se nedají, či dají velmi obtížně, kvantifikovat jiným způsobem. Zjišťování a vyhodnocování názorů obyvatelstva je podkladem pro rozhodování v mnoha oblastech. Je také jedním z vhodných nástrojů pro mapování hledisek informační bezpečnosti a zjištění, jak k ní obyvatelé přistupují. Proto je tato metoda zvolena návazně také v praktické části práce.

Aby byly informace, plynoucí z takového šetření hodnotné, neobejde se bez řádné přípravy.
Jednotlivé fáze lze popsat takto:

- Vytvoření projektu výzkumu
- Definování jednotek, stanovení nutného rozsahu výběru a způsobu výběru
- Vlastní rozpracování dotazníku
- Ověření dotazníku, provedení pilotního průzkumu
- Vlastní shromažďování materiálu
- Analýza získaného materiálu a jeho zobecnění

Pro vhodné stanovení rozsahu výběru je možné využít slepý odhad, který si ale většinou může dovolit jen expert, v závislosti na svých odborných zkušenostech. V opačném případě může dojít k výraznému znehodnocení výzkumu. Obecně je vhodnější zvolit statistický přístup, kdy se velikost reprezentativního vzorku

vypočítá stanoveným vzorcem, s ohledem na požadovanou míru přesnosti a spolehlivosti.

Vzorec:

$$n = \frac{u_\alpha^2 \cdot p \cdot q}{\Delta^2}$$

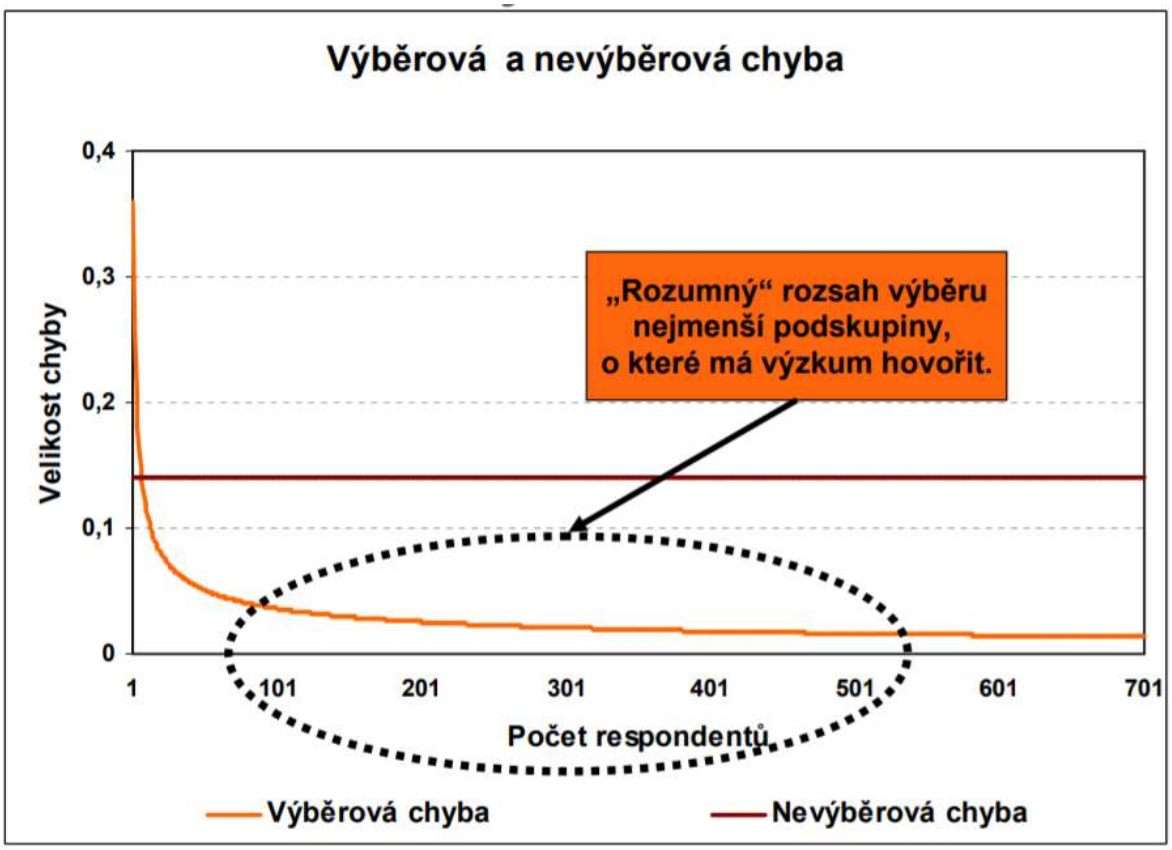
α = hladina významnosti (obvykle volíme 0,05 či 0,01)
uα = tabelovaná hodnota normovaného normálního rozdělení
p = podíl počtu respondentů přiklánějící se k jedné variantě
q = podíl počtu respondentů přiklánějící se k jiné variantě
Obvykle tyto počty dopředu neznáme a v takovém případě volíme p = q = 0,5
Δ = námi stanovená maximální přípustná chyba (podíl)
(40 str. 29)

V některých zdrojích se uvádí jako dostatečný počet respondentů pro celorepublikové šetření počet nad 1000 respondentů. (41) (42) (43)

Také Český statistický úřad při některých šetřeních využívá vzorek o takovémto rozsahu a některé zdroje uvádí, že přestože je důležité, mít reprezentativní vzorek, ne vždy je nutné (a reálné), dosáhnout enormního počtu respondentů, např. nad 5000. (44)

U malého výběrového vzorku se badatel potýká s vysokou výběrovou chybou, ale zároveň pokud se počet respondentů výrazně zvýší, pak s každým dalším navýšením již velikost výběrové chyby naopak roste pomaleji. Nicméně náklady na výzkum v takovém případě rostou lineárně. Proto je vhodné u výzkumů středního rozsahu zvolit kompromis. Také je nutné vzít v úvahu nevýběrovou chybu, která může být způsobena např. špatnou stylizací otázek a jejich rozdílnou interpretací. (42) (45)

Obrázek 2 Dotazníkové šetření – výběrová a nevýběrová chyba



Zdroj: https://slideplayer.cz/slide/2450885/8/images/21/Herzmann%3A+Marketing+Trend+2007.jpg

Před samotnou realizací je nutné, aby byl dotazník koncipován správným způsobem. Je nutné vhodně zvolit otázky, které mohou mít různou formu. V této práci budou použity otázky uzavřené, na které jsou pevně dané odpovědi a získané výsledky jsou následně snadno zpracovatelné. V šetření se objeví také otázky identifikační, které napomohou blíže určit skupiny respondentů.

Po vytvoření dotazníku je vhodné provést pilotní průzkum na menším vzorku pro ověření, že jsou otázky a odpovědi logicky a srozumitelně formulované. Také to poskytne informaci, zda vůbec se zvolená problematika hodí pro tento typ výzkumu a zda respondenti budou ochotni na dané téma odpovídat. Tím je zaručena vypovídací schopnost a kvalita provedeného šetření. Respondenti by také před započetím měli být informování, k jakému účelu dotazník slouží a jakým způsobem budou data

zpracována. Výsledky provedeného šetření je vhodné vyjádřit v relativních a zároveň i absolutních četnostech, aby měly co největší vypovídací hodnotu a byly dobře srozumitelné. (40 stránky 30, 31)

3.8 Právní aspekty ICT

Níže je uveden pouze výčet základních bezpečnostních předpisů a norem, které je nutné považovat za významnou pomůcku při návrhu, realizaci a provozu systémů řízení bezpečnosti ICT/IS, resp. jednotlivých bezpečnostních opatření nasazených do informačních systémů:

- Nařízení Evropského parlamentu a Rady (EU) 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 (eIDAS)
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů (General Data Protection Regulation – GDPR) – vstupuje v účinnost 25. 5. 2018
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
- Zákon č. 40/2009 Sb., trestní zákoník
  (6 stránky 12, 13)

S další právní úpravou, která ovládá odvětví ICT, je možné se setkat na úrovni Evropské unie ve směrnici e-Commerce 2000/31/ES, která má přispět úpravě některých právních aspektů služeb informační společnosti, zejména elektronického obchodu, na jednotném vnitřním trhu. Na směrnici reagoval český zákonodárce

přijetím zákona č. 480/2004 Sb., o některých službách informační společnosti, (dále též jen „ZSIS“), který upravuje například otázky spamu, jevů, které často vídáme v nabídkách, jako je políčko pro jednoduché odhlášení apod. (46)

V dalším textu budou uvedeny podrobnosti k vybraným zásadním skutečnostem, vyplývajícím z právních úprav dané problematiky.

Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation, GDPR)

Nařízení je v celé EU jednotně účinné od 25. května 2018. V Česku nahrazuje právní úpravu ochrany osobních údajů v podobě směrnice 95/46/ES a související zákon č. 101/2000 Sb., o ochraně osobních údajů. Práva a povinnosti v původním zákoně o ochraně osobních údajů budou nahrazena právy a povinnostmi vyplývajícími z Obecného nařízení. Nový zákon o ochraně osobních údajů bude již upravovat jen některé aspekty týkající se Úřadu pro ochranu osobních údajů (např. jeho ustavení, organizaci atd.) a některé dílčí záležitosti nutné k dotvoření celého rámce ochrany osobních údajů, které nejsou Obecným nařízením upraveny nebo které Obecné nařízení umožňuje upravit na vnitrostátní úrovni.

Návaznost na předcházející regulace

Jedním ze základních znaků ochrany osobních údajů podle obecného nařízení je kontinuita. Nařízení navazuje ve sledovaných cílech a obsahových zásadách zpracování a ochrany osobních údajů na směrnici 95/46/ES.

Z porovnání obsahu obecného nařízení a směrnice 95/46/ES je zřejmé, že jsou používány stejné definice klíčových pojmů (osobní údaj, subjekt údajů, zpracování - čl. 2 směrnice 95/46/ES a čl. 4 obecného nařízení) a obdobně formulované, obsahově velmi blízké, zásady zpracování (čl. 5 a 6 obecného nařízení a čl. 6 a 7 směrnice 95/46/ES). Pravidla pro ty, kdo osobní údaje zpracovávají, tedy správce a zpracovatele, jsou podrobnější a vesměs přesnější než ve výrazně stručnější směrnici 95/46/ES a zákoně o ochraně osobních údajů. Správcům jsou ukládány některé nové

povinnosti – ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu a ohlašování téhož dotčeným subjektům údajů.

Oproti předchozí obecné formulaci povinností při zabezpečení zpracování v § 13 zákona o ochraně osobních údajů jsou v obecném nařízení akcentovány „technické prostředky“ a jmenovitě určené technologie – pseudonymizace a šifrování, obnova dostupnosti, pravidelné testování a hodnocení účinnosti zavedených opatření.

Práva těch, jejichž osobní údaje musí být chráněny, tedy subjektu údajů podle směrnice 95/46/ES jsou zachována a nově upravena podrobněji, s tím, že jedinou skutečnou novinkou je právo na přenositelnost údajů podle čl. 20 obecného nařízení. Jako novinka je v České republice prezentováno právo na výmaz podle článku 17 obecného nařízení, často pod alternativním názvem „právo být zapomenut“. Novinka v ochraně osobních údajů v členských státech EU to není; právo existuje podle čl. 14 směrnice 95/46/ES a v českém právním řádu je zakotveno v zákoně o ochraně osobních údajů od jeho schválení v roce 2000. Svého práva podle § 21 odst. 1 a 2 subjekty údajů v České republice běžně využívají. (47)

Definice osobních údajů

Právní definice osobních údajů nemůže být výčtová, protože počet druhů osobních údajů je přirozeně neuzavřený a osobní údaje vznikají neomezeně nejen jako hodnoty vztažené k novým a novým konkrétním subjektům údajů, ale také s novými technologiemi zpracování osobních údajů, jako jsou např. právě internetové technologie. IP adresa je osobním údajem vždy, když se vztahuje k určené nebo určitelné osobě, ne od doby vynesení rozsudku Soudního dvora EU, ale od prvního použití IP adresy v provozu. GDPR již také nemá podmínku systematičnosti zpracování osobních údajů. (47)

Forma zabezpečení zpracovávaných osobních údajů

Obecné nařízení neukládá povinnost použít pro zabezpečení zpracování některé specifické opatření. V článku 32 GDPR se mluví o provedení vhodných technických a organizačních opatření, která zajistí zabezpečení odpovídající danému riziku

například formou šifrování osobních údajů, nejde ale o povinnost, jde pouze o doporučení.

Šifrování je doporučeno jako jedno z vhodných opatření. Při posuzování úrovně bezpečnosti by měl podnikatel zohlednit zejména rizika, která představuje zpracování, jako náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění osobních údajů a neoprávněný přístup k takovým údajům. Kromě šifrování tak lze využít i další nástroje. Může se jednat například o omezení přístupových práv k datům, procesy pro pravidelné testování a hodnocení účinnosti zavedených technických a organizačních opatření atd. (48)

Právo uživatele obdržet svá data

Některé společnosti práci s žádostí o zaslání informací o osobních údajích usnadnily tím, že na svých webových stránkách přidali sekci, kde si mohou uživatelé stáhnout archiv, který jejich osobní data shromažďuje. Kromě Facebooku to samé učinili i LinkedIn, Twitter, Google, Tinder či Snapchat.

Tyto archivy však nemusí nutně obsahovat všechny osobní údaje – Facebook například sleduje historii prohlížení webu a lokací, kde se uživatel nachází, což není do archivu zahrnuto; je však možné obdržet například kopie příspěvků, konverzací z Messengeru a fotografií.

V případě, že chce člověk obdržet kompletní soupis uchovávaných osobních údajů, musí o toto zažádat sám, nejsnáze prostřednictvím e-mailu. Je ale nutné se připravit na skutečnost, že společnost může požádat o ověření identity, např. formou scanu občanského průkazu nebo jinou formou autentizace. K podání písemné žádosti je možné využít vzor z Přílohy č. 1. (49)

4 Vlastní práce

Praktická část navazuje na kapitolu č. 3.2 (Informační bezpečnost) teoretické části práce. V souvislosti s tím je zaměřena na ochranu uživatelských dat, konkrétně hesel. Problematika je zpracována jak z pohledu uživatele, tak z pohledu poskytovatelů služeb, neboť tyto dvě oblasti se zpravidla prolínají. V práci nejsou řešena jiná témata bezpečnosti informačních technologií, protože problematika je velice široká a nelze ji komplexně pojmout. Zároveň bylo téma zvoleno z toho důvodu, že je v odborné literatuře vyzdviženo jako jedna z nejrizikovějších oblastí.

Jako základní metoda pro studium uvedené problematiky bylo zvoleno dotazníkové šetření. Účelem bylo získat vhled do způsobu, jakým uživatelé zacházejí se svými hesly, potvrdit hypotézy o bezpečnostní situaci v oblasti správy hesel a identifikovat a vyhodnotit hlavní rizika. Šetření proběhlo formou on-line dotazníku, šířeného sociálními sítěmi Linkedin a e-mailem. Respondenti byli informováni o skutečnosti, že dotazník slouží k průzkumu v rámci diplomové práce na téma Ochrana dat a rizika bezpečnostních incidentů. Zároveň jim bylo sděleno, že získaná data budou použita jen v agregované formě a na základě vyhodnocení dotazníku budou vyvozena doporučení. Záměrem těchto doporučení je přispět k informovanosti a zvýšit kvalitu zacházení s uživatelskými daty.

Jako podpůrná metoda byl proveden monitoring zásadních úniků hesel za posledních šest let. Následně jsou vyvozena nejčastěji používaná uživatelská hesla a chyby zpracovatelů dat (poskytovatelů služeb), které vznik těchto bezpečnostních incidentů umožnily. Je potřeba zdůraznit, že problematika se netýká jen jednotlivců a menších společností. Je znepokojivé, že bezpečnostní incidenty se týkají také renomovaných, celosvětově známých firem. Ty zacházejí s osobními údaji mnoha uživatelů a předpokládá se, že by pro ně mělo být zabezpečení těchto dat prioritou.

V návaznosti na zjištěné skutečnosti byla vytvořena testovací webová stránka pro ověření, jak rychle je možné dosáhnout prolomení hesel. Zároveň má testování prokázat, že je potřeba volit kvalitnější způsob ukládání uživatelských hesel, než

je pouze některý z jednoduchých algoritmů. K testování byl využit běžný osobní počítač s výkonem, který není nejlepší pro rozsáhlejší úlohy. Konkrétně se jedná o Acer Aspire One 722-C62kk s 2 GB operační paměti a procesorem AMD Ontario Dual-Core C60, jehož dvě jádra pracují na frekvenci 1 GHz. Účelem bylo prokázat skutečnost, že nejen heslo v čitelné podobě je rizikem. Také nedůsledně volené heslo a ukládání do databází nekvalitním způsobem je bezpečnostní hrozbou.

V rámci diplomové práce bylo také umožněno participovat na projektu Michala Špačka, vývojáře v programovacím jazyce PHP a uznávaného bezpečnostního experta, který působí také jako školitel v oblasti bezpečnosti informačních technologií.

Cílem projektu je informovat o stavu, jakým způsobem společnosti ukládají uživatelské údaje a také naučit firmy, aby se nebály tyto informace poskytovat. Na základě způsobu zacházení s hesly uživatelů jsou společnosti hodnoceny na stupnici A (nejlepší hodnocení) až F (nejhorší hodnocení). Seznam společností je zveřejněn na webových stránkách https://pulse.michalspacek.cz/passwords/storages. Seznam je v průběhu času dále rozšiřován. K tomu je využito aktivní ověřování přes vytvoření uživatelského účtu na daných službách, zaslání žádosti o obnovení hesla či žádosti o zaslání zapomenutého hesla. Dalším způsobem je obdržení podnětu od uživatelů dané služby, kteří o nedostatečně bezpečném způsobu ukládání hesel informují.

Společnosti jsou se způsobem hodnocení seznámeny a mají možnost na nedostatky reagovat. Pokud tak učiní a výsledkem je i průkazná změna způsobu ukládání hesel k lepšímu, je jim i písmenná známka upravena. K tomu ale musejí informaci o způsobu ukládání hesel uvést veřejně, a to buď na sociálních sítích nebo nejlépe na svých webových stránkách.

4.1 Pohled uživatele

Z průzkumu společnosti SplashData, Inc. za posledních šest let (viz tabulka č. 1) vyplývá, že nejčastěji používaná hesla zůstávají prakticky beze změny. Tento průzkum vychází z analýzy záznamů, které pronikají na internet v rámci hackerských útoků. Jedná se o data v řádu několika milionů údajů.

Nejčastěji používaná hesla

Mezi nejčastěji používaná hesla se řadí více méně pravidelně na prvních šesti příčkách hesla 123456, password, 12345678, 12345, qwerty a 123456789. Z toho lze usuzovat, že uživatelé nejsou při volbě hesel důslední, přestože jsou k dispozici veřejně dostupné informace o únicích dat.

Tabulka 1 Nejčastěji používaná hesla v letech 2013-2018

Příčka	Rok					
	2013	**2014**	**2015**	**2016**	**2017**	**2018**
1.	123456	123456	123456	123456	123456	123456
2.	password	password	password	password	password	password
3.	12345678	12345	12345678	12345	12345678	123456789
4.	qwerty	12345678	qwerty	12345678	qwerty	12345678
5.	abc123	qwerty	12345	football	12345	12345
6.	123456789	123456789	123456789	qwerty	123456789	111111
7.	111111	1234	football	1234567890	letmein	1234567
8.	1234567	baseball	1234	1234567	1234567	sunshine
9.	iloveyou	dragon	1234567	princess	football	qwerty
10.	adobe123	football	baseball	1234	iloveyou	iloveyou
11.	123123	1234567	welcome	log¡n	admin	princess
12.	Admin	monkey	1234567890	welcome	welcome	admin
13.	1234567890	letmein	abc123	solo	monkey	welcome

14.	letmein	abc123	111111	abc123	login	666666
15.	photoshop	111111	1qaz2wsx	admin	abc123	abc123
16.	1234	mustang	dragon	121212	starwars	football
17.	monkey	access	master	Flower	123123	123123
18.	shadow	shadow	monkey	passw0rd	dragon	monkey
19.	sunshine	master	letmein	Dragon	passw0rd	654321
20.	12345	michael	login	Sunshine	master	!@#$%^&*

Zdroj: Vlastní zpracování

4.1.1 **Dotazníkové šetření**

Dotazník byl směřován na respondenty ve věku od 19 let, u kterých se předpokládá, že mají dokončené středoškolské vzdělání a jsou již v pracovním procesu, bez ohledu na typ úvazku. Věkové rozmezí bylo zvoleno s přihlédnutím ke statistikám počtu uživatelů dle věku, kteří používají osobní počítače, tablety a mobilní telefony i za účelem připojení k internetu. Předpokládá se, že pro tyto uživatele jsou současné hrozby největším rizikem. V rámci šetření je ověřována hypotéza č. 1, že uživatelé nevolí dostatečně silné prostředky pro ochranu svých dat a hypotéza č. 2, že jsou ohroženi vnějšími faktory (poskytovateli služeb).

V prvním kole probíhal pilotní výzkum na menším vzorku 30ti respondentů, na základě kterého bylo ověřeno, zda je dotazník formulován srozumitelně a v případě potřeby byly některé otázky upraveny. Samotné šetření následně probíhalo tři týdny a zúčastnilo se ho celkem 1403 respondentů.

Soubor otázek a možných odpovědí:

Kolik je Vám let?

19-26	27-34	35-42	43-50	51 a více

V jakém oboru pracujete?

Informatika	Jiný technický obor	Služby	Administrativa	Jiné

Používáte rozdílné přihlašovací heslo do každé důležité aplikace?

Ano	Ne	Nechci odpovídat

Používáte password manager (správce hesel)?

Ano	Ne	Nevím, co je password manager	Nechci odpovídat

Pokud jste odpověděli ne, z jakého důvodu password manager nepoužíváte?

Považuji to za zbytečné	Nedůvěřuji mu	Neumím ho používat	Nechci odpovídat

Používáte při přihlašování do služeb vícefaktorovou autentizaci?

Ano, pokud je k dispozici	Ne	Nevím, co je vícefaktorová autentizace	Nechci odpovídat

Obdrželi jste někdy e-mailem své vlastní heslo v čitelné podobě (např. při obnovení hesla u některé služby apod.)?

Ano	Ne	Nechci odpovídat

Stali jste se někdy obětí úniku dat, konkrétně Vašich hesel?

Ano	Ne	Nevím	Nechci odpovídat

Pokud byste se dozvěděli, že Vaše hesla z některé služby unikla, používali byste službu dál?

Ano	Ne	V závislosti na mé újmě	Nechci odpovídat

Dotazník a výsledky šetření, obsahující grafy, jsou součástí Přílohy č. 2 a Přílohy č. 3. Souhrnné výsledky dotazníkového šetření jsou uvedeny níže. V rámci dodržení korektního postupu jsou u významných hodnot uvedeny jak relativní, tak i absolutní četnosti.

Věk respondentů

Ve věkovém rozmezí 19-26 let se pohybuje 57,9 % respondentů.
Ve věkovém rozmezí 27-34 let se pohybuje 24,7 % respondentů.
Ve věkovém rozmezí 35-42 let se pohybuje 9,3 % respondentů.
Ve věkovém rozmezí 51 a více let se pohybuje 4,8 % respondentů.
Ve věkovém rozmezí 43-50 let se pohybuje 3,3 % respondentů.

Největší podíl respondentů tedy tvořili občané ve věku 19-26 let (812 respondentů) a ve věku 27-34 let (346 respondentů).

Zaměstnání respondentů

V oboru Jiné pracuje 38,1 % respondentů.
V oboru Informatika pracuje 22,4 % respondentů.
V oboru Jiný technický obor pracuje 15,9 % respondentů.
V oboru Služby pracuje 13,2 % respondentů.
V oboru Administrativa pracuje 10,2 % respondentů.

Největší podíl respondentů tvoří zaměstnanci oboru Jiné, který zahrnuje i studenty (528 respondentů). Významné procento respondentů tvoří zaměstnanci oboru Informatika (310) a Jiný technický obor (220).

Použití rozdílného přihlašovacího hesla do každé důležité aplikace

Rozdílné heslo používá 56 % respondentů.
Stejné heslo používá pro více služeb 38,3 % respondentů.
Odpovídat odmítlo 5,7 % respondentů.

Největší podíl respondentů používá rozdílné heslo do každé důležité aplikace, pokud je to umožněno (786 respondentů). Nicméně významný je i podíl respondentů, kteří naopak rozdílná hesla nepoužívají (537 respondentů).

Použití správce hesel (password manageru)

Službu nevyužívá 47,4 % respondentů.
Službu používá 25,2 % respondentů.
Službu nezná 24,9 % respondentů.
Odpovídat odmítlo 2,5 % respondentů.

Největší procento respondentů nepoužívá password manager (665 respondentů). Službu také nepoužívají respondenti, kteří ji neznají (350 respondentů). Naproti tomu téměř stejná, ale o něco větší část respondentů tuto službu používá (353 respondentů).

Důvody, proč respondenti nevyužívají správce hesel

Za zbytečné to považuje 31,3 % respondentů.
Službu neumí používat 26,8 % respondentů.
Službě nedůvěřuje 26,6 % respondentů.
Odpovídat odmítlo 15,3 % respondentů.

Nejvíce respondentů službu nepoužívá, protože to považují za zbytečné (208 respondentů). Další část respondentů ji používat neumí (178 respondentů) nebo jí nedůvěřuje (177 respondentů).

Používání vícefaktorové autentizace

Vícefaktorovou autentizaci používá 58,4 % respondentů, pokud je k dispozici.
Tento pojem nezná 24,7 % respondentů.
Vícefaktorovou autentizaci nepoužívá 14,7 % respondentů.
Odpovídat odmítlo 2,1 % respondentů.

Nadpoloviční většina respondentů používá vícefaktorovou autentizaci (806 respondentů). Významné procento uživatelů neví, co je vícefaktorová autentizace (341 respondentů) nebo ji nevyužívá (203 respondentů).

Získání vlastního hesla v čitelné podobě

Své heslo obdrželo v čitelné podobě z některé z používaných služeb 59,8 % respondentů.
Své heslo nikdy neobdrželo v čitelné podobě 37,5 % respondentů.
Odpovídat odmítlo 2,7 % respondentů.

Významná část respondentů obdržela své heslo v čitelné podobě (839 respondentů). Více jak třetina respondentů své heslo v čitelné podobě neobdržela (526 respondentů).

Informovanost uživatelů o úniku jejich dat (hesel)

O tom, že nedošlo k úniku jejich dat, je přesvědčeno 57,2 % respondentů.
O úniku svých dat ví 24,5 % respondentů.
Zda došlo k úniku dat si není jisto 17 % respondentů.
Odpovídat odmítlo 1,3 % respondentů.

Nadpoloviční většina respondentů předpokládá, že nedošlo k úniku jejich dat (803 respondentů). Naproti tomu někteří respondenti vědí s jistotou, že jejich data někdy unikla (344 respondentů).

Reakce uživatelů na informaci o úniku dat (hesel)

Službu, ze které data unikla, by dále používalo pouze v závislosti na velikosti újmy 56,8 % respondentů.
Službu by přestalo používat 30,4 % respondentů.
Službu by dále používalo 10,6 % respondentů.
Odpovídat odmítlo 2,3 % respondentů.

Nadpoloviční většina respondentů by zvážila další používání služby, ze které unikla jejich data, v závislosti na své újmě (792 respondentů). Téměř třetina respondentů by přestala službu používat (426 respondentů).

4.1.2 Implementace webové stránky k demonstraci útoku na hesla

Byla vytvořena testovací webová stránka s přihlašovacím formulářem, na které je analyzováno, jak rychlé může být prolomení hesla už jen při použití běžného počítače. Webová stránka je implementována v programovacím jazyce Python s využitím webového frameworku Django. Umožňuje přihlášení uživatele pomocí přihlašovacího jména a hesla, zadaného do formuláře. Po přihlášení získá uživatel přístup k chráněným informacím.

Kód

```
{% load i18n %}
<!DOCTYPE html>
<html>
<head lang="en">
  <meta charset="UTF-8">
  <title>Zardos</title>
</head>

<body>
{% if user.is_authenticated %}
  <h1>The gun is good!</h1>
  <img src="/static/zardoz.jpg" alt="the gun is good"/>
  <p><a href="/admin/logout/">odhlásit</a></p>
  <p><a href="http://www.seznam.cz">seznam</a></p>
{% else %}

  <h1>Musíte se přihlásit</h1>

  <form action="." method="post">{% csrf_token %}
    {{ form.as_p }}
    <input type="submit" name="odeslat" id="" value="Odeslat"/>
  </form>

{% endif %}

<script type="text/javascript">
  document.getElementById('id_username').focus()
</script>

</body>
</html>
```

Nejprve je nutná instalace dvou hlavních programů, kterými jsou sqliteman a virtualenv. Sqliteman umožňuje prohlížet obsah odcizené databáze (ze které budeme porovnávat hashe s cílem získat heslo k uživatelskému účtu). Virtualenv vytváří izolované Python prostředí, které slouží k nainstalování knihovny. Vše co patří do tohoto testovacího projektu tedy není nainstalováno přímo do systému, ale v tomto virtuálním prostředí. Příkazem activate se spustí složka, aby bylo možné do ní instalovat knihovny.

```
sudo aptitude install sqliteman virtualenv
cd PycharmProjects/biska
virtualenv bis
source bis/bin/activate
pip install -r requirements.txt
```

Pro spuštění webové stránky na adrese http://localhost:8000/ je pomocí prvního příkazu vytvořena databáze (tato činnost se provádí jen jednou) a pomocí druhého příkazu je web uveden do provozu.

```
python app.py syncdb
python app.py runserver
```

Dále je vytvořen uživatel.

```
python app.py createsuperuser --username=admin --email=admin@test.com
```

Bylo přiděleno uživatelské jméno "admin" a byl vytvořen skript, který se pokouší přihlásit na stránku pod daným uživatelským jménem. Uživatelské jméno bylo zvoleno úmyslně, neboť je prokázáno, že je v profesním světě velmi často používáno. Bohužel nejen v testovacích aplikacích, ale také v rámci již běžících projektů.

Vytvořený skript postupně zkouší všechna možná hesla složená z malých písmen anglické abecedy o rozsahu jeden až čtyři znaky.

Skript

```
# -*- coding: utf-8 -*-

import itertools
import time
import sys
import requests

"""
priklad

a
z
aa
ab
ac
zz
aaa
dfg
zzz
aaaa
zzzz
"""
adresa = 'http://localhost:8000/'
passwords = []
max_delka_hesla = 4
delka_jednotlivych_pokusu = []

for delka_hesla in range(1, max_delka_hesla + 1):
    passwords.append(list(itertools.product('abcdefghijklmnopqrstuvwxyz', repeat=delka_hesla)))
    # print len(passwords[repeat-1])

# odesilame hesla o delce 1
```

```
34  def zkus_heslo(heslo):
35      heslo = ''.join(heslo)
36      pred = time.time()
37      zkus_na_strance(heslo)
38      po = time.time()
39      delka_jednotlivych_pokusu.append(po - pred)
40
41
42  def zkus_na_strance(heslo):
43      post_odpoved = requests.post(adresa, data={'username': 'admin', 'password': heslo, 'csrfmiddlewaretoken': csrf},
44                                   cookies=dict(csrftoken=csrf), allow_redirects=False)
45      if post_odpoved.is_redirect:
46          # jsme presmerovani a heslo je ok
47          print 'Heslo je %s' % heslo
48          print 'Jeden pokus trval prumerne', sum(delka_jednotlivych_pokusu) / len(delka_jednotlivych_pokusu), 's'
49          sys.exit()
50

51  # ulozime si csrf pro dalsi pouziti at nemusime volat GET dokola
52  session = requests.Session()
53  uvodni_pozadavek = session.get(adresa)
54  csrf = uvodni_pozadavek.cookies['csrftoken']
55
56  for delka_hesla in range(0, max_delka_hesla):
57      pred = time.time()
58      for heslo in passwords[delka_hesla]:
59          zkus_heslo(heslo)
60      po = time.time()
61      print "zkouseni %s hesel o delce" % len(passwords[delka_hesla]), delka_hesla + 1, "trvalo %.3f" % (po - pred), 's'
62
63  print 'Jeden pokus trval prumerne', sum(delka_jednotlivych_pokusu) / len(delka_jednotlivych_pokusu), 's'
```

Spuštění skriptu

```
python hackit.py
zkouseni 26 hesel o delce 1 trvalo 0.396 s
zkouseni 676 hesel o delce 2 trvalo 9.017 s
Heslo je abc
Jeden pokus trval prumerne 0.0133911237325 s
```

Následně byl skript upraven pro zkoušení číselných hesel o rozsahu jeden až 5 znaků.

```
zkouseni hesel o delce 1 trvalo 0.426 s
zkouseni hesel o delce 2 trvalo 4.534 s
zkouseni hesel o delce 3 trvalo 49.200 s
zkouseni hesel o delce 4 trvalo 456.508 s
Heslo je 12345
Jeden pokus trval prumerne 0.045897801318 s
```

Je možné pozorovat, že v tomto případě trvalo zjištění hesla téměř 8 minut. To je podstatně déle, nicméně skript již musel projít poměrně velké množství kombinací a byl spuštěn na úplně běžném zastaralém počítači. Z toho důvodu lze považovat výsledek za velmi uspokojivý z pohledu útočníka, respektive neuspokojivý v případě uživatele, který volí triviální hesla. K těm je možné se takto jednoduše dostat. Nemluvě o mnohem modernějších a profesionálních strojích s neporovnatelně vyšším výpočetním výkonem. Těm by takovéto lámání hesel nezabralo žádný čas.

Bezpečnost testovací webové stránky

Implementovaná stránka odpovídala v prvním případě velmi rychle, průměrně za 0.013 s, ve druhém případě za 0,046. To je v tomto případě na škodu, protože to umožňuje tento typ útoku.

V databázi jsou hesla ukládána algoritmem MD5 bez použití soli. Tento algoritmus je stále často používán. Byl zvolen úmyslně, aby bylo poukázáno na to, jak je snadné ho prolomit a proč by se používat neměl. Jediným bezpečnějším použitím tohoto algoritmu je přidání soli, díky které se změní hash a prolomení hesla se pak stává o něco složitějším. Vhodné opatření je omezit možnost přihlášení k účtu po několika neúspěšných pokusech zablokováním IP adresy, ze které je útok veden nebo zavést jinou ochranu, např. limitování počtu pokusů např. na jeden za vteřinu, aby bylo předejito využití robotů.

Použitý formulář využívá zabudované bezpečnostní funkce frameworku Django, ochrany proti CSRF útoku.

4.2 Pohled poskytovatele služeb

Tato část je úzce spojena s předcházející kapitolou, na kterou navazuje zkoumáním problematiky z pohledu zpracovatelů dat (poskytovatelů služeb). V rámci čím dál častějších úniků dat, která jsou k nalezení volně na internetu se tato část zaměřuje na zkoumání přístupu společností k ukládání uživatelských hesel. V rámci tohoto projektu bude ověřována hypotéza, že společnosti pružně reagují na bezpečnostní hrozby a zvyšuje se kvalita jejich přístupu k ukládání dat.

Projekt k ukládání uživatelských hesel

V rámci projektu jsou webové stránky společností hodnoceny na stupnici A – F, kdy A je hodnocení nejlepší při používání kvalitních hashovacích funkcí a F je hodnocení nejhorší, za ukládání hesel v plaintextu či nevhodnými funkcemi bez dalšího ošetření. Konkrétní způsob hodnocení je uveden níže.

Stupnice hodnocení

A
Použití pomalých hashovacích funkcí a zveřejnění informace na webových stránkách.

B
Použití pomalých hashovacích funkcí a zveřejnění informace skrytě na blogu, v komentáři, přednášce nebo na sociálních sítích.

C
Hesla hashovaná nevhodnou funkcí, ale alespoň s použitím soli a více iterací.

D
Použití nevhodné hashovací funkce, nicméně alespoň se solí.

E
Hesla bez použití soli, ukládaná pouze jednorázovým použitím nevhodné funkce.

F
Hesla ukládaná v plaintextu (čitelně).

V současné době je v evidenci 118 společností a některé z nich provozují více webových stránek, u kterých je ale způsob nakládání s uživatelskými údaji shodný. Kompletní seznam společností je součástí Přílohy č. 4.

Celkem 37 společností mělo jedno z nejhorších hodnocení, tj. buď známku E nebo F. Tyto společnosti byly osloveny prostřednictvím e-mailu, webových formulářů nebo dalších sociálních sítí se žádostí o informaci, zda došlo ke změně způsobu práce s uživatelskými daty.

Výsledky, plynoucí z kontaktování provozovatelů jednotlivých služeb jsou zobrazeny v tabulce níže.

Tabulka 2 Způsob ukládání uživatelských hesel – reakce poskytovatelů služeb

Způsob ukládání uživatelských hesel – reakce poskytovatelů služeb					
company	**web**	**rating**	**date**	**progress**	**notes**
ABCSPORT.CZ (LERKO SPORT, s.r.o.)	www.abcsport.cz	F	Aug 2016		bez reakce
Adveri s.r.o.	www.happyfeed.com	D	Oct 2016		**zrušená registrace / není ukládání hesel**
Affectio s.r.o.	www.mimibazar.cz	F	Oct 2016		bez reakce
Behej.com, s.r.o.	www.behej.com	F	Apr 2018		bez reakce
BetaNews, Inc.	fileforum.betanews.com	F	Mar 2018		bez reakce
České dráhy, a.s.	moje.inkarta.cz	F	Jan 2017	**beze změny**	e-mail
Czech Airlines (České aerolinie a.s.)	www.csa.cz	F	Jan 2017		bez reakce
eD' system Czech, a.s.	edshop.edsystem.cz	F	Sep 2017		komentář na sociální síti - reagovali, v řešení
eD' system Slovakia, s.r.o.	www.edsystem.sk	F	Sep 2017		koment fcb
ePojisteni.cz, s.r.o.	www.epojisteni.cz	F	Jul 2016	**nechtějí uvést**	e-mail
Event Service, s.r.o.	int.tymuj.cz	F	Aug 2017	**Bcrypt - B**	**info přidáno do FAQ, zn. B**
FORPSI (INTERNET CZ, a. s.)	www.forpsi.com	F	Aug 2014		bez reakce
Gigaprint.cz (Cetria s.r.o.)	www.gigaprint.cz	F	Feb 2018		bez reakce
Gigaprint.sk, s. r. o.	www.gigaprint.sk	F	Feb 2018		bez reakce

goodooga s.r.o.	www.nevyhazujto.cz	E	Feb 2018		bez reakce
ICE invest spol. s r. o.	www.veselekostky.cz	F	Mar 2018	**nechtějí uvést**	tech - komentář na sociální síti
Ing. Tomáš Petruška	www.zaluzie24.eu	F	Aug 2017		bez reakce
Internet Info, s.r.o.	all sites	D	Oct 2016		bez reakce
Jabber.org	www.jabber.org	F	Aug 2012		tech - US, e-mail - reagovali, v řešení
Kuma.cz s.r.o.	www.kuma.cz	E	Jul 2018		bez reakce
Lagoon Foto, a.s.	www.lagoonfoto.cz	F	Oct 2016		bez reakce
Leader Fox (BOHEMIA BIKE a.s.)	e-shop.leaderfox.com	E	Feb 2018		bez reakce
MAFRA, a.s.	www.aaapoptavka.cz	F	Oct 2016	**B**	Apr 2018
Maneo, s.r.o.	www.eshop.maneo.cz	F	Sep 2017		bez reakce
Městská část Praha 8	www.praha8.cz	F	Oct 2018		bez reakce
Mojevideo.sk, s.r.o.	www.mojevideo.sk	F	Jan 2017		bez reakce
MUNAP COMPANY, s.r.o.	www.munap.cz	F	Sep 2017		bez reakce
mySupermarket Limited	www.mysupermarket.co.uk	E	Jun 2015		bez reakce
NWT a.s.	www.patro.cz	F	Feb 2018		bez reakce
Pantone LLC	www.pantone.com	F	Mar 2018		bez reakce
Pavel Pola	www.paladix.cz	F	Oct 2016		bez reakce

PRONETmedia, s.r.o.	www.pay4t.cz	D	Sep 2014		bez reakce
Spotreba.sk, s. r. o.	www.spotreba.sk	E	Sep 2016		bez reakce
TANGER infosystems s.r.o.	www.seznamka.cz	F	Jan 2018		bez reakce
Veřejná informační služba, spol s.r.o.	www.strava.cz	F	Aug 2017	**nechtějí uvést**	komentář na sociální síti
Webfarm s.r.o.	www.cars.cz	F	Jun 2018		bez reakce
WEDOS (WEDOS Internet, a.s.)	hosting.wedos.com	D	Nov 2016		bez reakce

Zdroj: vlastní zpracování

Červeně jsou vyznačeny společnosti, které nezměnily rizikový způsob ukládání hesel a ty, které se odmítly k tématu vyjádřit. I u těchto společností se předpokládá, že hesla ukládají stále stejným způsobem. Zeleně jsou naopak vyznačeny příznivé reakce, kdy došlo ke změně způsobu práce s daty. U těchto společností jsou nyní hesla ukládána dokonce jedním z nejlepších způsobů, použitím pomalé hashovací funkce Bcrypt. U společností, které jsou zvýrazněny šedou barvou, komunikace ještě pokračuje. Převážná většina provozovatelů vůbec na oslovení nereagovala, přestože byli osloveni opakovaně a různými cestami. Jedna společnost zcela zrušila možnost registrace uživatelů.

5 Výsledky a diskuse

Ze šetření, provedených v rámci praktické části vyplývá, že přestože je téma ochrany dat již delší dobu moderní záležitostí, stále více se o něm mluví a úniky citlivých dat nejsou výjimečným případem, uživatelé ani zpracovatelé dat nezachází s osobními údaji nejlepším způsobem.

Výsledky dotazníkového šetření v grafickém vyjádření jsou součástí Přílohy č. 3 a jsou zobrazeny pomocí kruhových diagramů četností.

Věk respondentů se nadpoloviční většinou pohyboval mezi 19 – 26 lety kdy dotyční jsou převážně zaměstnáni v oboru Jiné, v Informatice nebo v Jiném technickém oboru.

Nadpoloviční většina respondentů uvedla, že používá pro důležité služby do každé z nich rozdílné přihlašovací heslo. Přesto je poměrně vysoká část respondentů (38,3 %) zvyklá, používat stejná hesla. Z jednoho pohledu je to sice jednodušší na zapamatování, ale z hlediska bezpečnosti to určitě není nejlepší přístup. Pakliže se k takovému heslu dostane neoprávněná osoba, má během okamžiku hesla i k dalším účtům, neboť i kdyby neměla k dispozici uživatelské jméno, to je většinou velmi snadné odvodit z dalších informací o uživateli. Ohledně používání Správce hesel uvedlo 47,4 % respondentů, že tuto službu nevyužívá. Hesla tedy vymýšlejí či generují a zároveň i spravují jinými způsoby. Důvody pro nevalnou oblíbenost tohoto nástroje kombinují neochotu zacházet s novými technologiemi, pohodlnost a samotnou nedůvěru uživatelů v některé produkty. Tato informace vyplývá z odpovědí respondentů, kdy téměř stejnou měrou bylo uvedeno, že uživatelé tuto službu považují za zbytečnou, neumí ji používat nebo jí nedůvěřují. Naopak pozitivním znakem je, že nadpoloviční většina si oblíbila používání vícefaktorové autentizace při přihlašování do služeb. Testovanou hypotézu tedy nebylo možné zcela potvrdit, neboť přístup uživatelů k zabezpečení hesel se liší v závislosti na používaných nástrojích. Přesto je možné z výsledků šetření pozorovat významná rizika.

Dále vyplynulo, že s vysokou četností uživatelé obdrželi svá hesla v čitelné podobě v rámci elektronické komunikace. To je rizikové nejen vzhledem k tomu, že se může

k účtu dostat někdo neoprávněný a komunikaci si jednoduše přečíst, ale také vzhledem k možnostem dnešních hackerských technik. Své heslo někdy obdrželo e-mailem celých 59,8 % respondentů. To prokazuje skutečnost, že firmy (poskytovatelé služeb) tato data nešifrují a poukazuje to na výrazná bezpečnostní rizika. V kombinaci s tím 24,5 % uživatelů ví s jistotou, že někdy došlo k úniku jejich dat. 17 % uživatelů si něčím takovým vůbec není jistých, což je jedna z možných a pochopitelných odpovědí. Naproti tomu alarmující je, že 57,2 % uživatelů odpovědělo na tuto otázku s přesvědčením, že k úniku jejich dat nikdy nedošlo. Toto je ošemetné tvrzení, které poukazuje na skutečnost, že uživatelé mohou být v uvažování o bezpečnostních hrozbách lehkovážní. Faktem totiž je, že takovou věcí si nikdy nemohou být jistí. Naopak odpověď „nevím“ je naprosto relevantní. Tato otázka měla poukázat na schopnost kritického myšlení dotázaných. Hypotéza č. 2 byla potvrzena v bodě, ve kterém se zkoumají rizika vyplývající z přístupu firem (zasílání uživatelských hesel v čitelné podobě a přítomnost úniků dat).

Závěrem s odpověďmi na poslední otázku vyplynulo, že v případě úniku dat by reagovalo celých 56,8 % uživatelů na službu, ze které data unikla tím způsobem, že by zvážili velikost své újmy. Pakliže by byla neúnosná, službu by opustili.

Dále se zkoumal pohled zpracovatelů dat na bezpečnostní politiku hesel. Účelem bylo potvrdit hypotézu, že vzhledem k informaci o svých předchozích nedostatcích v této oblasti se firmy snaží aktivně o zlepšení přístupu ke způsobu zpracování uživatelských dat. Převážná většina společností na opakovanou snahu o komunikaci nereagovala nebo odmítla informaci zveřejnit. Hypotéza tedy nebyla potvrzena. Některé společnosti důrazně argumentovali tím, že informace o způsobu nakládání s hesly nesdělí, samozřejmě z důvodu bezpečnosti. Nicméně často je právě toto známkou, že údaje v bezpečí nejsou.

5.1 Doporučení uživatelům

Ze zkoumaných skutečností vyplývá řada doporučení, která jsou uvedena níže.

Uživatelé by měli s hesly zacházet v souladu se základními bezpečnostními doporučeními:

- Informovat se průběžně z důvěryhodných zdrojů o možných rizicích a skutečnostech, souvisejících se zabezpečením údajů.
- Používat do každé důležité aplikace rozdílné heslo
- Volit heslo správného formátu, nejlépe náhodně generované a s různým typem znaků.
- Zvážit možnost využití podpůrných nástrojů, jako jsou správci hesel Esset Password Manager, Norton Password Manager, LastPass, 1Password, Stickypassword, Kaspersky Password Manager, Google Password Manager. Pro uživatele, kteří těmto službám nedůvěřují je možné doporučit open source nástroje, např. KeePass Password Safe, Passbolt, Lesspass, ale ne vždy je to zárukou vyšší bezpečnosti.
- Přihlašovat se, pokud možno, jen přes https protokol. Tam kde to není možné, neodesílat v rámci komunikace citlivé údaje.
- Používat vícefaktorovou autentizaci přinejmenším u bankovních a podobných služeb.
- Nezadávat hesla a další údaje na formuláře z podezřelých odkazů.
- Nesdělovat hesla jiným osobám a nepoužívat je viditelně na veřejnosti.
- Většinou se doporučuje také nemít hesla na papíře. Toto doporučení ale nelze vztáhnout na všechny uživatele. Například se netýká hesel k důležitým přístupům, na kterých závisí existence společnosti. Taková hesla by měla být naopak vždy spolehlivě dohledatelná, samozřejmě s použitím příslušných zabezpečení (např. trezor.).
- Změnit hesla v reakci na poskytovatele služeb v případě podezření, že došlo k úniku.
- Využít možnosti aktivního ověření úniku dat, např. pomocí služby Haweibeenpwned.com, která obsahuje poměrně širokou databázi.
- Správně interpretovat a ověřovat si podezření na bezpečnostní rizika. Například to, že uživatel obdrží ze služby na základě své registrace heslo e-mailem v čitelné podobě nevypovídá o způsobu, jakým jsou hesla ukládána

do databáze (neznamená to, že nejsou následně kryptograficky zabezpečena). Přesto není dobré, aby poskytovatelé služeb zasílali hesla v takovým způsobem

- Využít možnosti vyžádání evidovaných osobních údajů od poskytovatelů služeb na základě GDPR. Je možné využít vzorů z různých zdrojů (např. https://mydatarequest.com/#getstarted). V případě vyžádání údajů prostřednictvím elektronické pošty zpracovatelé často nezašlou kompletní osobní údaje – pak je nutná oficiální žádost. Žadatel by měl obdržet i svá hesla – má možnost prozkoumat, jakým způsobem jsou evidována a blíže se informovat o použitém algoritmu či funkci, pokud chce věnovat čas detailnějšímu pátrání a rozboru.
- Pravidelně aktualizovat software.

5.2 Doporučení poskytovatelům služeb

Tato doporučení jsou provázána se závěry ze zkoumané problematiky z pohledu uživatelů.

Poskytovatelům služeb (zpracovatelům dat) lze doporučit následující:

- Informovat se průběžně o aktuálních bezpečnostních rizicích a nových technologiích, kterými lze zajistit prevenci bezpečnostních hrozeb.
- S uživatelskými údaji zacházet co možná nejopatrněji.
- Pro ukládání/šifrování hesel volit kvalitní hashovací funkce
- V případě úniku dat jednat s dotčenými osobami korektně, o skutečnosti je informovat a přijmout příslušná opatření nejen k odstranění následků, ale také k odstranění budoucího rizika opakování incidentu.
- Testovat funkčnosti svých služeb a projevovat zájem o bezpečnost kódu.
- Poskytnout uživatelům webové stránky na https protokolu
- Umožnit uživateli vícefaktorovou autentizaci.
- Nezasílat hesla uživateli v čitelné podobě a volit časové omezení platnosti odkazů pro reset hesla při jejich jednorázové platnosti.

- Nevyžadovat po uživatelích častou periodickou změnu hesla. V současné době je tento postup považován spíše za riziko, neboť uživatelé mají tendenci hesla čím dál více zjednodušovat.
- Sledovat logy v rámci provozu na svých serverech a pružně reagovat na neobvyklé události.

5.3 Diskuse

Mé odborné zaměření prozatím nespadá do oblasti informačních technologií, ale pracuji dosud v oboru logistiky. Z toho důvodu mým původním záměrem při volbě daného tématu bylo, získat možnost bezplatné praktické stáže v některé z firem, zabývajících se poskytováním služeb v oblasti informatiky.

Chtěla jsem zpracovat téma ochrany dat a bezpečnostních rizik komplexně v rámci dané firmy, analyzovat jednotlivé oblasti informační bezpečnosti a tím také získat kvalitnější vhled do této problematiky. V souvislosti s tím jsem se zúčastnila několika pohovorů, přičemž jsem se ke své lítosti setkala s negativním přístupem, kdy mi podobná stáž nebyla umožněna. Společnosti argumentovaly především tím, že by nesvolily, aby toto téma vztažené na jejich interní procesy bylo zveřejněno v rámci diplomové práce, přestože jsem předem zdůrazňovala, že by nebyl uveden ani název společnosti, ani konkrétní data. Jen potřebné souvislosti a informace, plynoucí z hlavních výstupů. Domnívám se, že i tento přístup naznačuje nekvalitní zacházení s daty a obavy z odhalení dalších bezpečnostních nedostatků, což bylo také významné zjištění při zpracování tohoto tématu.

Nicméně z tohoto důvodu jsem byla nucena původní záměr upravit a praktická část nebyla zaměřena na komplexní analýzu v rámci podniku. Dostala jsem příležitost, participovat na projektu Michala Špačka, který je uznávaným bezpečnostním expertem a setkala jsem se s ním v rámci komunity informačních specialistů, se kterými jsem příležitostně v kontaktu.

Výstupy práce, především z rozsáhlého dotazníku, byly Michalem Špačkem vyžádány jako podklad do budoucích odborných sloupků, zabývajících se ochranou dat a riziky, spojenými s přístupem poskytovatelů služeb ke správě osobních údajů uživatelů.

6 Závěr

V rámci práce byly v teoretické části s pomocí studia odborné literatury a odborných článků uvedeny nejzákladnější pojmy a definice, týkající se ochrany dat a rizik bezpečnostních incidentů. Tento úsek práce sloužil k uvedení do tématu a jako podklad, ze kterého bylo možné vycházet při zpracování praktické části práce.

V rámci praktické části byly identifikovány současné hrozby, které představují pro uživatele informačních technologií riziko. Následně byla tato část pojata ze dvou pohledů, a to z pohledu uživatele služeb a z pohledu poskytovatele těchto služeb.

Byl proveden sociologický průzkum, jehož výsledky poskytly přínosné informace o současné situaci, jakým způsobem zacházejí uživatelé se svými údaji (hesly). Bylo zjištěno, že uživatelé často duplikují hesla mezi různými službami, což není vhodné, pokud se jedná o citlivé služby, jakými jsou například internetové bankovnictví a přístupy do firemních portálů. Z průzkumu také vyplynulo, že jsou často službami hesla zasílána v čitelné podobě, z čehož jsou odvozena další rizika. Na základě vyhodnocení všech odpovědí je možné říci, že uživatelé nezacházejí se svými hesly nejlépe, ale zároveň zabezpečení údajů nezávisí jen na nich a poskytovatelé služeb také dávají prostor zvýšení rizik. Ať už zasíláním hesel v čitelné podobě nebo způsobem ukládání hesel do databází. Tomuto hledisku se věnoval další úsek praktické části, kdy Výsledky tohoto průzkumu byly následně zohledněny v závěrech a doporučeních pro uživatele informačních technologií.

7 Seznam použitých zdrojů

1. 7 zásad pro kybernetické zabezpečení malé firmy. *BusinessInfo.cz.* [Online] https://www.businessinfo.cz/cs/clanky/7-zasad-pro-kyberneticke-zabezpeceni-male-firmy-118093.html.

2. Informační systémy a ochrana dat. *SystemOnLine.* [Online] https://www.systemonline.cz/clanky/informacni-systemy-a-ochrana-dat.htm.

3. Ochrana dat: Úvod. *Svět hardware.* [Online] https://www.svethardware.cz/ochrana-dat-uvod/29362.

4. Šifrování a ochrana dat, počítače a internetu. *Guard-dynamics.* [Online] http://www.guard-dynamics.cz/ochrana-dat.

5. SecurityWorld, autor -rd |. Na kolik vyjde ochrana dat a jejich ztráta. *Computerworld.cz, Deník pro IT profesionály.* [Online] 02. 06 2018. https://computerworld.cz/securityworld/na-kolik-vyjde-ochrana-dat-a-jejich-ztrata-54718.

6. Ing. Jindřich KODL, CSc., Prof. Ing. Vladimír SMEJKAL, CSc., LL.M. Bezpečnost ICT a ochrana dat. *MVŠO - Moravská vysoká škola Olomouc.* [Online] 2018. https://mvso.cz/wp-content/uploads/2018/02/Bezpe%C4%8Dnost-ICT-a-ochrana-dat-studijn%C3%AD-text.pdf.

7. KOLOUCH, Jan. *CyberCrime.* Praha : CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7.

8. incident, Kybernetická bezpečnostní událost a kybernetický bezpečnostní. Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident, § 7 odst. (1) (2). *Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů.* 2014.

9. JIRÁSEK, Petr, NOVÁK Luděk a POŽÁR Josef. *Výkladový slovník kybernetické bezpečnosti. Třetí doplněné a upravené vydání.* Praha : Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

10. HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce. 5., aktualiz. vyd.* Brno : Computer Press, 2011. ISBN 978-80-251-3176-3.

11. KUROSE, James F. a Keith W. ROSS. *Počítačové sítě.* Brno : Computer Press, 2014. ISBN 978-80-251-3825-0.

12. MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. *Hacking bez záhad.* Praha. Grada, 2007. ISBN 978-80-247-1502-5.

13. SELECKÝ, Matúš. *Penetrační testy a exploitace.* Brno : Computer Press, 2012. ISBN 978-80-251-3752-9.
14. PUŽMANOVÁ, Rita. *TCP/IP v kostce.* České Budějovice : Kopp, 2004. ISBN 80-723-2236-2.
15. KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP asystémem DNS. 5., aktualiz. vyd.* Brno : Computer press, 2008. ISBN 978-80-251-2236-5.
16. DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat.* Brno : Computer Press, 2004. ISBN 8025101061.
17. PETERKA, Jiří. Terminologie datových sítí. *Archiv článků a přednášek Jiřího Peterky.* [Online] [Citace: 18. 01 2019.] http://www.earchiv.cz/b00/b0003002.php3.
18. BOUŠKA, Petr. VPN 1 - IPsec VPN a Cisco. *SAMURAJ-cz.com - počítačové sítě, Cisco, Microsoft, VMware, administrace.* [Online] [Citace: 05. 01 2019.] https://www.samuraj-cz.com/clanek/vpn-1-ipsec-vpn-a-cisco/.
19. HNÍK, V., KRULÍK, O., STAŇOVÁ, E. Základní definice, vztahující se k tématu kybernetické bezpečnosti. *Dokumenty - kybernetické hrozby.* [Online] 2009. https://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx.
20. HOUSER, Robert. Priority bezpečnostní politiky v malých a středních firmách. *SystemOnLine.* [Online] [Citace: 14. 08 2018.] https://www.systemonline.cz/it-security/priority-bezpecnostni-politiky-v-malych-a-strednich-firmach.htm.
21. Největší bezpečnostní hrozbou jsou stále lidé. [Online] 06. 11 2018. https://www.braveshow.tv/cs/926314282/nejvetsi-bezpecnostni-hrozbou-jsou-stale-lide.
22. Cragg, Oliver. Beware! New Play Store scam uses Google's own pop-ups to steal money. *Android Authority.* [Online] 29. 03 2018. https://www.androidauthority.com/play-store-scam-game-pop-up-850595/?utm_source=feedly&utm_medium=webfeeds#c4ca4/.
23. Bezpečnostní chyby, se kterými se potýkají bezpečnostní odborníci. *SOCA blog - Blog o ICT bezpečnosti, které se nemusíte bát.* [Online] 04. 12 2017. https://www.soca.cz/blog/article/bezpecnostni-chyby-se-kterymi-se-potykaji-bezpecnostni-odbornici-314.
24. Jak na bezpečné heslo? Nejčastější chyby, které zřejmě děláte také. *Kvalitní internet.* [Online] 02. 09 2018. https://kvalitni-internet.cz/jak-na-bezpecne-heslo-nejcastejsi-chyby-ktere-zrejme-delate-take.

25. 8 bezpečnostních chyb, kterých se možná dopouštíte. *Antivirové centrum.* [Online] 04.07. 2017. https://www.antivirovecentrum.cz/aktuality/8-bezpecnostnich-chyb-kterych-se-mozna-dopoustite.aspx.
26. GÁLA, Libor, Jan POUR a Prokop TOMAN. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi, technologie informačních systémů, řízení a rozvoj podnikové informatiky.* Praha : Grada, 2006. ISBN 80-247-1278-4.
27. Secure Sockets Layer/Transport Layer Security. *IBM Knowledge Center.* [Online] https://www.ibm.com/support/knowledgecenter/cs/ssw_ibm_i_73/rzain/rzainoverview.htm
28. Několik poznámek k heslům - Zdroják. *zdroják.cz.* [Online] [Citace: 03. 02 2019.] https://www.zdrojak.cz/clanky/nekolik-poznamek-k-heslum/.
29. Změna hashování existujících hesel. *Michal Špaček.* [Online] [Citace: 15. 02 2019.] https://www.michalspacek.cz/zmena-hashovani-existujicich-hesel.
30. Čermák, Miroslav. Základy kryptografie pro manažery: PBKDF2. *Clever And Smart.* [Online] https://www.cleverandsmart.cz/zaklady-kryptografie-pro-manazery-pbkdf2/.
31. Vrána, Jakub. PHP triky - Ukládání hesel bezpečně. [Online] https://php.vrana.cz/ukladani-hesel-bezpecne.php.
32. Co je to logování? *IT Slovník.cz.* [Online] https://it-slovnik.cz/pojem/logovani.
33. Krčmář, Petr. Fail2ban: konec hádání hesel na serveru. *Root.cz.* [Online] https://www.root.cz/clanky/fail2ban-konec-hadani-hesel-na-serveru/.
34. HÜBNER, Miroslav, Zdeněk KAPLAN a Vlastimil ČEJP. *Trendy v architektuře IT: příručka manažera = IT architecture trends : manager's handbook.* Praha : TATE International, 2010. ISBN 978-80-86813-21-9.
35. Certificate Transparency je tu, všechny HTTPS certifikáty musejí být veřejné. *Root.cz.* [Online] https://www.root.cz/clanky/certificate-transparency-je-tu-vsechny-https-certifikaty-museji-byt-verejne/.
36. Ložkin, Sergej. Analýza rizik IT bezpečnosti. *SystemOnLine.* [Online] 03 2013. https://www.systemonline.cz/it-security/analyza-rizik-it-bezpecnosti.htm.
37. Informační společnost v číslech - 2018, Kapitola C Jednotlivci. *Český statistický úřad.* [Online] https://www.czso.cz/documents/10180/61601892/061004-18_C.pdf/d972dac5-2c5b-4330-9280-12e219604519?version=1.0.
38. PRO-CERT, s. r. o. Dotazník - PRO CERT. *PRO CERT.* [Online] http://www.pro-cert.cz/datab/2017210002-f25d_dotaznik_isms.doc.

39. Kubíčková, Ilona. Analýza rizik - základní dotazník pro vyhodnocení. *iT merit - konzultační firma v oblasti IT.* [Online] 08. 06 2016. http://itmerit.cz/dotaznik/.
40. SVATOŠOVÁ, Libuše, KÁBA, Bohumil. *Statistické metody II.* Praha : Česká zemědělská univerzita v Praze, Provozně ekonomická fakulta, 2008.
41. FAQ Stem. *Stem.cz Empirický výzkum pro fungující demokracii.* [Online] https://www.stem.cz/o-nas/faq/.
42. Je 1000 respondentů dost? - Centrum pro výzkum veřejného mínění. *Centrum pro výzkum veřejného mínění.* [Online] https://cvvm.soc.cas.cz/cz/caste-dotazy/4577-je-1000-respondentu-dost.
43. doc. Ing. Mgr. Radim Bačuvčík, Ph.D. Jak na marketingové průzkumy. *https://bacuvcik.webnode.cz/.* [Online] https://bacuvcik.webnode.cz/news/jak-na-marketingove-pruzkumy/.
44. Demografie - Revue pro výzkum populačního vývoje. *Český statistický úřad.* [Online] https://www.czso.cz/csu/czso/63002f6550.
45. Hermann, Jan. factum_invenio_jan_hermann_Kriticke_body_kvant_vyzkumu. *ihned.cz.* [Online] https://download.ihned.cz/download/marketing-trend/factum_invenio_jan_hermann_Kriticke_body_kvant_vyzkumu.pdf.
46. Mgr. František Korbel, Ph.D. Ne-odpovědnost poskytovatelů služeb informační společnosti v digitálním světě. *Právní prostor.* [Online] https://www.pravniprostor.cz/clanky/pravo-it/ne-odpovednost-poskytovatelu-sluzeb-informacni-spolecnosti-v-digitalnim-svete.
47. Desatero omylů: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů.* [Online] https://www.uoou.cz/desatero-omylu/ds-4818/p1=4818.
48. Mýty o GDPR: Šifrování osobních údajů je povinné. *Podnikatel.cz.* [Online] 27. 06 2018. https://www.podnikatel.cz/clanky/myty-o-gdpr-sifrovani-osobnich-udaju-je-povinne/.
49. Slouka, David. GDPR vzor: Jak vyžádat své osobní údaje od firem v Evropské unii. [Online] 24. 05 2018. https://insmart.cz/jak-vyzadat-sve-osobni-informace-od-firem-v-eu/.

8 Přílohy

Příloha č. 1 Český vzor žádosti o zaslání kopie ukládaných dat v souladu s GDPR

Příloha č. 2 Dotazník

Příloha č. 3 Grafické zobrazení výsledků šetření

Příloha č. 4 Způsob ukládání uživatelských hesel – kompletní hodnocení firem

Příloha č. 1: Český vzor žádosti o zaslání kopie ukládaných dat v souladu s GDPR

Vážená paní, vážený pane,

v souladu s čl. 15 Obecného nařízení o ochraně osobních údajů (GDPR) Vás žádám o následující informace o zpracování osobních údajů, které o mně jako zpracovatel osobních údajů sbíráte a/nebo ukládáte.

Pokud osobní údaje skutečně zpracováváte a/nebo ukládáte, zašlete mi prosím následující informace:

- Účel jejich zpracování a archivace.
- Kategorie osobních dat, kterých se zpracovávání a archivace týká.
- Třetí strany, kterým budou nebo mohou být osobní údaje poskytnuty.
- Je-li to možné, pak předpokládanou dobu, po kterou bude informace archivovány.
- Odkud jsou má data získávána a informace o těchto zdrojích.

Zároveň žádám o kopii veškerých o mně zpracovávaných osobních údajů.

Vyžadujete-li ode mě další informace, dejte mi prosím vědět co nejdříve. Právo na obdržení výše vypsaných informací ve standardizované podobě mám do 30 dnů od obdržení žádosti.

Nezpracováváte-li tyto informace Vy nebo Vaše oddělení, zašlete prosím tento text pracovníkovi zodpovědnému za ochranu osobních údajů ve firmě. Kontaktovat mne můžete na e-mailu, mobilním telefonu nebo poštou. Preferovanou metodou je e-mail.

S pozdravem

POPDIS (ideálně, avšak pravděpodobně se bez něj obejdete)

JMÉNO
ADRESA
TELEFONNÍ ČÍSLO (včetně předvolby)
E-MAILOVÁ ADRESA

Příloha č. 2: Dotazník

Přihlašovací hesla

Tento dotazník je anonymní a slouží k průzkumu v rámci mé diplomové práce na téma Ochrana dat a rizika bezpečnostních incidentů. Získaná data budou použita jen v agregované formě a na základě vyhodnocení dotazníku budou vyvozena doporučení. Záměrem těchto doporučení bude přispět k informovanosti a zlepšení ochrany dat.

*Povinné pole

1. **Kolik je Vám let?** *
   Označte jen jednu elipsu.
   - 19-26
   - 27-34
   - 35-42
   - 43-50
   - 51 a více

2. **V jakém oboru pracujete?** *
   Označte jen jednu elipsu.
   - Informatika
   - Jiný technický obor
   - Služby
   - Administrativa
   - Jiné

3. **Používáte rozdílné přihlašovací heslo do každé důležité aplikace?** *
   Označte jen jednu elipsu.
   - Ano
   - Ne
   - Nechci odpovídat

4. **Používáte password manager (správce hesel)?** *
   Označte jen jednu elipsu.
   - Ano
   - Ne
   - Nevím, co je password manager
   - Nechci odpovídat

5. **Pokud jste odpověděli ne, z jakého důvodu password manager nepoužíváte?**
   Označte jen jednu elipsu.
   - Považují to za zbytečné
   - Nedůvěřuji mu
   - Neumím ho používat
   - Nechci odpovídat

6. **Používáte při přihlašování do služeb vícefaktorovou autentizaci?** *
Označte jen jednu elipsu.

- Ano,pokud je k dispozici
- Ne
- Nevím,co je vícefaktorová autentizace
- Nechci odpovídat

7. **Obdrželi jste někdy emailem své vlastní heslo v čitelné podobě (např. při obnovení hesla u některé služby)?** *
Označte jen jednu elipsu.

- Ano
- Ne
- Nechci odpovídat

8. **Stali jste se někdy obětí úniku dat, konkrétně Vašich hesel?** *
Označte jen jednu elipsu.

- Ano
- Ne
- Nevím
- Nechci odpovídat

9. **Pokud byste se dozvěděli, že Vaše hesla z některé služby unikla, používali byste službu dál?** *
Označte jen jednu elipsu.

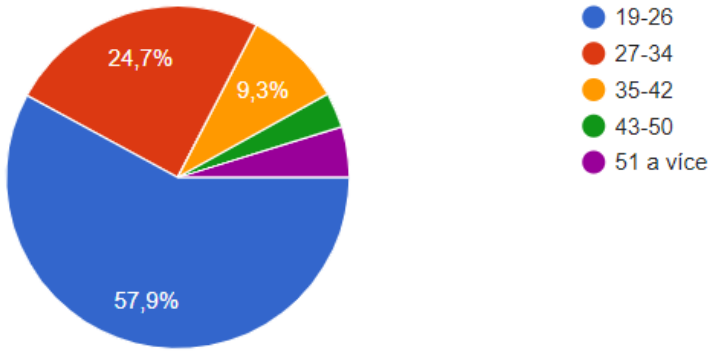
- Ano
- Ne
- V závislosti na mé újmě
- Nechci odpovídat

Příloha č. 3: Grafické zobrazení výsledků šetření

1403 odpovědí

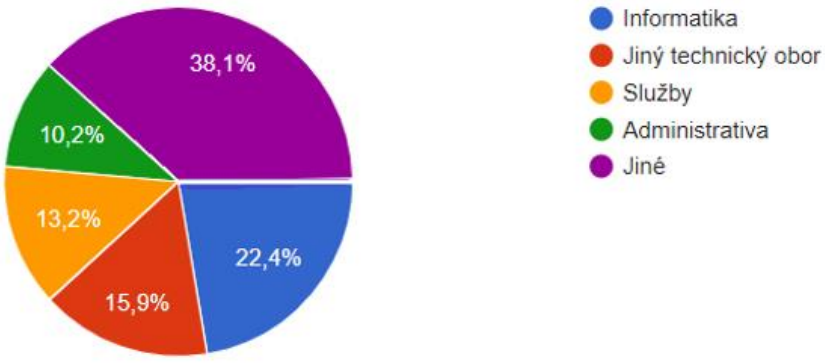
Kolik je Vám let?

1403 odpovědí



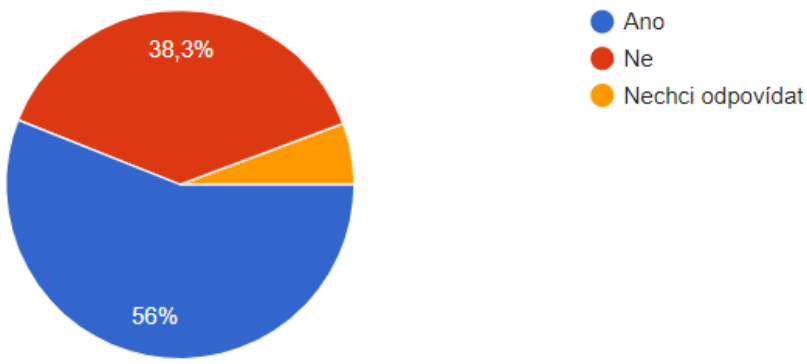
V jakém oboru pracujete?

1403 odpovědí



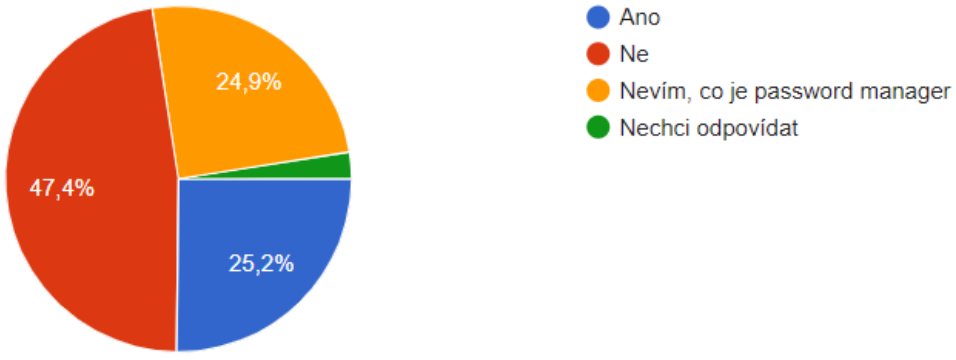
Používáte rozdílné přihlašovací heslo do každé důležité aplikace?

1403 odpovědí



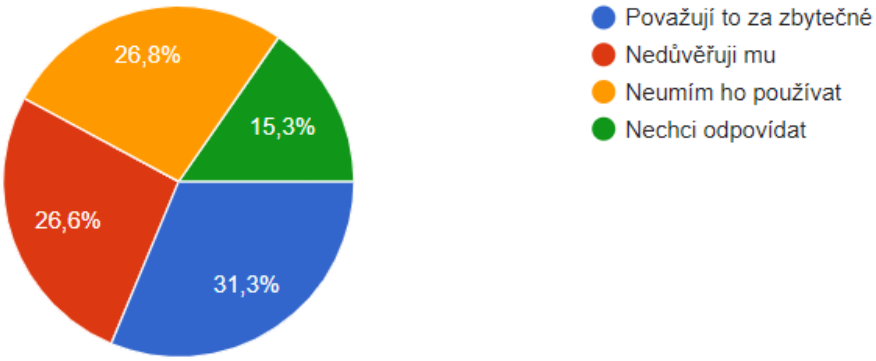
Používáte password manager (správce hesel)?

1403 odpovědí



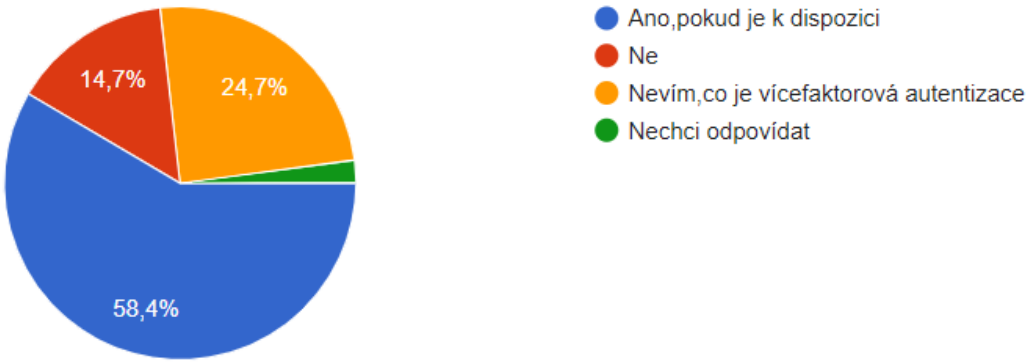
Pokud jste odpověděli ne, z jakého důvodu password manager nepoužíváte?

665 odpovědí



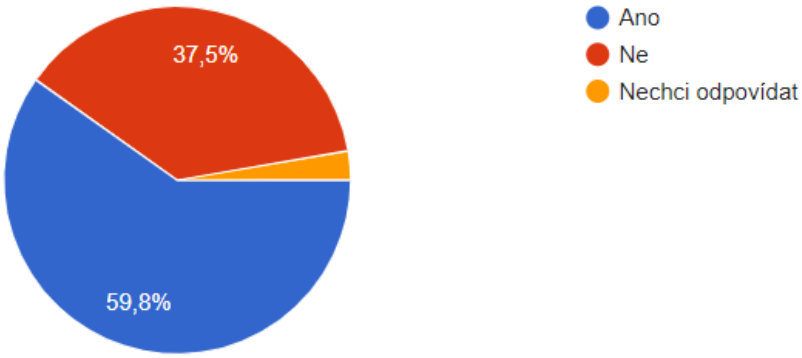
Používáte při přihlašování do služeb vícefaktorovou autentizaci?

1403 odpovědí



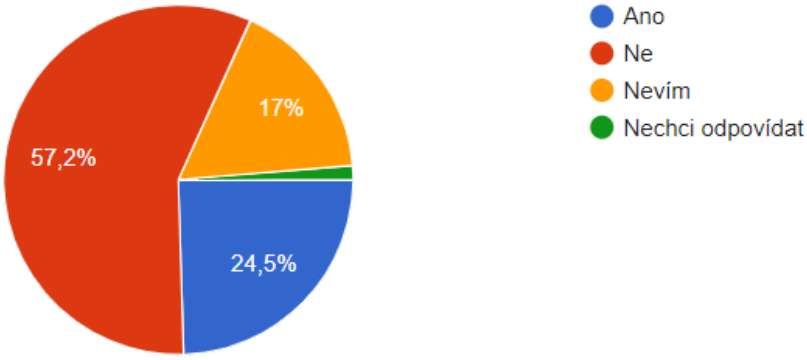
Obdrželi jste někdy emailem své vlastní heslo v čitelné podobě (např. při obnovení hesla u některé služby)?

1403 odpovědí



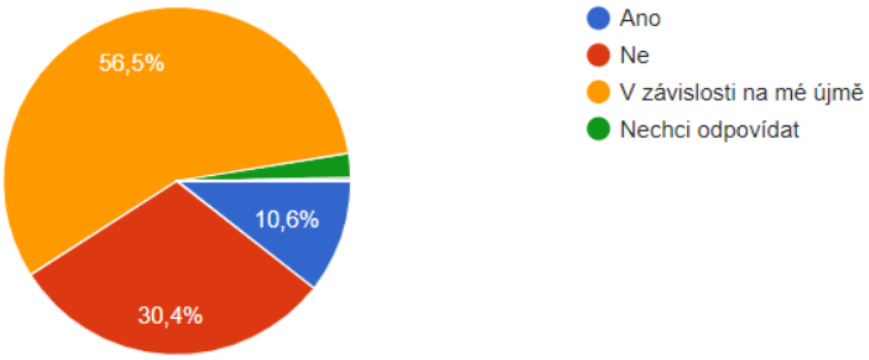
Stali jste se někdy obětí úniku dat, konkrétně Vašich hesel?

1403 odpovědí



Pokud byste se dozvěděli, že Vaše hesla z některé služby unikla, používali byste službu dál?

1403 odpovědí



Příloha č. 4

Způsob ukládání uživatelských hesel - kompletní hodnocení firem					
company	**web**	**rating**	**date**	**progress**	**notes**
ABCSPORT.CZ (LERKO SPORT, s.r.o.)	www.abcsport.cz	F	Aug 2016		bez reakce
Adafruit Industries, LLC	accounts.adafruit.com	B	Nov 2016		
AdGuard Software Limited	adguard.com	B	Sep 2018		
Adveri s.r.o.	www.happyfeed.com	D	Oct 2016		**zrušená registrace / není ukládání hesel**
Affectio s.r.o.	www.mimibazar.cz	F	Oct 2016		bez reakce
Alza.cz a.s.	www.alza.cz	A	Feb 2019		
	www.alza.sk				
	www.alza.at				
	www.alzashop.com				
	www.alza.de				
	www.alza.hu				
	www.alza.co.uk				
Apiary Inc.	apiary.io	A	Sep 2016		
Atlassian Pty Ltd	www.hipchat.com	B	Apr 2017		

Autoklub České republiky	is.autoklub.cz	A	Dec 2018		
Avocode, Inc.	manager.avocode.com	B	Jul 2017		
Behej.com, s.r.o.	www.behej.com	F	Apr 2018		bez reakce
	www.triatlony.com				
	www.bezkuj.com				
BetaNews, Inc.	fileforum.betanews.com	F	Mar 2018		bez reakce
bezrealitky.cz (Pricetown, s. r. o.)	www.bezrealitky.cz	A	Oct 2016		
BLINNKER (BLINNKER ONLINE LLP)	www.blinnker.com	B	Sep 2016		
Castle (Castle Intelligence, Inc.)	castle.io	B	Dec 2013		
CertSimple Limited	certsimple.com	A	Aug 2016		
České dráhy, a.s.	moje.inkarta.cz	F	Jan 2017	**beze změny**	e-mail
Český svaz kanoistiky na divokých vodách	www.kanoe.cz/prihlaskycsk	A	Mar 2018		
Collabim s.r.o.	www.collabim.cz	A	May 2018		
CZ.NIC, z. s. p. o.	www.mojeid.cz	A	Jul 2018		
CZC.cz s.r.o.	www.czc.cz	B	Dec 2018		
Czech Airlines (České aerolinie a.s.)	www.csa.cz	F	Jan 2017		bez reakce

Datadog, Inc.	app.datadoghq.com	B	Jul 2016		
Deliveroo (Roofoods Limited)	deliveroo.co.uk	B	Sep 2017		
DNSimple (Aetrion LLC)	dnsimple.com	B	Sep 2015		
Dropbox, Inc.	www.dropbox.com	B	Sep 2016		
Economia, a.s.	ihned.cz	A	May 2018		
	www.centrum.cz	A	Jun 2018		
eD' system Czech, a.s.	edshop.edsystem.cz	F	Sep 2017		komentář na sociální síti - reagovali, v řešení
eD' system Slovakia, s.r.o.	www.edsystem.sk	F	Sep 2017		koment fcb
Edmodo, Inc.	www.edmodo.com	B	May 2017		
eLens s.r.o.	www.cockyshop.cz	A	Dec 2017		
ePojisteni.cz, s.r.o.	www.epojisteni.cz	F	Jul 2016	**nechtějí uvést**	e-mail
Event Service, s.r.o.	int.tymuj.cz	F	Aug 2017	**Bcrypt - B**	**info přidáno do FAQ, zn. B**
Facebook, Inc.	www.facebook.com	B	Dec 2014		
Fakturoid s.r.o.	app.fakturoid.cz	A	Sep 2016		
Flexiana s.r.o.	all sites	B	Oct 2016		
FORPSI (INTERNET CZ, a. s.)	www.forpsi.com	F	Aug 2014		bez reakce
Foursquare (Foursquare Labs, Inc.)	foursquare.com	B	Jul 2011		

fruux GmbH	fruux.com	B	Sep 2012		
Geckoboard (Datachoice Solutions Ltd.)	app.geckoboard.com	A	Dec 2017		
Gigaprint.cz (Cetria s.r.o.)	www.gigaprint.cz	F	Feb 2018		bez reakce
Gigaprint.sk, s. r. o.	www.gigaprint.sk	F	Feb 2018		bez reakce
GitHub, Inc.	github.com	A	May 2018		
goodooga s.r.o.	www.nevyhazujto.cz	E	Feb 2018		bez reakce
	praho.nevyhazujto.cz				
Harvest (Iridesco, LLC)	id.getharvest.com	B	Feb 2015		
Hotjar Ltd.	insights.hotjar.com	A	May 2018		
HumboldTec spol. s r.o.	jabb.im	A	Aug 2017		
ICE invest spol. s r. o.	www.veselekostky.cz	F	Mar 2018	**nechtějí uvést**	tech - komentář na sociální síti
Imgur, Inc.	imgur.com	B	Nov 2017		
Ing. Tomáš Petruška	www.zaluzie24.eu	F	Aug 2017		bez reakce
Institut pro podporu elektronizace zdravotnictví, z. ú.	portal.zdravel.cz	B	Jan 2018		
Internet Info, s.r.o.	all sites	D	Oct 2016		bez reakce
Jabber.org	www.jabber.org	F	Aug 2012		tech - US, e-mail - reagovali, v řešení
Keboola s.r.o.	connection.keboola.com	A	Apr 2016		

KeyMaker s.r.o.	www.cereal.cz	A	Oct 2016		
Kuma.cz s.r.o.	www.kuma.cz	E	Jul 2018		bez reakce
Lagardere Travel Retail a.s.	www.paul-cz.com	A	Sep 2018		
Lagoon Foto, a.s.	www.lagoonfoto.cz	F	Oct 2016		bez reakce
Leader Fox (BOHEMIA BIKE a.s.)	e-shop.leaderfox.com	E	Feb 2018		bez reakce
	e-shop.leaderfox.cz				
LidskáSíla s.r.o.	lidskasila.cz	B	Oct 2016		
Linode, LLC	manager.linode.com	B	Feb 2016		
LMC s.r.o.	my.teamio.com/recruit	A	Aug 2018		
MAFRA, a.s.	www.aaapoptavka.cz	F	Oct 2016	**B**	Apr 2018
MALL.CZ (Internet Mall, a.s.)	www.mall.cz	B	Aug 2017		
Maneo, s.r.o.	www.eshop.maneo.cz	F	Sep 2017		bez reakce
Marek Demčák	www.vyplnto.cz	A	Mar 2017		
Martin Bárta	fitkram.cz	B	Oct 2016		
Maternia, s.r.o.	all sites	A	Dec 2018		
MEGAPIXEL s.r.o.	www.megapixel.cz	A	Dec 2017		
Městská část Praha 8	www.praha8.cz	F	Oct 2018		bez reakce

MEWS (MEWS SYSTEMS, s.r.o.)	www.mews.li	A	Sep 2017		
Mojevideo.sk, s.r.o.	www.mojevideo.sk	F	Jan 2017		bez reakce
MUNAP COMPANY, s.r.o.	www.munap.cz	F	Sep 2017		bez reakce
MyFitnessPal, Inc.	www.myfitnesspal.com	A	Mar 2018		
mySupermarket Limited	www.mysupermarket.co.uk	E	Jun 2015		bez reakce
NameMC	namemc.com	B	May 2018		
NWT a.s.	www.patro.cz	F	Feb 2018		bez reakce
OldanyGroup s.r.o.	frekr.me	A	Oct 2016		
Pantone LLC	www.pantone.com	F	Mar 2018		bez reakce
Pavel Pola	www.paladix.cz	F	Oct 2016		bez reakce
Peerio (Technologies Peerio Inc.)	www.peerio.com	A	Jul 2016		
Peerlyst, Inc.	www.peerlyst.com	B	Aug 2016		
Petr Kletečka	zonglovani.info	A	Mar 2018		
Planet Express Shipping LLC	app.planetexpress.com	A	Apr 2018		
POLET, s. r. o.	exon.io	B	Oct 2016		
Privacy (Pay With Privacy, Inc.)	privacy.com	A	Aug 2017		
PROLDEN Solution s.r.o.	www.livechat.cz	A	Feb 2018		

PRONETmedia, s.r.o.	www.pay4t.cz	D	Sep 2014		bez reakce
Queens Store s.r.o.	www.queens.cz	A	Jan 2018		
Quora, Inc.	www.quora.com	B	Dec 2018		
Reddit, Inc.	www.reddit.com	B	Oct 2011		
Retino.cz s.r.o.	app.retino.io	A	Nov 2017		
Scott Helme	report-uri.io	A	May 2015		
Shipito LLC	www.shipito.com	B	Sep 2016		
Shoptec.sk (Webtec s.r.o.)	all sites	A	Dec 2017		
Simplia, s.r.o.	all sites	B	Jun 2014		
Single Case, s.r.o.	www.singlecase.cz	A	Mar 2018		
Skrz.cz s.r.o.	skrz.cz	B	Sep 2016		
Slack (Slack Technologies, Inc.)	slack.com	B	Mar 2015		
Slacker, Inc.	account.slacker.com	B	Oct 2017		
Slevomat.cz, s.r.o.	www.slevomat.cz	A	Feb 2018		
	www.zlavomat.sk				
Solium (Solium Capital Inc.)	shareworks.solium.com	B	May 2016		
Spotreba.sk, s. r. o.	www.spotreba.sk	E	Sep 2016		bez reakce
SYSYstems, s.r.o.	www.webalert.cz	B	Jul 2018		

TANGER infosystems s.r.o.	www.seznamka.cz	F	Jan 2018		bez reakce
Technimax s.r.o.	www.technimax.cz	B	Sep 2019		
Tereza Miklová	delid.cz	A	Jul 2018		
Twitter, Inc.	twitter.com	A	May 2018		
Uloženka s.r.o.	partner.ulozenka.cz	A	Nov 2016		
Váš Hosting s.r.o.	www.freelo.cz	A	Oct 2016		
Veřejná informační služba, spol s.r.o.	www.strava.cz	F	Aug 2017	**nechtějí uvést**	komentář na sociální síti
Web4U s.r.o.	www.web4u.cz	B	Aug 2016		
WebDeal s.r.o.	www.copywriting.cz	B	Dec 2017		
Webfarm s.r.o.	www.cars.cz	F	Jun 2018		bez reakce
WEDOS (WEDOS Internet, a.s.)	hosting.wedos.com	D	Nov 2016		bez reakce
Weebly, Inc.	www.weebly.com	A	Oct 2016		
Xzone, s.r.o.	www.xzone.cz	B	Oct 2017		
Yahoo! Inc.	login.yahoo.com	A	Dec 2016		
Zapier, Inc.	zapier.com	A	Jun 2018		
Zee Source, Inc.	www.zeemaps.com	A	Jul 2018		
Zonky s.r.o.	app.zonky.cz	B	Sep 2017		