Bezpečnost dat ve firemní síti

Daniel Vašinka

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Daniel Vašinka**
Osobní číslo:	**A14295**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Bezpečnost dat ve firemní síti**
Téma anglicky:	**Data Security in Company Networks**

Zásady pro vypracování:

1. **Popište základní pojmy v oblasti bezpečnosti dat.**
2. **Popište aktuální hrozby a možnost ochrany před nimi (zálohování, šifrování, ...).**
3. **Zhodnoťte současný stav na poli nástrojů pro ochranu dat, zaměřte se na malé a střední firmy.**
4. **Na základě vyhodnocení současného stavu, vytvořte modelový příklad užití těchto nástrojů.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **JAŠEK, Roman a David MALANÍK. Bezpečnost informačních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj. ISBN 978-80-7454-312-8.**
2. **LUDVÍK, Miroslav a Bohumír ŠTĚDROŇ. Teorie bezpečnosti počítačových sítí.Vyd.1.Kralice na Hané: Computer Media, 2008, 98 s. ISBN 978-80-86686-35-6.**
3. **MAREK, ŠIMČÍK. Technologie datové bezpečnosti vnitřních sítí [online]. Zlín, 2008 [cit. 2017-11-19]. Dostupné z: https://digilib.k.utb.cz/handle/10563/6893.Univerzita Tomáše Bati ve Zlíně.**
4. **SZOR, Peter. Počítačové viry: analýza útoku a obrana. Vyd. 1. Brno: Zoner Press, 2006, 608 s. Encyklopedie Zoner Press. ISBN 80-86815-04-8.**
5. **MACÁK, Petr. Kritéria výběru software pro malé a středně velké společnosti. Systémová integrace, 2011, ročník 18, číslo 1, str. 121-133, ISSN 1210-9479.**

Vedoucí bakalářské práce: **Ing. Lukáš Králík**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **12. prosince 2017**

Termín odevzdání bakalářské práce: **24. května 2018**

Ve Zlíně dne 12. prosince 2017

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

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 23. 5. 2018

.....
podpis diplomanta

ABSTRAKT

V teoretické části se práce zabývá základními pojmy v oblasti bezpečnosti dat a popisuje aktuální hrozby a možnosti ochrany před těmito hrozbami jako je šifrování, zálohování nebo bezpečnostní politika. V praktické části se práce věnuje analýzou současného stavu nástrojů pro ochranu dat se zaměřením na malé a střední firmy. Na základě této analýzy je provedeno vyhodnocení současného stavu v těchto firmách a proveden modelový příklad užití nástrojů pro ochranu dat.

Klíčová slova:

bezpečnost dat, šifrování, zálohování, bezpečnostní politika, škodlivý software

ABSTRACT

In the theoretical part, the thesis deals with basic concepts in the field of data security and describes current threats and possibilities of protection against these threats, such as encryption, backup or security policy. In the practical part the thesis deals with the analysis of the current state of data protection tools focusing on small and medium-sized companies. Based on this analysis, an evaluation of the current situation in thesee companies is carried out and a model example of the use of data protection tools has been carried out.

Keywords:

data security, encryption, backup, security policy, malicious software

Rád bych poděkoval za odborné vedení, čas, rady a trpělivost při zpracování této bakalářské práce, panu Ing. Lukáši Králíkovi. Dále bych chtěl poděkovat své rodině, přátelům a své přítelkyni za podporu a pomoc při tvorbě této práce.

OBSAH

ÚVOD

V dnešní době se staly počítače nedílnou součástí života mnoha lidí, kteří na počítačích tráví i většinu svého všedního dne. Počítače nám usnadňují denní práci jak v osobním, tak pracovním životě, pomáhají nám ukládat naše data, která jsou pro nás velice důležitá a je třeba je chránit. Ochrana dat je čím dál tím aktuálnější téma, s vývojem výpočetní techniky se také vyvíjí hrozby, které naše data mohou ohrožovat.

Tato práce se zaměřuje především na ochranu dat v malých firemních sítích, kde mají ukládaná data velkou business hodnotu pro společnost a je třeba je také adekvátně chránit. Mnoho uživatelů či pracovníků ve firmách, kteří se setkávají při práci s počítači, často ani nevědí, jaké hrozby by mohli jejich data poškodit, či odcizit jejich data. Obyčejní uživatelé s omezenými vědomosti a zkušenosti v dané problematice, nemají proti zkušeným útočníkům mnohdy šanci a mnohdy přijdou zbytečně o firemní data a firma následně o své důvěrné obchodní data.

V této práci bych rád popsal a informoval o aktuálních hrozbách, které mohou tyto firmy a pracovníky těchto firem ohrozit. Také jak se proti těmto hrozbám přistupovat pomocí preventivních opatření ať už na fyzické, hardwarové či softwarové úrovni. Dále bych chtěl poukázat na možnosti zálohování a šifrování dat.

Mým cílem je v této práci zhodnotit současný stav na poli nástrojů na ochranu dat se zaměřením na malé podniky a firmy. Na základě tohoto vyhodnocení současného stavu, vytvořit modelový příklad užití těchto nástrojů pro běžné uživatel.

I. TEORETICKÁ ČÁST

1 DATA

Pojem data je velice široký pojem, který se nachází v mnoha oblastech všedního světa jako například (znalosti, vědomosti, atd.), která jsou vedena v tištěné formě (učebnice, kniha, atd.). V informatice lze data popsat jako informace, které jsou převedeny do vhodné digitální podoby pro lepší přenos a zpracování počítačem. V počítačové terminologii jsou data posloupnost bitů, která jsou počítačem rychleji zpracovávána, a je jim udělena nějaká činnost (ukládání, adresování, indexace, atd.).

1.1 Data ve firemní sféře

Data v digitální podobě mají v dnešní době velký význam pro rychlejší běh všech operací v různých odvětvích. Napomáhají ukládat naše zkušenosti, vědomosti, vzpomínky, ale také tyto data sdílet pomocí internetu. S tím přicházejí rizika, která data je vhodné sdílet a která naopak chránit a jakým způsobem je chránit. Pro firmy mají tyto data především business hodnotu, to znamená, že jsou zdrojem informací, s kterými firmy hospodaří. Proto cílem každého podniku musí být zachování bezpečnosti těchto dat.

1.2 Proč data chránit

Data jako taková mohou obsahovat veškeré citlivé informace, které by mohl někdo zneužít. Digitalizace dat sice přináší větší komfortnost, že veškeré operace můžeme dělat z pohodlí domova na počítači či mobilním zařízení ale s tím přichází i o to větší rizika. Data jako datum narození, číslo bankovního účtu, adresa bydliště, apod., jsou uloženy někde na nějakém serveru ať už v bance, pojišťovně nebo úřadě. Tyto data musí být dostatečně chráněna, aby bylo zachováno bezpečí peněz, soukromí a identity.

1.3 Jak data chránit

Dnešní doba přináší mnohem složitější a komplexnější hrozby, které mohou ohrozit firemní data. Naneštěstí existuji i komplexní metody, jak se proti těmto hrozbám chránit. Existuje řada možností, jak se chránit, ne však všechna jsou dostačující a kvalitní. Tyto typy ochrany dat lze rozdělit do několika kategorií. Ochraně dat je dále věnována samostatná kapitola.

2 SOUČASNÉ BEZPEČNOSTÍ HROZBY

S rostoucí bezpečností v informační sféře roste exponenciálně také míra nebezpečí, jak tyto bezpečností prvky překonat a zneužít firemní data uživatelů. Jedná se především o škodlivý software neboli viry.

2.1 Počítačový virus

Je v počítačové terminologii kód nebo škodlivý software, který má za úkol vniknout do koncového zařízení uživatele (PC, nootebook, mobil, atd.) a spustit se bez svolení uživatele. Viry jsou navrženy tak, aby získaly kontrolu nad operačním systémem a prováděly škodlivé a nežádoucí úkony. Dnešní doba přináší rozvoj těchto počítačových virů, které jsou při podcenění počítačové ochrany velice škodlivé.[1]

2.1.1 Malware

Velkou skupinou je tzv. Malware, který je typem škodlivého kódu nebo programu, který po vniknutí do uživatelského zařízení zajistí útočníkovi přístup do systému bez vědomí uživatele. Malware se šíří nejčastěji na internetu (webové stránky, multimediální soubory, zkušební verze, atd.) či pomocí emailových zpráv. Nejrizikovější zařízení, která jsou ohrožena, jsou právě ty bez antivirové ochrany.

Nejúčinnější ochranou proti Malware je antivirový a antimalwerový software s aktuální virovou databází a také vyvarování se otevírání různých příloh v emailu od neznámých odesilatelů. [1]

2.1.2 Nejrozšířenější Malware

Spyware

Je speciální typ Malweru, který je v systému uživatele těžce odhalitelné a to mu dává výhodu, že bez vědomí uživatele dokáže sbírat jeho důvěrné informace o pohybech na internetu (čísla účtu, čísla kreditních karet, hesla, atd.). Tyto nasbírané informace dokáže pak odesílat třetí straně.

Typickým příkladem je Keylogger, který dokáže zaznamenávat veškeré zadané znaky na klávesnici na uživatelském zařízení. [1]

Trojský kůň

Je počítačový typ viru, který se tváří, že uživateli přináší nějaký užitek např. v podobě programu či multimédia. Cílem tohoto škodlivého softwaru je však krádež dat nebo v horším případě způsobení značných škod v systému. [1]

Počítačový červ

Speciálním typem škodlivého programu je červ, který se dokáže sám šířit a množit a to především pomocí počítačové sítě nebo přenosovými medií. Červ nemá za úkol napadat soubory, ale šířit sebe sama a znemožnit nebo úplně přerušit chod zařízení. [1]

Rootkit

Je škodlivý kód, který byl vytvořen tak, aby dopomohl útočníkovi získat neomezený přístup k administrátorským právům zařízení. Jakmile se rootkit aplikuje, využívá systémové funkce ke svému zamaskování. V systému se může tvářit jako např. systémový soubor, složka nebo jako data v registru. Proto jsou velice těžké na odhalení. [2]

Ransomware

Škodlivý software, který když se dostane do systému uživatele, má za úkol omezit přístup k systému nebo datům uživatele. Za odměnu za znovu zpřístupnění dat si žádá zaplacení peněžní částky. V současnosti se za nejnebezpečnější druhy Ransomwaru považuji programy jako WannyCry, CryptoLocker nebo Locky. [1]

Phishing

Nejedná se o škodlivý software jako takový, ale o podvodný způsob získat citlivá data uživatelů pomocí falešných webových stránek. Uživateli přijde emailová zpráva, která se tváří jako z důvěryhodné adresy např. elektronické bankovnictví s odkazem na webové stránky. Uživatel je po rozkliknuti odkazu přesměrován na falešné webové stránky, které vypadají stejně jako ty pravé a v nevědomí zadá své přihlašovací údaje, které se odešlou útočníkovi. [1]

Pharming

Je obdobou Phishingu s rozdílem toho, že útočník v Domain Name System (DNS) tabulce uživatele změní adresu webové stránky např. elektronického bankovnictví, uživatel poté zadá webovou adresu své banky, ale je však přesměrován na falešné stránky, které jsou jen

napodobeninou. Uživatel poté zadá v nevědomí své přihlašovací údaje, které může poté útočník zneužít. [3]

Sociální inženýrství

Je metoda, která spoléhá na nejslabší článek v každém informačním systému a tím je lidský faktor. Techniky sociálního inženýrství jsou velice rozmanité a spoléhají na lidskou zvědavost, neopatrnost, závist či strach. Cílem je získat citlivá data či informace uživatelů, které jim sami bez vědomí nebo nechtěně poskytnou. Útočníci používají několik metod sociálního inženýrství například:

- Pretexting (útočník se vydává za někoho jiného s cílem získat informace uživatele).
- Scareware (pomocí falešného upozornění na nebezpečí škodlivým virem, doporučí instalaci antiviru, který infikuje následní zařízení uživatele).
- Phishing (získání citlivých dat uživatele pomocí podvodných webových stránek).
- Baiting (uživatel si místo svého hledaného multimediálního souboru např. filmu stáhne z internetu škodlivý software). [1]

3 OCHRANA DAT

Dnešní doba přináší pro naše data velká a komplexnější rizika a jenom kryptografii si již nevystačíme. Ve většině případů jsou data uložena v elektronické podobě na nějakém záznamovém mediu (pevný disk, flash disk, externí hardisk, atd.), avšak pomocí preventivních opatření můžeme naše data ochránit a předcházet rizikům jejich ztrátě.

3.1 Fyzická ochrana dat

Je jednou z nejpodstatnějších a prvotních úkolů při ochran dat, která zajišťuje, aby k našim datům neměla přístup neoprávněná osoba. Firemní data je také třeba chránit před přírodními živly a katastrofami, které by je mohli natrvalo poškodit.

3.1.1 Bezpečnostní přístup fyzických osob

V prvotním kroku ochrany dat je třeba definovat počet a konkrétní oprávněné osoby, které mají přístup k našim datům. Tento počet, by měl být co nejmenší, záleží však na důležitosti a míře rizikovosti našich dat.

V první řadě je třeba už při přístupu do budovy, či areálu kontrolovat identitu osob, které mají povolený přístup do areálu budovy a to například pomocí čipových karet, kamerového systému nebo ostrahy. Je prioritou zamezit přístupu neoprávněných osob do chráněné budovy. V dalším kroku je zajistit, abych k našim záznamovým médiím, měli přístup jen oprávněné a předem definované osoby. Data uložena na pevných discích jsou ve většině případů uložena v počítačových skříních, avšak do těchto skříni se lze snadno dostat pomocí obyčejného šroubováku. Proto je vhodné naše nejdůležitější data, například uložena na serveru, ukládat zvlášť do uzamčené místnosti, která může být bez oken, chráněna kamerovým systémem a přístup lze může být zajištěn například pomoci biometrické autentizace či pomocí čipové karty. [4]

3.1.2 Ochrana před přírodními katastrofami

Jedná se o oblast bezpečnosti, kterou nemůžeme nikdy předem přesně předvídat a tak abychom naše data naplno ochránili. Proto je třeba se pomocí preventivních opatření, tento dopad škod, co nejvíce minimalizovat.

Ochrana proti požáru je spojena s pojmem protipožární ochrana, která by měla být nedílnou a nutnou součástí každé organizace. Požár je velice zničující, ať už jde o jakékoliv zařízení a v případě výpočetní techniky tomu není jinak. Proto by každá

společnosti či organizace měla mít prostory chráněny alespoň základními protipožárními prvky, jakou jsou například detektory kouře, požární hlásiče, hasící práškové přístroje, atd. V neposlední řadě by chráněné místnosti neměly obsahovat prvky, které by požár ještě více rozšířily. Důležitá data, která by měly být chráněna, musí být uložena v prostorech s vysokou protipožární ochranou.

Ochrana proti vodě je spojena asi v nejčastějších případech s povodněmi nebo technickou závadou na vodovodní síti. Nejdůležitější opatřeni v tomto případě je asi umístění záznamových medii do vyšších pater, která budou částečně chráněna před povodněmi. Avšak je třeba také počítat s následnou a možnou vlhkostí, která je také velice zničující pro veškerou výpočetní techniku v tomto případě mohou pomoci opatření jako čističky proti vlhkosti vzduchu nebo klimatizace s filtrovacím zařízením.

Zemětřesení a špatný technický stav budovy tento problém ochrany se spíše týká zemí, které jsou tímto životním živlem postihovány a kde hrozí poškození nebo v horších případech zhroucení budovy. Proto by měly být disky s daty, chráněny v pevných skříních a obalech proti odolnosti prachu. [4]

3.1.3 Přerušení dodávky energie

Do skupiny fyzické ochrany dat lze taky zahrnout ochranu před výpadkem, anebo před přepětím elektrického proudu v elektrické síti. Většina nosičů dat, potřebuje ke své funkčnosti uchovávat eklektickou energii a v případě, kdy nastane odstávka elektrického proudu, nám slouží záložní napájecí zdroje neboli zdroj nepřerušovaného napájení (UPS) zařízení. Těmito zařízeními lze ochránit datová uložiště před dalšími vlivy, jako jsou například blackout, krátkodobý výpadek, napěťová špička, dlouhodobé přepětí, rušivý šum v elektrické síti, změna frekvence. [4]

Záložní napájecí zdroje lze rozdělit do dvou kategorií:

Záložní zdroj off-line je nejednoduší způsob, při výpadku elektrické energie. V případě výpadku, je schopen zahájit napájení, které vyrábí střídavý proud z akumulátoru. Pokud nastane v síti přepětí nebo podpětí, mohou některé dražší typy UPS tyto stavy vyrovnat, avšak jen na omezenou dobu, není to tedy dlouhotrvající řešení. [4]

U on-line zdroje je mnohem komplexnější a také mnohem finančně náročnější varianta. Používá se také v složitějších a náročnějších infrastrukturách, kde je potřeba neustálý provoz. Výhodou u těchto typů je ten, že je do nich stále veden vstupní proud a

tím nabijí zabudovaný akumulátor a z nich se měničem stále vyrábí výstupní napětí pro dané zařízení. Velkou výhodou je, že pří výpadku elektrické energie nepotřebuje žádný přechodový čas pro náhradní napájení. Dalším pozitivem je přesné výstupní napětí (hodnota, frekvence, tvar průběhu). [4]

3.2 Šifrování

Jedná se o zabezpečení dat pomocí šifer, touto disciplínou se zabývá vědní obor kryptologie, jenž obsahuje právě zmíněnou kryptografii a kryptoanalýzu. V principu jde o zašifrování dat pomocí určitých pravidel, čitelnou pouze pro majitele informace. Takto může vlastník tyto informace či data chránit před zneužitím. Šifry dělíme na dvě stěžejní oblasti a to symetrické a asymetrické šifrování.

3.2.1 Symetrické šifrování

Jsou to šifry, které pro zašifrování a odšifrování využívají totožné klíče. Už z principu vypovídá o výhodě těchto šifer a tím je velmi nízká náročnost na výpočetní výkon, tato výhoda vyplývá z jednoduchosti šifrovacích a dešifrovacích algoritmů daných šifer. Avšak tato výhoda je úzce spjata s největší nevýhodou těchto šifer, tím je nepříliš bezpečné předání šifrovacího klíče druhé straně a také samotný dešifrovací proces. V praxi se můžeme se symetrickými šiframi nejčastěji potkat u hybridních šifer, které jsou nejvhodnější pro zašifrování velkého objemu dat.

Další nevýhoda tohoto šifrování je právě spjata s šifrovacím klíčem, který vzniká, při dohodě na jednom klíčí mezi dvěma vzdálenými uživateli, jenž musí znát jen právě jen tyto strany. Z toho vyplývá, jak bezpečně dostat bezpečnostní klíč od jednoho uživatele ke druhému, aniž by došlo ke krádeži tohoto klíče. V souvislosti s touto problematikou by měli být tyto klíče delší, aby nedošlo k jejich prolomení. [5]

3.2.1.1 Nejznámější symetrické šifry

DES (Data Encryption Standard)

Šifra vyvinutá společností IBM, v 70 letech minulého století a stala se americkou vládní normou pro šifrování. Délka každého klíče, jak pro šifrování a dešifrování májí délku 56 bitů. V současnosti je tato šifra již nepoužitelná, vzhledem k vývoji výpočetní techniky se specializovaným HW lze přes tuto šifru hrubou silou (zkoušení všech možností) dostat do 24 hodin. [5]

3DES (Triple – DES)

Jde o novější a vylepšenou verzi šifrovacího algoritmu DES, v principu jde o využití algoritmu DES, kdy jsou data třikrát touto šifrou přešifrována, stejně tak je i bezpečností klíč zašifrován pomocí šifry DES. Výsledně má tady délka klíče 168 bitů, oproti původní délce DES algoritmu, které měl délku klíče pouze 56 bitů, tedy trojnásobně menší. [5]

IDEA (International Data Encryption Algorithm)

Šifrovací algoritmus, který oproti svým předchůdcům (DES a TripleDES) má nesrovnatelně vyšší stupeň bezpečnosti a i vyšší rychlost práce. Délka klíče tohoto algoritmu má 128 bitů. I když již v současnosti existují rychlejší algoritmy, je IDEA stále jedním z nejbezpečnějších algoritmů, doposud stále neexistuje žádná kryptoanalytická metoda proti tomuto algoritmu. Dnes již existuje i vylepšená a novější verze této šifry a to IDEA NXT. [5]

BlowFish

Jedná se o velice populární algoritmus s proměnou délkou klíče od 32 do 448 bitů. Obvykle je využíván s délkou klíče jako a to 128 bitů. Byl vytvořen jako alternativa za zastaralý DES. Na popularitě tento algoritmus získal díky jeho bezpečnosti, rychlosti a především díky tomu, že není pantátován a může být tedy kýmkoliv a kdekoliv použit. [4]

CAST

Algoritmus nesoucí počáteční jména svých vývojářů, jimiž jsou Carlisle Adams a Stafford Taverns. Jedná se opět o algoritmus, který může mít proměnné délky klíčů, ale opět je používán s délkou klíče 128 bitů. Co se týče bezpečnosti a rychlosti je velice podobný algoritmu BlowFish. [5]

3.2.2 Asymetrické šifrování

Oproti symetrickému šifrování používá asymetrické šifrování dva klíče. První je klíč pro zašifrování zprávy tzv. veřejný klíč (public key), který využívá jakýkoliv odesilatel zprávy, jenž chce zaslat šifrovanou zprávu příjemci. Druhý klíč – soukromý klíč (private key) je již tajný a je znám jen příjemci zprávy, tento klíč slouží k dešifrování zprávy a proto musí být za každou cenu chráněn proti zneužití.

Délka klíčů u asymetrických šifer má jiný význam než u šifer symetrických. Běžná velikost těchto klíčů je v dnešní době 1024 až 2048 bitů, tato velikost není omezena a pro

dlouhodobější použití klíče se může zvolit i vyšší velikost. Tím o všem vzniká jedna z nevýhod asymetrického šifrování a to oproti symetrickému je výpočetní náročnost šifrovacího dešifrovacího procesu. [5]

3.2.2.1 Nejznámější asymetrické šifry

RSA

Jedná se o šifru s širokým využitím, lze jí použít pro šifrování tak i pro digitální podepisování. Název této šifry je utvořen ze jmen autorů Ron Rivestovi, Adi Shamirovi a Leonardu Adlemanovi. Bezpečnost tohoto algoritmu je zajištěna na principu faktorizace, tedy rozložení velkého čísla na součin dvou prvočísel, zde velice taky hraje roli velikost použitého klíče. Jak již bylo uvedeno minimálně 1024 bitů, avšak ideálnější je využití 2048 bitového klíče z důvodu vyšší bezpečnosti. [5]

Bezpečnost RSA je dneska velice diskutabilní, již v roce 2017 bylo zveřejněn potřebný výkon k prolomení RSA šifer na čipových kartách s délkou klíče 1024 bitů a to pomocí výkonného výpočetního výkonu.

Algoritmus Diffie-Hellman

Slouží jako algoritmus pro společnou výměnu klíčů pro bezpečný komunikační kanál, kdyby došlo k jeho narušení. Pokud by došlo k útoku na tento komunikační kanál (odposlouchávání kanálu) útočník by nedokázal tyto klíče na základně získaných informací sestrojit. [6]

El-Gamal

Jedná si o asymetrickou šifru, která je velmi podobná algoritmu Diffie-Hellman, vzhledem k tomu, že na tento algoritmus vypršela autorská práva je nyní volně šiřitelná v podobě open-source. Tím vzniká riziko používání této šifry. Elgamal je stále nejznámější šifrou, ovšem oproti oblíbenosti RSA velice zaostává. Důvodem, proč je tak málo používám oproti RSA je ten, že šifrovaná data mají větší velikost než data nešifrovaná a to je v praxi velice nepraktické. Důvodem této velikosti je ten, že šifra je založena na sofistikovaném matematickém algoritmu při výpočtu logaritmu. Proto oblíbenost a využití El-Gamal šifry lehce upadá. [7]

3.2.3 Hash algoritmy

Jde o oblast šifrování, kdy potřebnou informaci potřebujeme zašifrovat, ale už nikoliv dešifrovat. Jedná se tak například v případě hesel do systému. Uživatel si nastaví například heslo „Karel07“, systém si tuto informaci zašifruje a uloží do systému v zašifrované podobě jako například „a8t./08e“. Poté, když se uživatel znovu přihlašuje, tak systém opět vezme heslo uživatele, zašifruje a porovná s uloženou hodnotou. Ve výsledku to znamená, že systém nezná heslo uživatele ale pouze jeho zašifrovanou podobu. [5]

3.2.4 Elektronické podpisy

V principu se jedná o totéž jako o písemný podpis až na to, že je v digitální podobě. V digitálním světě nelze důvěřovat tomu, zda osoba, která datovou zprávu odeslala, je opravdu tou osobou, za kterou se vydává. Ve většině případů je elektronický podpis připojen k datové zprávě a tím zaručuje identitu odesílatele zprávy. Elektronický podpis využívá metody asymetrické kryptografie. V praxi to znamená, že se využívá pár kryptografických klíčů (private key) pro identifikaci komunikujících subjektů. Subjekt, který vlastní pár daných kryptografických klíčů musí svojí identitu prokázat pomocí certifikátů, jež vydává certifikační autorita.

Elektronický podpis obsahuje i informaci, kdo elektronický podpis vytvořil, o to se stará právě nějaká certifikační autorita.

3.2.4.1 Certifikační autorita

Jedná se o nezávislý subjekt, jenž má za úkol ověřit identitu žadatele o certifikát. Na základě ověření identity, vydá certifikační autorita žadateli certifikát, který je pevně sváže jeho identifikaci s daty pro vytvoření elektronického podpisu. Svým způsobem, žadatel získá „elektronický občanský průkaz“, pomocí kterého se prokazuje v digitální sféře. [5]

Přehled kvalifikovaných certifikačních autorit a poskytovatelů certifikačních služeb v České republice podle Ministerstva vnitra:

- První certifikační autorita a.s.,
- Česká pošta, s.p.,
- eIdentity a.s.,
- Software602 a.s.

3.2.4.2 Zaručený elektronický podpis

Jedná se o elektronický podpis, který nezaručuje identitu podepsané osoby, a tudíž se za podepisovanou osobu může vydávat kdokoliv jiný nebo dokonce někdo, kdo vůbec neexistuje. Mnoho uživatelů si myslí, že zaručený elektronický podpis ověřuje identitu už odesílatele, avšak zaručuje jen neměnnost toho, co bylo napsáno (obsah odeslané zprávy).

Zaručený elektronický podpis je výsledkem podepisovaného dokumentu (tím se zaručí, že to co je podepsáno je neměnné a je chráněno proti změně) a soukromého klíče (neboli privete key, který nemá nikdo jiný a jedinečný pro podepisující osobu). V realitě však neví, kdo tento klíč použil a odeslal danou zprávu z důvodu, že u zaručeného elektronického podpisu není kladen požadavek na důvěryhodnost certifikátu. [8]

3.2.4.3 Kvalifikovaný elektronický podpis

Je druh elektronického podpisu, kterému už můžeme ze zákona důvěřovat. Tento druh se používá v celé EU. Součásti vytvoření kvalifikovaného elektronického podpisu je kvalifikovaný certifikát a nutnost využití čipové karty nebo tokenu (obr. 1-2), který slouží jako prostředek pro vytvoření elektronického podpisu (bezpečné uložení soukromého klíče). [8]

Obr. 1. Tokeny [9]

Obr. 2. Čipová karta [10]

3.2.4.4 Uznávaný elektronický podpis

Je českou specialitou mezi elektronickými podpisy, protože se jedná o druh elektronického podpisu, který figuruje pouze na území ČR. Stejně jak u kvalifikovaného elektronického podpisu, tak u uznávaného podpisu se vyžaduje pro vytvoření kvalifikovaný certifikát. Oproti kvalifikovanému elektronickému podpisu, uznávaný nepotřebuje ke svému vytvoření certifikovanou čipovou kartu nebo USB token (v praxi se jedná o úsporu po finanční stránce). [8]

3.2.5 Elektronické pečetě

Je speciálním případem pro právnické osoby nebo orgánům veřejné moci, avšak vždy vázáno na nějaké hardwarové zařízení. Oproti kvalifikovaným elektronickým podpisům, mají především za úkol ověřit integritu a správnost dat, které jsou připojeny v datové zprávě.

Kvalifikované certifikáty určené pro elektronické pečetě lze využít pro vytvoření a ověření elektronických pečetí. [11]

4 ZÁLOHOVÁNÍ

Pokud chceme, aby firemní data byla dostatečně chráněna je potřeba je i dostatečně zálohovat a tím se vyvarovat případným ztrátám, které by mohli být i z finančního hlediska velice postihující. Ke ztrátě dat může dojít poškozením či krádeží, proto je velice důležité data nějakým způsobem v pravidelných intervalech zálohovat.

4.1 Zálohování firemních dat

Jelikož dnešní doba přináší veškerou digitalizaci firemních dat, s kterými se pracuje na koncových zařízeních, jako jsou počítače, mobilní zařízení, tablety, atd. nejsou tyto data ve fyzické podobě, ale pouze uloženy na nějakém záznamovém médiu v podobě digitální informace. Je tedy velice snadné o ně přijít, pokud je dostatečně nezálohujeme.

Mezi nejčastější ztráty dat může dojít při:

- Provádění systémových operací nezkušených uživatelů (formátování, mazání, atd.).
- Mechanická závada záznamového média (zkrat flash-disku, pád zařízení, atd.).
- Ztráta záznamového média (krádež, ztráta v důsledku lidského faktoru, atd.).
- Přírodní živly (povodeň, požár, bouřka, atd.).
- Nedostatečná ochrana firemních dat (napadení škodlivým softwarem, sociální inženýrství, atd.). [12]

Aby bylo možné se těmto rizikům vyvarovat je potřeba firemní data řádně zálohovat a vytvořit tak kopii, jenž bude složit jako obnova důležitých firemních dat.

4.2 Jaká firemní data zálohovat

Zálohovat by se měla především data, která jsou pro firemní účely velice důležitá a nelze je nějakým způsobem nahradit či získat zpět. Především se jedná o data či informace, které mají z hlediska firmy nějakou business hodnotu a jejíž ztráta by byla pro firmu z finančního hlediska ztrátová, jsou to například:

- smlouvy,
- faktury,
- instalační programy,
- výpisy,
- manuály k výrobě,

- účetnictví,
- přístupové údaje (hesla, účty, atd.),
- atd. [12]

4.3 Kam je možné firemní data zálohovat

Dnešní doba a pokrok s sebou přináší velkou řadu způsobů, jak firemní data bezpečně zálohovat. Aby každá záloha splnila svojí funkci, je potřeba záložní kopii ukládat na jiné záznamové médium, než kde je uložena originální kopie dat. Záznamové médium, kde je uložena záložní kopie dat, by měla sloužit pouze k zálohování, nikoliv však k aktivnímu používání (kopírování dat, stahování, instalace, atd.).

Výběr záznamového média velice závisí na několika faktorech:

- Velikost firemních dat.
- Business hodnota dat.
- Velikost společnosti a počet zaměstnanců.
- Časový interval zálohování.
- Četnost přístup k zálohovaným datům.
- Čas, po který mají být data zálohována.
- Atd. [12]

Nejčastější a nejpoužívanější média pro zálohování dat:

Magnetické pevné disky

Disky založené na mechanickém principu výroby používanému už několik let, avšak na trhu stále zaujímají místo jako nepoužívanější záznamové médium. Výhodou těchto disků je v dnešní době nízká nákladová cena, velikost, rychlost čtení a zápisu, i když ta už oproti elektronickým pevným diskům zaostává. Velkou nevýhodou je technologie těchto disků, která je velmi náchylná na mechanické poškození (otřesy, pád, opotřebení, atd.). Proto dnes už nejsou příliš vhodné pro zálohování důležitých dat a jejich alternativou může být datové úložiště na síti (NAS) technologie. [13]

Elektronické pevné disky

Jsou nástupcem starších pevných disků, jež pracují na mechanickém principu. Začaly se používat teprve v průběhu několika let a už dávno dosáhly svojí kapacitou na pevné mechanické disky. Jejich největší výhodou je velká rychlost čtení a zápisu. Nevýhodou je

stále pořizovací cena těchto disků, která je několika násobně vyšší, než u starších technologií. Vyplatí se tedy jen pro větší firmy či datová centra. Další a velmi podstatnou nevýhodu je životnost těchto disků, která je dána počtem přepisů a zápisů na disk a také se jedná o nutnost mít tyto disky neustále zapojené v napájení, neboť bez něj může dojít po čase ke ztrátě uložených dat. [13]

Magnetické pásky

Technologie, která se v dnešní době používá nejčastěji pro zálohování a archivaci firemních dat. Největší výhodou této technologie je vysoká rychlost zápisu a čtení, která díky neustálému vývoji dokáže předejít i rychlosti pevných disků. Nevýhodou však stále zůstává vysoká pořizovací cena, která se však firmám vyplatí pro každodenní zálohování. Magnetické pásky lez rozdělit do dvou kategorií. První je DAT páska, která je z hlediska pořizovací ceny nižší avšak nedosahuje tak vysokých přenosových rychlostí dat. Oproti tomu DLT páska má vyšší pořizovací ceny na úkor vyšší přenosové rychlosti dat a proto je i vhodnější pro větší objemy dat. Je tedy vhodná pro větší podniky či podniky, které potřebuji v krátké době zálohovat velké množství dat. [14]

Externí disky

Může se jednat jak o mechanický či elektronický externí disk, který se k zařízení připojuje pomocí rozhraní USB, Local Area Network (LAN) nebo eSATA. Je velice praktický a cenově dostupnější. Dosahuje stejně přenosové rychlosti jako obyčejné pevné disky. Nevýhodou je však riziko mechanického poškození z důvodu přenášení, snadného odcizení disku či ztráty.

Optická média

V dnešní době téměř nevyužitelné, jedná se o média typu DVD či Blu-ray. Nízké pořizovací náklady. Nevýhoda spočívá v malé kapacitě, nutnosti vlastnit DVD vypalovačku a možnosti mechanického poškození optického disku. V praxi dnes téměř nevyužitelné pro velké zálohování firemních dat či instalace programů.

NAS

Je také jedním z nejpoužívanějších metod pro zálohování dat ve firmách, pracovníci firmy ukládají svá data na společné uložiště umístěné ve firemní síti. Za tuto síť a bezpečnosti poté zodpovídají správci sítě, kteří za tato data zodpovídají. Velkou výhodou je, zálohování dat na dálku z firemních zařízení, které jsou mimo firmu. [15]

Vzdálená zálohovací služby (Cloud)

Jedná se o služby, které využívají vysokorychlostního připojení na internet. Velkou výhodou těchto služeb je, že nevyžaduje žádné technické zacházení či nákup zařízení. Další velkou výhodou je, že data jsou uložena na vzdáleném serveru a zaměstnanci firmy se k těmto datům můžou připojit odkudkoliv na světě. Nevýhodou je přenos velkých objemů dat přes internet, bezpečnost při přenosu těchto dat a především bezpečnost těchto dat (firma neví, kde jsou její data uložena a kdo k nim má přístup). [14]

USB flash disk

Médium, které je vhodné pouze pro zálohování malých a méně důležitých dat. Výhodou je malá pořizovací cena a snadné uskladnění. Nevýhodou je malá úložná kapacita, možnost opotřebení elektronické paměti z důvodu častého přepisování, snadné odcizení či ztráta. Nevhodné pro ukládání firemních dat.

5 BEZPEČNOSTNÍ POLITIKA VE FIRMĚ

V každé firmě, která má za prioritu chránit svá data, by měl být pracovník či skupina pracovníku, kteří by měli zodpovídat za bezpečnost, šifrování a zálohování dat. Může se jednat o interní pracovníky na odborných pozicích, externí firmu spravující IT chod firmy nebo v menších podnicích i majitele či ředitele společnosti. Informační bezpečnost by měla být ustanovena v každé bezpečností politice firmy.

5.1 Provoz firmy

Jedním ze základních pravidel firmy je důraz na vzdělání a proškolení pracovníků. Na jednotlivé pracovní pozice, kde dochází k práci s firemními daty, by mělo být požadováno příslušné vzdělání a proškolení o bezpečnosti a zálohování dat. Zaměstnanci, kteří mají přístup k business datům, by měli být seznámení protokolem know-how.

5.1.1 Pohyb zaměstnanců

Pro příchody a odchody z firmy by měl fungovat například nějaký elektronický docházkový systém, který by zabránil pohybu neoprávněných osob, které by chtěli například odcizit nebo poškodit firemní data. Dále by firmy měli preventivně své zaměstnance po vyzvání vystavit namátkové kontrole, za účelem zjistit, zda nevynáší firemní data nebo nějakým způsobem neohrožují svým chování či prací bezpečnostní nařízení pro ochranu dat.

Pro ochranu datových uložišť či úložných médií, by měla být tato zařízení uložena v místnostech s omezeným přístupem nebo zabezpečeny systémem kontrol vstupu, kdy každý zaměstnanec má vyhrazená práva pro vstup do těchto místností. Proto by měl do místnosti, kde jsou uložená záložní data firmy, mít přístup pouze vedoucí firmy nebo vedoucí IT bezpečnostní pracovník.

5.1.2 Práce z domova

Firma by si měla určit, zda svým zaměstnancům povolí vynášet firemní zařízení či firemní data s sebou domů. Práce z domů přináší mnoho výhod pro zaměstnance, ale tím vzniká i riziko úniku či ztrátě firemních dat. Proto, když se firma pro tento krok rozhodne, by nejprve měla schválit pracovní skupinu zaměstnanců, kteří prošli bezpečnostní prověrkou. Neměli by to být řádový zaměstnanci ale pouze zaměstnanci z vyšších pozic, kteří budou sami ručit za bezpečnost firemních dat a za firemní zařízení.

5.2 Informační bezpečnost

Při přijetí do firmy by mělo být každému novému zaměstnanci vytvořen vlastní účet s příslušnými uživatelskými právy pro užívání počítačové sítě a práci s daty. Správu nad těmito účty bude zajišťovat pracovník informační bezpečnosti či externí IT firma, která bude monitorovat aktivitu uživatelů, aby nedošlo k úniku informací.

Hlavní částí informační bezpečnosti by bylo být i využití vhodného antivirového softwaru a firewallu. Aby se předešlo chybovosti lidského faktoru, měli by zaměstnanci v rámci vstupního školení být seznámeni se zásadami bezpečného chování na síti. Data by měla být při ukládání rozřazena do adresářů dle jejich charakteru (např.: administrativní, výzkumná, ekonomická…) a přístup k nim by jim měl být umožněn pouze příslušným pracovníkům dle jejich pozice.[5]

5.2.1 Zabezpečení sítě

Zabezpečení bezdrátové infrastruktury sítě ve firmě by mělo být realizováno zabezpečením např. WPA2-PSK, tedy chráněný přístup k Wi-Fi (WPA) zabezpečení s Pre-SharedKey) a vhodným šifrováním. Přihlašování do sítě by mělo probíhat například zadáním hesla do wifi sítě. Firemní Wi-fi síť může být chráněna buď tak, že po zadání hesla se zaměstnanci objeví přihlašovací formulář, kde zadá své jméno a zařazení (kancelář/oddělení). Formulář také zjistí MAC adresu zařízení, které zaměstnanec používá. Po odeslání formuláře administrátor sítě přidá do acces tabulky Wifi routeru daná MAC adresu zařízení, tím zamezí přístupu do sítě neautorizovaných osob.

Bezpečnost může být také podporována sledováním aktivity na síti, kdy administrátor (informační bezpečnostní pracovník nebo externí IT firma) při zjištění podezřelé aktivity bude moct daného zaměstnance odpojit od sítě podle jeho IP adresy či fyzické adresy (MAC). V konečném stádiu může být identifikátor bezdrátové sítě Wi-Fi (SSID) skryté a do sítě se budou moci připojit jen zaměstnanci, kteří již jsou v síti přihlášeni.

5.2.2 Bezpečnostní politika hesel

Hesla jsou nedílnou součástí každého systému, slouží nám k přihlášení do systému, k intranetu, emailové schránky či k šifrovacím nástrojům dat. Heslo jako takové, slouží k autorizaci a autentifikaci uživatele. Pokud uživatel heslo nemá nebo zadá nesprávné heslo, nebudou mu zpřístupněny funkce systému nebo se nedostane k zabezpečeným datům.

Pokud heslo uživatel využívá, musí také znát své přihlašovací údaje, pokud je nemá, musí učet vytvořit (například systém Windows, emailová schránka, apod.), po zadání uživatelského jména a hesla, systém ověří zadané údaje s databází a pokud se shodují, je uživatel přihlášen a získá přístup k předem definovaným funkcím a datům. Aby byla zachována bezpečnost, heslo musí splňovat bezpečnostní podmínky. [16]

Bezpečnost hesel

Jak bylo zmíněno, pro přístup k nějakému chráněnému zdroji představuje autentizace s využití přihlašovacích údajů. Právě heslo by bylo být pro útočníky překážkou, avšak problém nastává, že většina uživatelů volí snadno zapamatovatelná hesla, která mohou být snadno prolomena. Proto bychom měli při vytváření hesla dbát na několik zásad:

Délka hesla - obecně by mělo platit, že čím je heslo delší, tím narůstá složitost jeho prolomení. Proto platí, že čas k prolomení se zvyšuje exponenciálně s jeho délkou. Doporučená dálka hesla se udává 8 znaků. Pokud nastane případ, že heslo je příliš krátké, riziko hrozby se navýší. Avšak většina dnešních systému a serverů, nepovolují vytváření hesel kratších jak 8 znaků. Pokud je heslo příliš krátké, útočník má několik možností jak toto heslo prolomí. Může se jednat o útok hrubou silou, kdy útočník použije slovníkový útok, což znamená, že si že útočník najde seznam nejpouživatelnější hesel na internetu a odesílá průběžné dotazy pro přihlášení. Druhou možností je vytvoření skriptu, který generuje nejrůznější hesla a odesílá opět průběžné dotazy o přihlášení na server. Ochranou proti těmto útokům je časový zámek, jenž po zadání série chybných hesel si vynutí časovou prodlevu při zadávání hesla (obvykle kolem jedné minuty), proto je útok hrubou silou velice časově náročný. [15]

Tab. 1. Tabulka nejpoužívanějších hesel[17]

1.	123456	**6.**	123456789
2.	password	**7.**	Letmein
3.	12345678	**8.**	1234567
4.	qwerty	**9.**	Football
5.	12345	**10.**	Iloveyou

Použité znaky - To znamená výběr znaků z klávesnice, jako jsou číselné hodnoty (0-9) a písmena abecedy a-z (26 písmen), pokud započítáme i velká A-Z, tak je to dvojnásobek. Česká klávesnice také obsahuje písmena s diakritikou (12 písmen), tyto znaky není však doporučeno používat, protože některé zahraniční servery tyto znakové sady nemusí podporovat. Všechny tyto vyjmenované možnosti lze kombinovat se speciálními znaky nebo interrupčními znaky.

Forma hesla – heslo, které se uživatel vytvoří, by nemělo obsahovat naše osobní údaje, jako například naše jméno, jména domácích mazlíčků, datum narození, rodné číslo, telefon nebo dokonce název přihlašovacího účtu. Což by útočník mohl využít, právě k prolomení uživatelského hesla. Heslo by také nemělo být na seznamu nejpoužívanějších hesel. Bezpečnostní politika hesla by tedy měla splňovat všechny výše uvedené kritéria a po dodržení těch pravidel by naše heslo mělo být bezpečné. Heslo by tedy mělo odpovídat délce více jak 8 znaků, dále by mělo obsahovat alespoň nějaké velké písmeno, nebo speciální znak a pro každý systém používat různorodá hesla. Avšak nikdy nelze zaručit jeho 100% bezpečnost, proto existují nástroje a metody, díky kterým lze docílit vyšší bezpečnosti. [16]

Obměna a správa hesel

Bezpečnostní politika hesel, také několik pravidel pro dodržování:

Uchování hesla je jedním z pravidel, které doporučuje nikomu heslo nesdělovat, zaznamenávat v písemné formě (na papírek u monitoru, v bloku, atd.), ani zaznamenávat v digitální podobě (poznámka na ploše, heslo napsané v dokumentu na ploše, nápověda pro heslo, atd.), nedoporučuje se ani hesla ukládat pro zapamatování.

Životnost hesla se odvíjí od bezpečností politiky firem, které si určují délku životnosti hesla, nejčastěji se dá setkat s délkou půl roku či roční obměnou hesla. Avšak bezpečnostní odborníci doporučují měnit heslo jednou za 14 dní či jednou za měsíc. V praxi se potkáme s obměnou hesla jednou za půl roku.

Různorodost hesel pokud máme ve správě více hesel a neleze si všechna zapamatovat, není doporučeno používat stejné heslo pro všechny systémy, například heslo do přihlášení do firemního systému (systém windows) a heslo pro emailového klienta. Užv ůbec se nedoporučuje používat stejná hesla ve firemní sítě a soukromá hesla jako například pro sociální sítě, či osobní email. [16]

II. PRAKTICKÁ ČÁST

6 SOUČASNÝ STAV BEZPEČNOSTI DAT V MALÝCH A STŘEDNÍCH FIRMÁCH

Současný stav v malých a středních firmách úzce závisí na finančních prostředcích společnosti, znalostí současných hrozeb, které by mohli poškodit firemní data či proškolení zaměstnanců. Nutnost prevence vůči současným hrozbám neleze podcenit a každá společnost či podnik by měli věnovat veškeré úsilí, aby své data chránily.

6.1 Dotazníkový průzkumu

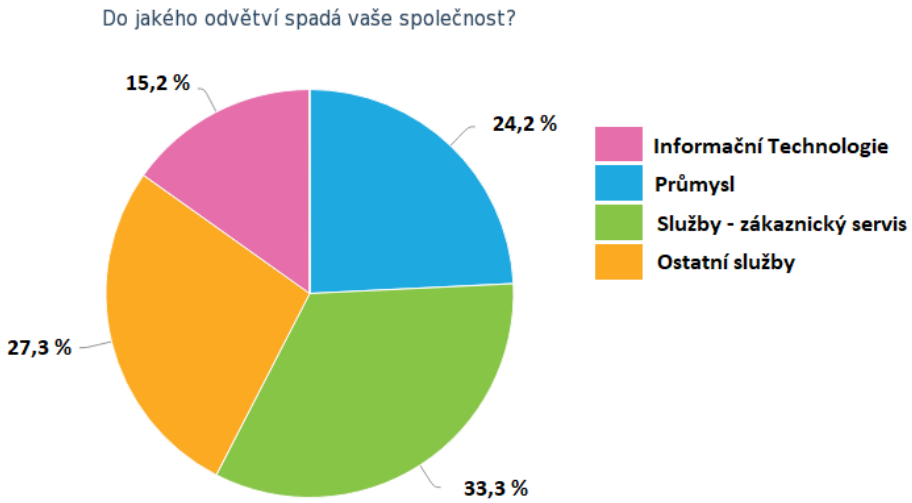
Jedním z cílů této praktické části bylo pomocí dotazníků zjistit, jak si firmy stojí v ochraně svých dat. Průzkum byl proveden pomocí online dotazníkové formy na stránkách www.survio.cz.

Dotazník byl elektronicky rozeslán malým a středním firmám v okrese Přerov, kdy byly vyzvány k anonymnímu vyplnění svého současného stavu bezpečnosti dat. Otázky se týkaly jak bezpečnosti, zálohování, tak nadcházejícího příchodu obecného nařízení o ochraně osobních údajů (GDPR).

6.2 Výsledky dotazníkového průzkumu v malých a středních firmách

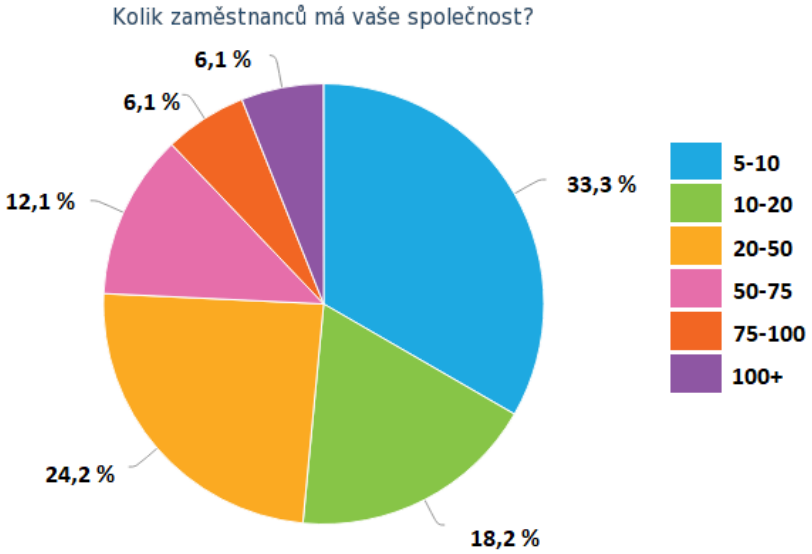
Dotazník obsahoval 15 otázek, které se týkaly především bezpečnosti dat, šifrování, zálohování a bezpečnostní politiky firmy. Ze všech otázek kromě jedné se dala vybrat jedna nebo více možností. Jedna otázka byla dotazovací, kde účastnící průzkumu museli vyplnit vlastním textem.

Dotazník byl rozeslán náhodným malým a středním firmám v okrese Přerov, kde odpovědělo na dotazník 33 firem či společností z různých odvětví (obr. 3), největší zastoupení mají firmy, které se zabývají službami a službami zaměřenými na zákaznický servis. Poté jsou, zde ve stejném poměru zastoupeny firmy z oblastí průmyslu a informačních technologii.



Obr. 3. Odvětví společnosti

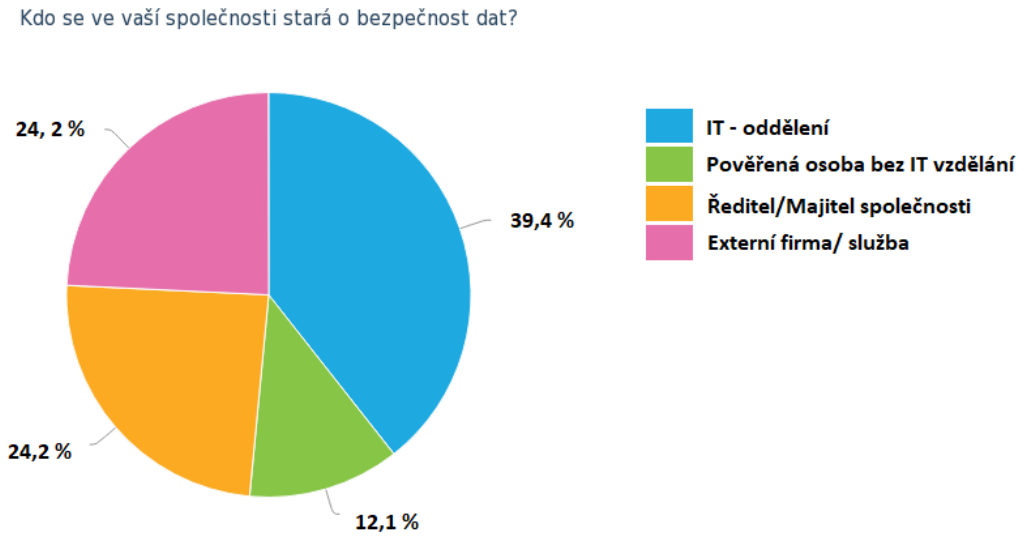
Cílem této otázky (obr. 4) bylo zjistit a rozčlenit, jak velké firmy jsou zastoupeny v tomto dotazníku. Velikost firem, je zde definována počty zaměstnanců. Podle výsledku této otázky jde vidět, že jedná o malé a střední podniky, kde jsou nejvíce zastoupeny firmy do 50 zaměstnanců a v menší míře společnosti nad 50 zaměstnanců.



Obr. 4. Počet zaměstnanců ve firmě

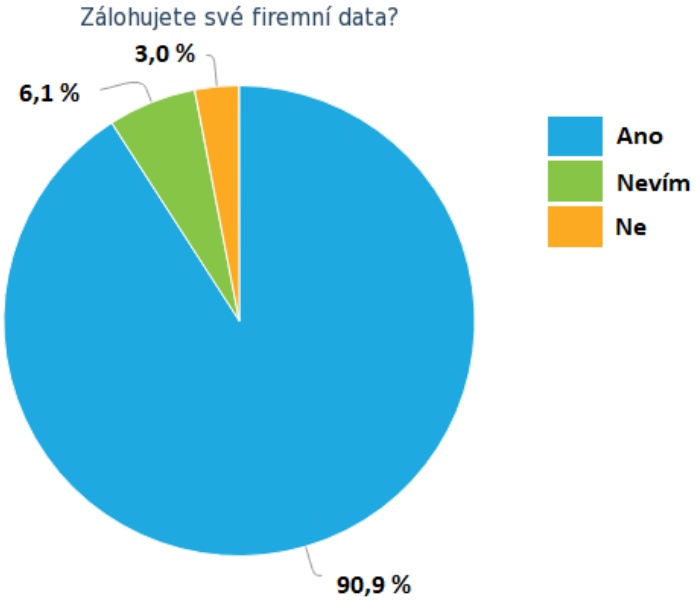
Velkou otázkou ve všech firmách je ta, kdo je zodpovědný za bezpečnost dat a infrastruktury sítě (obr. 5). Ve většině případů se firmy spoléhají na vlastní zaměstnance z IT oddělení (39,4%), tato možnost s sebou nese velkou výhodu v rychle reakci na řešení problémů či bezpečnostnímu zásahu do systému. Hned po této možnost následují ve stejném poměru možnosti využití externí firmy (24,2%) a možnosti, kdy se sám majitel či ředitel menší firmy sám stará o bezpečnost firemních dat.

Využití externí firmy (služby) pro správu bezpečnosti a zálohování dat s sebou přináší výhodu, kdy se firma nemusí starat o chod a bezpečnost dat, externí firma se pomocí vzdálené služby snadno o vše postará a zajistí. Firma, která těchto služeb využije, sice platí za tyto služby, avšak odpadají jí náklady spojené se zajištěními vlastního IT oddělení. Nevýhoda, když firma potřebuje okamžitý zásah či pomoc při hrozícím riziku. Proto se tato možnost doporučuje pro menší podniky, kdy firma neoperuje s velkým množstvím dat. Možnost, kdy sám majitel či ředitel malé firmy sám stará o bezpečnost dat, závisí na jeho vzdělání a proškolení v této oblasti. Pokud je firma a pracuje s malým objemem dat, může díky této možnosti ušetřit v nákladech za externí firmu či vlastní IT oddělení.



Obr. 5. Kdo se stará o bezpečnost ve firmě

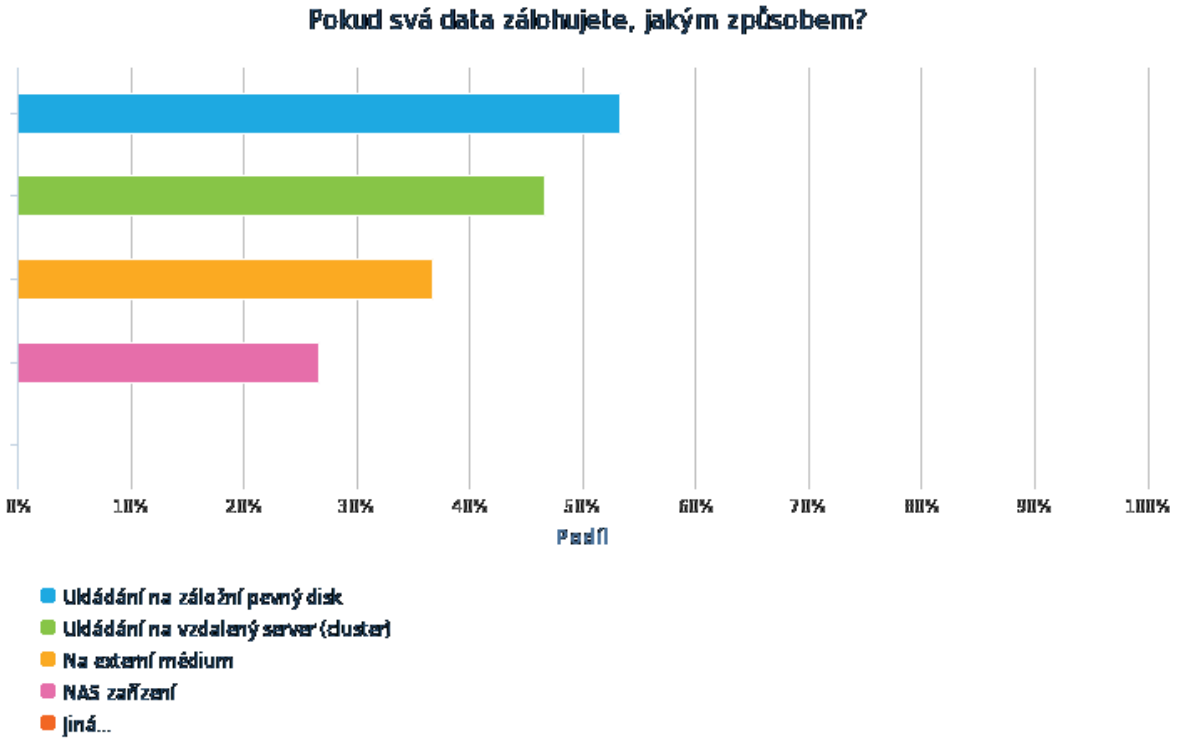
Podle výsledků dotazníkové průzkumu ve většině případů firmy svá data nějakým způsobem zálohují (obr. 6) téměř (90,9%) dotázaných si dělá záložní kopie svých dat. Pouze malé procento malých podniků svá data žádným způsobem nezálohuje (6,1%) nebo nemají povědomí o tom, zda se v jejich firmách data zálohují (3%).



Obr. 6. Zálohujete firemní data?

Dotázaným firmám, jenž svá data zálohují (90,9%) byla položena další otázka, jakým způsobem svá data zálohuji (obr. 7). Na otázku se dalo opovědět více možnosti (v případě, že firma zálohuje současně více způsoby). Nejvíce firem svá data ukládá na klasické záložní pevné disky (53,3%), hned poté zaujímá místo metoda vzdáleného zálohování na vzdálený server (46,7%), další metodou jsou hned externí zařízení (36,7%) a NAS nařízení (26,7%). Dotázané firmy tedy nejvíce stále využívají metody zálohování na záložní pevné disky nebo vzdálené servery.

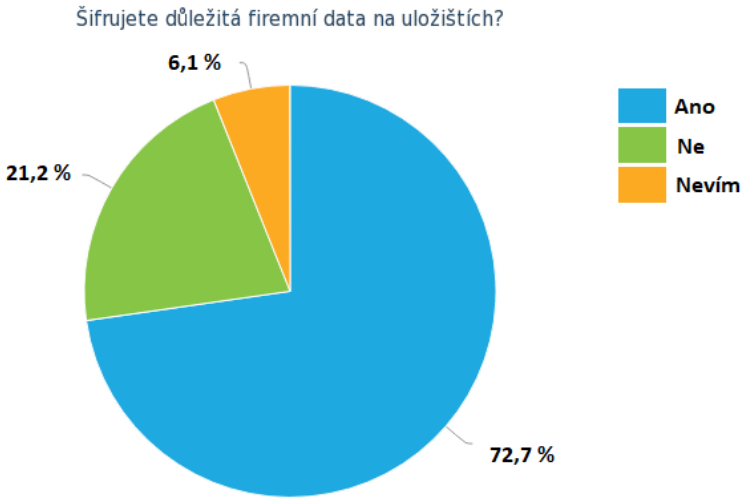
Následně byla položena doplňující otázka, kdy měli firmy napsat, jaký software či cloudovou službu využívají pro zálohování svých dat. V odpovědích byla zastoupena řady softwarových nástrojů jako např. Acronis True Image (6x), Cobian Backup (2x), Symantec Backup Exec (2x) nebo z cloudových služeb např. Windows Azure (3x), Google Drive (2x) nebo DropBox (4x). Mnoho firem si nebyla vědoma, zda nějaký software či nástroj používá (7x) a naopak některé firmy nepoužívaly nástroj žádný (4x).



Obr. 7. Jakým způsobem zálohujete data

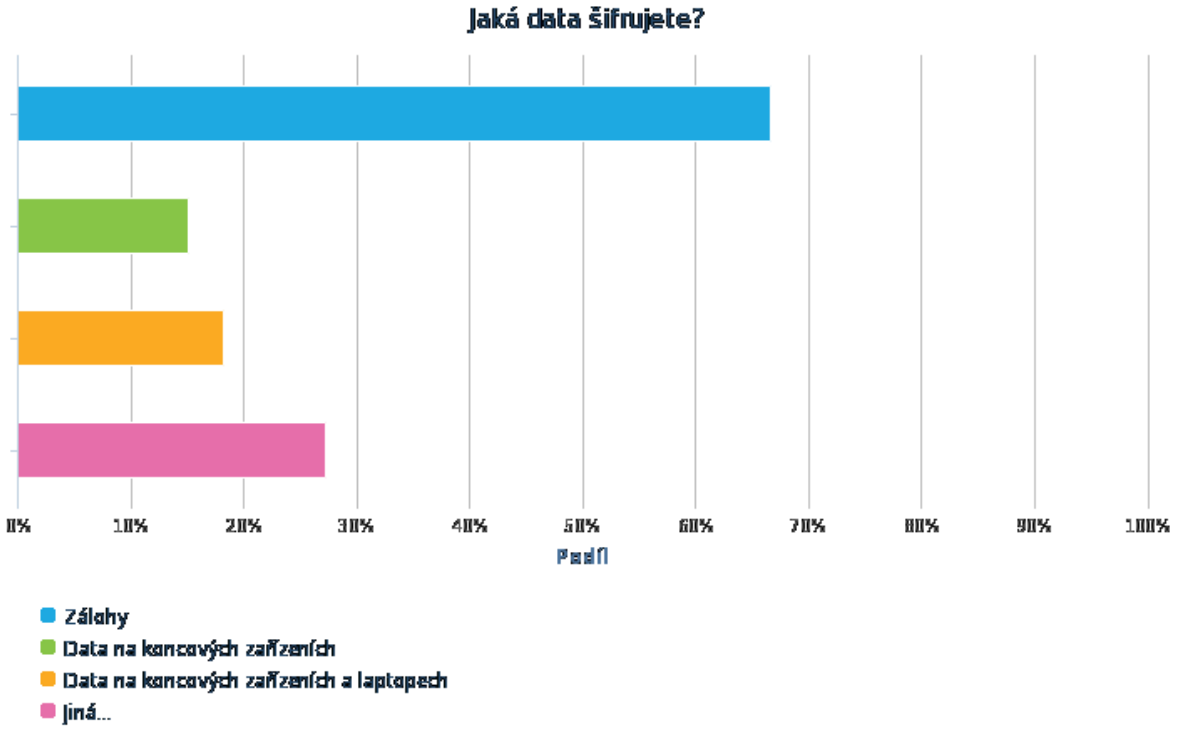
Respondenti firem se dále vyjadřovali, zda šifruji svá firemní data (obr. 8). Drtivá většina firem svá data šifruje (72,7%), dále pak (21,2%) odpovědělo, že svá data nešifrují a pouze (6,1%) firem odpovědělo, že nemělo o šifrování svých dat přehled.

Jak tedy vyplývá z dotazníku, většina firem své data chrání pomocí metody šifrování a je si teda vědoma případných rizik. Naopak malé procento firem se o tuto problematiku nezajímá nebo se nechce zajímat.



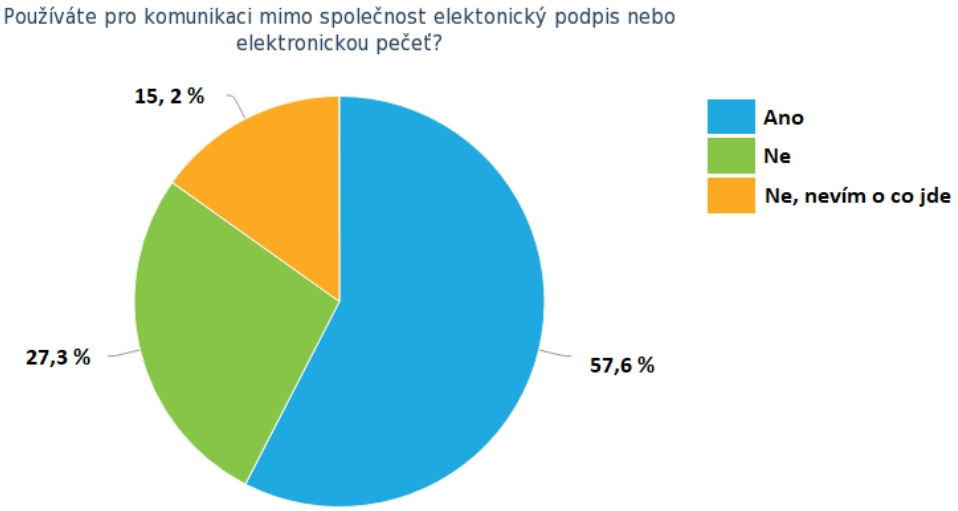
Obr. 8. Šifrujete důležitá firemní data?

Další otázku z oblasti šifrování bylo, pokud firmy svá data šifrují, tak jaká (obr. 9). Podle níže uvedeného grafu si lze povšimnout, že se jedná především o šifrování zálohovaných dat (66,7%), dále pak data na koncových zařízeních (15,2%) a data na koncových zařízeních a laptopech (18,2%). V položce „jiná“ byly zařazené i odpovědi, že firmy neví, která data zálohují (3x). Výsledně tak malé a střední podniky šifrují své zálohované kopie dat a v menší míře data uložená na koncových zařízeních.



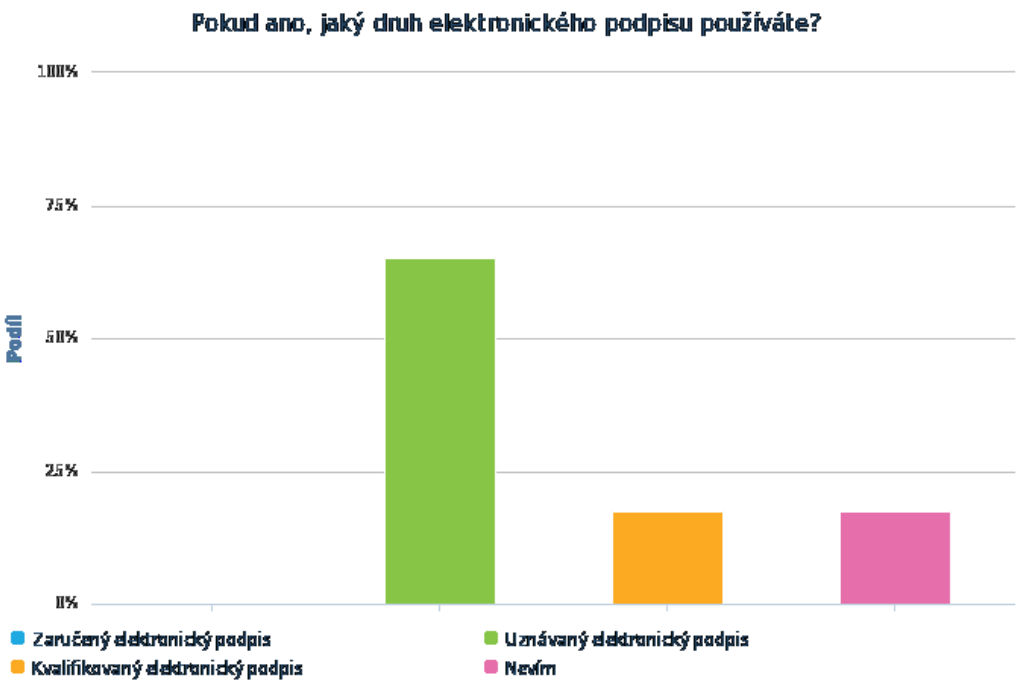
Obr. 9. Jaká data šifrujete?

Na používání elektronického podpisu nebo elektronické pečetě (obr. 10), které se přikládají při odesílání elektronických dat, odpovědělo (57,6%) firem, že jeden z těchto způsobů využívá, tedy více jak polovina dotázaných firem. V menší míře byla zastoupena skupina firem, které tento způsob ověřování dat nevyužívají (27,3%) a malé procento firem (15,2%) nevědělo, co to elektronický podpis či pečeť je. Jak tedy vyplývá z výsledků, většina firem chrání svojí identitu elektronickými podpisem či pečetí a tím chrání svá data. Oproti tomu malé procento firem tento způsob ochrany nevyužívá nebo o něm nemá přehled, může se tedy jednat o malé rodinné firmy, které vidí zbytečně vynaložené úsilí či finanční ztrátu.



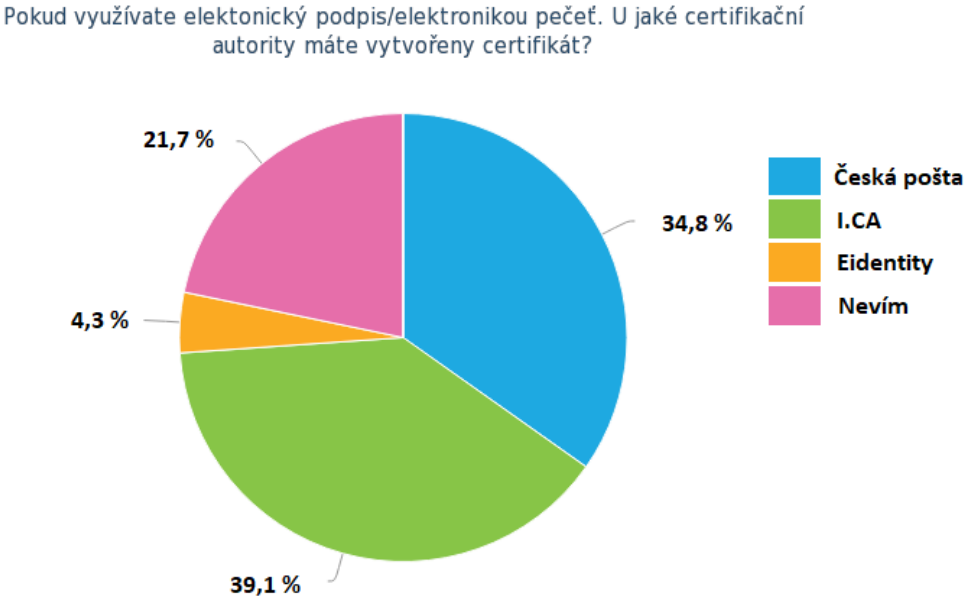
Obr. 10. Využití elektronického podpisu ve firmách

Podniky, které využívají elektronického podpisu, odpověděly, jaký druh elektronického podpisu využívají (obr. 11). Ve většině případů se jedná o uznávaný elektronický podpis, jenž je českou specialitou a využívá jej (65,2%) dotázaných firem, dále pak kvalifikovaný elektronický podpis využívá (17,4%) a stejný podíl tedy (17,4%) neví, jaký druh využívá. Většina firem tedy používá český speciální případ elektronického podpisu, tedy uznávaný elektronický podpis.



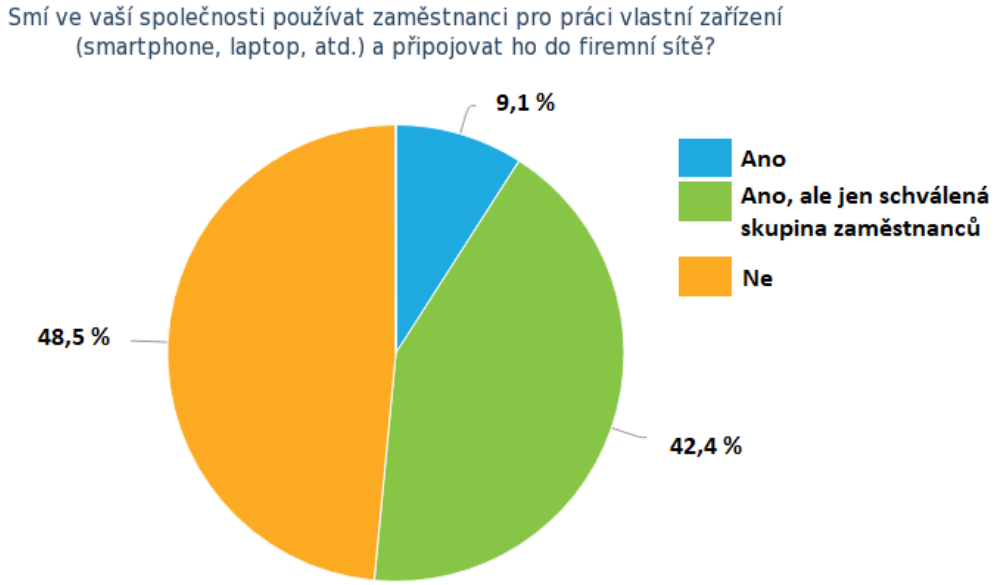
Obr. 11 Nejpoužívanější druh elektronického podpisu

Z možných autorizačních autorit, které se v česku nacházejí, se pro vydání certifikátu pro elektronický podpis (obr. 12), nejvíce firem hlásí k využití služeb společnosti I. CA (39,1%), dále pak služeb České Pošty (21,7%) a v neposlední řadě služeb Eidentity (4,3%), zbytek využívá jiných služeb.



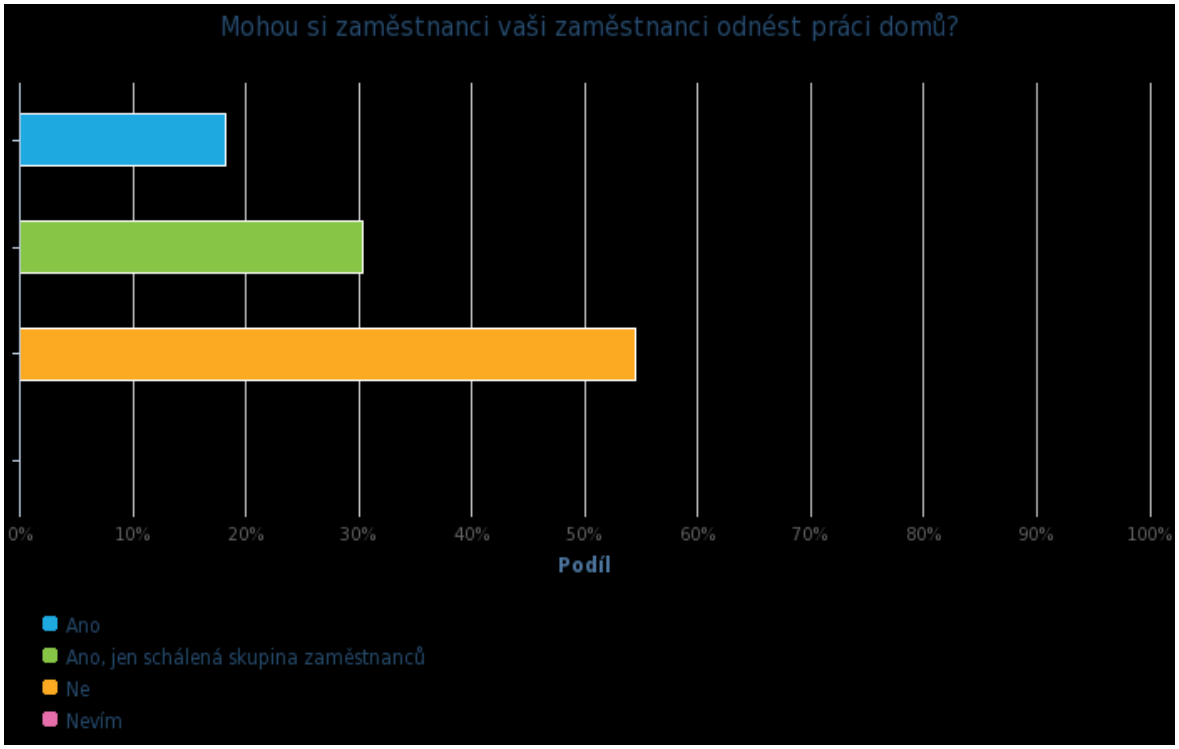
Obr. 12. Nejvyužívanější certifikační autorita

Co se týče bezpečnostní politiky ve firmách, byla dotazujícím firmám položena otázka, zda dovolují svým zaměstnancům pracovat na svých vlastních zařízeních (obr. 13). Ve většině případů to firmy striktně zakazují (48,5%), aby zabránily riziku, že zaměstnanec bude vynášet firemní data ve svém zařízení nebo infikuje firemní síť svým zařízením. Některé firmy však toto privilegium některým svým zaměstnancům dopřávají (42,4%), jedná se o skupiny zaměstnanců, kteří prošli bezpečnostní prověrkou a školením a ručí sami za bezpečnost firemních dat. Malé procento firem svým zaměstnancům svá zařízení povoluje bez výjimek (9,1%). V tomto případě, se společnosti dělí na dva tábory, kdy jedna striktně zakazuje svým zaměstnancům využití svých zařízení a tím předcházejí možným rizikům a na druhou stranu firmy, které spoléhají a věří skupině schválené skupině odpovědných pracovníků.



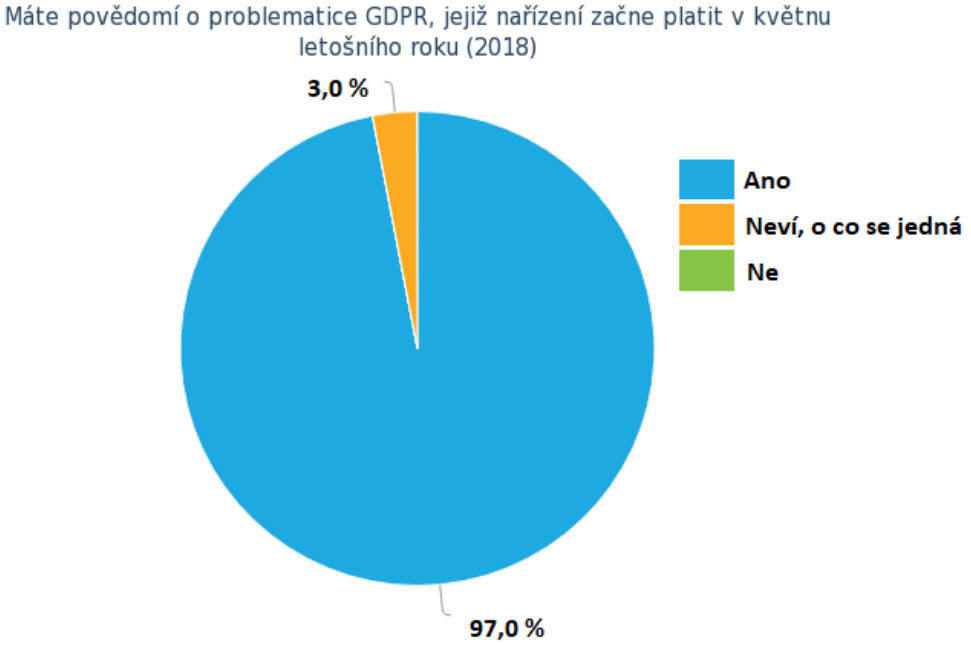
Obr. 13. Využití vlastních zařízení ve firmách

Na základě předchozího dotazu, byla firmám položena otázka, zda nechávají své zaměstnance si svojí práci odnést domů (obr. 14). Jen malé procento (18,2%) firem tuto možnost zaměstnancům povoluje. Další skupinou jsou firmy, které to povolují jen schválené skupině zaměstnanců (30,3%) a ve většině případů (54,5%) to svým zaměstnancům striktně zakazuje. Je tedy zřejmé, že firmy si své data chrání a nechtějí, aby byla vynášena mimo společnost. Oproti tomu malé procento, to svým zaměstnancům povoluje, ale bude se jednat o výše postavené zaměstnance, kteří svojí práci nemohou odložit na druhý den.

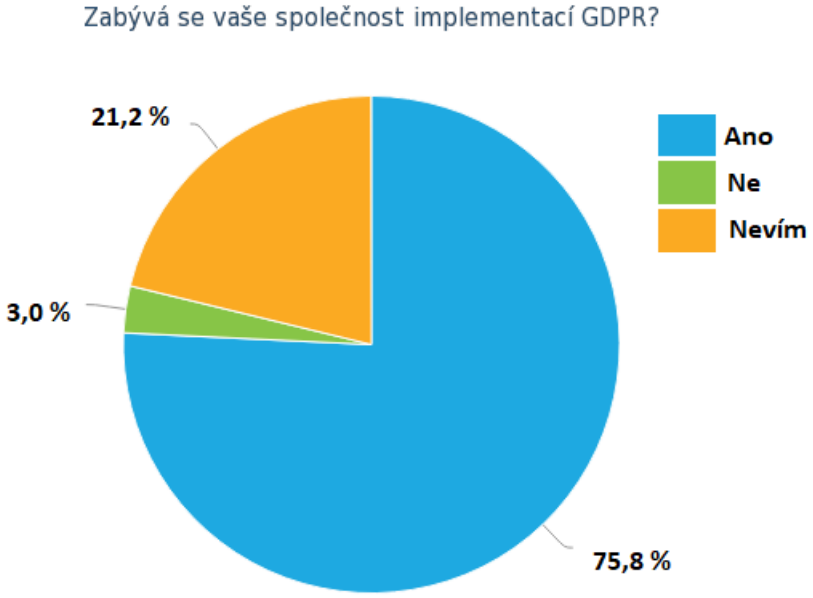


Obr. 14. Četnost práce z domova

Poslední dvě otázky se týkaly nadcházející problematice GDPR (obr. 15-16), snad většina odpovídacích měla povědomí o přicházejícím nařízení GDPR (97%) a jen malé procento (3%) nevědělo, co to GDPR je. Jak je patrné z odpovědí většina firem s touto problematikou seznámena a chce jí nějakým způsobem řešit (75,8%), naopak některé odpovídající firmy si ještě nejsou jistí, jak budou GDPR implementovat (21,1%) a jen (3%) odpovídáních zatím nebude nadcházející nařízení řešit (3%). Jak je patrné z odpovědí, většina firem si je vědoma problematikou a také možných sankcí, které je můžou v případě porušení implementace GDPR postihnout. Malé procento odpovídajících firem není patrně s možnými následky opomenutí GDPR seznámeno.



Obr. 15. Povědomí firem o GDPR



Obr. 16. Implementace GDPR ve firmách

7 MODELOVÝ PŘÍKLAD FIRMY A APLIAKCE PROGRAMOVÉHO VYBAVENÍ PRO MALÉ A STŘEDNÍ PODNIKY

Na základě dotazníkového průzkumu a výsledků, bude vytvořen modelový příklad malé firmy. Cílem je navrhnout dostatečné programové zabezpečení firmy s nízkými náklady pro malé a střední podniky. Dále pak bude i součásti navrhnout bezpečnostní politiky firmy, která by měla sloužit jako prevence při ochraně dat.

7.1 Popis modelového podniku

Malá či střední firma o 20 zaměstnancích, pracující v oboru služeb pro zákazníky. Firma se potýká každý den s citlivými daty uživatelů, které dále zpracovává pro svůj průzkum. Zisky firmy jsou dostačující pro chod celého podniku a je ochotna investovat menší částku do nového programového zabezpečení svých dat.

Vzhledem blížící se mu termínu (25. 5. 2018), kdy přijde v platnost nové nařízení o ochraně osobních údajů neboli GDPR, je potřeba, aby firmy na zabezpečení svých dat dbali. Toto nařízení má přinést větší a spolehlivější ochranu osobních dat klientů či občanů. Firmy se proto musí tomuto nařízení přizpůsobit, protože se toto nařízení týká všech firem či osob, které nějakým způsobem zpracovávají osobní údaje. V případě porušení nebo nedodržení některých z nových nařízení firmám hrozí astronomické pokuty, které by mohly většinu firem finančně poškodit.

7.2 Bezpečnostní politika firmy

V každé firmě je nejslabším článkem v bezpečnostním systému lidský faktor. Aby se míra rizika minimalizovala, je potřeba sepsat dokument, kterým se budou zaměstnanci řídit a dodržovat jej. Jedná se o bezpečnosti politiku firmy, která sepisuje určitá pravidla v ochraně firemních dat.

V první řadě je třeba si určit, kdo je zodpovědný za ochranu firemních dat a určit tak zodpovědnou osobu či oddělení, které se o tuto problematiku bude starat. Tato osoba/oddělení by měla navrhnout dostatečně efektivní zabezpečení a správu dat.

Vlastní zařízení na pracovišti

Firma by si měla určitě, zda svým zaměstnancům dovolí používat svá vlastní zařízení. Velkou výhodou pro malé firmy je v tomto případě velká úspora finančních zdrojů s pořizováním technického vybavení. Zaměstnanec používá vlastní zařízení a není třeba mu pořizovat firemní zařízení (PC, noteebook, mobil, atd.). S tím je však spojena i míra rizika, která tato výhoda přináší a tím je bezpečnost těchto zařízení. Zařízení mohou být infikovaný od škodlivých virů, neaktualizovaná a bez dostatečné ochrany.

Doporučením tedy zůstává, že pokud firma svolí svým zaměstnancům používat vlastní zařízení, měli by nejprve schválit skupinu zaměstnanců, kteří se mohou připojit do firemní sítě. Například filtrace MAC adres na routeru, zvláštní oddělená síť, atd. Připojování do primární firemní sítě by tedy mělo zůstat pouze výsadou klíčovým zaměstnancům.

Práce z domu

Je problematika úzce spojená s používáním vlastních zařízení na pracovišti, pokud zaměstnanec pracuje na vlastním zařízení, je velice pravděpodobné, že si svojí práci odnese i domů na svém zařízení. Tím vzniká řada rizik, jako ztráta zařízení, únik dat, zpronevěření informací, krádež, atd.

Doporučení je tedy opět, pokud je to nezbytně nutné, schválit klíčovou skupinu zaměstnanců, kteří si mohou brát svojí práci domů. Také, aby tito zaměstnanci řádně svojí práci zálohovali např. pomocí cloudové služby, nebo na firemní záložní disk či NAS zařízení. Pokud má zaměstnanec svá data uložena ve svém zařízení, je potřeba je i šifrovat v případě ztráty tohoto zařízení. Také velkým problém je zálohování citlivých dat na přenosné flashdisky, které si snadno mohou ztratit nebo mohou být odcizeny. Tento způsob zálohy nedoporučuji z hlediska vysoké míry rizika ztráty nebo odcizení.

7.3 Návrh programového vybavení

Jsou to programy, které napomáhají k lepší bezpečnosti firemních dat. Výběr těchto programů bude brán z hledisek funkčnosti, popularity a především ceny. Výběrem jsem se řídit podle výsledků dotazníků, hodnocení a recenzí na internetu. Výsledkem by měly být, co nejefektivnější programové vybavení pro ochranu malých a středních firem, za co nejpřijatelnější cenu.

7.3.1 Programy pro šifrování

Skupina programů, která má na trhu velké zastoupení. V rámci tohoto výběru je nutné si uvědomit, co vše chceme od programu, aby uměl šifrovat. Podle vyhodnocení dotazníků firmám nejvíce záleží na šifrování záloh, které by měli být jednoznačně šifrovány, ať už se nalézají na externích zařízeních nebo NAS zařízeních. Poté by to měli být data uložená přímo na koncovém zařízení, pokud hrozí riziko, že na PC může vniknout neznámá osoba. Do výběru těchto programů byly zařazeny 3 programy, které se svojí funkčností vyrovnají a jsou nejvhodnější volbou.

VeraCrypt

Je nástroj pro šifrování dat, který navazuje na historicky oblíbený a dnes již nepoužívaný TrueCrypt. Velkou výhodou VeraCryptu je cena licence, která je naprosto zdarma. Licence je volně šiřitelná a proto je firmy Veracrypt optimálním řešením. V principu pracuje s datovými kontejnery, které zašifruje, tyto kontejnery se poté tváří jako běžný soubor a je možno je přesouvat, kopírovat, atd.

AxCrypt

Posledním z kandidátů je AxCrypt, nástroj která dokáže šifrovat celé diskové oddíly, tak i zvolené data nebo složky. Výhodou opět zůstává licence, která je volně šiřitelná a především možnost dočasného šifrování, které může uživatel využívat v případě zašifrování přílohy email, po stažení emailu je příloha automaticky dešifrována.

7.3.2 Programy pro zálohování

Jednoduché pravidlo, zní, kdo nechce přijít o své data, musí zálohovat. Právě proto existují nástroje pro zálohu, většina těchto programů je dostupná opět přímo na webu a je tak lehce získatelná pro využívání ve firemní sféře. Do výběru byly opět vybrány tři možnosti nástrojů, které by měly být to nejvhodnější volbu pro zálohování firemních dat.

Záloha ve Windows

Funkce historie souborů, která je již zabudovaná v operačních systémech přímo od Microsoft Windows, nám napomáhá uchovávat naše data. Stačí vybrat disky, který chceme do této zálohy přidat umístění pro zálohu (NAS, záložní disk, atd.). V případě, že chceme tyto data obnovit v případě ztráty či poškození lze touto funkcí tyto data opět obnovit. Ve Windows lze také pomocí staršího nástroje v ovládacích panelech vytvořit celou bitovou zálohu disku. Výhodou tohoto řešení, je jednoduchost, kdy se nástroj nachází přímo

v systému a firma se nemusí starat o hledání jiných nástrojů a pak je to pochopitelně cena, která je zahrnuta přímo v ceně licence operačního systému.

Acronis True Image

Velmi používaný a spolehlivý nástroj pro zálohování dat. Je vybaven funkcemi pro zálohování jednotlivých složek nebo celých disků. Tyto zálohy je pak možné ukládat na záložní disk, NAS zařízení nebo externí zařízení. Velkou výhodou tohoto nástroje je i přítomnost možnosti šifrování citlivých dat pomocí šifry AES. Acronis True Image 2018 pro tři PC lze získat v ceně 1599 Kč.

Bvckup 2

Jednoduchý a kvalitní nástroj pro zálohování. Nástroj hraje na svojí jednoduchost, ocení především malé firmy, které nemají moc IT zkušeností a nechtějí se jim studovat ovládání složitých programů. V programu stačí zadat, co chceme zálohovat a kam to chceme zálohovat. Záloha se poté bude provádět každý 6 hodin (zkušení uživatelé mohou toto nastavení změnit). Zálohovat jde opět na externí uložiště, NAS zařízení či záložní disky. Bvckup 2 lze vyzkoušet ve zkušební verzi na 2 týdny, licence stojí okolo 500 Kč.

7.3.3 Programy pro ukládání klíčů a hesel

Programy určené spíše IT správcům sítě. Tyto programy se využívají pro uchování hesel, nelze si nikdy zapamatovat všechna používaná hesla ve firmě.

KeePass

Program pro správu hesel, který se chlubí licenci zdarma. Hesla jsou uložena v programu a zašifrována na lokálním disku. O bezpečnost je v tomto případě postaráno pomocí certifikátu, kdy útočníkovi nebude stačit získání hesla do programu.

LastPass

Jeden z velmi populárních a oblíbených programů pro správu hesel. Výhodou je propojení s mobilní aplikací, která je velmi praktická nebo vygenerování nového bezpečného hesla. LastPass má možnost uchovávat krom hesel také různé přílohy jako dokumenty, poznámky, apod., které jsou poté odkudkoliv dostupné. V základní verzi je tento program zdarma a pokročilé služby si lze doobjednat za 50 Kč/na měsíc.

ZÁVĚR

Tato diplomová práce měla za úkol zjistit současný stav na poli nástrojů a situaci zabezpečení dat se zaměřením na malé a střední firmy. Případným firmám by měla poukázat a přiblížit současné bezpečnostní hrozby, které firemním datům hrozí. Na základě poukázaní hrozeb také poukázat na možnosti ochrany dat jako šifrování, zálohování a využití elektronických podpisů. Výsledkem dotazníkového průzkumu bylo zjištěno, že většina firem se bezpečností dat zabývá a není jim lhostejná. Každá menší či střední firma by měla mít zavedenou bezpečností politiku své firmy k ochraně svých firemních dat. Zaměstnanci by měli být vždy poučeni a proškoleni, jak firemní data chránit a jak předcházet možným rizikům. Zejména svá firemní data, zálohovat a nadále šifrovat pomocí programů. V závěru byly doporučeny vhodné softwarové nástroje pro ochranu dat, pro malé a střední firmy s ohledem na ekonomickou stránku.

Teoretická část je zaměřená na pojmy v oblasti dat, také se zaobírá problematikou současných hrozeb, které mohou ohrozit či poškodit firemní data. Dále se teoretická část zabývá šifrováním, elektronickými podpisy a pečetěmi. Jsou zde vymezeny základní druhy elektronických podpisů. V poslední řadě se práce zaobírá šifrováním, kde jsou popsány možnosti, jaké druhy zařízení lze využít pro zálohování firemních dat. V práci je také popsána bezpečnostní politika zaměřená na využívání vlastních zařízení ve společnost, na práci z domu či na bezpečnost a vytváření bezpečných hesel.

V praktické části byl proveden dotazníkový průzkum, který měl za úkol zjistit současný stav zabezpečení dat v malých a středních firmách. Dotazník obsahoval 15 otázek zaměřené na bezpečnost, šifrování, zálohování, využívání elektronických podpisu a povědomí o nadcházejícím příchodu GDPR. Dotazník byl podán v elektronické podobě, kde se firmy anonymně vyjadřovali. Výsledky byly analyzovaný a posouzeny.

SEZNAM POUŽITÉ LITERATURY

[1] Online hrozby. In: *Avast.com* [online]. [cit. 2018-05-22]. Dostupné z: https://www.avast.com/cs-cz/c-online-threats

[2] Rootkity. In: *eset.com* [online]. [cit. 2018-05-22]. Dostupné z: https://help.eset.com/eav/11/cs-CZ/rootkits.html

[3] Phishing a pharming. In: *bezpecnyinternet.cz* [online]. [cit. 2018-05-22]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

[4] DOBDA, Luboš. Ochrana dat v informačních systémech. Praha: Grada Publishing, 1998, 286 s. ISBN 80-716-9479-7.

[5] JAŠEK, Roman a David MALANÍK. Bezpečnost informačních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 139s. ISBN 978-80-7454-312-8.

[6] NECKÁŘ, Jan. Diffie-Hellman. In: *algoritmy.net* [online]. 2016 [cit. 2018-05-22]. Dostupné z: https://www.algoritmy.net/article/84/Diffie-Hellman

[7] Asymetrická kryptografie. In:*Wikisofia.cz* [online]. [cit. 2018-05-23]. Dostupné z: https://wikisofia.cz/wiki/Asymetrick%C3%A1_kryptografie

[8] PETERKA, Jiří. Praktický pohled na elektronické podpisy a jejich fungování. In: *earchiv.cz* [online]. 2018 [cit. 2018-05-22]. Dostupné z: http://www.earchiv.cz/papers/p81/slide.php3?l=1&me=1

[9] Kvalifikované prostředky pro vytváření elektronických podpisů. In: *postsignum.cz* [online]. 2010 [cit. 2018-05-22]. Dostupné z: http://www.postsignum.cz/kvalifikovane_prostredky_pro_vytvareni_elektronickych_podpisu.html

[10] HW řešení a čipové karty. In: *ica.cz* [online]. [cit. 2018-05-22]. Dostupné z: http://www.ica.cz/HW-cipove-karty

[11] Kvalifikovaný certifikát pro elektronickou pečeť. In: *ica.cz* [online]. [cit. 2018-05-22]. Dostupné z: http://www.ica.cz/Kvalifikovany-certifikat-pro-ePecet-SR

[12] Zálohování. In*: jaknainternet.cz* [online]. 2014 [cit. 2018-05-23]. Dostupné z: https://www.jaknainternet.cz/page/1180/zalohovani/

[13] VÍTEK, Jan. Zálohování a archivace dat: jaké jsou možnosti?. In: *svethardware.cz* [online]. 2016 [cit. 2018-05-23]. Dostupné z:

https://www.svethardware.cz/zalohovani-a-archivace-dat-jake-jsou-moznosti/43212-4

[14] Malý přehled zálohovacích médií. In: *ictsecurity.cz* [online]. [cit. 2018-05-23]. Dostupné z: http://www.ictsecurity.cz/component/content/article?id=2815

[15] Jak a kam zálohovat data. In: *servispckupka.cz* [online]. 2018 [cit. 2018-05-23]. Dostupné z: http://www.servispckupka.cz/jak_a_kam_zalohovat_kam_zalohovat_data.php

[16] Bezpečnostní politika hesel a vícefaktorová autentizace. In: *systemonline.cz* [online]. [cit. 2018-05-23]. Dostupné z: https://www.systemonline.cz/it-security/bezpecnostni-politika-hesel-a-vicefaktorova-autentizace.html

[17] Nejpoužívanější hesla roku 2017. In: *railsformers.com* [online]. [cit. 2018-05-23]. Dostupné z: https://railsformers.com/nejpouzivanejsi-hesla-roku-2017

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

DNS	Domain Name System
UPS	Uninterruptible Power Supply
EU	Evropská Unie
USB	Universal Serial Bus
LAN	Local Area Network
SATA	Serial ATA
NAS	Network Attached Storage
DLT	Digital Linear Tape
IT	Informační Technologie
MAC	Media Access Control
WPA	Wi-Fi Protected Access
SSID	Service Set Identifier
GDPR	General Data Protection Regulation

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: OBSAH DISKU CD

\fulltext.pdf

\prilohy\data\elektronicky_dotaznik.pdf