Univerzita Palackého v Olomouci

Fakulta tělesné kultury

BEZPEČNOSTNÍ HROZBY INTERNETU VE FIREMNÍ STRUKTUŘE

Bakalářská práce

Autor: Lukáš Gajda

Vedoucí práce: doc. Ing. Jaromír Novák, CSc.

Olomouc 2018

Bibliografická identifikace

Jméno a příjmení autora: Lukáš Gajda

Název bakalářské práce: Bezpečnostní hrozby internetu ve firemní struktuře

Pracoviště: Katedra aplikovaných pohybových aktivit, Ochrana Obyvatelstva

Vedoucí bakalářské práce: doc. Ing. Jaromír Novák, CSc.

Rok obhajoby bakalářské práce: 2018

Abstrakt: Bakalářská práce pojednává o dnešní problematice informační bezpečnosti. Klíčovým faktorem je bezpečnost internetu ve firmách, státní správě či jiných institucích. Charakterizují se zde ochranné prvky firemní informační struktury a incidenty, které ji ohrožují. Na druhé straně se zde charakterizují prvky útočné, tedy kybernetické útoky, speciální způsoby útoku a další aspekty spadající pod kyberterorismus. Závěrem jsou nástiny protiopatření a technologický vývoj do budoucna.

Klíčové slova: kyberterorismus, riziko, hrozba, internet, bezpečnost, informatika, hacking, struktura, firma, stát, útok, ochrana, data, software, hardware

Author's first name and surname: Lukáš Gajda

Title of the bachelor thesis: Security threats of the Internet in the corporate environment, impacts, prevention, and solution design

Department: Department of Applied Physical Activity

Supervisor: doc. Ing. Jaromír Novák, CSc.

The year of presentation: 2018

Abstract: The bachelor thesis deals with today's information security issues. A key factor is Internet security in companies, government or other institutions. I characterize here the protective elements of the corporate information structure and the incidents that threaten it. On the other hand, there are elements of attack, cyber attacks, special methods of attack and other aspects of cyber-terrorism. In the end, countermeasures and technological developments are in the future.

Keywords: cyber terrorism, risk, threat, internet, security, informatics, hacking, structure, firm, state, attack, protection, data, software, hardware

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně pod vedením doc. Ing Jaromíra Nováka, CSc. a konzultanta Mgr. Ladislava Pacovského, uvedl všechny použité literární a odborné zdroje a dodržoval zásady vědecké etiky.

V Olomouci dne: Podpis:

Děkuji doc. Ing. Jaromíru Novákovi, CSc., konzultantovi Mgr. Ladislavovi Pacovskému za pomoc a cenné rady, které mi poskytli při zpracování bakalářské práce.

Obsah

Úvod

Jsme v 21. století, jinak jako digitální věk moderních technologií a největším rozmachu informačních technologií. Není dnes člověk, který by neznal počítače chytré telefony a jiné technické věci. Tyto výmysly technické vědy nám mají zlepšovat životní úroveň. Vše je propojeno internetem a ten je všude. Avšak s lidským pokrokem roste i míra rizika nových hrozeb v informačním odvětví. Toto odvětví je velmi důležité, protože zasahuje do každodenní činnosti každého z nás.

Dnešní věk je i politicky a kulturně velmi exponovaný, to má za následek vzniku různých skupin lidi, kteří se snaží napadat informační struktury jiných skupin, státu či organizací. Skrze internet a vypočtení techniku je to skvělá volba pro útoky „z pohodlí domova“ s velkou účinností.

Proto se tato práce zaměřuje na charakteristiku základních pojmů z oblasti informační bezpečnosti, dále pak rozvadím pojmy jako jsou ochrana dat, kybernetické útoky, prevence a návrhy řešení proti těmto útokům. Práce je doplněna o aktuální hrozby a reálné incidenty.

1 Cíle práce

Cílem práce je charakterizovat bezpečnostní hrozby internetu ve firemní struktuře a jednotlivé dílčí části informační bezpečnosti. Práce bude rozebírat základní informační pojmy, potencionální kyberteroristické hrozby a způsoby ochrany před nimi. Dílčím cílem je uvést konkrétní incidenty kybernetických útoku a výhled do budoucna informačních technologií z pohledu bezpečnosti a také ochrany obyvatelstva.

2 Přehled poznatků

2.1 Internet

V této kapitole se podívám na to, co vůbec je to internet.

Internet je celosvětový systém navzájem propojených počítačových sítí, chápejme to jako extrémní množství sítí v síti, ve kterých mezi sebou počítače komunikují pomocí rodiny protokolů TCP/IP (primárně protokol pro přenos dat). Hlavním cílem všech uživatelů je v rámci sítě si bezproblémově vyměňovat data (Dostálek & Kabelová, 2008).

Internet lze rozdělit do dvou kategorii připojení. Je to připojení s veřejnou IP adresou (IP adresa slouží k rozlišení síťových prvku v síti, jako identifikační značka) a připojení bez veřejné IP adresy. Daleko častějším způsobem je to ta druhá možnost. Kde účastník, který se chce připojit k internetu musí využít prostředníka, který tuto IP adresu veřejnou má. Toto řešení je obvyklé ve firmách i domácnostech. U firem je to obvykle jedna IP adresa a ostatní účastníci lokální sítě ji využívají jako bránu do internetu. Jde to v situaci, kdy pro velký počet místních uživatelů máme k dispozici pouze malý počet veřejných adres.

Připojení k internetu dělíme na dočasné připojení (mobilní, dial-up, ISDN) a pevné, nepřerušovaná služba stále přístupná (bezdrátové připojení, DSL technologie, kabelová televize, satelit, pronajatá datová linka).

Dial-up – vytáčené připojené, počítač je na internet připojen přes telefonní linku za použití modemu

ISDN – digitální simultánní přenos hlasu, videa, dat, paketů a jiných síťových služeb tradičními obvody veřejné telefonní sítě

DSL – umožňuje využít stávající vedení telefonu nebo kabelové televize pro vysokorychlostní přenos dat

V zásadě je internet komplexní globální síť, která se skládající z mnoha dalších nezávislých sítí, které jsou propojené mezi sebou. Tuto službu zprostředkovávají velké společnosti, výzkumné instituty a vlády.

Definice internetu z pohledu globálně společenského, je internet považován za:

- informační médium, podobné jako noviny, časopisy, knihy, televize, kde najdeme každý den nejaktuálnější informace a množství různých služeb, přičemž stále více informací je přístupných v multimediální formě,
- komunikační médium, umožňující miliónům lidí na celém světě být v neustálém kontaktu v reálném čase, které vytváří nové pracovní příležitosti, odstraňuje geografické bariéry a není pouze zdrojem vzdělávání, ale také zábavy a oddychu,
- reklamní médium a marketingové médium, které postupně svým globálním rozsahem a možností zpětné vazby stále více konkuruje televizi, rozhlasu a tisku,
- obchodní médium, které vytváří nové možnosti obchodu a spolupráce pro firmy a jednotlivce v globálním měřítku (IJS, 2018).

Myslím si, že pojem internet je celosvětově velmi známý. Avšak, mnoho lidí mnoho názoru, může mít za následek interpretace jednoho pojmu více smysly. Podle mě je internet, jako velké množství lokálních sítí spolu propojených, což částečně koresponduje s výše zmíněným.

2.2 Informační bezpečnost

Nejdříve popíši, co je informační systém (IS). Pro představu – vše, co jsem sbíral a dělal v papírové podobě. Všechny data o zákaznicích, schůzky, nákupy, faktury a jiná rozhodnutí. Jsem schopen převést do elektronické podoby tedy do informačního systému.

2.2.1 Informační systém

Je celek složený z počítačového hardwaru k tomu navazujícího softwaru, k obsluze jsou potřební lidé, kteří tento hardware a software využívají, s tím spojené procesy, které přitom vykonávají za účelem sběru, zpracování a šíření informací potřebných k fungovaní a prosperitě firmy či organizace. S vývojem firmy a stoupajícím množstvím důležitých informací, proto je nezbytné, aby byla data pohromadě a uložená na jednom místě, v jednom systému (Jašek, 2002).

Základní okruhy funkčnosti IS

Popíšu nejčastěji používané okruhy v IS, ne vždy toto musí korespondovat u všech firem:

- Zaměstnanci – docházkový systém, výkazy práce, mzdy, zaměstnanecké výhody, školení, kontroly, hodnocení zaměstnanců
- Nákup – přehledy všech nákupů, pobídek, faktury, objednávek
- Logistika – doprava, sklady, inženýrské sítě
- Výroba – plánování, sledování průběhu výroby, řízení jakosti, údržba
- Projekty – projektová dokumentace, řízení projektů, rizik, finanční náročnosti
- Prodej – distribuce, obchod, e-shop, mobilní prodej, cenotvorba, přehled nabídek
- Marketing – marketingové akce, rozdělení trhu, direct mailing, propagace, podpora, katalogy produktů, sledování konkurence
- Zákazníci – analýza chování zákazníků, kontaktní centrum, servis
- Účetnictví – vnitropodnikové, daňové, faktury, celní deklarace, DPH, cizí měny, přístup k internet bankingu
- Majetek – krátkodobý a dlouhodobý, umístění a inventarizace majetku
- Správa dokumentů – příjem a archivace dokumentů, vyhledávání

- Správa IT – správa událostí, správa konfigurací, řešení problémů, řízení změn, kontrola IS

Základní podoby protiopatření v informačním systému před působením hrozeb:

- Administrativní – zákaz přístupu, či manipulace s daty
- Logická – nastavení oprávnění
- Fyzická – zabezpečení, před přístupem nepovolaných osob
- Technická – šifrování dat

2.2.2 Informační bezpečnost je definována jako:

Schopnost informačního systému (IS) jako celku odolat s určitou spolehlivosti před náhodným výpadkem hardwarové, softwarové součásti, před nezákonným jednáním. Cílem je posoudit spolehlivost a integritu systému na tyto nenadále situace a posoudit chovaní informačního systému (IS) v těchto událostech. Při posuzování se kontroluje dostupnost, integrita, autenticita, spolehlivost informací a jiných služeb informačního systému (Jašek, 2002).

Nebo také jako:

„IT bezpečností se rozumí proces dosažení a udržení integrity, dostupnosti, vedení evidence, autenticity, nepopiratelnosti a spolehlivosti informací a služeb, a to na přiměřené úrovni, tj. na takové úrovni, která splňuje předem stanovená kritéria.“ (Staudek & Hanáček, 1999).

Ve zkratce bych řekl, že informační bezpečnost se zabývá ochranou informačně-komunikačních technologií.

Informační technologie zpracovávají stále více informací s velkými hodnotami a významem. Zpracováním informací v rámci informačních technologií se rozumí zachování, přenos, vyhodnocení a prezentování informací pro případ potřeby. V dnešní době se informace umístěné v počítačích stávají nehmotným statkem.

Typy informací s nezanedbatelnou hodnotou:

- bankovní účty
- daňové přiznání
- elektronické platební nástroje

- obchodní záměry
- výsledky výzkumů a vývojů
- zdravotní záznamy

Ochrana při výše zmíněných typech musí splňovat:

- přístup smí mít pouze oprávněné osoby
- nutnost ověřených informací
- možnost logování činnosti – kdo je vytvořil, upravil a odstranil
- neodborné zacházení – nekontrolovaným způsob vyřazení
- redundantnost – musí být dostupné vždy, když je to třeba, pokud možno s náhradou

2.2.3 Definice bezpečného informačního systému

Bezpečný informační systém můžu popsat jako systém, který chrání data a jejich uživatele, po celou dobu, kdy uživatel vytváří, zpracovává nebo jinak nakládá s daty v rámci informačního systému. Každý informační systém se skládá z modulu, které zajištuji jistou ochranu před zhroucením celého systému. Toto vytváří komplexní systém vrstev, které snižují riziko vypuknutí hrozeb.

Je důležité podotknout, že neexistuje dokonale bezpečný informační systém. V dnešní době to není technicky ani lidsky možné. Proto se udává, jak moc je systém schopen snížit riziko na určité hrozby jemu vystavené.

Dále zde popíši základní pojmy spojené z informační bezpečnosti a ukážeme význam těchto pojmů v relativně nově se rozvíjejícím se oboru informatiky (Jašek, 2002).

2.2.4 Základní pojmy v informační bezpečnosti

Postupem času se pojem informační bezpečnost dostává stále více do popředí. Je třeba si uvědomit, že pokrok nejde zastavit. Je však nutné se stejně chránit v informačním prostředí, jako bychom to dělali v reálném prostředí. Zde si vysvětlíme základní pojmy pro pochopení problematiky informační bezpečnosti (Jašek, 2002).

Algoritmus

Přesný návod, popis instrukcí nebo postupu v přesně daném pořadí, jak řešit daný problém (Jašek, 2002).

Aktiva

Aktivum je vše, co má pro uživatele nebo firmu hodnotu, která může být snížena při nenadálé situaci – působení hrozby.

V našem případě jsou to z fyzické stránky všechny počítače, routery, kabely, disky a jiná výpočetní a informační technika. Fyzické zabezpečení těchto periferií (Gála, Pour & Toman 2006).

V případě druhém jsou to tzv. nehmotná aktiva která zahrnují veškeré programové vybavení a data. Pro představu jsou zde operační systémy, informační systémy, antiviry a jiné aplikační programy. S nehmotných aktiv mají nejvyšší cenu obvykle data cenná pro danou společnost (Gála, Pour & Toman 2006).

Charakteristika aktiva je její hodnota. Hodnota je založena na objektivním vyjádření obecně vnímané ceny nebo přiřazení puncu důležitosti (kritičnosti) aktiva. Nejčastěji se skládají oba tyto způsoby. Hodnota aktiva není přesně daná. Pro každého hodnotitele a každou firmu má aktivům jiný klíčový dopad, tedy i jiné vyčíslení hodnoty (Gála, Pour & Toman 2006).

Při hodnocení aktiva bereme na vědomí např. nákupní cenu, důležitost aktiva pro chod informačního systému, důležitost skladovaných informací, cenu informací, náklady v případě škod – výpadků některých služeb (fyzické poškození, softwarová chyba) nebo logistických návazností v důsledku výpadku proudu, internetu apod.

Dalším krokem je hodnota pro tato aktiva odvozována nepřímo přes soustavu nepeněžních měřítek (ztráta dostupnosti v časových jednotkách, poškození dobrého jména firmy). Podle standardu ISO/IEC TR 13335 můžeme definovat nepeněžní parametry a z nich vyplývající ztráty nebo náklady:

- Nedodržení legislativy předpisů.
- Zhoršení výkonu činnosti firmy.
- Ztráta dobrého jména nebo negativní vliv na pověst firmy.
- Narušení důvěrnosti spojené s osobními informacemi.
- Ohrožení osobní bezpečnosti.
- Nepříznivý vliv na prosazení práva.
- Porušení obchodního tajemství.
- Nerušení veřejného pořádku.

- Finanční ztráty.
- Přerušení aktivit činnosti firmy.
- Zhoršení bezpečnosti prostředí.

ISO/ IEC TR 13335 – česká verze technické normy řízení informační bezpečnosti.

Zranitelnost aktiva

Zranitelností chápeme citlivost na působení hrozby. Každé aktivum má zranitelné místo nebo nepřímo může způsobit škody. Zranitelná místa mohou být následující:

- fyzické – prvek fyzicky v prostředí, kde může vzniknout poškození,
- zničení nebo ztráta
- přírodní – poškození přírodní katastrofou
- technologické – konstrukční vada, nedostatečná automatizace, vadná implementace
- fyzikální – elektromagnetické záření
- lidské – faktor lidské chyby, omyly, nedostatečná vzdělanost a školenost
- Podle citlivosti aktiva se hodnotí míra důležitosti – jeho náchylnost k poškození (Gála, Pour & Toman 2006).

Autentizace

Ověření osoby, nebo přístupu (Jašek, 2002).

Autorizace

Rozdání pravomoci pověřené osobě, nebo přístupů k nakládání s daty informačním systému (IS) nebo provádění jiných změn v IS (Jašek, 2002).

Bezpečnost

Určuje míru ochrany pro hrozbám, jako jsou ztráta, zneužití, poškození, odcizení nebo zničení. Pod pojmem bezpečnosti si můžeme představit stupně ochrany, které zabrání negativní události. V našem případě se bude jednat o bezpečnost informačních systémů a informačních technologií ve firmě.

Hrozby

Hrozby a zranitelná místa tedy zvyšují riziko bezpečnostního incidentu, který negativně ovlivní fungující systém. Závažnost rizika je určen hodnotou aktiva, zranitelnosti aktiva a úrovně hrozby (Novák, 2015) a (Jašek, 2002).

U hrozeb vybíráme takové protiopatření, jejichž náklady se musí přiměřeně rovnat hodnotě chráněných aktiv nebo hodnotě škod zaviněných hrozbou. V tomto případě si stanovíme referenční úroveň rizika, pod kterou je riziko zbytkové a pro systém přijatelné, neboť není nutné podnikat další protiopatření ke snížení rizika (Jašek, 2002) a (Gála, Pour & Toman 2006).

Riziko

Je míra pravděpodobnosti vypuknutí hrozby, tedy stavu, který na základě nějaké příčiny ohrožuje stabilitu systému. Uvádí míru nebezpečí, ohrožení nebo míru jinak negativně ovlivňující fungující systém (Novák, 2015) a (Jašek, 2002).

Útočník

Útočníkem lze chápat člověka, který chce vědomě ohrozit organizaci či firmu. Může to být osoba vně firmy nebo i osoba mimo tuto strukturu. Útok může mít jasný úmysl, ale je i možnost neúmyslného útoků (Gála, Pour & Toman 2006).

- Zde označení si rozdělíme útočníky, páchají úmyslné útoky:
- hacker – v IT velice sběhly, útokem získává prestiž
- vyzvědač – útokem získává informace pro politické účely
- terorista – útoky chce vyvolat strach a paniku
- kriminálník – útoky sleduje finanční zisk
- vandal – útoky chce poškodit systémy
- cracker – v IT velice sběhlý, snaží se proniknout do systémů za účelem krádeže, orientuje se na odcizení duševního vlastnictví – systémů s autorskými právy
- phracker – útokem získává bezplatný přístup k telefonním službám
- phreaker – útoky získává telekomunikační informace a jimi získává přístup k dalším informacím

2.2.5 Bezpečnostní požadavky

Při stanovení bezpečnostních požadavků vycházíme z celé řady standardů, norem, zákonů a nařízení. Formulujeme je následovně:

- důvěrnost – přístup k aktivům mají autorizované subjekty – pouze ověřené osoby, procesy mohou vykonávat činnosti v informačním systému

- zachování dostupnosti – autorizovaná osoba má neomezený přístup do informačního systému, nevyskytují se výpadky
- zachování integrity – aktivum nemůže měnit neautorizovaný osoba, nepovolená činnost, ani nekompatibilní nastavení změn

Další z faktoru ovlivňující bezpečnost systému:

Zajištění identifikace – veškeré aktivity jsou zaznamenávány (logování) a všechny změny v aktivu mají specifikovaného svého autora.

Zachování spolehlivosti – chování systému je konzistentní s nutnou archivací a dokumentací systému (Gála, Pour & Toman 2006).

2.3 Základy kryptografie

Kryptografie je věda využívající matematických metod pro šifrování dat. K přeměně čitelných dat do nečitelných tedy šifrovaných, k tomuto je zapotřebí šifrovací klíč. Tento klíč je potřeba k šifrovaní i dešifrovaní dat. Šifrování se dále dělí na asynchronní a synchronní. S tímto se dále pojí kryptoanalýza, která má za úkol dostat se k šifrovaným datum bez klíče (Doseděl, 2004).

Využití kryptografie je v celém informačním odvětví, kdy všechny data, které uživatel nebo firma vlastní, potřebuje nějakým způsobem ochránit. Šifrování jako takové můžu představit jako bránu ke svým datům, ke kterým se dostanu pouze se správným klíčem, tedy jen oprávněný vlastník.

Správný vlastník se správným klíčem – bezpečí

Špatný vlastník se správným klíčem – nebezpečí

Proto je potřeba v rámci firmy nebo organizace mít přísně daná pravidla a ty dodržovat, aby se minimalizovala šance na únik dat.

S rozsáhlým vývojem informačních technologii roste i objem dat, který uživatel nebo firma produkuje, to má za následek zpracovávaní větších množství dat, které jsou potencionálním bezpečnostním rizikem pro danou firmu. (Tento fakt je potřeba zmírnit příslušnými opatřeními softwarovým i hardwarovým vybavením doplněné o funkční implementaci doplněné vzdělaním personálu.)

2.4 Ochrana dat

Jak jsme již zmínil jsme v moderní době pokroku kde se nároky na informační techniku zvyšují. Jsou potřeba výkonnější hardwarové prvky v sítí a z hlediska softwaru se to vyvíjí stejně. Nové aplikační programu a sofistikovanější informační systémy jsou pohodlnější a výkonnější, než předešlé. To má za následek i větší množství zpracovaných dat, a tedy větší množství potencionálních škod při úniku dat. Proto si myslím, že je tato data potřeba chránit, před zničením, odcizením, přírodními katastrofami, či jiným poškozením. Jedinou možnou volbou je šifrování těchto dat. Kdy se zamezí přístupu k datům nepovolanému uživateli.

Šifrování, jinak kryptografie je nauka o metodách, které jsou schopny utajit čitelná data do obrazu nečitelných. Za pomocí šifrovacích algoritmů, které data znepřístupní. Každý algoritmus je specifický podle nějakého klíče. Zde rozeberu základní druhy šifrování (Doseděl, 2004).

Pro kryptografii s veřejným klíčem: RSA, Diffie-Hellman, DSA

Pro symetrické šifrování: RC2, RC4, IDEA, DES, Triple DES, AES, Camellia

Pro jednosměrné hešování: Message-Digest algorithm (MD2, MD4, MD5), Secure Hash Algorithm (SHA-1, SHA-2, SHA-3)

Jedná se všechno o algoritmy šifrující podle nějakého klíče.

2.4.1 Symetrické šifry

Jedná se o šifrování využívající stejný šifrovací klíč jak pro zašifrování, tak pro dešifrování. Výhoda šifrování jednoho klíče spočívá v rychlosti operace. Na druhé straně je zde nevýhoda snadného kompromitování všech dat, při prozrazení tohoto klíče. V praxi se symetrická šifra používá u méně využívaných dat jako jsou zálohy (Jašek, 2002) a (Doseděl, 2004).

Z pohledu symetrické šifry, to vidím jako hudbu minulosti. V dnešní době výkonných zařízení si myslím, že symetrická šifra bud ustupovat na úkor asymetrické.

2.4.2 Asymetrické šifry

Při asymetrickém šifrování jsou použity dva klíče. Jeden je veřejný a druhý soukromý. Veřejný klíč se využívá k zašifrování dat a je šiřitelný, dostupný. Soukromý klíč musí zůstat v tajnosti, obvykle u vlastníka celého klíče a tento klíč zajišťuje

dešifrovaní dat. Tyto dva klíče se berou jako jeden celek. Tedy jedna část bez druhé jsou k ničemu. Zároveň veřejného klíče není možné dopočítat soukromý klíč, díky silným matematickým funkcím a náročnosti výpočtu. Při dnešní technice nemožné. Nevýhodou asymetrického šifrování je pouze rychlost. Proto se využívá kombinace obou šifer (Jašek, 2002) a (Doseděl, 2004).

Podle mého celý koncept asymetrického šifrování není špatný, bezpečnostně dostatečný. Avšak při implementaci řešení asymetrické šifry mohou být udělány chyby a toto je hlavní úskalí této metody.

Následkem špatné implementace může dojít k infiltraci do datového přenosu, který je touto chybou postižen. Útočník je pak schopen odposlouchávat přenos dat nebo s ním jinak manipulovat, jako zadržet data či je pozměnit. V praxi při přenosu dat v rámci složek IZS, může dojít k dezinformaci – následkem špatně implementovaného informačního systému nebo jejich součástí. Výsledkem můžou být materiální ztráty, kvůli pozdnímu příjezdu, v krajních situacích i ztráty na životech.

2.4.3 Hash algoritmy

Je zde ještě jedna varianta, a to je hashovací algoritmus, ten nejčastěji slouží k šifrování hesel v systému. Hash je schopen zašifrovat heslo podle určitého klíče a zpětně nejde dešifrovat. Výsledkem je zahashovaná (zašifrovaná) hodnota která se dá porovnat, tedy při zadání stejného hesla bude hash hodnota stejná. Proto systém nepotřebuje znát naše heslo, ale pouze zašifrovanou hodnotou pomoci hashe (Jašek, 2002).

Úkolem hashovacích algoritmů je primárně identifikovat, jestli se jedná o stejný obsah textu.

Podmínky pro silnou hashovaní funkci:

- jednosměrnost – nesmí být možné z hodnoty hash odvodit původní zprávu
- bezchybnost a nezaměnitelnost – nesmí být možné dostat na dvě různé textové hodnoty tutéž hodnotu hash

Výborné k zašifrování (zamaskováni) nějakých hodnot na serveru. Poté stačí porovnávat pouze hash hodnoty, aniž by server musel znát pravou hodnotu dat. Postupem času si myslím, že budou potřeba složitější algoritmy pro hashování.

2.4.4 Zabezpečené protokoly a zabezpečení

Při přenosu veškerých dat v lokální sítí nebo mimo lokální sít, tedy přes internet, jsou využívány komunikační protokoly. Protokoly se používají k odeslání a přijímání elektronické pošty, jiný na přenos dat, další na zobrazovaní internetových stránek a podobné (Doseděl, 2004).

Můj názor je, že bez těchto šifrovaných služeb bychom nebyli schopni adekvátně chránit citlivá data firem či států. Bylo by velice jednoduché tato data zneužít. Celkově bez šifrovaného přenosu dat by docházelo k tolika datovým únikům, že na následky toho by mohly zkolabovat i velké mocnosti (Německo, USA, Rusko) – firmy a podniky uvnitř státu by byly znehodnoceny a nebyly by schopny konkurovat na trhu. To by mělo za následek poškození státní ekonomiky.

HTTPS

Hypertext Transfer Protocol Secure – Jedná se o protokol, který slouží k šifrovanému prohlížení webových stránek. Aktivně reagují na uživatele a podporuje různé nadstavbové skripty.

V dnešní době se toto stává pomalu standardem, avšak je třeba si dávat pozor na stránky, které toto ještě nepodporuji. Tedy při zobrazení stránek je v hlavičce stránek nešifrovaná podoba http protokolu na zobrazovaní stránek (Ludvík, 2008).

Následkem nešifrované komunikace http (nešifrovaná podoba https) by mohlo dojít ke zneužití – v podobě odposlechu na síti. Prostřednictvím tohoto protokolu v nezašifrované podobě by bylo jednoduché odcizit citlivá data, jako přihlašovací údaje do bankovnictví či jiných citlivých služeb. Vznikly by, tak materiální ztráty a ovlivnilo by to úroveň žití. V krajních případech zcizené údaje by mohly vést k fiktivním kontraktům či vykradení bankovních účtů, kde peníze by potencionálně sloužili k financováni dalších kybernetických útoků.

SFTP

Secure File Transport Protocol – Tento protokol slouží k přenosu dat v zašifrované podobě. Jeho předchůdce FTP slouží k samému účelu, avšak bez jakékoli ochrany, tedy bez šifrování dat. Šíření dat pomocí tohoto protokolu je velice oblíbený ve firemním prostředí, proto je třeba dbát i zde na bezpečnost (Ludvík, 2008).

WEP

Wired Equivalent Privacy – Při rozvoji bezdrátových sítí nastala otázka, jak zabezpečit tyto sítě. Dočasnou odpovědi bylo kódování WEP standartu IEEE 802.11i, které zajišťovalo autentizaci, tedy přístup do sítě a zabezpečení přenášených dat. Bohužel řešení zabezpečení WEP mělo konstrukční vady a muselo být nahrazeno novým zabezpečením WPA (Ludvík, 2008).

IEEE 802.11i – standart podle kterého se šifruje bezdrátový provoz na sítí.

WPA/WPA2

Wi-Fi Protected Access – Nástupcem bezdrátového zabezpečení WEP. Jedna se o vylepšené techniky zabezpečení standartu IEEE 802.11i. Toto zabezpečení má vyřešenou problematiku předchůdce a nedlouho na to vyšla WPA2, která využívá nového bezpečnějšího algoritmu. V dnešní době nedešifrovatelná. Všechny standarty zabezpečení jsou zpětně kompatibilní.

SSL/TSL

Protokol Transport Layer Security a jeho předchůdce Secure Sockets Layer se zaměřuje na bezpečný přenos dat mezi uživatelem, tedy klientem a serverem. Součásti přenosu je tzv., sdílené tajemství to jsi můžeme představit jako soubor čísel, které znají oba účastníci na základě sdíleného tajemství se může přenos šifrovat synchronně i asynchronně (Ludvík, 2008).

SSH

Secure shell – Umožnuje vzdáleně se přihlásit k počítači, opět je to náhrada za nešifrovanou službu. SSH je oblíbený, protože pomoci tohoto protokolu jsme schopni vytvořit šifrovaný tunel a zde nechat proudit data v nezašifrované podobě, pakliže je zde nějaký důvod, který to nedovoluje, např. ftp, http (Ludvík, 2008).

Digitální podpis

Využívá se pro digitální podepisování elektronické pošty. Zde zajišťuje autenticitu, kdy příjemce zjišťuje, zdali odesilatel souhlasí. Celý princip digitálního podpisu je založen na kryptografii přesněji na asynchronní šifře. Přeneseně si to můžeme představit jako klasicky podpis na papír (Doseděl, 2004) a (Jašek, 2002).

Ochrana fyzického přístupu

Je vhodné připomenout, že veškerá data jsou fyzicky umístěna na serverech a jejich diskových polích. Proto bychom měli vynaložit zvláštní úsilí pro to, aby se zde fyzicky nebyl nikdo schopen dostat. Např. do serverovny a zde odcizit, zničit, či, jinak manipulovat s daty, ke kterým nemá mít přístup. Samozřejmě s tím korespondují veškeré periferie, které jsou na servery nebo datová uložiště připojena. Řadíme zde veškerou hmotnou sít, od datové kabeláže, přes elektrické vedení až po koncové zpracováni dat nebo přistupování k datům, jakožto uživatele a jejich zařízení např. stolní počítače, notebooky, případně vysílače (routery).

Tuto ochranu můžeme zajistit více způsoby. Obvyklým způsobem je fyzické zamezení přístupu – zámky, čipovými bránami, lidskou ostrahou, nebo monitorovacím systémem, případně opět lidskou ostrahou (Jašek, 2002).

Z pohledu ochrany obyvatelstva, bychom měli zajistit, ochranu pro prostředky informačního charakteru, vykonávající činnost složek IZS a jiných složek ochranného charakteru. Při lehké dostupnosti tohoto vybavení jako vysílačky, pracovní notebooky, navigace či jiného technického vybavení (výjezdové vozy) by mohlo dojít k manipulaci tohoto zařízení. Výsledkem může být poškození těchto složek za účelem vědomého ohrožení kritické infrastruktury státu či organizace. Kde by mohlo dojít ke špatné koordinaci hasičů při následném zásahu např. při požáru firemních objektu nebo jiných významných budov jako jsou nemocnice, banky, úřady, logistická centra, sklady, rozvodny apod.

Ochrana před katastrofami

Dalším aspektem jsou přírodní vlivy a snížení rizik propuknutí jednotlivých hrozeb této kategorie. Později specifikuji v další kapitole analýze rizik.

Do této kategorie si můžeme představit, ochranu před požárem, zemětřesením, vodou, jinými silovými vlivy země (Jašek, 2002).

Jsem toho názoru, že v České republice a okolních státech, máme to štěstí, že zemětřesení (která by ohrožovala kritickou infrastrukturu), zde nejsou. Průmyslové parky velkých firem jsou na zelených loukách, kde je ohrožuje potencionálně zejména vichřice, povodně nebo požáry.

2.5 Analýza rizik

Při analýze rizik se snažím zjistit na jaké úrovni je bezpečnost. Je potřeba odhalit slabá místa a zjistit, jestli provedená opatření mají slibovaný efekt. Výsledkem analýzy je podrobná dokumentace o bezpečnostní situaci ve společnosti. Již jsem vysvětlil pojmy jako jsou aktiva, hrozby a riziko. Podle těchto faktorů postupuju v řadě úkonů pro analýzu rizik následovně (Jašek, 2002).

Identifikace aktiv:

Zjištění aktiv ve firmě a nahodnocení jednotlivých elementů v systému (Doseděl, 2004).

Identifikace hrozeb:

Identifikuji možné hrozby, které mohou nastat ve firmě, či organizaci (Doseděl, 2004).

Míra rizika:

Na základě výše zmíněných faktorů přiřazujeme k jednotlivým aktivům hrozby. Posuzováni je subjektivní veličina, podle důležitosti každého aktiva ve firmě (Doseděl, 2004).

Takto může vypadat příkladná tabulka sestavena na míru aktiv, které je hodnoceno v závislosti míry zranitelnosti nějaké hrozby.

Zranitelnost Hrozba	Nízká	Střední	Vysoká
Velmi nízká	Přijatelná	Přijatelná	Poškozující
Nízká	Přijatelná	Poškozující	Poškozující
Střední	Přijatelná	Poškozující	Nepřijatelná
Vysoká	Poškozující	Nepřijatelná	Nepřijatelná
Velmi vysoká	Poškozující	Nepřijatelná	Nepřijatelná

Obrázek 1 Tabulky popisující přijatelnost hrozeb (Jašek, 2002).

Ochrana a bezpečnost informací nezahrnuje pouze technickou část. Jsou zde veškeré činnosti, které přichází do styku s informačními technologiemi potažmo internetem jako takovým. Proto je zde velký blok zabývající se sociální oblasti, který je v informační bezpečnosti jeden s nejdůležitějších. Řeším zde spolehlivost zaměstnance, který často bývá tím nejrizikovějším faktorem celé analýzy. Nemusí to být ani člověk technického směru.

Představme si zde opraváře, obslužný personál (uklízecí služba), externí pracovníky. Tito zaměstnanci se mohou bez povšimnutí dostat do zakázaných prostor, třeba do serverovny, kde jsou uloženy všechna data. Zde může servery sabotovat fyzicky nebo zanést škodlivý software – spyware (škodlivý software pro špionáž oběti) na špionáž, či jiný malware (obecné označení pro škodlivý software), který data stáhne nebo bude sledovat.

Úklidová služba má možnost se dostat do kanceláří vysoce postavených lidi. Kde může infikovat počítač škodlivým softwarem, umístěným na flash disku připraveným útočníkem. Případně má prostor na fyzické odcizení či poškození počítače.

2.5.1 Lidský faktor

Zde rozeberu pojem lidský faktor a co si pod tím můžeme představit. Často se jedná o mechanismy sociálního inženýrství, které si podrobněji rozepíšeme v dalších kapitolách. Také si nastíníme možné obrany proti němu.

"Při posuzování bezpečnosti je třeba si uvědomit, že každý systém je jen tak silný, jak silný je jeho nejslabší článek. V případě zajištění informačních systémů je nejslabším článkem jednoznačně uživatel (Tvrdíková, 2008).

Lidský faktor je nejslabším článkem bezpečnostního systému, nejčastěji pro neznalé a nepřipravené uživatele. Často se jedná o zaměstnance v malých firmách, kteří nemají ani tušení, že něco jako pravidla informační bezpečnosti firmy, existují. Podle průzkumu Kaspersky.com (2017) pouze 12 % zná pravidla (směrnici) informační bezpečnosti firmy. Druhým průzkumem dodává, že až 46 % kybernetických incidentu je způsobeno neopatrnosti či nepozornosti, zaměstnancem firmy (systemonline.cz, 2018).

V praxi se setkávám s názorem, že informační bezpečnost není důležitým faktorem pro běh firmy. V tomto případě si můžeme představit na jakou míru je brána bezpečnost firmy. To má za následek nedůležitost při vytváření bezpečnostní směrnice firmy a následně její aplikováni. V krajních případech, tato informačně bezpečnostní směrnice úplně chybí. Od toho odvozujeme školení a vzděláváni zaměstnanců firmy v bezpečném užíváni výpočetní techniky a bezpečném chování na internetu. Mnohé opatření navrhuji v pozdější kapitole.

Zaměstnanci si především neuvědomují, že i svým chováním za osobními účely (návštěva sociálních sítí, osobní email) ohrožují firemní bezpečnost a její data. Mnohdy využívají stejná hesla pro osobní účty i firemní účty. Neoddělují osobní data od

firemních. Při komunikaci na sociálních sítích nebo emailem nehledí na svou bezpečnost – klikají na vše co uvidí, připojují se na veřejných Wi-Fi sítích, dostatečně si nechrání heslo. I fyzicky se vystavují nebezpečí ve formě zanecháni pracoviště bez dozoru. Neuzamknutí počítače, nebo se nechají nalákat „náhodou flashkou“ (flash disk) který připojí do počítače a zde je riziko zavlečení škodlivého softwaru. Dále se připojují na neznámých Wi-Fi sítích, mají uložená hesla v počítači (většinou jednoduchá hesla) nebo fyzicky v jeho blízkosti. Případně si odnášejí firemní data domů, kde to může vést k vědomému i nevědomému úniku dat.

Pro shrnutí popíšu základní body, které jsou potřeba udělat, abychom chránili uživatele (zaměstnance) před jimi samými a zajistili ochranu firemních dat. Uživatelé mohou napadat nejčastěji infikované e-maily či flash disky (externí uložiště). Pokud to není ošetřeno firemním kodexem, tak velmi často využívají Wi-Fi free síti a zde v nechráněném prostředí řeší firemní záležitosti.

Další významnou slabinou je pohodlnost, čím větší pohodlí, tím úměrně klesá bezpečnost. Tedy problematika jednoduchých nebo stejných hesel do více účtů jak soukromých, tak firemních – toto musí vymizet. Takové chování uživatele či zaměstnance firmy je velmi problémové. Zde jsou i moderní technická řešení krátká.

Proto je velmi důležité bezpečnostní trendy sledovat a průběžně vzdělávat své zaměstnance – formou celofiremních školení nebo podle zaměření zaměstnance, sdělování informací je možné pojmout formou hry. Dále průběžně je kontrolovat – namátkově fyzicky, jestli nastavené procesy a pravidla dodržují či poslat email kontrolující jejich chování (phishingový email). Tím jsme částečně schopni reflektovat potencionální hrozbu s parametrem lidské chyby. Na základě této a jiných hrozeb jsme nuceni vytvářet bezpečnostní politiku firmy pro její ochranu a stanovení pravidel.

Bez opatření nutných pro tuto potencionální hrozbu se můžeme setkat s rozsáhlý únikem dat ve všech různých odvětvích. Z praxe jde o nejčastější unik dat v podobě přihlašovacích údajů, osobních údajů (jméno, adresa apod.), firemních strategií a zakázek. Následkem toho může dojít k sabotáži firmy ekonomicko-politického charakteru. Zřejmě by došlo ke snížení životní úrovně obyvatelstva či charakteristickým škodám v daném odvětví. Příkladem může být energetika a únik přístupových údajů, kdy je útočník schopen na dálku poškodit fyzické zařízení energetické firmy, a tak může dojít k výpadku proudu ovlivňující širší okolí.

2.6 Bezpečnostní politika

Bezpečnostní politika je soubor opatření zahrnující formální a normativní pravidla bezpečnostních informací ve firmě či instituci. Současně je popisem postupu implementace a zavedení těchto pravidel do denní praxe (Tvrdíková, 2008).

Bezpečnostní politika neboli bezpečnostní opatření jsou popsána v zákoně kyberterostické bezpečnosti.

Zákon o kybernetické bezpečnosti (Zákon č. 181/2014 Sb., 2014) definuje:

„Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru.“

Plánováním informační bezpečnosti je první krok k budování bezpečnostní politiky. Zjistíme skutečný stav informační bezpečnosti v dané organizaci. Řízení bezpečnosti rozdělujeme na dvě části:

První část je legislativně organizační, kde nastavují procesy v rámci vztahu uživatel a firemní prostředí. Zde je důležité nastavit tyto procesy důsledně a uživatele pravidelně kontrolovat.

Při plánování pravidel bezpečnosti je potřeba vybudovat pravidla, která budou běžní uživatele znát a dodržovat. Jedním s dalších aspektu práce ve firemních prostředích je práce s firemní informační technikou (počítače, notebooky,aj.).

Dodržovat pravidla týkající se zakázaných typů příloh, nestahovat a neotevírat tyto přílohy ani žádné jiné, které nejsou výslovně povoleny. Do toho patří další aspekty bezpečnostních pravidel a doporučení, které si rozebereme v příštích kapitolách. Pote dostaneme komplexnější pohled na bezpečnostní politiku firmy a zejména na normu informační bezpečnosti firmy.

Dále pak, sledování zakázaných aplikací a samo spustitelných souborů, zakázaných a rizikových stránek.

Potřebné je správné nastavení firewallu, proxy serveru a jiných sítových prvku v rámci firemní sítě, aby se zamezilo nechtěnému kontaktu uživatele s připadnou hrozbou.

Druhou částí je část technická s následnou implementaci vybraných technických opatření (Doseděl, 2004).

2.6.1 Softwarová ochrana

Firewall

Otázka zní, co je jednoduší? Bránit vesnici ze všech stran nebo hrad s jedním vchodem? Takto si můžeme představit firewall, který je definován jako:

Sada opatření může být hardwarového, softwarového nebo personálního charakteru a má za úkol, propojit dvě a více sítí s různou úrovní nastavené bezpečnosti. Kde snižuje předem daná rizika vyplývající se spojení.

Dělíme je na tři základní skupiny:

Jednoduchý IP filtr – jednoduchý a prostý, funguje na bázi povolení nebo zakázaní jednotlivých portu.

Stavovy IP filtr – zde je tabulka stavu která reaguje na podněty na jehož základě se vyhodnotí a podle definovaných pravidel reaguje.

Sítový port – je speciální číslo, které slouží v počítačových sítích při komunikaci – do a vně počítačové sítě

Proxy – nejpokročilejší a nejnáročnější je při vytváření firewallu aplikační proxy. Ten se nastavuje pro každý konkrétní protokol, ten filtruje pakety podle aplikací, které s portem pracují. Implicitně je vše zakázané (Doseděl, 2004).

Firewall je běžná věc u každého počítače, avšak jen dobře nastavený firewall, může být nedobytnou pevnosti před útoky skrze komunikační protokoly. Ve firemním prostředí jsem toho názoru, že stačí mít jeden dobře nastavený firewall než sto špatně nastavených.

Antivirus

Jeden s hlavních elementu softwarové ochrany je antivirus. Bránit virům a jinému škodlivému softwaru páchat v počítací škody. Chování škodlivých softwaru je velmi různorodé. V pozdější kapitolách si ukážeme, jaké to jsou.

Je důležité udržovat antivirus aktualizovaný a držet se bezpečnostních zásad pro uživatele internetu. V opačném případě to může mít za následek obrovské škody ve formě hmotné – poškození, zničení, nebo odcizení dat, anebo nehmotné, jako je špionáž

jedince, tedy zasahování do soukromí, nebo celkový dopad na společnost a ztráta důvěryhodnosti při úniku informací (Doseděl, 2004) a (Jašek, 2002).

Do této kategorie můžeme zařadit ochrany software antimalware a antispyware. Tento software je specificky zaměřen na hrozby malware (obecné označení po škodlivý software) a spyware (špionážní škodlivý software).

Podle mého je to jeden s posledních prvků, který může zabránit neštěstí, když zklame nastavení sítí i vzdělanost (nevědomost) zaměstnanců. Kvalitní aktualizovaný antivirus a jeho užívaní, je základem pro všechny typy škodlivého softwaru, který lze do sítě, počítače zavléct.

Šifrování

Jak jsme již zjistili data jsou cenné informace, a jejich zneužití neoprávněnou osobou by mohlo mít značný dopad. Šifrování dat nám umožní ochránit data před jejich zneužitím. Při samotném šifrování, můžeme využít funkce operačních systémů nebo speciální software třetích stran (Doseděl, 2004) a (Jašek, 2002).

2.6.2 Hardwarová ochrana

Síťové prvky a nadstavbové moduly

Zde patří zmíněny hardwarový firewall a jiné síťové prvky fyzického charakteru poskytující ochranu. Také je to doplňováno nadstavbovými moduly – čipové karty. Pro ošetření přístupu, ochraně proti přepsaní a formátování nebo jen pro správné zálohování nebo kódovaní.

Záloha

Většina dnešních informací je již v elektronické podobě. Jak jsme již zmínili, objem dat se vývojem informačních technologií stále zvyšuje, a i přes všechny bezpečnostní prvky, které můžeme nastavit, je třeba zajistit zálohu dat. Může nastat situace, která všechny bezpečnostní opatření překoná. Potom by nám zbyla pouze dobře uchovaná záloha. Nejlépe mít zálohu mimo objekt ostrého provozu. Např. při požáru by záloha na stejném místě neměla žádný smysl.

Možnosti datových uložišť pro zálohováni dat:

- Přenosná média (cd, dvd, flash disk): Jednoduchý způsob zálohy. Výhodou je nejnižší cena. Nevýhodou pak možnost odcizení, popř. ztráty.

- Pevný disk interní/externí: Opět jednoduchý způsob zálohování, výhoda je zde větší uložiště než u předchozí možnosti. Cenově přijatelné. Nevýhodou je nemožnosti rozšíření a komplexnost řešení.
- Server: Zálohovací server se sloty pro pevné disky. Výhodou je možnost zálohování dat přes síťové LAN rozhraní, větší zálohovací kapacita (v závislosti na počtu a velikosti použitých pevných disků), Je zde možnost zrcadlení, ochrana proti selhaní některého disku zálohovacího serveru.
- SAN systémy: Vysokorychlostní síť. Síť je tvořena množstvím vzájemně propojených úložných prostorů. Výhody – Snadná správa, otevřenost řešení, vysoká úložná kapacita. Nevýhody – Vyšší pořizovací náklady.
- NAS systémy: Speciální servery pro připojení úložných zařízení k síti. Výhody – Nízké náklady na pořízení, jednoduchá implementace. Nevýhodou je špatná rozšiřitelnost.

Po seznámení se základními pojmy a strukturou bezpečnostní politiky, řeknu, co tuto bezpečnostní politiku firmy ohrožuje. V dalších kapitolách rozvedu podrobnější další legislativně organizační aspekty, normy informační bezpečnosti a také rozvedu technické parametry bezpečnosti politiky firmy.

Všechny tyto ochranné prvky tvoři směsici neprostupné bariéry, která je schopna odolat útokům a ochránit, tak firmu nebo instituci, před ztrátami. V případě nevěnování pozornosti prvkům softwarové a hardwarové ochrany by mohlo dojít k poškození firmy, instituce či státu s těmito následky.

Informační únik dat, s následkem neschopnosti konkurenčního boje – znehodnocení podniku pro odkup cizí firmou jiné velmoci (tvorba zázemí pro další mezistátní boje).

Z pohledu ochrany obyvatelstva může dojít k smazání nebo modifikaci dat jízdních řádu či jiných logistických uzlů. Důsledkem nedokonalého zabezpečení nebo pozdní obnovou dat, by mohlo dojít k dopravnímu kolapsu a znemožnění práce složkám IZS (integrovaný záchranný systém). Případně z druhé strany nedostatku personálu nemocnic, bank a jiných podniku kritické infrastruktury či nedodaného materiálu do těchto odvětví. To by mělo za následek nepokoje nebo zhoršení kvality životní úrovně.

Řada dat v oblasti bezpečnosti, ochrany obyvatelstva, krizového řízení, se přenáší po sítí a zde je potencionální riziko modifikaci, ztráty, či úniku dat.

2.7 Kyberterorismus

Oficiální definice kyberterorismu napsána D. E. Denningem (2001) zní:

„Kyberterorismus je konvergencí terorismu a kyberprostoru obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů.“

Definice bohužel není zcela shodná s praxi. Kyberterorismus je chápan jako útoky výhradně proti kritické infrastruktuře a její ovládnutí. V dnešní době se setkáváme spíše s útoky narušující určíte služby než komplexní kolaps vládního systému nebo nadnárodní firmy.

Definice kyberterorismu dle Janczewski a Colarik (2005): „Kybernetický terorismus lze definovat jako představitele aktivit vedených nebo koordinovaných státem s cílem získat informační převahu nebo vyřadit technologickou infrastrukturu protivníka.“

Zákon o kybernetické bezpečnosti (Zákon č. 181/2014 Sb., 2014). definuje:

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.“

Kyberprostor – „kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“

Je dle mého nehmotný svět vytvořený vzájemným propojením počítačových, informačních a komunikačních systémů.

Kritická infrastruktura – „kritickou informační infrastrukturou prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti.“ – informační systémy definuje krizový zákon (§ 2 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů – krizový zákon, ve znění pozdějších předpisů. Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.)

Dle mého se rozumí každý prvek nebo systém prvků kritické infrastruktury v odvětví komunikačních a informačních systému v oblasti kybernetické bezpečnosti, který je důležitý pro bezpečnost informací, zajištění důvěrnosti, integrity a dostupnosti informací a dat. Dále může plnit základní roli informační služby státu. Řadíme zde i nestatní podniky, které svými prvky v odvětví komunikačních a informačních systému mohou nepřímo ohrozit informační bezpečnost státu.

Jsem toho názoru, že kritická infrastruktura v oblasti informační bezpečnosti (kybernetické bezpečnosti) je velice provázaná. Napadením nestátního podniku může vést k získání informačních (výpočetní síly) zdrojů k napadení státních podniků a ochromení celé informační struktury státu nebo více firem.

Kybernetický útok – je útok skupinou hackeru – útočníku. Odehrávají se v kyberprostoru.

Útoky a útočníci jsou hrozbou dnešní doby. Omezují žití dnešní společnosti a ohrožují její existenci. Jsou schopni zničit výpočetní i jinou techniku, a proto bylo nutné pro její ochranu vydat zákon o kybernetické bezpečnosti. Dle mého názoru toto jsou příčiny vydání tohoto zákona.

2.7.1 Útočníci

Vnitřní útočník

Osoba připojena do lokální sítě, často se jedná o zaměstnance firmy. Příklady těchto útoku vypadají často jako nehody. Obrana proti těmto útokům je zvedáním loajality a spolehlivosti zaměstnance, ten pak nemá důvod, tak činit (Doseděl, 2004).

První je potřeba vědět, jaká motivace je pro zaměstnance důležitá. Může to být motivace finanční (formou odměn nebo zvýšením platu), dále uznání (písemné, ústní) někdo ocení materiálního typu (firemní zájezd, poukaz do zoo apod.) či prodloužení dovolené nebo práce z domova. To všechno může zvednout loajalitu zaměstnance.

Vnější útočník

Osoba, která nemá přístup do lokální sítě firmy. Zde musí překonat překážky, které firma připravila nezvanému návštěvníkovi. Je to série bezpečnostních opatření jako firewall, zabezpečovací protokoly a jiné. Zde je horší vystopovatelnost případného útočníka (Doseděl, 2004).

2.7.2 Nebezpečnost útočníku

Zde útočníky rozdělím do kategorii podle znalosti a množství dostupných prostředků:

Amatéři

Jedna se o jedince z minimální znalosti technického směru jejich motivace je zvědavost, tedy zkoušejí známe bezpečnostní díry a využívají programy jiných. Tato skupina je charakteristický středoškolský student, nebo člověk s nedostatkem času a prostředků (Doseděl, 2004).

Hackeři

Jsou to osoby znalé v oblasti informačních technologií často vysokoškolští či zdatní středoškolští studenti. Tito lidé mohou napáchat významné škody, avšak jejich motivace není uškodit nýbrž, opět zvídavost a poznaní čeho dosáhnou. Tato skupina má znalosti, avšak ne čas a prostředky (Doseděl, 2004).

Profesionálové

Tito lidé mají bohaté zkušenosti na poli informačních technologií. Jsou velice dobře vybavení, jak znalostně, tak prostředky, které mají k dispozici. Často se jedná o organizované skupiny, které jsou najímány na vyšší instituce (stát, úřady) nebo větší firmy. Obrana proti této skupině je obzvlášť nákladná (Doseděl, 2004).

Nebezpečnost útočníku je taková, jak moc kladu důraz na informační bezpečnost. Jestli jim dovolím činit ve firemní sítí co chci, tak se nemusím divit následkům, které mi je schopen udělat i amatér. Myslím si, že většinu útoku jsem schopen preventivními opatřeními eliminovat, ale přiznávám, že jsou zde i profesionální skupiny, před kterými není obrany.

Je pravděpodobné, že ochrana dat a informační bezpečnosti bude nekonečná práce. V důsledků neustálého vývoje škodlivého softwaru a jiných metod, útočníků. Motivací se stává, stále větší vliv elektronických dat na svět.

2.8 Hrozby a zranitelnosti

Firemní sítě a počítače v nich jsou připojeny na internet, kde je čeká spousty bezpečnostních rizik a tyto rizika stále přibývají. Útočnicí vytvářejí, stále důmyslnější techniky pro to, aby se dostali k hodnotným datům. Používají různé viry, zamaskované jako běžné programy, které mají postranní úmysly, ve smyslu ovládat počítač oběti, bez jeho vědomí (Doseděl, 2004).

Spousta lidí si pod pojmem virus představí všechny možné typy infiltrací, aniž by rozlišovali druhy těchto hrozeb.

Vývoj škodlivého softwaru je v dnešní době lukrativní byznys, proto jde vývoj rychle dopředu. Proto se zvyšuje míra rizik, jednotlivých hrozeb, které je třeba řešit.

Každý virus, trojský kůň nebo červ může být pojat jako nemoc, kterou je potřeba vyléčit. Je zde mnoho faktoru, jak se vyvarovat nakažení škodlivého viru do firemní sítě. Hlavním řešením vidím jako osvětu zaměstnanců. Před veškerým škodlivým softwarem. Protože ve všech případech, napadení nějakým malwarem mohou být následky, jak lokálního charakteru, tak i globálního. Paradoxní nejúčinnější obranou, proti veškerým těmto malwarum je práce v lokálním prostředí bez přístupu internetu.

Množství a druhy útoku zaznamenané a oznámené v průběhu deseti let. S obrázků vychází nejvyšší četnost phishingových útoků, které každoročně stoupají. Proto je třeba si dát pozor na tento typ útoků a zaměstnance (uživatele) na tento typ útoků školit. V posledních letech je již malware na ústupu, avšak pořád činí významnou položku při pohledu na obrázek, bezpečnostních incidentů.

Druhy incidentů (otevřené a zavřené)

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	sum
IDS*				491	3924	2121	2380	3771	9944	13858	8782	45271
Phishing	65	220	209	144	159	175	368	367	363	409	231	2710
Spam	47	28	103	26	43	73	159	108	290	121	73	1071
Other	1	5	13	62	14	75	102	264	181	200	84	1001
Malware	53	134	121	10	20	45	117	240	104	99	36	979
Trojan	66	6	26	5	5	12	56	90	79	94		439
Probe		3	14	25	12	26	86	42	13	26	2	249
DOS	2	4	2	2	68	72	32	37	12	14	3	248
Virus		84	99									183
Botnet		3	46	5	8	15		4	71	29		181
Portscan	10	4	1	6	1	3	2	5	6	13	1	52
Pharming							18	3	2	3	3	29
Unknown											1	1
sum	244	491	634	285	330	496	940	1160	1121	1008	434	7143

Obrázek 2 tabulka množství a druhy útoku (csirt.cz, 2018).

Zde doplňující pojmy:

Botnet – V současné době je termín nejvíce spojován s malwarem (škodlivý software), kdy botnet označuje síť počítačů infikovaných speciálním softwarem, který je řízen z jednoho centra (Wikipedia, 2017).

Zombie – infikované počítače v sítí botnetu

Visual Basic – program

OS – operační systém

BAT – dávkovací soubor v operačním systému Windows

.jpg, .exe – zkratky označující druh souboru (.jpg - obrázek)

Rozčleníme si zde jednotlivé druhy škodlivého softwaru:

2.8.1 Viry

Pojmenování počítačového viru, má základ v biologických virech. Jejich charakteristická vlastnost je množení sama sebe, což splňuje biologickou definici. Je k tomu potřeba hostitel, což v tomhle případě splňuje počítač oběti tedy jeho úložný disk. Nejčastěji to bývají spustitelné soubory, systémové oblasti disků nebo soubory specifických aplikací (což mohou být dokumenty MS Excel, skripty Visual Basicu –

program a mnohé další). Je zapotřebí spuštění hostitelského kódu jako původce, zde se aplikuje a replikuje (Doseděl, 2004).

Druhy virů a jejich projevy

Souborové – napadají spustitelné soubory (.exe), přepisují části kódu sama sebou, to má za následek odlišné chování programu.

Makroviry – cílem jsou dokumenty MS Office (.xls, .docx, .doc), tyto viry jsou nejčastějším druhem viru a také by mohli být v budoucnu rizikem.

Boot viry – útočí na jádro OS, při zavedení tohoto viru do systému se při každém použití flash disku infikuje a slouží k šíření viru.

Rezidentní viry – nachází se v operační paměti, skenují diskové operace

Stealth – Ukrývají se před antivirovými programy, tím že podávají mylnou zprávu. Projevy počítačových virů mohou být různé, já uvedu ty nejzásadnější.

Blokování místa, nestabilita systému, zpomalení systému – nejčastější funkce skrytých virů, uživatel o jejich operování na pozadí počítače nemá žádné ponětí. Často modifikuji sama sebe, využívají výkon procesoru pro svůj prospěch nebo se jen bezúčelně množí.

Dále to mohu být různá vyskakovací okna a jiné projevy – některé viry se snaží na sebe upozorňovat různými způsoby, textem a zvukem.

V neposlední řadě se mohou projevit úkony jako:

Krádež dat, Ničení dat – V těchto případech je schopen útočník bez našeho vědomí odcizit nebo zničit data. Často to bývá agresivním způsobem, který zamezuje obnovení dat.

2.8.2 Trojské koně

Přímo spustitelný soubor, nemá sebe-replikační schopnost. To znamená, že při odstraňování škodlivého kódu postačí smazání souboru. Tváří se jako nějaký užitečný program, ale ve skutečnosti obsahuje škodlivý kód. Nazýván tak podle legendy o Troji.

Password – stealing trojské koně (PWS)

Druh trojského koně, který je naprogramován tak, aby zjišťoval hesla. A to pomocí sledování stisků kláves. Stisknutá tlačítka ukládá a poté je odesílá na emailové adresy, tvůrcům – útočníkům. často problém s českou diakritikou (Bitto, 2006).

Destruktivní trojské koně

Klasicky tip trojského koně, po spuštění maze všechny data. Lze zde řadit i jednoduché BAT trojany, tyto dávkovací soubory jsou jednoduché pro detekci.

Downloader

Program, který má za úkol stahovat k oběti další škodlivý software, v podobě dalších viru apod. Častý případ situace je konečný pád systému.

Proxy trojský kůň

Napadená oběť se stane rozesílačem spamu – tedy nevyžádané

pošty.

2.8.3 Červi

Červ je druhem viru distribuován skrze email. Většinou uložen v příloze, obsahující jenom škodlivý kód červa. Často pošle adresář kontaktu útočníkovi pro další zneužití.

Zde se využívá lidský faktor, jako hlavní zbraň tohoto druhu škodlivého kódu. Pod záminkou "výher" a jiných „prémiových věci" se snaží oběť oklamat. Ještě se zde využívá nepozornosti uživatele ve dvojí příponě „.jpg.exe". Jsou i červi které mají upraveny obsah emailové zprávy a jen pouhé otevření je nebezpečné.

Síťový červ

Druh pohybující se na lokálních sítích. Jeho vlastnosti jsou podobné ostatním červům.

2.8.4 Spyware

Spyware se dá definovat jako infiltrace a nepozorovatelný provoz bez vědomí uživatele. Pak je druhá skupina řazena do rodiny spyware a ta má za úkol neustále uživatele obtěžovat a neustále na sebe upozorňovat (Bitto, 2006).

Z pohledu ochrany obyvatelstva, je zde riziko napadení státních i nestátních podniků a institucí. Kdy špionáž těchto podniků může prospět útočníkovi v manipulaci rozvoje státní ekonomiky (pozorování dění ve firmě, zakázky, uvedení produktu na trh apod. – reakce na to mohou být v podobě podhození ceny, uvedení konkurenčního produktu dříve). Na následky toho, se může změnit podílové zastoupení firem na trhu a poskytnout, tak výhodu infiltrujícímu se investorovi nebo firmě, která za tím stojí.

Adware

Má za úkol zobrazovat reklamy a vyskakující okna s reklamou. Velice často bývá adware součásti jiného programu, co chceme naistalovat. Zde se sází na nepozornost uživatele, který nevědomě odsouhlasí instalaci tohoto softwaru spolu s potřebným programem (Bitto, 2006).

Hijacker browser

Software má za úkol přepisovat navštívenou domovskou stránku na stránku chtěnou útočníkem. Nejčastěji to bývají stránky, které jsou sponzorované. Jsou různé typy provedení tohoto softwaru, v nejhorší variantě může poškodit systém – přepisuje hodnoty registru. Program často blokuje vyhledávání antivirových a antispywarerových aplikací. Opět se jedná o software, který se do počítače dostane nepozorností uživatele. Ovšem využívají se i nedostatky ochrany počítače jako je neaktualizovaný prohlížeč, tedy je schopen proniknout do systému bez vědomí uživatele.

Keystroke Logger

Dělím je na hardwarové a softwarové. První zmíněný je fyzicky namontován v počítači, kde snímá stisky na klávesnici. Druhy typ, softwarový je program, který umí sledovat stisky na klávesnici v reálnem case. Tyto data se přeposílají útočníkovi.

2.8.5 Backdoor

Útočník zdolá zabezpečovacího mechanismu, užívaného nejčastěji ke vzdálenému přístupu do systému. Po získání kontroly nad systémem, se stává z počítače tzv. „zombie“. Při více počítacích se používá pojem „botnet“. Může přispět ke kriminální činnosti např. DDoS útok (Bitto, 2006).

2.8.6 Ransomware

Lze definovat jako vyděračský software, který má za úkol znepřístupnit data uživatele a vyžadovat za něj výkupné. Je to relativně nový druh škodlivého kódu, který se rychle vyvíjí. Principem je šifrováni dat uživatele a na odblokování dat je vyžadované výpalné, které pokud nebude zaplaceno, tak útočník hrozí trvalým smazáním dat (Wikipedia, 2018).

Charakterově se chová jako trojský kůň či červ. Znepřístupnění uživatelových dat je činěno formou šifrování celého disku, nebo jen zamknutí důležitých části operačního systému.

V praxi je tento druh škodlivého softwaru velmi oblíbený. Proto si myslím, že by si uživatel měl dávat pozor, co na svém potažmo firemním počítači provádí. Zavléct si tento druh malwaru, je podle mého jednoduché jako samotný ransomware. V případě napadení tímto ransomwarem je dobré mít k dispozici zálohy. Ze zkušenosti se oběť již k datum nedostane, popř. riskuje riziko zavlečení nějakého spywaru – když oběť zaplatí, útočník pošle klíč na dešifrování obsahu, ale je zde riziko, že útočník již zde nechal nastražený jiný škodlivý software.

2.8.7 DoS útoky

Jednou s největších kybernetických hrozeb je tzv. DoS útok. Jedna se o techniku odepření služeb – Denial of Service. Jedna se o nejpoužívanější a nejnebezpečnější formu kyberútoku. Často postihující větší část informační infrastruktury než jen jednoho uživatele.

Podle Janczewski a Colarik (2005) – DoS Představuje „přehlcování cílové stanice požadavky, které vedou ke zpomalení či k odstavení systému na nějž je útok veden“.

To má za následek zhroucení výpočetní techniky oběti a celkové znepřístupnění jeho služeb. Pod tímto si můžeme jednoduše představit zamezení přístupu do všech známých služeb v rámci výpočetní techniky jako je email, webové stránky, online účty, bankovnictví apod.

Rozšířenější formou tohoto útoku je DDoS útok, který je jako DoS velice podobný. Rozdíl je popisován ve formě útočníka. Zde je útočníku vice, tedy přesněji jeden útočník má sít ovládnutých jiných zařízení – této sítí se říká „botnet“ a účastnici botnetu jsou „zombie“. Skrze, které utočí na oběť s více míst. Proti tomuto typu útoku je složitější se bránit, protože útoky jsou prováděny vícenásobně a naráz.

V praxi jsem toho názoru, že je to poměrně jednoduché, útočník s dostatečnou výpočetní a datovou silou napadne (zahltí) informační zdroje nějaké z institucí a poměrně dlouho je schopen držet oběť v šachu. Pro představu to mohou být informační weby všech státních ministerstev – kdy zahltí příslušné weby, velkým množstvím přístupů a na následky toho budou veřejně sdělovací prostředky státu omezeny.

2.9 Speciální techniky útoku

Do této skupiny patří hlavně sociální inženýrství a metody od něho odvozené. Hlavní pointou těchto kyberteroristických technik je přinucení oběti tomu, aby nám odevzdala citlivé údaje – míněny informace pro vstup do kyberprostoru. Pro představu to mohou být přístupové údaje do informačních systému, různých účtů nebo i kontaktu na jiné osoby apod. (Vítek & Vítková, 2004).

2.9.1 Sociální inženýrství

Jak již z názvu vyplývá sociální inženýrství je způsob manipulace s lidmi za účelem obohacení na úkor oběti. S tím koresponduje pojem lidský faktor, který popisuje možnosti náchylnosti na jednotlivé hrozby v rámci lidského faktoru. Od hodnocení míry jednotlivých rizik jsme schopni říct, jak moc velkou hrozbou pro nás může být sociální inženýrství, případně co proti němu dělat (Mitnick, 2003).

Můžeme to definovat jako metodu psychologického ovlivňování za pomocí cizí nebo smyšlené identity, kterou útočník používá ke klamání lidí.

Při použití této techniky může být systém vysoce zabezpečen, ale jeho slabinou bude stále uživatel. Můžeme si uvést příklad.

Tuto techniku můžeme považovat za nejpřístupnější způsob, jak získat informace, navíc použitím komunikačních technologií, jako jsou emaily, IM (instant messaging – kecálek) nebo telefon, nám dovoluje vydávat se za někoho jiného. Oběť není pak schopna poznat kdo je na druhé straně. Útočník se většinou snaží navázat s budoucí obětí jisté přátelství nebo důvěru tím, že se vydává za pracovníka technické podpory nebo nadřízeného s firmy. V tomto případě může použít direktivní formu nátlaku a donutit pracovníka bezmyšlenkovitě poslat informace útočníkovi.

Nepřímá technika sociálního inženýrství spočívá v ponechání nakaženého media v dosahu oběti, která si sama nevědomě aplikuje vir do svého zařízení. Tak se infikuje.

Útočníkovi postačí někde na parkovišti nebo u vchodu do společnosti, z které chceme získat informace, položit například USB flash disk nebo DVD s virovým obsahem. Pokud ji uživatel zvedne a poté vloží do počítače, dojde k rozšíření škodlivého obsahu do uživatelova systému a může se šířit dál ve firemní síti (NÚKIB, 2018).

2.9.2 Phishing

Phishing znamená získávání citlivých informací nelegálním a neetickým způsobem.

Je prováděn pomocí podvodného emailu, který je posílán danému uživateli nebo skupině uživatelů s cílem získat především přihlašovací údaje k účtům, pro jejich další zneužití. V drtivé většině případů se jedná o pokus vylákat údaje k platebním kartám nebo přihlašovací údaje do internetového bankovnictví. Mimo údaje k bankovním účtům se útočníci snaží získat údaje i k jiným institucím, kde se manipuluje s penězi pro příklad alternativní platební brány, aukční síně, e-shopy renomovaných značek.

V phishingových emailech se používají psychologické a technické prostředky k přesvědčení adresáta k předání informací, a to co nejjednodušším způsobem.

Fungování phishingu je použití sociálního inženýrství, ve výsledku to znamená, že v adresátovi, po přečtení emailu, bude nabyt dojem, který ho oklame a on nepozná, jestli se jedná o důvěryhodnou osobu či nikoli.

Dalšími klíčovými znaky pro udržení hodnověrnosti podvodného emailu, je zachování grafiky institutu, který se útočník snaží napodobit. Je důležité, aby se snažil o co největší autentičnost doprovázenou i gramaticky a stylisticky správným textem. To dává věrohodnou a ucelenou formu hodnověrnosti podvodného emailu.

Dalším důležitým znakem je zfalšovaná emailová adresa, kde jde o co nejpodobnější a nejvěrohodnější originálu. Často se v podvodných emailech používají stručné tabulky, žádající jejich vyplnění, citlivými udají. Další forma může být podvodný odkaz směrující na podvodné stránky útočníka, opět žádající o citlivé údaje.

Pěkný případ je záměna písmena malé L „l“ za číslici jedna „1“, pro běžného uživatele maličkost, které si nevšimne.

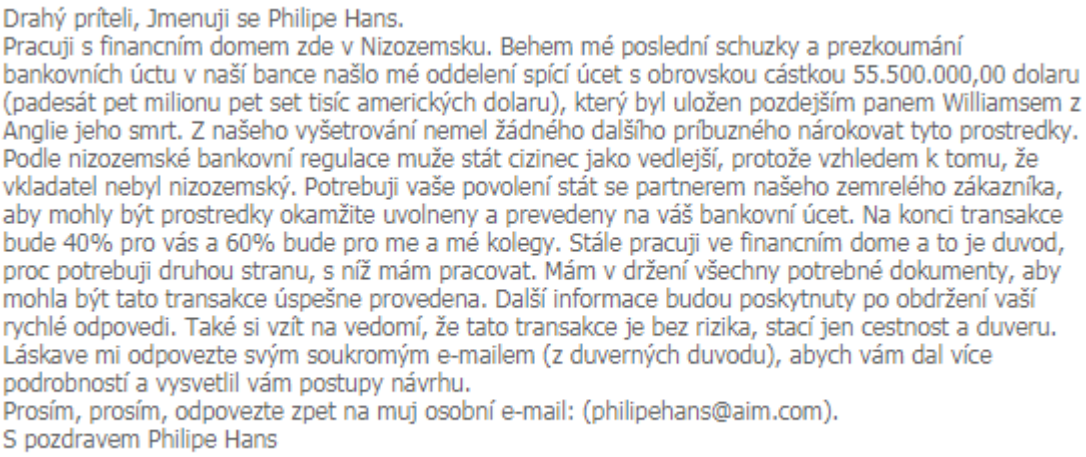
Další z možnosti jsou sociální sítě, instant messaging (chatovací aplikace př. Messenger, Twitter) Jedná se formu útoku, kdy se útočník vydává za přítele oběti, popř. zcizí účet přítele oběti a vyžaduje po oběti pomoc. Nejčastěji ve formě posláni peněz nebo ověření přes SMS. V obou případech je peněžní ztráta (NÚKIB, 2015).

Nigerijské dopisy

Další odnoži jsou tzv. nigerijské dopisy. Jde opět o podvodný email s průvodním textem. Obsahem zprav tvrdí pisatel, že disponuje velkým majetkem a potřebuje ho

pomoc poslat do jiné země. Princip podvodu je v nečekaných poplatcích v průběhu celé administrace (NÚKIB, 2018).

Předmětem emailu je obnos peněz, o který se rád rozdělí za protislužbu ve formě přeposlání peněz. Jakmile oběť začne reagovat, začíná útočník vyžadovat citlivé informace, které může využít proti oběti, ta pokračuje ve hře útočníka a platí nečekané výdaje při transakci.


Drahý príteli, Jmenuji se Philipe Hans.
Pracuji s financním domem zde v Nizozemsku. Behem mé poslední schuzky a prezkoumání bankovních úctu v naší bance našlo mé oddelení spící úcet s obrovskou cástkou 55.500.000,00 dolaru (padesát pet milionu pet set tisíc amerických dolaru), který byl uložen pozdejším panem Williamsem z Anglie jeho smrt. Z našeho vyšetrování nemel žádného dalšího príbuzného nárokovat tyto prostredky. Podle nizozemské bankovní regulace muže stát cizinec jako vedlejší, protože vzhledem k tomu, že vkladatel nebyl nizozemský. Potrebuji vaše povolení stát se partnerem našeho zemrelého zákazníka, aby mohly být prostredky okamžite uvolneny a prevedeny na váš bankovní úcet. Na konci transakce bude 40% pro vás a 60% bude pro me a mé kolegy. Stále pracuji ve financním dome a to je duvod, proc potrebuji druhou stranu, s níž mám pracovat. Mám v držení všechny potrebné dokumenty, aby mohla být tato transakce úspešne provedena. Další informace budou poskytnuty po obdržení vaší rychlé odpovedi. Také si vzít na vedomí, že tato transakce je bez rizika, stací jen cestnost a duveru. Láskave mi odpovezte svým soukromým e-mailem (z duverných duvodu), abych vám dal více podrobností a vysvetlil vám postupy návrhu.
Prosím, prosím, odpovezte zpet na muj osobní e-mail: (philipehans@aim.com).
S pozdravem Philipe Hans

Obrázek 3 Ukázka dopisu (hoax.cz, 2018)

2.9.3 Pharming

Pharming je vylepšena forma phishingu. Na rozdíl od phishingu, kde se vás snaží oklamat pro vstup na podvodnou stránku, zde dochází k automatickému přesměrováni na cizí stránku bez vědomí uživatele. Jsou dva způsoby, jak útočník může docílit tohoto podvodu. Jako první případ je infiltrace uživatelova počítače virem nebo malwarem (Bezpecnyinternet.cz, 2018).

Ten zajistí, aby při zadání korektní adresy došlo k automatickému přesměrování. Tento druh pharmingu bývá většinou identifikován antivirovými nebo antispywarovými aplikacemi.

Druhý složitější způsob, navíc je z počítače uživatele téměř nezjistitelný a je obtížné se proti němu bránit. Útočník napadne vnější DNS server a pokud se mu podaří změnit DNS záznam například u internetového bankovnictví, tak veškerý přístup na stránky je přesměrovaný jinam.

DNS server – překládá názvy stránek na odpovídající IP adresy. Je to z toho důvodu, lepšího pamatovaní slov než číslic, proto se tyto servery používají.

2.9.4 Defacement

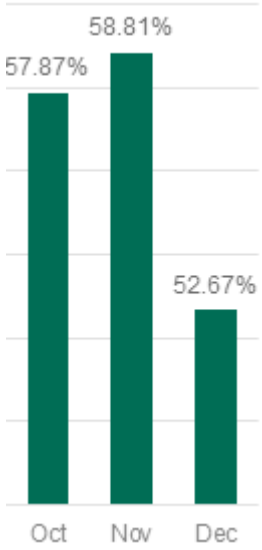
Je to známa metoda kyberterorismu, která spočívá v modifikování webových stránek jiným často zavádějícím obsahem. V podstatě jde o zmatení uživatelů, to zvyšuje riziko neočekávaného chovaní uživatelů. Jedna se o tzv. spam a hoax.

Spam

Označení spam se používá pro masové zasílání nevyžádané elektronické korespondence. Ve většině případu je to reklamní sdělení. Avšak patří zde i cílené útoky na danou skupinu uživatelů nebo nigerijské dopisy – jeden z druhů sociálních technik.

Obrana proti spamu je částečně technická, kdy jsme schopni nastavit na emailovém serveru firmy filtry. Tyto filtry jsou schopny s určitou procentuální úspěšností tyto emaily odchytávat. Nicméně ani toto řešení není dokonalé. Proto jsme schopni ještě omezit tzv. „vyžádané“ nevyžádanou postu. Pod tímto termínem si představíme reklamní sdělení na bázi nákupu v internetovém obchodě, kdy při objednávce odsouhlasíme využití emailové adresy k těmto účelům. Proto je třeba přistoupit k osvětě uživatele, který to částečně může kompenzovat. A to omezením registrace emailového účtu pro webové portály, např. různé internetové obchody (Ludvík, 2008).

Průměrné množství spamu podle antivirové společnosti Kaspersky Labs (2018) za měsíce říjen, listopad, prosinec roku 2017.



Obrázek 4 Množství zachyceného spamu (Kaspersky.com, 2018)

Hoax

Hoax je z anglického překladu vyjádřeni pro falešnou, poplašnou, podvodnou zprávu, kdy hlavním cílem této zprávy je způsobit rozruch ve společnosti. Často se jedná o upozornění před novým virem, který má napáchat obrovské škody ve firmě.

Hoax je nebezpečný, ač to na první pohled nevypadá. Z fyzického pohledu vytěžuje datové linky a servery společnosti, stejně jako spam.

Druhý zásadnější faktor je důvěryhodnost firmy. Díky sdílení hoaxu mohou uniknout citlivá data např. jméno, adresa, emailové adresa apod. na následky toho to může poškodit dobré jméno firmy a následující zřetězené dopady – ekonomického a společenského charakteru Hoax.cz (2018).

Tyto falešné zprávy dělíme podle výzvy či varování, které obsahují:

- Varování před smyšleným virem, různé internetové útoky, jiné nepravděpodobné nebezpečí
- Falešné prosby o pomoc, petice a výzvy
- Snadné výdělky, podvodné loterie
- Dopisy štěstí nebo žertovné zprávy

Struktura dopisu obvykle obsahuje:

- Stručný popis nebezpečí
- Ničivost – míru následku, reálných či nereálných
- Důvěryhodná autorita – zfalšovaná loga důvěryhodných společnosti např. Microsoft, Apple.
- Výzva – nabádáni k šíření zprávy

3 Metody práce

Heuristika – metoda získávání, shromažďování a třídění historických pramenů a informací

Analýza – rozbor, rozklad, postup od abstraktního ke konkrétnímu

Syntéza informací – spojení, sjednocení, systematický souhrn, výklad, objasnění

4 Výsledky

4.1 Aktuální bezpečnostní hrozby

Přehled aktuálních bezpečnostních hrozeb zpracované Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB):

Meltdown – chyba v moderních procesorech

Chyba označovaná jako Meltdown dovoluje uživatelským procesům číst data z libovolné části fyzické paměti (hardwarová součástka, každého počítače), tedy i data jiných procesů (i privilegovaných) nebo jádra systému. Tímto způsobem mohou být ohrožena i data mezi virtuálním a fyzickým zařízením. Chyba je způsobena mapováním adres jádra systému do uživatelského prostoru paměti a nesprávnou manipulací s vyrovnávací pamětí.

Aktualizace běžných operačních systémů opravující chybu Meltdown jsou již k dispozici.

Některé antiviry mohou způsobit problémy se stabilitou systému po nainstalování opravy této chyby.

Postižení systémy – všechny operační systémy na zařízeních s procesory Intel, AMD a ARM (praktické zneužití nepotvrzené) (NÚKIB, 2018).

Spectre – chyba v moderních procesorech

Chyba označovaná jako Spectre umožňuje čtení libovolných dat v rámci jednoho procesu. Například u webového prohlížeče tedy dovoluje kódu na jedné webové stránce číst data na všech ostatních právě otevřených stránkách.

Pro odstranění chyby je nutná aktualizace firmware zařízení. Dostupnost aktualizace závisí na konkrétním výrobci hardware. Některé webové prohlížeče dovolují nastavit funkci otevírání každé webové stránky v rámci samostatného procesu, která omezí dopady případného zneužití.

Postižené systémy – všechny operační systémy na zařízeních s procesory AMD, Intel a ARM (NÚKIB, 2018).

ROCA – zranitelnost v generování RSA klíčů

Výzkumníci z Masarykovy univerzity (Centre for Research on Cryptography and Security) a z dalších dvou zahraničních týmů objevili zranitelnost v procesu generování RSA klíčů, který se odehrává v softwarové knihovně implementované například v kryptografických čipových kartách, bezpečnostních tokenech (ověřovací USB klíče – flash disky) a dalších hardwarových čipech vyrobených společností Infineon Technologies AG.

RSA klíč – je šifra s veřejným klíčem, jedná se o první algoritmus, který je vhodný jak pro podepisování, tak šifrování.

Dopad zranitelnosti – vzdálený útočník může z hodnoty veřejného klíče spočítat privátní RSA klíč. Soukromý klíč může být zneužit k podvržení identity legitimního vlastníka, dešifrování citlivých zpráv, padělání podpisů (například pro vydávání softwaru) a další související útoky (NÚKIB, 2018).

KRACK – zranitelnost protokolu WPA2 umožňuje čtení šifrovaných dat

Chyba v protokolu WPA2, která útočníkům umožňuje číst šifrovanou komunikaci na bezdrátových sítích standardu IEEE 802.11 zabezpečených právě tímto protokolem. Chyba byla nazvána KRACKs (Key Reinstallation Attacks).

Útok je veden na komunikaci, která je nutná k sestavení spojení při přihlašování klientské stanice k přístupovému bodu. Této komunikaci se říká 4-way handshake (ověřovací výměna dat), jelikož dojde k výměně čtyř paketů (zjednodušeně zprávy) za účelem ověření pravosti hesla k bezdrátové síti a sestavení šifrovacích klíčů pro další komunikaci.

Obranou vůči tomuto útoku je co nejdřívější aktualizace firmwaru přístupových bodů (např. routeru). Vydání záplat však může zejména u starších zařízení určených primárně pro domácí použití trvat déle a v některých případech nemusí být aktualizace vůbec vydána (NÚKIB, 2018).

Petya/Petrwrap/NotPetya – nová hrozba ransomwaru

Ransomware Petya/Petrwrap/NotPetya se začal šířit během úterý po hackerském útoku na ukrajinskou softwarovou společnost M.E.Doc. Útočníci napadli účetní software, který tato společnost vydává. Automatická aktualizace tohoto software způsobila, že počítače uživatelů byly infikovány. Malware tak velmi rychle infikoval

velké množství počítačů zejména na Ukrajině, dále v Rusku, Francii, Dánsku, ve Španělsku a několika dalších státech.

Po infekci se malware snaží získat přihlašovací údaje doménového administrátora a šířit v lokální síti. K šíření využívá několik metod:

My si v kostce popíšeme základy pronikání tohoto ransomwaru. V první řadě se pomoci zranitelného protokolu v systému Windows dostal k pravomocem pro správu a přepis pevného disku. Kdy v druhé fázi využil těchto pravomoci a zašifruje (Master Boot Record) startovací část systému Windows. Při opětovném spuštění není systém schopen fungovat bez nezašifrované části systému. Chyby využívající tento ransomware jsou součásti uniklých dat americké NSA.

Postižené systémy – Počítače s OS Microsoft Windows.

Řešení je kontinuální aktualizace operačního systému, antivirových ochran a zabezpečení. Zvýšit obezřetnosti při práci s nevyžádanými e-maily a neznámými soubory. Různé antivirové společnosti nabízí řadu řešení, které dokáží detekovat infikované soubory ještě před jejich spuštěním, případně blokovat IP adresy, které distribuují škodlivý obsah. Žádná ochrana však není stoprocentní, a tak nejúčinnějším řešením je zálohování (NÚKIB, 2018).

Crash Override – Win32/Industroyer – nová hrozba pro průmyslové řídící systémy

Industroyer je sofistikovaný malware určený k narušení činností průmyslových řídících systémů, především systémů používaných v elektrických rozvodnách.

Jedná se o zvláště nebezpečnou hrozbu, malware je schopný přímo ovládat vysokonapěťové přepínače. K tomu používá implementaci průmyslových komunikačních protokolů, které se používají po celém světě – v infrastruktuře rozvodu elektrické energie, v systémech řízení dopravy i v jiných systémech kritické infrastruktury (voda, plyn a jiné). Vysokonapěťové přepínače uvedeny výše jsou digitálními ekvivalenty analogových ovládacích zařízení a z technického hlediska mohou být navrženy tak, aby obstarávaly nejrůznější funkce v elektrických rozvodnách. Výsledkem může být vypnutí rozvodu elektrické energie, kaskádové poruchy i vážnější poškození elektrického rozvodného zařízení. Závažnost se může lišit typem elektrické rozvodny. Netřeba dodávat, že narušení těchto systémů může přímo či nepřímo ovlivnit fungování kritické infrastruktury.

Nebezpečnost malwaru spočívá v tom, že používá komunikační protokoly způsobem, kterým byly navrženy. Problém je v tom, že komunikační standardy byly navrženy před desítkami let, kdy byly průmyslové systémy izolovány od okolního světa, a tudíž nebyly navrženy s ohledem na kybernetickou bezpečnost. To znamená, že útočníci nemuseli hledat zranitelnosti v komunikačních protokolech (NÚKIB, 2018).

4.2 Případy bezpečnostních incidentů

Únik dat – Equifax

Equifax je jedna ze tří úvěrových kanceláří v USA, která funguje podobně jako registr dlužníků. Věřitelé spoléhají na informace shromážděné úvěrovými kancelářemi, které jim pomáhají při schvalování půjček na bydlení, auta a poskytnutí kreditních karet. Někdy je využívají i zaměstnavatelé při rozhodování, koho přijmout.

Útočníkům se podařilo získat přístup o 143 milionu lidi a jejich citlivých dat, převážné o data narozeni, čísla sociálního pojištěni, adresy, řidičské průkazy, čísla kreditních karet a další. Podle dostupných informací se útočníkům povedlo dostat skrze zranitelnosti ve webové aplikaci společnosti. Událost je o to citlivější, protože unik trval skoro tři měsíce bez povšimnutí. To má za následek únik dat 40 % americké populace.

Dalším znepokojujícím faktorem je fakt, že společnost Equifax hned neinformovala poškozené o této události a podrobněji se nevyjádřila k celému incidentu. Odbornici tedy spekuluji o přesném důvodu úniku. Nejčastější domněnka spočívá v nedodržovaní správných bezpečnostních standartů a postupu při zabezpečení aplikací.

Vzhledem k rozsáhlosti celého incidentu, to má veliký dopad i na samotnou společnost Equifax. Akcie firmy spadly v první vlně o 15 %, následovanou vlnou kritiky z celé společnosti sociálně-prestižní dopad. Rozsáhlost uniklých dat je velká, z hlediska ochrany obyvatelstva můžeme očekávat zhoršení kvality života pro poškozené jedince tímto incidentem, případně poškození instituci jako jsou nemocnice nebo banky, kterých se to také týká.

„Na stupnici od jedné do deseti je to desítka z hlediska možnosti krádeže identity," řekl bezpečnostní analytik firmy Gartner Avivah Litan (SOCA.cz, 2017).

Pří pohledu na tento incident, jsem toho názoru, že přístup firmy byl absolutně neadekvátní v poměru dopadu, který to mělo. Absolutní neřešení krizové situace a selhání celého informačního oddělení i managementu firmy vidím jako jeden s nejhorších případu současnosti.

Oběti se stal klient této společnosti, který na následky toho mohl přijít k finanční škodě či administrativnímu zahlcení (možné vysvětlování, zařizování opatření proti tomuto poškození – doklady, ověření). Při zcizení osobních dat, je mohl útočník použít

na sjednání úvěru či koupit zboží. Následkem toho mohla být oběť právně napadána, či musela dokazovat nelegálnost této aktivity s ní svázanou.

Phishingový email v praxi – Komerční banka

Předmětem tohoto phishingového emailu je přelstít oběť a donutit ji ke stažení škodlivého softwaru do svého zařízení. Záminka pro tento podvodný email je SWIFT platba od Komerční banky.

Lze si všimnout přílohy v jednoduchém emailu, kde příloha SWIFT (slouží zejména k mezinárodnímu platebnímu styku) představující zmiňovanou SWIFT platbu je ve formátu .jar. Ovšem žádný textový dokument s touto příponou neexistuje nýbrž soubor spustitelný jako aplikace, tedy aplikace obsahující škodlivý kód.

Dopady pro neinformovaného uživatele mohou být ve formě ztracení přístupu, ke svému zařízení. Kde může dojít ke ztrátě či odcizení dat.

Jako širší pohled dopadu, se škodlivý software může rozšířit do firemní sítě, kde se nachází napadené zařízení. V tomto okamžiku, by byla v nebezpečí cela firemní sít s možnými datovými či peněžními ztrátami.

Ukázka e-mailu s nebezpečnou přílohou .jar níže (Hoax.cz, 2017). Počet přiznaných phishingových útoků každoročně stoupá. Za rok 2017, 409 případů.

Obrázek 5 Ukázka e-mailu s nebezpečnou přílohou (hoax.cz, 2017).

Únik dat - Mall.cz

Úřad pro ochranu osobních údajů (ÚOOÚ, 2017) zahájil na začátku října kontrolu internetového obchodu Mall.cz. Zaměří se na zabezpečení osobních údajů zákazníků společnosti, která po hackerském útoku přišla téměř o 750 000 údajů o svých klientech. Úřad to oznámil v tiskové zprávě. O výsledku kontroly bude ÚOOÚ informovat po jejím ukončení.

Internetovému obchodu Mall.cz odcizili hackeři údaje až ke 750 000 starším uživatelským účtům. Firma pak v srpnu část hesel vymazala, aby zabránila jejich zneužití. Ohrožena byla starší databáze z roku 2014, zakódovaná nyní již nepoužívaným způsobem, který útočníkovi umožnil některá hesla prolomit.

Z pohledu bezpečnostní informatiky se Mall.cz podle mého názoru choval odpovídajícím způsobem a reagoval velmi rychle: zablokoval účty podezřelé z napadení a informoval všechny dotčené uživatele. Uživatele také vyzval ke změně svých přístupových hesel a v řádu několika málo dnů zpřístupnil všem svým uživatelům zdarma online aplikaci, která jim pomáhá ověřit, zda byl jejich účet napaden či nikoliv a jak mají postupovat.

Při včasné reakci firmy, nevznikly vysoké škody na majetku, nebyla narušena kritická infrastruktura ani nebyla ohrožena bezpečnost uživatele z pohledu ochrany obyvatelstva. Zde předpokládáme, že utrpěla pověst firmy, popř. některé heslo ze seznamu mohl nějaký uživatel používat jinde, a to mohlo být zneužito. Avšak celá reakce společnosti byla poměrně rychlá.

Poučení z tohoto incidentu vidím jako včasnou reakci, která je nezbytná pro rychlé řešení incidentu, aby na následky útočníkova chování vznikly co nejmenší škody. Rychlost reakce a včasná informovanost měla za následek, rychlé reakce jak samotného Mallu, tak případnou reakci uživatelů, kterých se to týkalo – změna hesla na účtu mall.cz i jiných účtů s podobným nebo stejným heslem.

Ještě si položme otázku mohlo to dopadnout hůř? Jako v případu Equifaxu?

Můžeme podívat, jak by řešení takových incidentů nemělo vypadat. V případě Equifaxu, kdy podcenění míry rizik jednotlivých hrozeb bylo hlavní příčinou selhání této společnosti. Jsem toho názoru, že IT oddělení Equifaxu zaspalo aktualizaci a modernizaci bezpečnostních opatření, a to mělo za následek, tak rozsáhlého incidentu.

Znemožnění přístupu – Plzeňské školy napadli hackeři

Útočník napadl Plzeňské gymnázium, kdy se mu podařilo dostat do školní sítě a zde zašifroval přístup k datům.

„Hacker většinou zanechá stopu. Na tu jsme poslali e-mail. Přišla odpověď, že nás zašifrovali a pokud chceme data zpět, musíme dát šest bitcoinů, v přepočtu 991 440 korun," popsala ředitelka soukromého Křižíkova gymnázia v Plzni Šárka Chvalová.

Poté útočník snížil výkupné zhruba na 40 tisíc, ale gymnázium rozhodlo, že vyděračům nezaplatí. Byl zde risk, že útočník nedodrží svou část dohody. Dále zde bylo riziko zanesení ukrytého škodlivého softwaru.

Gymnázium se vydalo cestou nastavení celého systému od začátku a obnovením ze záloh, kdy v této variantě gymnázium vynaložilo náklady ve výši 400tisic. Avšak škody se ještě navýší z hlediska nesplněných pohledávek školy vůči jiným subjektům. Z důvodu nepřístupného systému.

Tento incident můžeme hodnotit jako mimořádnou situaci lokálního charakteru, avšak z mého pohledu i tyto incidenty mají svou váhu. Pro samotnou školu jsou to obrovské výdaje navíc. Pro jiny případ si představme, kdyby to byla nemocnice?

Obdobného charakteru se obětí stala i Střední odborná škola obchodu, užitého umění a designu v Nerudově ulici. „Naštěstí jsme na prolomení počítačového systému přišli včas, takže se hackeři nedostali k citlivým datům a k datům, se kterými potřebujeme pracovat," uvedla ředitelka školy Marie Klesová.

Škola ztratila pouze práce žáků, například různé grafické návrhy. I v tomto případě hackeři školu vydírali. Tyto incidenty poukazuji na to, jak jsou statní instituce nechráněné. Dalším faktem je ten, že v České republice je těchto incidentu mnoho, bohužel se na informační bezpečnost neklade takový důraz, jaký by měl (Šrámková, 2018).

4.2.1 Dopady bezpečnostních incidentů

Blackout – je přerušení dodávky elektrické energie, ať už z důvodu poruchy elektrárny, nebo kvůli selhání přenosové soustavy (Wikipedie, 2018).

Dle mého je to rozsáhlý výpadek (např. dodávek elektrické energie) na velkém území.

Možné dopady pro každou ze společností byly popsány v reálných případech výše. Avšak nejsou to všechny možné dopady informačních bezpečnostních incidentu. Mnoho jiných firem či instituci se může potýkat s podobnými nebo rozvíjejícími dopady. Ty mohou mít za následek poškození pouze firmy samotné nebo mohou zasáhnout do kritické infrastruktury daného státu.

Již jsme si v této práci popsali, jaké hrozby z hlediska informační bezpečnosti hrozí. Nastínili jsme si zde i dopady těchto hrozeb, od zničení či zcizení citlivých dat jednotlivých institucí a firem.

V dnešním reálném prostředí naštěstí nejsou dopady bezpečnostních incidentů takového charakteru, kdy by to ohrozilo svrchovanost státu, znemožnilo normálního fungování státu či jinak omezilo v tak rozsáhlém měřítku. Ovšem není dobré si myslet, že toto riziko zde není.

Dopady mohou být v širším spektru následující: ekonomicky, sociálně-prestižní, politicko-kulturní, materiální, logisticky, strukturální.

Jmenovitě se může jednat o zničení dat, ukradnutí dat, znemožnění přístupu, zneužití přístupů nebo dat apod. Dopady mohou být lokálního charakteru v rámci jedince nebo malé skupiny až v globálním charakteru př. Equifax s cíleným nebo náhodným dopadem pro společnost.

Příkladem může být napadnutá banka, při špatném zabezpečení může útočník skrze technické opatření proniknout do informačního systému banky, kde pustí škodlivý software na mazání všech dat. V případě smazání i záloh by to mělo obrovský dopad na všechny klienty banky i ekonomický vliv daného státu. Kdo by platil náhrady v tomto případě? Obdobně by to vypadalo při incidentu, kde vinou by byl lidský faktor. Tedy nepozornost či neznalost zaměstnance. V tomto případě se může jednat o phishingový email, nařizující splnění důležitého příkazu. V nepozornosti si zaměstnanec neověří pravdivost tohoto požadavku, a tak dojde k provedení příkazu a finanční ztrátě. V některých případech může jít o financování další trestné aktivity z těchto zcizených peněz.

V globálním charakteru bychom se mohli bavit o širších dopadech pro společnost.

Pro příklad napadnutí energetických rozvoden virem Crash Override – Win32/Industroyer by mělo za následek výpadek proudu. Který by ohrozil kritickou infrastrukturu, pro přiklad by to mělo dopad na nemocnice, kde by musely být spuštěny

náhradní diesel agregáty – pro chod nemocnice. Avšak útočník by mohl, napadnout také informační systém nemocnic – doktoři by neměli potřebné informace o pacientech, výpadek energie by zamezoval komunikace mimo lokální zdravotní centrum. Tak by se celý zdravotnický systém dostal do informačního blackoutu.

Z hlediska informační bezpečnosti před kybernetickými útoky, jde o zajištění ochrany dat a jejich přístupnost oprávněným uživatelům, což se také ukazuje na vybraných konkrétních případech kybernetických útoků a jejich rozborů.

4.3 Preventivní opatření a návrhy řešení bezpečnostní informatiky firmy

4.3.1 Monitoring – systému i kamery fyzicky

Monitorováni systému

Je důležité sledovat co se v informačních systémech děje. Proto je vhodné nastavit pravidla pro uživatele tak, aby o tomto věděli.

- Legislativní ošetření, vnitřní směrnice firmy obecná
- Informační směrnice firmy

Druhou fází je technické opatření, které sleduje přístupy uživatelů do jednotlivých částí informačního systému a způsobu operací, které zde provádějí. To má za následek podrobného logování (zapisování) činnosti.

- Navštěvované weby
- Stahování a nahrávaní dat
- Přenos dat na přenositelná media
- Změna nastavení důležitých zařízení apod.

Toto lze docílit softwarem třetí strany na tuto činnost uzpůsobenou např. Safetica.

Na základě těchto dat jsme schopni identifikovat potencionálního útočníka v sítí. Případně můžeme odhalit špatně nastavené procesy ve firmě a optimalizovat je.

Totéž platí obdobně pro sledování síťové komunikace do firemní sítě, ven z firemní sítě i přenos dat v rámci firemní sítě. Zde by odpovědná osoba – administrátor měla klást důraz na to, co se na firemní sítí pohybuje a v jaké transportní vrstvě daná data putují. Obecně se doporučuje porty transportních protokolů zakazovat, jestliže nejsou využívány. Pro příklad:

- **FTP** – File Transfer Protocol využívající pro přenos dat mezi počítači v síti.

Další části je sledování přístupných portu pro komunikaci v sítí i mimo ni. Mohou být zde otevřené porty, které daná organizace či firma nevyužívají, ale je zde riziko napadení. Na tyto otevřené porty lze aplikovat sofistikované útoky. Mohou to být i „obslužné“ porty jako je třeba:

- **Telnet** – protokol pro dálkovou správu klienta nebo serveru, komunikace zde probíhá v nešifrované podobě

Platí základní pravidlo: Co není potřebné využívat je implicitně zakázané.

Na základě těchto informací by měl administrátor mít ucelená pravidla vymezující přenos dat a komunikací ve vnitřní sítí. Zakázané typy protokolu, souboru a aplikací.

K tomuto koresponduje i **fyzicky monitoring** firemních prostor.

Je nutné monitorovat prostor v kritické infrastruktuře firmy jako jsou všechny datová centra a logistické uzly. Z pohledu ochrany dat a osob v informační bezpečnosti. Patří zde:

- Serverové prostory
- Zálohové prostory
- Rozvodná elektrického proudu
- Důležité datové uzly – páteřní internetová linka, firemní datové linky, rozbočovače, routery, opakovače
- Vstupní konektory do firemní sítě – zástrčky RJ45 (konektory)

4.3.2 Pravidelné kontroly – uživatelů, namátkové kontroly, testy uživatelů

Nedílnou součástí preventivních opatření je dohled nad uživateli – již známý lidský faktor. Uživatel je definován jako nejslabší článek informační bezpečnosti, a tak musíme k tomu přistupovat.

Největší nebezpečí představují menší firmy, které nemají odborníky zaměřené na kybernetickou bezpečnost. Zde dochází k zanedbání základních postupů při změně hesla nebo instalaci důležitých aktualizací. Následky to má často na celou firmu. V případě kyberútoku na malé firmy jsou nejvíce v nebezpečí manažeři, HR pracovníci a finanční pracovníci.

Je vhodné zaměstnance čili uživatele pravidelně kontrolovat. Počínaje kontrolou pracoviště, kontrolou samotných procesů na zařízení – zdali uživatel nenechává citlivé informace, kde by neměl. Případně kontrola pracoviště po opuštění zaměstnancem – zamknutý počítat v případě odchodu na oběd.

Druhou etapou je náhodné testování uživatelů za účelem ověření znalosti směrnice informační bezpečnostní firmy. Tato vnitřní norma firmy by měla být pro uživatele potažmo administrátory firmy – jako modla, která sníží míru rizika potencionálních hrozeb. Leč jsou zde i jiné faktory toto ovlivňující – technického

charakteru (nastavení a implementace hardwarových a softwarových doplňku pro správné fungování firemní sítě a informačního systému).

Kontrolu lze provádět i principem útoku, tedy řízeným phishingovým kybernetickým útokem vůči vlastním zaměstnancům. Zde bude ukazatelem úspěšnost, respektive neúspěšnost převedení znalosti směrnice a obezřetnosti do praxe.

4.3.3 Školení zaměstnanců

Je důležitou součástí každé firmy. Z výsledku vyvozených při kontrolách a jiných auditech jsme schopni reagovat na potřeby firmy a jak její zaměstnance vzdělávat k vyššímu pohodlí, efektivnosti a bezpečí firmy. Platí zde přímá úměra, čím lépe je uživatel potažmo zaměstnanec vzdělaný, tím je menší riziko propuknutí hrozby. Je podstatné provádět pravidelné školení zaměstnanců. Informační svět je jeden s nejrychleji se rozvíjejících, proto je potřeba aktualizovávat směrnici pro zaměstnance a včasně je upozorňovat před možnými hrozbami.

Není nic horšího, když je technické zabezpečení silné a implementováno správně, ale útočník se dostane do firemní sítě jednoduše přes uživatele. Školení obnáší soubor technických i organizačních prvku, jako jsou zásady chování uživatele s výpočetní technikou, tak i instruktáž ovládání jednotlivých aplikací potřebných k práci zaměstnance.

4.3.4 Základní bezpečnostní pravidla

Zásada bezpečného přístupu

- Používat silná hesla, chránit si je a nesdělovat je nikomu jinému.

Heslo by mělo byt zvoleno tak aby nebylo lehce odhadnutelné (ne např. jméno, datum narození, jméno dítěte, pouze číslo, obecně známá hesla apod.). Pro zvýšeni bezpečnosti je vhodné mít unikátní heslo pro každou službu zvlášť. Hesla nezapisovat na papírky, monitory, poznámkové bločky apod., neumisťovat je nikdy na přístupná a viditelná místa. Pokud je problém se zapamatováním hesel je možné využít ověřenou aplikaci na správcování těchto hesel, tzv. správce hesel, doporučuji to konzultovat s IT odborníkem. Své heslo za žádných případu nesdělovat cizí osobě, ani ve firemní struktuře (nadřízený). Hesla rovněž nezasílat e-mailem.

- Neukládat hesla a přihlašovací údaje na veřejných počítačích.

Při práci na veřejně dostupných počítačích nebo na cizím počítači, nikdy neukládat hesla ani přihlašovací údaje, přestože to systém umožňuje či nabízí.

- Citlivé služby jako např. bankovnictví využívat pouze ze známých počítačů a bezpečných sítí.

Nepoužívat citlivé služby z cizích nebo veřejných počítačů a na veřejně dostupných sítích (zejména otevřených Wi-Fi). U citlivých služeb vždy nutná kontrola řádku pro zadávání internetové adresy – tento musí odpovídat původnímu zadání adresy, a v případě citlivých služeb by měl také disponovat bezpečnostním certifikátem (znaky zámku a zeleného podbarvení.).

Zásada omezení rizika

- Nenavštěvovat pochybné či rizikové stránky.

Navštěvovat pouze stránky ověřené a související s výkonem práce. Vyhýbat se stránkám podezřelým nebo rizikovým (například stránky s pornografií jsou často využívány k infikování počítačů škodlivým softwarem nebo kódem apod.).

- Nestahovat podezřelé či pochybné soubory.

Pokud to není nutné, vyvarovat se stahováni souboru. Vyhnout se nedůvěryhodným či pochybným zdrojům. Stahování některých obsahů může být nelegální nebo trestné.

- Nenastavovat a neprovádět změny bez souhlasu administrátora.

Neprovádět žádnou činnost na základě podnětu z emailu nebo telefonního hovoru. Nečinit tak i když se na druhé straně hovoru představí administrátor nebo osoba nadřízená. V případě možnosti propuknutí hrozby nebo podezřele činnosti je vhodné si tuto skutečnost ověřit u nadřízeného nebo administrátora na svůj vlastní podnět. Pamatujte, že administrátoři systémů nepotřebují pro správu, servis apod. spolupráci uživatele v podobě zadávání jeho hesel, přihlášení pod účtem uživatele apod.

Zásada bezpečné komunikace

- Komunikace na internetu vyžaduje míru obezřetnosti.

Ne vždy je ten, s kým na internetu komunikujete je ten, za koho se vydává. Internetová komunikace v sobě skrývá anonymitu a nikdy nevíme jaké má protistrana úmysly, v tomto se skrývá riziko hrozby.

- Neotvírat e-maily ani přílohy z neznámých zdrojů.

Nikdy neotvírat e-maily ani jejich přílohy, pokud pochází z neznámých nebo podezřelých zdrojů (zcela cizí adresy, podivné tvary adres, zahraniční neznámé domény apod.). Takovéto e-maily a přílohy mohou obsahovat škodlivý kód či software. Na podezřelé e-maily nereagujte.

- Nesdělovat důvěrné informace.

Na internetu nešiřte ani nikomu neprozrazujte důvěrné nebo firemní informace. Informace na internetu jsou dostupné prakticky pro všechny. Chovejte se proto jako v běžném životě – představte si, o co jste ochotni se podělit se svým okolím.

- Sociální sítě jsou rizikové prostředí.

Je vhodné se chovat na sociálních sítích obezřetně a důsledně si nastavit profil (například neveřejný profil sdílený pouze s přáteli). Při sdělování informací na svém profilu berte v potaz, že tyto informace bude moct vidět kdokoli. Digitální stopa na sociálních sítích může zůstávat velmi dlouho a může ovlivňovat i vaši budoucnost.

Zásada bezpečného ukončení činnosti

- Vždy bezpečně ukončete činnost na počítači.

Po ukončení činností na počítači je nutné uvést pracoviště do původního stavu – odhlásit se z počítače, při práci s internetovými prohlížeči ukončit všechna okna, případně vymazat v prohlížeči historii činnosti. Při přerušení činnosti vždy počítač uzamykejte (například kombinací kláves Windows + L) – zabráníte tak neoprávněnému přístupu k počítači a datům na něm.

Zásada předávání informací

- Podezřelé skutečnosti nahlaste.

Hlásit všechny podezřelé a netypické události správci nebo administrátorovi firemní sítě. Co nevím, se zeptám – v případě nejistoty je lepší zeptat se i na základní věci než udělat něco rizikového. S tím koresponduje další část a tím je informovanost, uživatel v případě nevědomosti je povinen si tyto informace zjistit.

Je žádoucí dodržovat pravidla nastavené v rámci bezpečnostní politiky firmy, zásady jsou jedním z faktorů pro celistvost bezpečnostních opatření pro ochranu firmy.

Tyto zásady jsou implementovaný ve vnitřní normě firmy a s toho vychází směrnice pro uživatelé – zaměstnance firmy. Nedbalé chování může poškodit firmu.

4.3.5 Obrana proti phishingu

Základní obranou proti phishingu je selský rozum. V případě emailu vyžadující naše citlivé informace se pečlivě zamysleme, popř. ověřme, jestli možné či vhodné tyto informace sdělovat.

Obrana proti phishingu v bodech:

- Neexistuje jednotné řešení pro ochranu proti phishingovým útokům, ale můžeme shrnout body, které k tomu přispívají:
- Podezřele e-maily ignorujte, neklikejte na žádné odkazy v takovém e-mailu.
- Pro přihlášení do služby použijte standardní způsob, ruční zadání adresy www přímo nahoru do adresního řádku internetového prohlížeče.
- Po zobrazení stránky opět kontrolujte, jestli zadaná adresa souhlasí.
- U podezřelých e-mailů kontrolujte podrobnosti – výchozí odesilatel, uživatel musí informovat administrátory, který vyhodnotí tento email (ověří odkud email přisel, trasování ip adresy)
- Při nestandardním požadavku na citlivé údaje nebo finanční výpomoc, od vašich přátel skrze e-maily či sociální sítě, ověřte, zdali je požadavek reálný (např. osobně, nebo telefonicky).
- Pravidelně aktualizovaný internetový prohlížeč, antivirový program a e-mailový klient ve většině případů informují uživatele, že se jedná o phishing.
- Používejte zabezpečená – šifrovaná spojení.
- Platný bezpečnostní certifikát instituce.
- Při přihlašování, pokud je to možné, používejte dvou faktorovou autentizaci. Pečlivě čtete ověřovací SMS, co přichází.
- V případě pochybností si obsah podezřelého e-mailu ověřte u dané instituce.

4.3.6 Implementace vhodných technických opatření

Zavedením vhodných technických opatření zvedneme míru bezpečí a zajistíme přístup do vnitřní sítě z hlediska technického obtížnějším. Můžeme takto aplikovat pasivní prvky technického směru jako jsou správná nastavení DNS serveru, emailových

serveru, různých spam filtru, antivirových opatření, antimalwarových opatření, firewallu hardwarového (ve směrovači) i softwarového (proxy server), omezení přístupu uživatelů k datům podle jejich potřeby a podle důležitosti dat, nastavení práv uživatelů, kteří komunikují na internetu, ale i v rámci lokální sítě apod.

Dále pak aktivních technických prvků, kdy díky těmto prvkům můžeme uživateli chránit jejich identitu a uměle snižovat riziko lidského faktoru. Představme si pod tím přístupové karty, čipy, biometrické čtečky do důležitých části objektu apod.

4.3.7 Aplikace softwarové ochrany

Obecně jsme již specifikovali, co si představit pod softwarovou ochranou. Nyní si nastíníme kroky či doporučení, které jsou vhodné učinit pro snížení rizika nakažení virem, či jak se ochránit před sofistikovaných kybernetickým útokem.

V dnešním moderním světě je mnoho cest, jak napadnout cílový objekt, ale berme na vědomí, že je zde mnoho cest, jak útočníkovi znesnadnit průnik do firemní sítě.

Opatření, které mohou snížit riziko nakažení viry a kybernetickými útoky:

- Zakoupení a instalace antivirového softwaru,
- Udržet všechny komponenty aktuální, počínaje antivirem (popř. antimalware, antispyware) i jiné softwarové prvky (operační systém, ovladače, software třetích stran, IS)
- Správné nastavení sítových prvků
- Neotevírat podezřelé soubory
- Používat funkce zabezpečení aplikací
- Dodržovat zásady chovaní uživatele na internetu:
  - Neotvírat neznámé přílohy emailů
  - Nepřistupovat na webové stránky, vyžadující přihlašovací údaje skrze email
  - Důležité emaily od banky nechodí (informaci ověřit telefonicky)

4.3.8 Síťové prvky

Servery – zajistit ochranu antivirovou, antispywarovou dále nastavení spamového filtru skenování rizikových protokolu, nastavení otevřených portu, nastavení firewallu či samotný proxy server, senzory (čidla před vnějšími vlivy – oheň, voda), monitoring (monitorování přístupu kamerovým systémem)

Routery – fyzické zabezpečení přístupu (vysoko položené), nastavení MAC filtru, nastavení portu, nastavení zabezpečení WPA2 (WPA3) s šifrováním, oddělení privátních a otevřených návštěvníků dvěma Wi-Fi sítěmi

Sítové kabely, datové zásuvky – fyzické zabezpečení přístupu (kryty, obecná nepřístupnost, ochrana před vnějšími vlivy počasí (izolace) – voda, oheň), senzory (čidla před vnějšími vlivy – oheň, voda), monitoring (monitorování přístupu kamerovým systémem)

4.4 Výhledově pohled do budoucnosti internetového prostředí

4.4.1 Rozvoj nových technologii a nových oboru internetového prostředí

Nová bezpečnostní technologie WPA3

Téměř 14 let od schválení technologie WPA2 (Wi-Fi Protected Access 2) přichází sdružení Wi-Fi Alliance s další generací tohoto typu ochrany bezdrátových sítí. Novinka – s nijak překvapivým názvem WPA3 – hodlá vypořádat se známými problémy svého předchůdce.

WPA3 přinese nové bezpečnostní prvky:

- Odolnost vůči hrubé síle: k dispozici bude ochrana proti útokům využívajícím při pokusech o prolomení Wi-Fi hesel hrubou sílu. V budoucnu tak bude autentizace po několika neúspěšných pokusech o přihlášení zablokována. Tento přístup by měl – teoreticky – vést ke snížení počtu úspěšných bezpečnostních incidentů spojených s příliš slabými hesly.
- Bezpečnější veřejné sítě: nový standard posílí ochranu uživatelů v otevřených sítích, a to prostřednictvím individuálního šifrování dat. V této chvíli ale není jasné, co se za tímto vylepšením vlastně skrývá. Na obzoru je řešení veřejných Wi-Fi sítí (například na letištích, v kavárnách, ve veřejné dopravě), které nevyžadují použití hesla. A technologie WPA3 může nabídnout automatický systém pro sjednání šifrovaného připojení také v otevřených sítích.
- Nový standard WPA3 by se měl úspěšně vypořádat se všemi implementačními chybami technologie WPA2, očekává se zlepšení situace na poli bezdrátových sítí, přispívá tomu i fakt, že by WPA3 měla být kompatibilní s WPA2 (Kočí, 2018).

Zviditelnění blockchainu databáze budoucnosti

Blockchain je v informatice speciální druh distribuované decentralizované databáze uchovávající neustále se rozšiřující počet záznamů, které jsou chráněny proti neoprávněnému zásahu jak z vnější strany, tak i ze strany samotných uzlů peer-to-peer sítě (sít se skládá z uživatelů, ti mezi sebou komunikují).

Nejčastější aplikací technologie blockchainu je použití jako účetní kniha kryptoměn (např. bitcoinu), jež uchovává transakce provedené uživateli. Kombinace s

kryptografií umožňuje zajistit anonymitu operací a zamezit neoprávněné transakce (Bínek, 2018).

IT oddělení se promění

Do roku 2021: 40 procent IT zaměstnanců budou „všeumělové“ zastávající více rolí, z nichž většina bude spíše na straně byznysu než technologií.

IT specialisté v současné době představují asi 42 % všech zaměstnanců v IT odděleních.

Předpokládám, že prolínaní informačních technologii do jiných odvětví bude vysoký. Odpovědi na to bude větší poptávka lidi rozumějící základní implementaci technických řešení a zapojování informačních technologií do všeobecného fungování ostatních odvětví. První to zasáhne v oblasti správy infrastruktury a provozu IT. Následně bude prolínaní pokračovat do netechnických oborů zvláštně ekonomicko-manažerského směru. IT pracovnici budou bráni jako více univerzálnější pracovníci než doposud (BusinessIT.cz, 2017).

4.4.2 Rizika s tím svázaná

Bezpečnost IoT

Co to vůbec IoT je? Ve zkratce internet věcí (anglicky Internet of Things) je v informatice označení pro síť fyzických zařízení, vozidel, domácích spotřebičů a dalších zařízení, která jsou vybavena elektronikou, softwarem, senzory, pohyblivými částmi a síťovou konektivitou, která umožňuje těmto zařízením se propojit a vyměňovat si data. Mají za úkol zjednodušit a zefektivnit prací.

V dnešním světě moderních technologii, jde vývoj nové techniky dopředu. Avšak vždy se musí nějak začít. Takhle jde vidět svět IoT věci, kdybychom si mohli představit počítače před 20 lety, nevýkonné a zranitelné. Zvláštně u druhého faktoru zranitelné bychom se zastavili. Vývoj IoT věci je ještě na svém začátku a zabezpečení této techniky, tak vypadá. Proto bychom se měli zaměřit na tři oblasti, jak IoT věci zabezpečit.

Za prvé je třeba zajistit fyzickou bezpečnost koncových bodů IoT, aby se maximálně omezila možnost neautorizovaného přístupu k nim. Za druhé je třeba zajistit bezpečnost jejich přístupu do sítě, a to mimo jiné sestavením seznamu povolených zařízení a správným řízením bezpečnosti aplikací. A za třetí je nutno zajistit bezpečnost

přenášených dat prostřednictvím šifrovaných tunelů. Přitom je třeba stále monitorovat koncové body a reagovat na možné anomálie (BusinessIT.cz, 2017).

Bezpečnost cloudu

Základní pojmy:

TLS – protokol pro šifrovanou komunikaci dat po sítí.

AES – šifrovací standart pro šifrovaní dat v informatice

2FA – Dvou faktorové ověřování (SMS) používá se před neoprávněným vstupem do účtu

End-to-end šifrovaní – způsob ochrany dat před třetí stranou a během přenosu.

Technologie cloudového uložiště je komfortní a cenově dostupné řešení, jak ukládat svoje data. Přitom se dotyčný uživatel nemusí starat o implementaci a správu těchto dat. Je mnohem pohodlnější data někam nahrát a nestarat se než počítat, každý kousek fyzického uložiště a strachovat se, jestli kapacita dostačuje.

Všechny tyto cloudové služby jsou velice komfortní a nabízejí uživatelům i firmám službu, která ušetří čas i peníze. Avšak jak je to z bezpečnosti těchto uložišť? Když svěříte všechny svá data třetí straně?

Nastínil bych to jako otázku důvěry. Podle průzkumu technického časopisu CHIP má většina společnosti poskytující cloudové uložiště splněné normy pro základní bezpečnostní prvky (TSL, AES, 2FA). Šifrovaní přenosu je v dnešní době standardem a několik datových center šifruje i data na serveru. Avšak jsou zde mezery, na které je třeba dát pozor.

Poskytovatele sice šifrují data na serverem, ale pořad mají od nich dešifrovací klíče, což v případě uniku není dobře. Celou tuto situaci by vyřešilo tzv. End-to-end šifrovaní na straně uživatele – toto šifrovaní provádí uživatel u sebe na zařízení a data již jdou šifrovaná na server. Zamezilo by to i nešťastnému fyzickému uložení datových center např. uložiště fyzicky v USA podléhá americkým zákonům o ochraně osobních dat (Geiger & Kubeš, 2017).

Proto na závěr je důležité kam svá data nahráváme a jak citlivá pro nás jsou.

Útoky na mobilní platformy

Počet kybernetických útoku na mobilní platformu Android vzrostl v uplynulém roce o 40 %. A to z průměrných 1,2 milionů útoků měsíčně na 1,7 milionu. Mezi tři největší hrozby patří špehování uživatelů, krádeže osobních dat anebo zasílání nevyžádané reklamy, i mimo aplikace. Zaznamenalo se v průměru 788 variant virů za měsíc, což je nárůst o 22,2 procent.

„Počet kybernetických útoků na mobilní zařízení rychle roste a strategie hackerů jsou stále účinnější a nebezpečnější. V ohrožení jsou především osobní údaje a soukromí uživatelů," řekl Gagan Singh.

Nejrozšířenější hrozby jsou tzv. rootery, které požadují root (administrační oprávnění) přístup k telefonu, případně se snaží hledat mezery v zabezpečení. U této hrozby hrozí ovládnutí zařízení, a to včetně sledování činnosti a odcizení osobních informací.

Druhou nejčastější hrozbou jsou techniky sociálního inženýrství a jako třetí se řadí falešné a podvodné aplikace, které zanesou do uživatelova zařízení reklamní spam (Trlica, 2017).

5 Závěr

Cílem práce je charakterizovat bezpečnostní hrozby internetu ve firemní struktuře a jednotlivé dílčí časti informační bezpečnosti. Práce bude rozebírat základní informační pojmy, potencionální kyberteroristické hrozby a způsoby ochrany před nimi. Dílčím cílem je uvést konkrétní incidenty kybernetických útoku a výhled do budoucna informačních technologií z pohledu bezpečnosti a také ochrany obyvatelstva.

Primárním zdrojem byla analýza informací z dokumentů, profesionálních technických rubrik a informační zdroje státních orgánů, na základě poznatku s těchto zdrojů jsem mohl charakterizovat bezpečnostní hrozby internetu ve firemní struktuře a jednotlivé dílčí časti informační bezpečnosti. Problematika je natolik obsáhlá, že je možný i jiný pohled na věc, avšak jsem toho názoru, že charakterizování tématu informační bezpečnosti naplňuje smysl práce. Dále je problematika informační bezpečnosti aktuální, a proto jsem uvedl konkrétní případy a analyzoval je. S vidinou prudkého vývoje v oblasti informačních technologii potažmo informační bezpečnosti, jsem uvedl budoucí trendy a hrozby v informační bezpečnosti. Tímto považuji cíle práce za splněné.

Položme si ještě otázky ohledně výpočetní techniky a internetu obecně. Jsme schopni stále reflektovat potencionální nebezpečí, které se dále vyvíjí? Co zabráni zhroucení všech sítí, výpočetní techniky potažmo internetu? To je dle mého otázka, která se zodpoví za řadu let. Potencionální změnu v tomto odvětví vidím s příchodem nových technologií, které změní celé odvětví informačních technologií z pohledu bezpečnosti a ochrany obyvatelstva.

Myslím si, že je třeba neustále zdokonalovat technická i organizační řešení. Stálým vývojem jsme nuceni zvyšovat laťku bezpečnosti před útočníky.

6 Souhrn

Na závěr práce můžu konstatovat, že téma této bakalářské práce je víc než obsáhle. Jednotlivé kapitoly popisující dílčí části informační bezpečnosti se dají charakterizovat s mnoha pohledů. Avšak vidinou této práce bylo zaměřit se informačně ochranou část tohoto odvětví. Kde jsem charakterizoval nezbytné pojmy k pochopení problematiky. Dílčí kapitoly popisuji nezbytné faktory pro ochranu firemní sítě, kde jsme si popsali potencionální útoky a útočníky, kteří to provádějí.

V této prací jsem využil zejména analýzy odborných textů, profesionálních technických rubrik a informační zdroje státních orgánů. Na základě popsaných pojmu jsme se hlouběji podívali do informační struktury firmy či instituce. Zde jsme se podívali na možné hrozby, které se v tomto prostředí se mohou vyskytovat.

Dále jsme se podívali na praktické příklady ze světa i u nás, kde byli nastíněny i dopady těchto incidentů. Poté jsem popsal preventivní opatření a možné řešení těchto incidentu i všeobecných pravidel které jsou nezbytné pro snížení rizika ve firemní sítí.

Závěrem jsme se mohli podívat co nás nemine z pohledu budoucího v odvětví informační bezpečnosti a jaké kybernetické útoky můžeme očekávat. V dnešní době je svět techniky velice rozsáhlý a rozvoj tohoto odvětví je jedno s nejrychlejších. Proto si myslím, že do budoucna bude informační bezpečnost jedním s klíčových faktorů pro suverenitu státu potažmo pro přežití firmy či instituce.

7 Referenční seznam

Bezpecnyinternet.cz (2018). Phishing a pharming. *Internetové bankovnictví*. Retrieved 11. 5. 2018 from the World Wide Web: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

Bínek, V. (2018). Blockchain v oblasti ochrany dat. *IT Security*. Retrieved 11. 5. 2018 from the World Wide Web: https://www.systemonline.cz/clanky/blockchain-v-oblasti-ochrany-dat.htm

Bitto, O. (2006). *Jak zabezpečit domácí malou síť Windows XP: účty, práva, firewally, antiviry a další nástroje*. Brno: Computer Press.

BusinessIT.cz (2017). Top 10 technologických předpovědí pro IT na rok 2018. *Business IT*. Retrieved 11. 5. 2018 from the World Wide Web: http://www.businessit.cz/cz/top-10-technologickych-predpovedi-pro-it-na-rok-2018.php

Csirt.cz (2018). Statistiky řešených incidentů. *Statistiky*. Retrieved 11. 5. 2018 from the World Wide Web: https://www.csirt.cz/page/2635/statistiky-resenych-incidentu/

Denning, D. E. (2001). Activism, Hacktivism, and Cyberterrorism. *The Internet as a Tool for Influencing Foreign Policy, (37),* 234-239.

Doseděl, T. (2004). *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press.

Dostálek, L., & Kabelová, A. (2008). *Velký průvodce protokoly TCP/IP a systém DNS.* Praha: Computer Press.

Gála, L., Pour, J., & Toman, P. (2006). *Podniková informatika*. Praha: Grada Publishing.

Geiger, J., & Kubeš, R. (2017). Bezpečí dat v cloudu. *CHIP, 12,* 88-91.

Hoax.cz (2017). KB – INFORMACE O PLATBĚ(SWIFT) (20170621). *Malware*. Retrieved 11. 5. 2018 from the World Wide Web: http://www.hoax.cz/malware/kb---informace-o-platbeswift-20170621/

Hoax.cz (2018). Hoax. *Hoax.* Retrieved 11. 5. 2018 from the World Wide Web: http://www.hoax.cz/hoax/

Hoax.cz (2018). PHILIPE HANS – DRAHÝ PRÍTELI (20170427). *SCAM419*. Retrieved 11. 5. 2018 from the World Wide Web: http://www.hoax.cz/scam419/philipe-hans---drahy-priteli-20170427/

IJS. (2018). Definice Internetu. *Internet*. Retrieved 11. 5. 2018 from the World Wide Web: http://ijs2.8u.cz/index.php?option=com_content&view=article&id=31&Itemid=133

Janczewski, L., & Colarik, A. (2005). *Managerial Guide For Handling Cyber-Terrorism And Information Warfare*. Auckland: Information Science Reference.

Jašek, R. (2002). *Ochrana znalostí a dat v podnikových informačních systémech*. Zlín: Univerzita Tomáše Bati.

Kaspersky.com (2018). Kaspersky Lab Spam and Phishing report: FIFA 2018 and Bitcoin among 2017's most luring topics. *Press releases*. Retrieved 11. 5. 2018 from the World Wide Web: https://usa.kaspersky.com/about/press-releases/2018_fifa-2018-and-bitcoin-among-2017-most-luring-topics

Kaspersky.com (2017). The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. *Blog*. Retrieved 11. 5. 2018 from the World Wide Web: https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Kočí, M. (2018). Wi-Fi Alliance představila standard WPA3 pro lepší ochranu sítí. *Aktuální zprávy*. Retrieved 11. 5. 2018 from the World Wide Web: https://pctuning.tyden.cz/component/content/article/1-aktualni-zpravy/50171-wi-fi-alliance-predstavila-standard-wpa3-pro-lepsi-ochranu-siti

Ludvík, M. (2008). *Teorie bezpečnosti počítačových sítí*. Kralice na Hané: Computer Media.

Mitnick, K. (2003). *Umění klamu*. Gliwice: Helion.

Novák, J. (2015). *Vnitřní a vnější bezpečnost státu*. Olomouc: Univerzita Palackého.

NÚKIB (2015). Phishing – stále aktuální hrozba. *Informační servis*. Retrieved 11. 5. 2018 from the World Wide Web: https://www.govcert.cz/cs/informacni-servis/doporuceni/2325-phishing-stale-aktualni-hrozba/

NÚKIB (2018). Hrozby. *Informační servis*. Retrieved 11. 5. 2018 from the World Wide Web: https://www.govcert.cz/cs/informacni-servis/hrozby/

NÚKIB (2018). Sociální inženýrství. *Informační servis*. Retrieved 11. 5. 2018 from the World Wide Web: https://www.govcert.cz/cs/informacni-servis/doporuceni/2486-socialni-inzenyrstvi/

SOCA.cz (2017). Úvěrovou kancelář Equifax postihl masivní únik dat. *Článek.* Retrieved 11. 5. 2018 from the World Wide Web: https://www.soca.cz/blog/article/uverovou-kancelar-equifax-postihl-masivni-unik-dat-293

Staudek, J., & Hanáček, P. (1999). *Bezpečnost elektronického obchodu.* Praha: neznámá.

Staudek, J., & Hanáček, P. (2000). *Bezpečnost informačních systémů*. Praha: Úřad pro státní informační systém.

Šrámková, J. (2018). Plzeňské školy napadli hackeři. Za vrácení dat chtěli milionové výkupné. Zprávy. Retrieved 11. 5. 2018 from the World Wide Web: https://plzen.idnes.cz/hacker-internetovy-utok-krizikovo-gymnazium-stredni-skola-plzen-kybernetika-vypalne-grf-/plzen-zpravy.aspx?c=A180510_084940_plzen-zpravy_vb

Systemonline.cz (2018). Lidský faktor je zásadní slabinou bezpečnosti firemního IT. *Zprávy.* Retrieved 11. 5. 2018 from the World Wide Web: https://www.systemonline.cz/zpravy/lidsky-faktor-je-zasadni-slabinou-bezpecnosti-firemniho-it-z.htm

Trlica, D. (2017). Kybernetické útoky na Android zařízení se rapidně zvyšují. *Zprávičky.* Retrieved 11. 5. 2018 from the World Wide Web: https://www.svetandroida.cz/android-zarizeni-kyberneticke-utoky/

Tvrdíková, M. (2008). *Aplikace moderních informačních technologií v řízení firmy.* Praha: Tiskárny Havlíčkův Brod.

ÚOOÚ (2017). Zahájena kontrola Mall.cz. *Titulní strana*. Retrieved 11. 5. 2018 from the World Wide Web: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=27253&n=zahajena-kontrola-mall-cz

Vítek, M., & Vítková, M. (2004). *Sociální vědy a inženýrství*. Hradec Králové: Gaudeamus.

Wikipedia (2017). Botnet. *Wikipedia*. Retrieved 11. 5. 2018 from the World Wide Web: https://cs.wikipedia.org/wiki/Botnet

Wikipedia (2018). Ransomware. *Wikipedia*. Retrieved 11. 5. 2018 from the World Wide Web: https://cs.wikipedia.org/wiki/Ransomware

Wikipedia (2018). Výpadek dodávky elektřiny. *Wikipedia*. Retrieved 11. 5. 2018 from the World Wide Web: https://cs.wikipedia.org/wiki/V%C3%BDpadek_dod%C3%A1vky_elekt%C5%99iny

Zákon č. 181/2014 Sb. (2014). Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). *Ochrana dat.* 11. 5. 2018 from the World Wide Web: https://www.zakonyprolidi.cz/cs/2014-181