VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, O. P. S., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

BEZPEČNOST INFORMACÍ

Autor práce: Halenkovský Petr
Studijní obor: Bezpečnostně právní činnost ve veřejné správě
Forma studia: Kombinovaná
Vedoucí práce: doc. JUDr. PhDr. Jiří Bílý, CSc.
Katedra: Katedra právních oborů a bezpečnostních studií

2014

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně s využitím uvedených pramenů a literatury.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47b zákona č. 111/1998 Sb. v platném znění.

.....

Děkuji vedoucímu bakalářské práce doc. JUDr. PhDr. Jiřímu Bílému, CSc. za cenné rady, připomínky a metodické vedení během mé práce.

ABSTRAKT

HALENKOVSKÝ, P. *Bezpečnost informací : bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2014. XX s. Vedoucí bakalářské práce : doc. JUDr. PhDr. Jiří Bílý, CSc**.**

Klíčová slova: Počítačová kriminalita, internet, firemní bezpečnost, bezpečnost informací, šifry

Bakalářská práce se zabývá bezpečím informací a příčinami útoků na chráněná data. Úvodní teoretická část je zaměřena na historický vývoj a základní rozdělení do skupin. V další části práce poukazuje na současné druhy a možnosti zabezpečovacích systémů. Mimo jiné je zde vysvětleno, co to vlastně bezpečnost informací je a jaký vliv má na dnešní společnost. Poslední část obsahuje aktuální problémy bezpečnosti informací a informačních systémů a jak ohrožují státy, firmy, či jednotlivce.

ABSTRACT

HALENKOVSKÝ, P. *Information Security : bachelor thesis.* České Budějovice : The College of European and Regional Studies, 2014. XX p. Supervisor : doc. JUDr. PhDr. Jiří Bílý, CSc**.**

Key words: Computer crime, internet, company security, information security, code

This Bachelor's work deals with security of informations and reasons of attacks on protected data. Theoretical opening focuses on historical developement and basic sorting into groups. In the next part the work points to actual kinds and possibilities of security systems, including what actually the security of informantions is and what influence it has on current society. Last part of the work incorporates actual problems of information security and information systems and how they endanger states, firms and individuals.

OBSAH

ÚVOD

Informace mají ve společnosti velmi vysokou hodnotu. Již od dávných dob se informace vyvažovaly zlatem. Proto vznikla potřeba je schraňovat i za podmínky vysokých nákladů.

V dřívějších dobách se informace daly přenášet pouze slovem, či písmem. Velká ochrana byla tedy kladena hlavně na ty, kteří informaci vlastnili, či informaci nějakým způsobem přepravovali. Jednalo se hlavně o ochranu poslů, například tělesnou stráží, či o šifrovanou ochranu samotné informace. Postupem času byly vymýšleny různé šifry k zakódování písemnosti. Samozřejmě, že také docházelo k rozšifrování a nabourávání šifer, tudíž byl kladen větší nárok na kryptology, kteří vymýšleli různé algoritmy k zašifrování informací. V té době začal vznikat obor kryptografie.

První doložená zašifrovaná zpráva byla objevena roku 480 př. n. l. a za prvního kryptologa a vynálezce šifrované zprávy je považován vojevůdce Gaius Julius Caesar. Jeho šifra dostala název Caesarova šifra.

K největšímu rozmachu bezpečnosti informací docházelo a dochází při válečných konfliktech, kdy je zašifrování zpráv životně důležité. Postupem času s výrobou prvních telegrafních zařízení, docházelo i k důkladnějšímu šifrování zpráv. Vymýšlely se stále nové šifrovací algoritmy, které by mohly udržet krok s dobou. Šlo hlavně o to, být alespoň krok před dešifrovateli.

Dnes se šifrují hlavně firemní a osobní data. S rychlým vývojem přístrojů, jako jsou například počítače, tablety, chytré telefony a hlavně s vývojem internetu, je stále větší potřeba chránit si své citlivé informace, či soukromá data. Jedná se hlavně o kódování bankovních účtů, firemních know how a další. Tímto se zabývá obor bezpečnosti informací. Jeho úkolem je vyhodnotit cenu chráněných informací a podniknout dané kroky k jejich ochraně. Cena za ochranu dat by neměla převyšovat samotnou cenu informace. Pokud mluvíme o informaci jako takové, nemusí se jednat jen o data v počítačích. Bezpečnost informací se zabývá i ochranou fyzických dat, tedy různých listin, přístrojů a dalších. Proto když mluvíme o oboru bezpečnosti informací, nemyslí se tím jen ochrana skrze antivirové programy, ale i o zabezpečovací zařízení, jako například trezory a různé detektory k zabezpečování objektů s uskladněnými listinami.

Každý osobní počítač či osobní zařízení by mělo být chráněno minimálně antivirovým programem. Pokud se jedná o firemní přenosné počítače, na ochranu je kladen značně větší důraz. Největší nebezpečí plyne z internetu, ať se jedná o trojské koně či různé spamy. Proto například počítače na úřadech nejsou připojeny k internetu, pouze k jakési interní síti. Data jsou zde zálohována na několika místech, aby nedošlo při útoku ke ztrátě dat.

S rychlým vývojem počítačových komponentů a zrychlování systémů se z kryptologie stává lukrativní obchod, kdy jsou firmy ochotny platit astronomické částky za ochranu svých dat.

1 Cíle a metodika bakalářské práce

Cílem bakalářské práce je charakterizovat závažnost bezpečí informací a dopad na společnost, firmy, jednotlivce z hlediska úniku citlivých dat. Vyhodnotit nejúčinnější metody ochrany citlivých dat a přiblížit vývoj oboru bezpečnosti informací. Cílem je i navrhnout možnosti rozvoje do budoucnosti z hlediska techniky a využití nových prostředků, které budoucnost nabízí. Jedním z dalších záměrů je přiblížit právní stránku bezpečnosti informací a následné právní ochrany jak vlastních dat, tak i dat zaměstnavatele.

Bakalářská práce bude rozdělena na tři části. První část se bude zabývat historickými poznatky o ochraně informací. Bude zde přiblížen první výskyt ochrany dat a začátky vzniku oboru kryptologie. Tato část bude doplněna o praktické příklady prvních šifer a seznámení se s jejich principem. Také bude poukázáno na první známky luštění šifer a nabourávání se do zabezpečovacích opatření. Vysvětlování principiálního fungování a míru zabezpečení s ohledem na prostředky dostupné v době výskytu.

Druhá část objasní současné druhy zabezpečení a jejich možnosti použití při současném technologickém vybavení. Bude zde vysvětlena spojitost a návaznost na historická řešení šifrovacích algoritmů a postupů při zabezpečování. Tato část bude také obsahovat známé praktické ukázky šifrování a dostupná zabezpečovací zařízení.

Poslední část bakalářské práce se bude zabývat aktuálními problémy bezpečnosti informací. Budou zde popsány ukázkové příklady hackingu, tedy nabourávání se do zašifrovaných zpráv a některými známými úniky informací a jejich problematikou. Cílem bude poukázat na současné nebezpečí hrozící z útoků po internetu, či útoků na fyzická datová shromaždiště.

Práce bude zpracována na základě dostupné literatury a volně přístupných informací z internetu. Nejčastější právní podmínky bezpečnosti informací budou čerpány ze základů softwarového práva. Historické příklady budou inspirovány jak dějinami policie a četnictva, tak kriminalistickými příklady, či policejní vědou. Hacking a příklady nabourávání šifer či bezpečnostních protokolů, budou jen teoreticky rozebrány bez přesnějších specifikací. Tedy bez přesných funkčních proporcí, aby nemohlo dojít k jejich zneužití a tedy aby se z bakalářské práce nestal návod na softwarovou trestnou činnost. K popsání řízení bezpečnosti informací bude použita volně dostupná kazuistika všeobecných postupů, které slouží jako jakýsi návod na řízení zabezpečovacích systémů. Aktuální problémy bezpečnosti informací budou čerpány

z internetových zdrojů. Tedy z oficiálních webových stránek velkých firem, či státních složek, kde jsou zveřejněny současné potíže. Budou použity i některé články seriózních médií.

2 Bezpečnost informací

Úkolem informační bezpečnosti je zajistit citlivá data a informace před narušiteli, zloději, či jinými subjekty, kteří se snaží dané informace odcizit. Nejedná se pouze o ochranu dat před odcizením, ale jde i o ochranu před zničením, změnou či jakoukoliv jinou deformací dat. Bezpečnost informací, dat a systémů se v dnešní době stává prioritou každého podniku. V každém z těchto podniků je založen bezpečnostní management, který se touto otázkou neustále zabývá. Manažer informační bezpečnosti je profese velice žádaná. Manažeři musí mít široké znalosti v bezpečnosti a k tomu odpovídající praxi. Tito specialisté jsou vyžadování ve velkých organizacích, firmách, podnicích. Bezpečnost informací obsahuje technologické, právní, fyzické a sociální složky.[1]

Téma bezpečnosti dat a informací se týká nás všech, co využíváme jakoukoliv novou technologii. Tedy pokud využíváme chytré telefony, přenosná média, herní konzole či možnosti internetu. Všechna tato zařízení s sebou nesou rizika odcizení našich dat. Jedná se například o viry, červy, škodlivé kódy a malware. Informační bezpečnost tedy není jen pro firmy a podniky, ale zahrnuje i osobní počítače a výše uvedená zařízení.[2]

2.1 Historický vývoj bezpečnosti informací

Vývoj bezpečnosti informací je poměrně mladá disciplína, která začala být potřebná v době, kdy se začaly spojovat počítače ve firmách, podnicích či úřadech. V té době bezpečnost informací jako taková se spíše zaměřovala na bezpečnost systémů a technologií, než přímo na bezpečnost informací.[3]

V roce 1983 Národní středisko počítačové bezpečnosti sídlící v USA vytvořilo **Kritéria hodnocení důvěryhodných výpočetních systémů (TCSEC)**. Dále pak v roce 1985 se tento dokument stává normou Ministerstva obrany USA a je jakýmsi základním kamenem, který je tvořený soubory norem a doporučení. V Evropě si zatím otázku bezpečnosti informací řeší každý stát jednotlivě. Však rok 1990 byl v tomto sektoru pro Evropu zlomový. Francie, Německo, Velká Británie a Nizozemí spolupracují na vytvoření normy **Kritéria hodnocení bezpečnosti informačních systémů (ITSEC)**,

[1] KALAMÁR, Š., POŽÁR, J. *Vybrané aspekty informační bezpečnosti*. Praha, 2010. s. 11-12.
[2] DOUCEK, P., NOVÁK, L., SVATÁ, V. *Řízení bezpečnosti informací*. Praha, 2008. s. 11.
[3] DOUCEK, P., NOVÁK, L., SVATÁ, V. *Řízení bezpečnosti informací*. Praha, 2008. s. 64.

která byla pak Evropskou unií převzata. Kanadská kritéria hodnocení bezpečnosti však nezůstávají pozadu a jsou v téže době rozpracována (CTCPEC). Americké normy jsou však v roce 1992 znovu přepracovány kvůli nedostatkům v kritériích. V tomto roce jsou tedy vydána Federální kritéria (FC) pro bezpečnost informačních technologií, která vydala organizace National institute of Standards and Technology ve spolupráci s National Security Agency. V devadesátých letech startuje konečné hodnocení bezpečnosti a od této chvíle odpovědné orgány jednotlivých zemí dávají vzniknout **Všeobecným kritériím** (CC).[4]

2.1.1 Kritéria hodnocení důvěryhodných výpočetních systémů

TCSEC neboli Trusted Computer Security Evaluation Criteria, které jsou nazývány jinak Oranžová kniha dle barvy svého obalu. Tento dokument je soubor norem a doporučení sloužící k určení stupně bezpečnosti informací dle splněných požadavků, ty jsou rozděleny do částí. Základní rozdělení tvoří čtyři třídy, které jsou ještě tvořeny podtřídami. Celkem je tedy sedm tříd, jež slouží k identifikaci bezpečnosti:[5]

- **Třída D:** Slouží jako třída, do níž se zařazují systémy, jenž nesplnily žádané požadavky. Jedná se o systémy s minimální ochranou, tedy o takové, které nesplnily nějaké ze zadaných kritérií.
- **Třída C:** Tato třída pracuje na principu nepovinného řízení přístupu k informacím. Dále je tvořena dalšími dvěma podtřídami. Obsahuje požadavky na oddělení uživatelů. Tedy, že každý z uživatelů má svůj přístup k informacím, které nejsou přístupné jiným uživatelům. Také je kladen požadavek na oddělení procesů. Pokud tedy dojde k chybě u některého z uživatelů, nesmí dojít k poruše celého systému.
- **Třída B:** Je tvořena třemi podtřídami a uplatňuje povinné řízení přístupu k datům. Jako v třídě C od sebe musí být uživatelé a data odděleni. Například uživatel A, který se odhlásí, musí mít zaručeno, že uživatel B se nedostane spolu s přidělenou pamětí i ke zbytkům dat, které zanechal uživatel A. Tato třída však na rozdíl od třídy C obsahuje i stupeň utajení. Tedy že uživatelé mají různá práva nahlížení a editování dat.

[4] DOUCEK, P., NOVÁK, L., SVATÁ, V. *Řízení bezpečnosti informací*. Praha, 2008. s. 65.
[5] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 146-147.

- **Třída A:** Je nejvyšší bezpečnostní stupeň obsahující jednu podtřídu. Systém, který by chtěl dosáhnout této třídy, musí být formálně specifikován. Celý systém by tedy musel být složen za pomoci formálních matematických prostředků a následně i touto metodou otestován. Tato třída má návaznost na třídu B. U této třídy je však zvýšený rozsah verifikace.

2.1.2 Kritéria hodnocení bezpečnosti informačních systémů

ITSEC – Information Technology Security Evaluation Criteria. Certifikát je vydáván po splnění požadavků, které jsou rozloženy do dvou částí. První část obsahuje bezpečnostní funkce, kterými je systém vybaven. Druhá část zase způsoby, jakými je kvalita těchto funkcí zaručena. Kritéria ITSEC jsou tvořena sedmi třídami, ty nesou označení od E0 až do E6. V těchto třídách je uveden postup, jenž je potřeba dodržet při tvorbě systému nebo produktu. Záruky za správnost neboli záruky za zaručitelnost bezpečnosti tvoří tyto třídy:[6]

- **Třída E0:** Slouží k umístění systémů, které nesplnily požadavky na udělení certifikátu. Tato třída tedy neklade žádné požadavky.
- **Třída E1:** Obsahuje neformální zadání modelu bezpečnosti a návrh architektury systému.
- **Třída E2:** Musí mít neformálně popsaný projekt, který obsahuje popis návrhu systému. Dále je zde zařazeno testování funkčnosti systému.
- **Třída E3:** Hodnotí zdrojové kódy, či v jiných případech schémata hardwarového vybavení obvodových schémat.
- **Třída E4:** První z tříd, požadující formální část. Jedná o část dokumentace, která zahrnuje definování zadání systému. Také provedení analýzy zranitelnosti systému.
- **Třída E5:** Musí zahrnovat formální návrh. Implementace systému, musí být s návrhem ve shodě. Tedy návrh musí mít jednoznačnou vazbu s prvky zdrojového kódu.
- **Třída E6:** Je poslední třídou, ve které se nachází formální popis návrhu celého systému. Navíc však musí obsahovat důkaz o shodě s modelem bezpečnosti. Tedy musí se dokázat a definovat vše, co se dá.

[6] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 149.

Druhá skupina tříd obsahuje záruky za efektivnost a funkčnost bezpečnostních funkcí. Tím se myslí odolnost proti útokům, které mohou nastat. Funkčnost zase naopak obsahuje například:[7]

- Identifikaci a autentizaci
- Řízený přístup
- Odpovědnost
- Audit
- Opakované využití
- Přesnost
- Spolehlivost služeb
- Výměnu dat

Jako poslední třídy v kritériích jsou třídy F-IN, F-AV, F-DI, F-DC a F-DX. Tyto třídy nemají danou hierarchii. Jsou to vlastně dobrovolné třídy, které může uživatel využít dle svého uvážení, či dle potřeb projektovaného systému:[8]

- **F-IN:** Vysoké nároky na integritu systému
- **F-AV:** Vysoké nároky na dostupnost systému
- **F-DI:** Zajištění integrity dat při přenosu
- **F-DC:** Zajištění důvěrnosti dat při přenosu
- **F-DX:** Zajištění důvěrnosti a integrity dat při přenosu

2.1.3 Kanadská kritéria hodnocení bezpečnosti počítačových produktů

CTCPEC –Canadian Trusted Computer Product Evaluation Criteria. Bezpečnostní kritéria, která byla vydána v Kanadě. Jedná se o soubor bezpečnostních funkcí, které jsou rozděleny do čtyř částí hodnocení:[9]

- **Důvěrnost**: Obsahuje bezpečnostní funkce zajišťující ochranu proti úniku informací.
- **Integrita**: Do této části spadá jak fyzická integrita (fyzická bezpečnost), tak funkce, které slouží k zotavení systému po chybě, útoku či jinému pádu systému.

[7] DOUCEK, P., NOVÁK, L., SVATÁ, V. *Řízení bezpečnosti informací*. Praha, 2008. s. 68.
[8] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 149-150.
[9] DOUCEK, P., NOVÁK, L., SVATÁ, V. *Řízení bezpečnosti informací*. Praha, 2008. s. 69.

- **Dostupnost**: Část, v níž je zařazen požadavek na udržení dosažitelnosti služeb. Patří sem například chybová tolerance, či zotavení systému po nějaké chybě.
- **Odpovědnost:** Tedy požadavky na odpovědnost uživatelů, nebo také požadavky na funkce, zajišťující bezpečnou komunikaci se systémem.

Každá z částí má své bezpečnostní funkce a každá funkce zase několik úrovní. Každá z těchto úrovní je přesně měřitelná. Platí tedy, že funkce obsahující vyšší úroveň, poskytují kvalitnější ochranu proti hrozbám jako jsou útoky, pády systému a další.[10]

2.1.4 Federální kritéria

FC – Federal Criteria. Federální kritéria jsou vyjádřena třemi požadavky na bezpečnost systému:[11]

- **Funkční složky**: Vyjadřují kvalitu bezpečnostních prvků jako jsou například logická ochrana, fyzická ochrana, spuštění, zotavení a snadnost použití.
- **Vývojové záruky**: Zabývají se kvalitou tvorby bezpečnostního systému a určují práci, která musí být provedena na bezpečnosti. Funkční složky tuto skupinu rozdělují na skupiny: vývojový proces, provozní podpora, vývojové prostředí, vývojová dokumentace.
- **Hodnotitelské záruky**: Určují úroveň bezpečnosti, které bylo dosaženo. Také jsou funkčními složkami rozděleny do skupin: testování, hodnotitelské posudky, hodnotitelské analýzy.

Federální kritéria seskupily vlastnosti do profilu bezpečnosti. Jednotlivé profily přinesly nové ucelené pohledy na bezpečnost a tedy i upřesnění podmínek pro použití. Díky tomu je vytvořeno ideální prostředí pro budoucí modifikaci kritérií při změnách informačních technologií. Snaží se o srozumitelné vysvětlení bezpečnosti.[12]

2.1.5 Společná kritéria

CC – Common Criteria jsou kritéria, která byla uznána mezinárodní komunitou. Jde o jakousi snahu sjednocení hodnocení bezpečnosti. Cílem je především vytvoření jednotných bezpečnostních kritérií, které budou uznávány po celém světě. Nápad na

[10] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 150.
[11] DOUCEK, P., NOVÁK, L., SVATÁ, V. *Řízení bezpečnosti informací*. Praha, 2008. s. 70-71.
[12] DOUCEK, P., NOVÁK, L., SVATÁ, V. *Řízení bezpečnosti informací*. Praha, 2008. s. 72.

společné normy pro hodnocení bezpečnosti se vyskytl už v roce 1990, ale kvůli pomalému postupu v realizaci se dokončení stále neblížilo konci. Rok 1993 pomohl k urychlení prací, hlavně tedy díky aktivitě sedmi evropský a amerických organizací, které uzavřely spolupráci na spojení svých již rozpracovaných činností. První verze kritérií na základě společné aktivity se objevila v roce 1996. ISO tato kritéria přijala jako pracovní návrh. Však v roce 1999 dochází ke schválení poslední pracovní verze a vytvoření mezinárodní normy ISO/IEC 15408. Nejnovější verze byla zavedena v roce 2008.[13]

Common Criteria používá pojmu komponenta funkčních požadavků, které je nahrazeno za pojem bezpečnostních funkcí. Tyto komponenty jsou řazeny do skupin podle funkcí, které zajišťují. Je to tedy jakýsi katalog, který slouží pro vývojáře či uživatele. Ti si vybírají jednotlivé komponenty, které jim vyhovují k zabezpečení daného systému.[14]

[13] DOUCEK, P., NOVÁK, L., SVATÁ, V. *Řízení bezpečnosti informací*. Praha, 2008. s. 73.
[14] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 151.

3 Současné druhy a možnosti zabezpečení

Současných možností zabezpečení dat a informací je mnoho. Proto v této kapitole dojde k vysvětlení jak základních pojmů, kterých se bezpečnost týká, tak k ukázce možností, jak svá citlivá data chránit před útočníky.

3.1 Základní pojmy

Informační bezpečnost zavádí řadu nových pojmů a definic. Kvůli správnému pochopení bezpečnosti je nutné vysvětlit ty nejzákladnější a nejdůležitější:[15]

Aktivum je nazýváno vše, co má pro majitele informačního systému nějakou hodnotu. Jedná se například o peníze, majetek a v našem případě o data a informace. Taková data, kvůli kterým by firma nebo organizace utrpěla škodu, pokud by došlo k jejich odcizení, ztrátě či jakémukoliv pozměnění ze strany útočníka.

Bezpečnost je vlastnost objektu nebo subjektu, která ukazuje úroveň zabezpečení proti útokům a hrozbám. Jde jak o informační systémy, tak i o technologie, které systém využívá ke svému chodu.

Hrozba neboli událost, osoba či jakékoliv jiné působení na systém, který svou činností může způsobit škody na hodnotě aktiv. Hrozba souvisí s mírou bezpečnosti. Jedná se například o útoky hackerů, ale i o přírodní jevy.

Útok je bezpečnostní incident, který buďto využije slabého místa v zabezpečení, nebo se jedná o úmyslnou akci na poškození aktiv. Při analýze možných útoků je potřeba počítat s tím, kdo útočí na daná aktiva, kdo může páchat tento druh zločinů a jak se bránit před útoky.

Zranitelnost určuje míra slabin bezpečnostního systému. Takových slabin, které mohou být zneužity k poškození či zničení daných aktiv. Kvůli nekonečnému množství možností vlivů, které mohou nastat, se každé aktivum stává zranitelným.

Zranitelné místo je slabina informačního systému, kterou lze využít k útoku na data a systém. Zranitelná místa vznikají v důsledku chybné analýzy, návrhu, nebo ve špatné implementaci daného systému. Aktiva jako jsou například peníze a majetek jsou nejvíce ohrožena živelnými pohromami, nebo krádeží ze strany lidských útočníků. Kvůli takovýmto případům jsou zranitelná místa chráněna bezpečnostními mechanismy,

[15] POŽÁR, J. *Informační bezpečnost*. Plzeň, 2005. s. 37-39.

jako jsou například antiviry, přihlašovací formuláře do systému, ale jedná se také o bezpečnostní kamery, uzavřené firemní úseky zabezpečené omezeným přístupem aj.

3.2 Kryptologie

Pro citlivá data, která mají vysokou míru utajení, se používá šifrovacích technik. Toto šifrování má za úkol zabránit odcizení či spíše prozrazení důvěrných informací, které jsou například přenášeny či ukládány. Tedy pokud dojde k odcizení některých informací, či jejich částí, útočník nebude schopen informaci přečíst, pokud nezná klíč či techniku, kterou byla informace zašifrována. Důležité je také pochopení základních pojmů v tomto oboru, kterými jsou:[16]

Kryptologie: Matematický vědní obor zabývající se tvořením, používáním a prolamováním šifer. Kryptologie se dále dělí na kryptografii a kryptoanalýzu.

Kryptografie: Zabývá se navrhováním šifrovacích algoritmů, nástrojů, které lze ke kryptografii využít a hardwarovými implementacemi algoritmů. Úkolem kryptografie je řešit problematiku mezi převáděním srozumitelné informace na informaci nesrozumitelnou. Tedy informaci, která je zašifrovaná a pro eventuelní útočníky nesrozumitelná.

Kryptoanalýza: Je vědou, zabývající se luštěním šifer. Hledá možnosti a slabiny zašifrovaného textu a snaží se ho přečíst bez znalosti klíčů či šifrovacích algoritmů. Algoritmus je prolomený ve chvíli, kdy lze číst zašifrována data. Takovýto stav je však nežádoucí, jelikož by pak k textu či informacím měla přístup jakákoliv nežádoucí osoba.

Šifrování: Je matematický algoritmus, který je vytvořen s cílem utajit data, na která je aplikován. Aby mohly určené osoby následně informaci rozluštit, algoritmus je šifrován podle klíče, kterého pak lze využít i k opětovnému rozšifrování informace. Stejný algoritmus lze využívat pro několik osob, ale každá ze stran musí poskytnout k šifrování i dešifrování jiný klíč.[17]

Kódování: Je také algoritmus, který se snaží uchránit kódovaná data. Od šifrování se však liší tím, že nemá žádný vlastní klíč. O jeho utajení se stará samotný algoritmus. Ke kódování a dekódování slouží například slovníky, které obdrží každá

[16] POŽÁR, J. *Základy teorie informační bezpečnosti.* Praha, 2007. s. 83-84.
[17] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 23.

z komunikačních stran. U této metody se však jeví velký problém v utajení. Stačí, aby pouze jedna ze stran zveřejnila dekódovací slovník, a každý již bude moci číst utajované informace.[18]

Šifry jako takové mají své hluboké kořeny v historii. Ještě poměrně nedávno bylo šifrování výsadou hlavně armád, diplomatických služeb či zpravodajců. Výsadou hlavně proto, že šifrování má vysokou složitost a s tím i odpovídající vysokou cenu zařízení, kterých je potřeba k šifrování (kryptografických zařízení). Však v dnešní době s rychlým vývojem informačních technologií dochází ke zvratu, kdy počítače umějí pracovat i s těmi nejsložitějšími algoritmy potřebnými k šifrování informací.[19]

3.2.1 Sdílený klíč – symetrické šifry

Symetrické šifrování je založeno na principu, kde odesílatel i adresát používají stejného klíče k dešifrování či zašifrování zprávy. Obsahem se tedy stává text, který je složený z domluvené abecedy a klíče. Za pomoci klíče se z otevřeného textu udělá kód, který se může odeslat příjemci. Příjemce pak použije stejného klíče a kód, který obdržel rozšifruje do původního textu a ten si může přečíst. Slabinou symetrického šifrování je sdílení klíče mezi uživateli. Pokud si tedy dvě strany chtějí vyměnit tajný text, musí také dojít k výměně klíče, který musí být u obou stran shodný. Klíč se přenáší přes bezpečný přenosový kanál, aby se nestalo, že klíč dostane do rukou třetí strana.[20]

Symetrické šifrování je známkou rychlého výpočtu, jelikož matematické výpočty nejsou tak složité jako u asymetrických šifer. Jako největší nevýhodou se tedy jeví počáteční výměna klíče. V dnešní době je využíváno mnoho symetrických šifrovacích algoritmů, které musí odolat zejména útoku hrubou silou. Za hrubou sílu se bere vyzkoušení všech možných klíčů. Jako nejpoužívanější algoritmus pro symetrické šifry se používal DES (Data Encryption Standard). Je to 56 bitový klíč, a tedy k jeho rozluštění hrubou silou existuje 2^{56} možností. Bohužel se však postupem času podařilo DES prolomit. Jako nejrychlejší prolomení se počítá případ, který potřeboval k rozluštění pouhých 22 hodin. Po překonání DES vznikl požadavek na nový a účinnější algoritmus. V té době tedy vzniká nový algoritmus AES (Advanced Ecryption Standard), který obsahuje klíč o velikosti 128 bitů.[21]

[18] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 23-24.
[19] POŽÁR, J. *Základy teorie informační bezpečnosti.* Praha, 2007. s. 84.
[20] POŽÁR, J. *Informační bezpečnost*. Plzeň, 2005. s. 201.
[21] NORTHCUTT, S., ZELTSER, L., et al. *Bezpečnost počítačových sítí*. Brno, 2005. s. 572.

Výhody symetrických metod jsou zejména jejich rychlost a nenáročnost na výpočetní výkon. Jsou skvěle využitelné pro šifrování dat, která se nikam neposílají a zůstávají na jednom místě. Tedy hlavně pro šifrování dokumentů v počítači, které chceme chránit před přečtením druhou stranou. Jako největší nevýhodou se jeví předání klíče, což se v některých případech stává hlavním problémem. U velkých organizací se o předání klíče starají speciálně určení lidé neboli kurýři. Její další znevýhodnění tkví v závislosti klíče na jeho délce. Tedy čím delší klíč, tím by měla šifra být bezpečnější. Snad největší nevýhodou je však počet potřebných klíčů ke komunikaci. Pro určení počtu klíčů slouží tento vzorec N = n*(n-1)/2, kde n je počet osob a N zastupuje klíče. Pokud tedy komunikace dosáhne vyššího počtu osob, správa klíčů se stává zásadním problémem. Pokud by například organizace měla 10 000 členů, tak k jejich bezpečné komunikaci by bylo zapotřebí 5 miliónů klíčů.

Caesarova šifra je hodnocena jako symetrická substituční monoalfabetická proudová šifra. Tento šifrovací algoritmus je brán jako úplně první známý pokus o šifrování. Jejím autorem je známý římský vojevůdce a politik **Julius Caesar**. Ten používal tento algoritmus k šifrování svých vojenských zpráv. Princip byl zcela jednoduchý. Šlo o posunutí celé abecedy o určitý počet pozic, tedy pokud jeho klíčem bylo číslo 4, posunul celou abecedu o 4 pozice. Písmeno A bylo v zašifrovaném textu E, písmeno B bylo písmenem F a tak dále. Když tedy zpráva došla příjemci, ten musel vědět, o kolik pozic jsou písmena (abeceda) posunuta, aby mohl následně text rozluštit a získat tak otevřenou zprávu. Tato šifra je tedy šifrou symetrickou, jelikož máme jeden klíč, který je potřeba nějakým způsobem předat druhé straně, která pak může následně text číst. Postupem času se však tento algoritmus stal méně bezpečným, jelikož k jeho prolomení stačí útok hrubou silou, nebo takzvaná frekvenční kryptoanalýza. Oba tyto útoky jsou rozebrány v útocích na kryptografické algoritmy.[22]

Vigenérova šifra je symetrickou substituční polyalfabetickou proudovou šifrou. Tato šifra byla vymyšlena v 60. letech 15. století ve Florencii a její zakladatelem byl Leon Battista Alberti. Však konečnou podobu dal šifře v 16. století francouzský diplomat Blaise de Vigenére, který výhody šifry využíval k diplomatickým účelům. Tato metoda se od Caesarovi liší v jediném bodu a tím je, že místo jedné šifrovací abecedy jsou k zašifrování textu využity všechny posuny dané abecedy. Pokud má tedy

[22] HUB, M. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice, 2013. s. 47-48.

abeceda 26 písmen, je možné využít až 26 možných abeced k šifrování textu. Princip byl takový, že na liché znaky byla použita jiná abeceda, než pro znaky sudé.[23]

Vernamova šifra je řazena jako symetrická substituční polyalfabetická proudová šifra, kterou v roce 1917 nechal patentovat Gilbert Vernam. Její princip je obdobný jako u předchozích šifer, však s tím rozdílem, že každý znak zprávy může být nahrazen libovolným písmenem v abecedě. Tedy jde o to, že každý znak je v šifrovaném textu posunutý o jiný počet míst v abecedě. Tím dochází, že je každé písmeno nahrazeno prakticky jiným náhodným písmenem a tudíž se tato šifra stává defakto nerozluštitelnou. Pokud jsou dodrženy základní požadavky na tvorbu takové šifry a těmi jsou:[24]

- Klíč má stejnou délku, jako zpráva, která je přenášena.
- Klíč musí být dokonale náhodným.
- Klíč nemůže být opakovaně použit k šifrování jiné zprávy.

Tato šifra je však velice složitá na použití. Jelikož náhodný klíč se stává velice dlouhým a nesnadno zapamatovatelným, musí být někde zaznamenán. Tím dochází k oslabení šifry, pokud dojde k jeho ztrátě či odcizení třetí stranou. Stejně tak se stává nesnadným úkolem vytvoření náhodného klíče. Dále muselo dojít k výměně složitého klíče mezi odesílatelem a příjemcem, nějakou z bezpečných cest na předání. Tato šifra ač velice silná proti útoku a prolomení útočníkem a tím nechtěného úniku informací, se používala jen velice málo. Jeden ze známých výskytů této šifry je například za studené války, kdy díky této šifře probíhala komunikace mezi Moskvou a Washingtonem. Tento algoritmus byl využíván i při špionážních akcích.[25]

3.2.2 Veřejný a privátní klíč – asymetrické šifry

Asymetrické šifrování je druhou skupinou kryptografických metod. Asymetrickou se nazývá z toho důvodu, že k zakódování zprávy využívá jiného klíče než k rozšifrování. Jedná se tedy o pár klíčů. Odesílatel zašifruje zprávu pomocí svého veřejného klíče a příjemce zase naopak rozšifruje svou zprávu pomocí svého soukromého klíče. Tato technika je tedy závislá na vytvoření dvou klíčů, kterými jsou veřejný a soukromý. Veřejný klíč slouží k tomu, aby když uživatel chce přijmout

[23] HUB, M. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice, 2013. s. 48.
[24] HUB, M. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice, 2013. s. 47-48.
[25] HUB, M. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice, 2013. s. 48.

nějakou zprávu, musí dát k dispozici svůj veřejný klíč. Odesílatel použije tohoto klíče k zakódování zprávy. Příjemci pak k dekódování slouží jeho soukromý klíč, kterým je schopný text rozluštit do čitelné podoby. Veřejný klíč tedy slouží všem odesílatelům zpráv k šifrování, tento klíč je volně přístupný. Soukromý klíč si však uživatel musí dobře uschovat, jelikož tento klíč zase slouží k dešifrování.[26]

Mezi veřejným a soukromým klíčem je zajímavý vztah a to ten, že žádnou reverzní metodou nelze rozluštit z daných klíčů klíč opačný. Proto pomocí veřejného klíče může zašifrovat zprávu kdokoliv, ale pouze držitel klíče soukromého může zprávu otevřít. Ale i asymetrické šifry mají svou nevýhodu a tou je vysoká matematická náročnost na výpočet algoritmů. Algoritmy jsou tedy podstatně pomalejší a náročnější než šifry symetrické.[27]

Asymetrické algoritmy jsou velice pomalé, a tudíž jejich použití v hlavních datových tocích je neproveditelné. Jsou však skvělým prostředkem k výměně utajených informací, díky svému vysokému zabezpečení. Protože symetrické šifrování je zase naopak velice rychlé, ale má problémy s výměnou klíčů, spojením těchto dvou šifrovacích metod dostáváme poměrně dokonalé řešení. Na základě asymetrické šifry se spojíme s druhou komunikační stranou a vyměníme si klíče pro symetrický přenos. Dostáváme tedy rychlou a bezpečnou komunikaci pro hlavní datové toky.[28]

3.2.3 Elektronický podpis

Digitální nebo také elektronický podpis je poslední možností v běžné komunikaci. Od symetrických či asymetrických šifer se liší v tom, že obsahuje i autentizaci a nepopiratelnost. Jeho přednost je tedy v tom, že pokud nám přijde nějaká zašifrovaná informace, tak my si můžeme ověřit, od koho pochází. Pokud tedy dostaneme zprávu, která je zašifrována klíčem, který drží určitá osoba, je tedy zřejmé, že zpráva pochází skutečně od ní. Elektronický podpis využívá principu asymetrických šifer. Dokument je tedy zašifrován skrze náš privátní klíč a k jeho rozluštění musí příjemce použít náš veřejný klíč. Pokud se mu dešifrování povede, je zřejmé, že zpráva pochází od nás. Digitální podpis nám tedy přináší nepopiratelnost a kontrolu, jelikož

[26] POŽÁR, J. *Informační bezpečnost*. Plzeň, 2005. s. 202-203.
[27] NORTHCUTT, S., ZELTSER, L., et al. *Bezpečnost počítačových sítí*. Brno, 2005. s. 573.
[28] NORTHCUTT, S., ZELTSER, L., et al. *Bezpečnost počítačových sítí*. Brno, 2005. s. 573.

jakákoliv změna textu, který je šifrovaný, by po dešifrování přinesl nečitelný výsledek.[29]

Elektronický podpis se skládá z jedniček a nul v binární soustavě. Jeho velikost je až 4096 bitů a proto je jeho výpočet velice složitý matematický proces. Takovýto výpočet nelze provádět písemně, ale musí být vyjádřen pomocí výpočetní techniky. Takovýto výpočet vykonávají počítače, ale i speciální miniaturní čipy, které se například vejdou do čipové karty či do jiných běžných zařízení jako jsou například mobilní telefony a jiné. Digitální podpis je jedinečný jako náš ruční podpis. Rozdíl je pouze v tom, že podpis je na elektronickém dokumentu a je tvořen podepisovacím číslem. Každá osoba má svoje unikátní podepisovací číslo. Klasický podpis je zde tedy nahrazen složitými matematickými výpočty. Elektronický podpis má tedy unikátní schopnost, že může náležet i k obsahu dokumentu. Tím se tedy zaručuje, že podpis má i vypovídací schopnost. Lze zjistit, zda se obsah, pro který byl klíč vytvořen, shoduje s obsahem aktuálním. Díky této vlastnosti se tedy eliminuje možnost, že by byl dokument přepsán do jiné podoby, než pro kterou byl vytvořen podpis. Podpis je nepřenositelný na jiný dokument a pro každý dokument má různý elektronický podpis.[30]

Elektronický podpis je tedy tvořen soukromým a veřejným klíčem. Pokud však obdržíme zprávu a ověříme si veřejný klíč, tedy identitu odesílatele, jak si ve skutečnosti můžeme být jisti, že se skutečně jedná o danou osobu. Naskýtá se tedy otázka, zda lze zcela důvěřovat veřejnému klíči, za kterým se může skrývat jiná osoba. Tímto problémem se zabývá potvrzovací certifikát. Pokud dojde k potvrzení naší identity, dostatečně důvěryhodnou třetí stranou, je vystaven certifikát. Ten slouží jako důkaz o potvrzené identitě vlastníka veřejného klíče. Tato třetí strana vystaví certifikát k tomu, aby se identita vlastníka nemusel neustále znovu potvrzovat. Elektronický formulář je pak potvrzen značkou potvrzující strany.[31]

3.3 Další možnosti zabezpečení

V úvodní časti, bylo řečeno, že existuje mnoho zabezpečovacích možností našich soukromých dat a informací. Dosud bylo poukazováno spíše na techniky, které probíhají na pozadí našich uživatelských operací a o kterých mnoho uživatelů nemá ani tušení. Nyní si ale ukážeme, jak můžeme sami přispět k bezpečnosti našich dat, nejen

[29] NORTHCUTT, S., ZELTSER, L., et al. *Bezpečnost počítačových sítí*. Brno, 2005. s. 574.
[30] POŽÁR, J. *Základy teorie informační bezpečnosti.* Praha, 2007. s. 94-95.
[31] PETERKA, J. *Báječný svět elektronického podpisu.* Praha, 2011. s. 37-39.

skrze uživatelská rozhraní a programy k tomu určenými, ale například i fyzickou ochranou.

Data, která se snažíme chránit, jsou uložena v tabulkách v nějaké databázi, také v souborech na různých zařízeních jako jsou disky a telefony. Data mohou být přenášena skrze e-mailové schránky, nebo také jen napsána na papíře a odesílána skrze poštu či kurýry. Informace a data, která odesíláme určitým příjemcům, se snažíme chránit, jelikož ne všechny informace chceme jen tak zveřejnit, či je ohrozit tím, že by mohly být zničeny nebo přepsány. Od ochrany čekáme tři základní druhy obrany před nebezpečím:[32]

- **Prozrazení**: Data se snažíme ochránit před třetí stranou.
- **Přepsání**: Nechceme, aby byla data jakkoliv modifikována a měněna.
- **Zničení**: Ochrana dat před úmyslným či neúmyslným zničením

Pokud chceme svá data efektivně chránit, ať už se jedná o naše osobní data, nebo data firem a organizací, je potřeba kombinovat i několik bezpečnostní prvků najednou. Jako základní rozdělení lze použít:[33]

- **Fyzický přístup**: Jde o prvky, kterými se snažíme ochránit svá fyzická úložiště či majetek. Jde tedy o to, aby se například k diskům, nebo penězům, nedostala nepovolaná osoba. Toho docílíme zabezpečenými dveřmi, trezory a mnoha dalšími zařízeními.
- **Logický přístup**: Pokud máme ke svému úložišti nějaký vzdálený přístup, vzniká riziko, že se k našim datům dostane nepovolaná osoba, proto je zapotřebí chránit systém řízeným přístupem. Jedná se například o přihlašovací programy a jiné.
- **Ochrana uložených dat**: Snažíme se chránit data uložená na přenosných zařízeních. Aby nedošlo například k situaci, kdy nám někdo odcizí disk, připojí ho ke svému zařízení a bude se snažit data stáhnout a analyzovat.
- **Ochrana sítě**: Pokud data přenášíme po síti, mezi různými stanicemi, je zapotřebí zasílaná data šifrovat. Pokud po síti budou kolovat v nezabezpečené podobě, jejich odcizení je pak velice snadné.

[32] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 47.
[33] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 48-49.

- **Ochrana před zničením**: Jedná se o ochranu dat před úmyslným či neúmyslným zničením. K takovéto ochraně je použito například řízeného přístupu, kryptografie, zálohy dat a dalších bezpečnostních protokolů.

3.3.1 Fyzická ochrana

Jelikož nejslabším článkem v bezpečnosti je vždy lidská loajalita, je třeba dbát na výběr osob, které mají přístup k datům a informacím. Proto se při výběru do pracovních pozic přihlíží k vlastnostem daného zaměstnance. Hlavním rizikem je, že pracovník nemá totožné zájmy jako organizace, pro kterou pracuje. Z tohoto důvodu firmy a organizace shromažďují reference z dřívějších působišť, podrobují pracovníky psychologickým testům atd. I pokud je pracovník na dané místo dosazen, má zprvu omezený přístup k informacím, než si k němu organizace vybuduje důvěru. Mohlo by totiž docházet k úniku různých dat, které by zaměstnanec mohl vynášet například konkurenčním firmám.[34]

Jak již bylo mnohokrát řečeno, data jsou ukládána na různých discích a na různých nosičích. O vlastní ochranu dat se stará nějaký program, který je chrání před nepovolaným přístupem. Co se však stane, když někdo přistoupí k fyzickým úložištím? Toto téma právě řeší fyzická ochrana, která se stará o bezpečnostní prvky, zabraňující přístupu nepovolaným osobám. Pokud by se někdo dostal například k úložnému serveru firmy, mohlo by dojít poměrně k jednoduchému zničení dat za pomoci mechanických nástrojů. Fyzická ochrana však není jen zabránění přístupu fyzickým osobám, ale řeší i problematiku živelných pohrom. Jakými jsou například povodně, požáry ve firmě či zřícení budovy v následku zemětřesení.[35]

Fyzickou ochranu lze započít u vstupních dveří do firmy, nebo do místnosti se zařízeními, obstarávající chod systému firmy. Pokud vcházíme do budovy nějaké větší firmy, je většinou vstup zabezpečen vrátným nebo recepčním. Tato oprávněná osoba kontroluje přístup oprávněných osob či návštěv. Dveře jsou zajištěny například systémem na čipové karty. Místnosti jsou skenovány snímači pohybu a kamerovým systémem, který kontroluje bezpečnostní orgán firmy. Tyto ochranné prvky slouží k monitorování osob v budově. Samotné servery však podléhají důkladnější ochraně. Například jsou skladovány ve speciálních skříních, které nejsou žádným způsobem

[34] POŽÁR, J. *Informační bezpečnost*. Plzeň, 2005. s. 147.
[35] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 52.

rozebíratelné. Pokud dojde k narušení jejich obalu, data na discích se smažou, či nějakým způsobem zablokují.[36]

Pokud však přijde živelná pohroma, dveře s čipovým zajištěním ani ochranka nám nepomohou. Proto se zavádí spousta dalších ochranných prvků. Pokud budovu zachvátí *požár,* je vhodné vlastnit protipožární ochranu. Za ochranu se počítá nehořlavá podložka, která se zavádí pod skříně, kde je uloženo hardwarové vybavení. Další prvky představují manuální a samočinné hlásiče a hasiče požáru. Skříně, ve kterých jsou zařízení uložena, by měly být vodotěsné a prachotěsné. Jelikož disky jsou elektronické zařízení, nemělo by při hašení dojít ke styku s vodou, nebo v případě hašení práškovým hasicím přístrojem s prachem. Další katastrofou, která nás může postihnout, je *borcení* budovy například kvůli zemětřesení. Je tedy potřeba zajistit skříně proti nárazům a samočinnému posunu po místnosti. Důležité je, aby nedocházelo k pádům a nárazům zařízení. Ani zde není na škodu prachuvzdorná skříň. Počítačové vybavení je velice citlivé na *prostředí*, ve kterém funguje. Není vhodné, aby docházelo k velkému kolísání teploty, či velkému víření prachu v místnosti. Jelikož zařízení při své funkci vyvíjí teplo, je potřeba tato zařízení chladit. Tyto problémy řeší zavedení klimatizace, která se stará o vhodné podmínky v prostředí. Posledním velkým faktorem, ohrožující fyzickou bezpečnost počítačového vybavení, je *voda*. Kupříkladu když přijde povodeň, je vhodné mít vodotěsné skříně, umístěné ve vyšších patrech budovy. Není ku škodě, pokud je i sama místnost vodotěsná. Dále by v místnosti neměla být žádná okna, která by skýtala zbytečné ohrožení kvůli malé vodotěsnosti.[37]

Jedno z dalších fyzických opatření je i zajištění ochrany podpůrných zařízení. Jedná se například o zdroje energie, které svou nepřetržitou dodávkou udržují servery v chodu. UPS (Uninterruptible Power Suply), neboli nepřerušitelný zdroj energie, který udržuje v chodu počítačová zařízení, pokud dojde k výpadku proudu. Nesmí se podcenit ani ochrana kabelových rozvodů, kterými jsou přenášena data. Neměly by být lehce dosažitelné, aby nedocházelo k odposlechu. Také by neměly být vedeny se silovými rozvody. To by mohlo zapříčinit jejich rušení a jiné obtíže s přenosem dat. Jako ochranu lze také brát udržování ochranných prvků. Je potřeba je pravidelně udržovat a servisovat, aby zařízení měla co nejvyšší životnost. Nesmí se opomenout ani zajištění

[36] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 53.
[37] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 54.

bezpečí zařízení mimo prostor organizace. Tedy nějaká pravidla o přenášení a přemisťování majetku.[38]

Ochranné prvky se soustředí i na likvidaci datových zařízení. Je to hlavně z důvodů, že i po smazání jsou data lehce obnovitelná. Je potřeba tedy data likvidovat za pomoci k tomu určeného a spolehlivého softwaru či elektromagnetickými impulsy, které vymažou data na mediích využívající magnetického pole. Poslední možností je fyzická likvidace datových zařízení, za použití mechanických nástrojů.[39]

Fyzickou ochranou dat se zabývá disciplína s názvem CPTED, tedy anglická zkratka pro Crime Prevention Trough Enviromental Design, což v překladu znamená prevence kriminality prostřednictvím návrhu prostředí. Jejím hlavním cílem je navrhnout fyzické prostředí tak, aby se co nejvíce snížila kriminalita na daném objektu. Bere tedy v potaz fyzické, sociální a psychologické potřeby člověka. Snaží se přímo působit na lidské chování a tím potlačit kriminalitu. Jako za příklad může posloužit opatření, které udává, aby kamery, které monitorují venkovní prostory, byly dobře viditelné. Jde o působení na lidskou psychiku v tom, že útočník se může zaleknout už jen toho faktu, že prostory jsou monitorovány. Tato opatření však slouží i k ochraně potencionálních obětí, které vyhledají dané monitorované místo ve snaze odradit útočníka. CPTED se však nezabývá jen ztížením útoku pro potencionálního útočníka či jeho zdržením, ale zaobírá se i otázkou estetiky prostředí. Mimo jiné je cílem této disciplíny udělat taková opatření, aby nedocházelo k jakémukoliv snížení použitelnosti a pozitivního dojmu. Takže místo toho, aby u budovy vykonstruovali postranní dveře, které budou hlídány alarmy a kamerami, snaží se návrh udělat tak, aby žádné takové místo nebylo vůbec potřebné. Jejich strategie je následující:[40]

Řízení přístupu osob, na základě umístění vstupních dveří, oddělení zón v budově, kde každá zóna má jiná ochranná opatření udělená podle toho, co se v prostorech ukrývá a zda je potřeba tam vpouštět neoprávněné osoby. Jedná se také o ploty, různá osvětlení či úprava krajiny v prostorách kde objekt leží. Hlavním cílem řízení přístupu je minimalizovat vstupní body, aby se dal snadněji kontrolovat vstup osob. Pokud například přijde host, je požadavek, aby prošel přes vrátnici, kde bude identifikován a na základě toho mu bude například udělena karta s omezeným

[38] DOUCEK, P., NOVÁK, L., SVATÁ, V. *Řízení bezpečnosti informací*. Praha, 2008. s. 141.
[39] DOUCEK, P., NOVÁK, L., SVATÁ, V. *Řízení bezpečnosti informací*. Praha, 2008. s. 141.
[40] HUB, M. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice, 2013. s. 56-62.

přístupem. Aby něco takového bylo možno uskutečnit, je zapotřebí kontrolní osoby, která hosta identifikuje a přidělí vstupní kartu. Je potřeba tedy zajistit ochranku, jež bude kontrolovat identifikační údaje a fotku, nebo vyhradit zaměstnance, který bude hosta doprovázet. Také dochází ke školení zaměstnanců, aby rozpoznávali podezřelé osoby pohybující se v nepřístupných prostorách.

Pokud je tedy ve firmě řízený přístup řešený skrze ochranu, je potřeba aby osoby, které tuto činnost vykonávají, byly dostatečně psychicky vyspělé. Jde tedy o to, že osoba chápe základní smysl své existence a netrpí psychickými stavy v rozporu s výkonem této pozice. Také je potřeba fyzické vyspělosti a obratnosti, tyto stavy jsou doprovázeny dobrým zdravotním stavem jedince. Vykonavatel této pozice by také měl mít příjemný vzhled a vykazovat vysokou úroveň spolehlivosti.[41]

Přirozený dohled je jedním z dalších bodů, jež si CPTED zadává do své základní strategie. Jeho principem je povědomí pro zaměstnance, že jsou v pořádku a v bezpečí a naopak pro útočníky, že mohou být kdykoliv viděni a snaží se jim útok co nejvíce znepříjemnit. Takového stavu lze dosáhnout skrze ochranku, velká místa, kde se zaměstnanci často potkají, zavedením průmyslových kamer, nebo třeba vystavěním skleněných zdí, díky kterým nevznikají slepá místa. Vzhledem k položení objektu se například navrhuje velká rovina, díky níž je umožněn velký dohled a světlost. Podle studií tyto vlastnosti značně přispívají k pocitu bezpečí zaměstnanců.

Pachatel se totiž v mnoha případech předem připravuje na svůj čin, je proto snadnější monitorovat podivné chování jak zaměstnanců, tak hlavně návštěvních osob, které se pohybují v objektu, či okolí. Pachatel se totiž snaží vybrat místo, kde nejlépe trestnou činnost spáchá, kudy uteče, nebo kam zcizený předmět schová. Může se jednat o přenosné disky či papírovou podobu důležitých firemních dat.[42]

Teritoriální ohraničení je posledním jakýmsi psychologickým tahem v ochraně proti útoku. Jedná se o snahu útočníkovi vytvořit takové prostředí, do kterého nezapadá a naopak pro zaměstnance vytvořit pocit souznění s ostatními zaměstnanci. K takovýmto praktikám se využívají ploty, různá ohraničení prostoru či například vytvoření firemních triček, jejichž další výhodou je lehké rozpoznání hostujících návštěvníků.

[41] PORADA, V., HOLCR, K. a kolektiv. *Policejní vědy*. Plzeň, 2011. s. 140-141.
[42] PORADA, V. a kol. *Kriminalistika.* Plzeň, 2007. s. 47-49.

CPTED se mimo jiné zabývá kompletním návrhem budov a jejich analýzou. Tedy jaká poloha, viditelnost a přístupnost je vhodná, zda se v místě výstavby nevyskytují velké hrozby kupříkladu z živelných pohrom a jiné. Pokud se naplánuje vhodná poloha pro budovu, následuje kompletní plánování konstrukce budovy. Je potřeba navrhnout správný materiál pro stěny, stropy, podlahu, vhodné rozvody elektřiny, vody a jiné. Pokud je budova a různé materiály, které budou místnost chránit naprojektovány, dalším bodem jsou vstupní místa pro samotnou budovu. Opět přichází v potaz jaké dveře na jaké místo, tím se myslí, zda je zapotřebí trezorových dveří či postačí kupříkladu dveře na čipovou kartu. I okna mají mnoho různých provedení, která je potřeba do projektu zahrnout. Jako poslední věcí při projektování je výbava budovy a místností. Jde o umístění různých detektorů (požáru, pohybu, atd.), nebo trezorů a ochranných stanic, které slouží k ochraně proti výpadkům proudu.

3.3.2 Logická ochrana dat

Logická ochrana dat má za úkol zabezpečit data, která se nacházejí na discích a ke kterým je přes zařízení přistupováno. Hlídá, aby do systému neměl přístup neoprávněný uživatel, který nemá práva na čtení či přepisování dat. Aby počítač poznal, o jakou osobu se jedná, musí vyžadovat její identitu.

Metodě na logickou ochranu dat se říká řízený přístup. Každý uživatel, který vstupuje do systému, by měl mít svou unikátní identitu. Není vhodné, aby více uživatelů sdílelo jednu identitu, jelikož pak nelze jednotlivé osoby stíhat kvůli odpovědnosti. Uživatel by měl dostatečně chránit své heslo, zajistit tím tak ochranu zařízení před nepovolaným přístupem. Nejedná se však jen o problém úniku hesla. Uživatel by měl po dokončení své práce provést odhlášení ze systému, či dodržovat zásady prázdného stolu a prázdné obrazovky. Tedy aby nikdo nepovolaný nemohl zachytit informace, na kterých se pracuje. Řízení přístupu má své tři kategorie:[43]

- **Řízení přístupu k síti**: Ať už se jedná o vzdálený, nebo místní přístup například k nějaké databázi ve firmě.
- **Řízení přístupu k systému**: To je například vytvoření více profilů s různými právy. Může se jednat o profily na jednom zařízení.

[43] DOUCEK, P., NOVÁK, L., SVATÁ, V. *Řízení bezpečnosti informací*. Praha, 2008. s. 144-145.

- **Řízení přístupu k aplikacím**: Jelikož nechceme, aby se běžný uživatel dokázal pohybovat v nastavení různých firemních aplikacích, dostává omezené možnosti, které v aplikacích může provádět.

Řízený přístup funguje na základě autentizace uživatele. To znamená, že uživatel prokáže svou identitu na základě zadané informace. Například lze zadávat tajné heslo, prokázat se bezpečnostním předmětem, nebo se uživatel prokáže nějakou unikátní tělesnou vlastností. Za takovouto vlastnost se počítá například otisk prstu, či skenování obrazu sítnice[44]. Řízení přístupu tedy obsahuje:[45]

- **Identifikace:** Je první fáze procesu rozpoznání uživatele. Probíhá za pomoci unikátního prostředku, kterým je například uživatelské jméno. Tato jména jsou unikátní a jsou zaznamenána v databázi uživatelů.
- **Autentizace**: Druhá fáze procesu, kde dochází k ověřování vstupující identity do systému. Jde tedy o ověřování pravosti identifikace. Tato fáze zajišťuje ochranu před falšováním identity.
- **Autorizace**: Je poslední krok k oprávněnému vstupu do systému. V této fázi již dochází k povolení vstupu. Na základě autorizace, jsou zpřístupněna data či zařízení, která jsou danému uživateli povolena.

Na autentizaci jsou kladeny speciální požadavky. Je potřeba, aby tento proces probíhal na základě získané informace od uživatele. Tato informace by měla být lehce uchovatelná a měla by mít schopnost snadného uchránění před odcizením. Také jsou u ní kladeny požadavky na tajnost, aby mohla být použita jen tím, kdo tuto informaci zná. Autentizace se dělí na tři možné druhy:[46]

Dokázáním znalostí: Tento způsob dokázání je asi tím nejrozšířenějším. Jedná se o zadávání autentizační informace například na klávesnici počítače. Zadávaná informace jsou písmena a čísla v různém pořadí. Buďto jde o kombinaci obou možností, nebo jsou zadávány jen číselné kódy, jako je tomu například u kreditních karet. Také záleží na tom, zda jsou uživateli povolena práva na změnu hesla. U některých účtů a přístupů, lze hesla měnit, aby si je uživatel lépe zapamatoval. U kreditních karet jsou však jasně dána číselná hesla neboli PINy. Hlavním problémem se zde jeví nároky na paměť uživatele. Ten by měl své heslo dobře chránit a neměl by si ho nikde

[44] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 56.
[45] DOUCEK, P., NOVÁK, L., SVATÁ, V. *Řízení bezpečnosti informací*. Praha, 2008. s. 145.
[46] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 66-68.

zaznamenávat, aby nedošlo k jeho odcizení. Heslo by se mělo pravidelně měnit a hlavně by mělo být dostatečně složité, aby nedošlo k jeho snadnému uhodnutí. Není vhodné používat rodinná jména či data narození. Jako dokonalé heslo se považuje řetězec, který obsahuje písmena, čísla a některý ze znaků jako jsou tečky, čárky a jiné.

Dokázáním vlastnictvím: Autentizační informaci lze získat na základě využití předmětu, který dokazuje pravost uživatele. Uživatel tedy obdrží například čipovou kartu, která se po načtení v zařízení (například čtečka karet), stává jeho autentizací. Daný předmět obsahuje všechny potřebné informace, které si čtecí zařízení z předmětu samo získá. Takováto metoda má však své nevýhody. Jednak uživatel musí předmět nosit neustále u sebe a předmět nesmí ztratit. Kladnou stránkou ale je, že předměty bývají přizpůsobeny snadnému nošení. Mají tedy přiměřenou velikost a tvar. Nejčastějším identifikačním předmětem jsou karty s magnetickým proužkem, či integrovaným čipem. Buďto tedy k přečtení informace z karty slouží čtečka karet, nebo v dnešní době vznikají zařízení, která se připojí k USB portu počítače. Bohužel ztracení předmětu je velmi snadné a pravděpodobné. Proto je vhodné kombinovat více bezpečnostních prvků. Tedy pokud chce vlastník pomocí předmětu vstoupit do zařízení, měl by ještě zadat kontrolní kód. Kdyby ke vstupu stačila pouze karta samotná, při jejím ztracení by mohl kdokoliv kamkoliv přistupovat bez větších problémů.

Dokázáním vlastností: Tato metoda spočívá v autentizaci uživatele, na základě měřitelných anatomických charakteristik. Informace o právech je tedy předávána například skrze otisk palce, skenování sítnice nebo také vzorem hlasu. Hlavním problémem se však jeví, jak systém zjistí, že předvedený důkaz je od živé osoby? Takovýto systém jde například obelstít fotografií v případě, že čtečka skenuje obličej. Otisk prstu zase lze ošálit skrze vytištěný otisk na laserové tiskárně, či pomocí gumových rukavic s daným vzorem otisku. Abychom zajistili, že nebude možné takto snadno ošálit čtečky, je potřeba tyto stanice dát do blízkosti lidské ostrahy. Tedy aby nějaká osoba mohla dohlížet na přistupující uživatele. Jde však zavést i další kontrolní prvky, jakými jsou například měření tepu, kontrola teploty. Dále lze také vyzvat uživatele ke kontrolním pohybům atd.

3.3.3 Monitoring

Účelem monitoringu je zjišťování nevyžádaných a zlomyslných aktivit. Takovými aktivitami jsou pokusy o útok na informační systém. Monitoring také slouží

jako pomocník při rekonstrukci událostí, dokáže vytvářet upozornění a vyvolání analýzy vzniklého problému. K zajišťování kvalitního monitoringu jsou využívány různé systémy a softwarové programy, jež pomáhají detekovat útok či pomáhají k pozdějšímu trestnímu stíhání tím, že dokáží evidovat stavy vzniklého útoku.[47]

Úkolem systémů, které detekují útoky a různé aktivity, je kontrola vznikajících událostí v reálném čase. Ačkoliv jsou hlavně vytvářeny proto, aby bylo možno kontrolovat útoky, jež ohrožují informační systém, mohou však také upozorňovat na různá selhání informačního systému či zaznamenávat poklesy výkonnosti. Hlavním cílem je ale dosáhnutí včasné a kvalitní reakci na vzniklý útok. Kvalitní systém by měl disponovat těmito funkcemi:[48]

- Sledování aktivit, které se jeví jako podezřelé.
- Čtení zapsaných záznamů, které slouží ke zpětné kontrole.
- Oznamování veškerých událostí administrátorovi, které nastanou v důsledku napadení či ohrožení systému.
- Možnost uzamknutí různých částí systému, zahrnující soubory, služby a data o různých stupních důležitosti a utajení.
- Detekce slabin, vyskytujících se v různých částech hierarchie informačního systému.
- Důležitou funkcí je možnost vystopování pachatele, tedy jeho umístění z fyzického a logického pohledu.
- Přerušení probíhajícího útoku.

Monitoring a detekce útoků dále spolupracuje s řadou dalších programů a systémů. Používá se různých technik k odražení útočníka. Jako za příklad mohou sloužit tyto ukázky:

1. **Honey pot** je jedna z prvních metod. Jedná se o počítač či o celou počítačovou síť, která je na útočníka nastražena jako past. Pro toho kdo se snaží na systém zaútočit, se počítač či síť jeví jako skutečný bod. Data, která jsou však v zařízení poskytnuta, jsou zfalšovaná. Úkolem Honey potu je tedy pouze zaujetí penetrátora a odvedení jeho pozornosti od skutečné funkční a používané sítě. Do těchto oblastí nejsou běžní

[47] HUB, M. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice, 2013. s. 39.
[48] HUB, M. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice, 2013. s. 40.

uživatelé vpouštěni. Tato metoda tedy slouží čistě k zachycení hrozeb v podobě útočníků.

2. Metoda **Padded cell** má značnou podobnost s metodou Honey pot. Její odlišností se jeví jiný postup při izolaci útočníka od skutečné sítě či zařízení. Funkčnost je závislá na kvalitní detekci útočníka, jelikož teprve po jeho detekování je penetrátor přesunut do zóny, která je pod kontrolou a zdá se být stejná, jako skutečná počítačová síť. Útočník, který do této vypolstrované cely vstoupí, má stále dojem, že se nachází ve skutečné síti. Zde však nemůže provádět aktivity, jež by mohly vést k poškození či odcizení dat, jelikož vše co útočník vidí, jsou pouze falešné dokumenty. Díky tomu, že do této zóny škůdce spadne, je veškerá jeho aktivita monitorována a všechny vstupy jsou zaznamenávány k pozdějšímu vyvolání, jako důkaz při trestním řízení.
3. **Vulnerability scanner** napomáhá k hledání slabých a zranitelných míst, která se vyskytují v systému. Pokud scanner nalezne chybu, vytvoří jakýsi report, což je název pro zprávu obsahující detailní popis nalezené slabiny. Report pak dále slouží jako vodítko pro opravu nalezené chyby, kterou lze odstranit mnohými metodami. Jedná se například o záplaty, rekonfigurace či zavádění různých bezpečnostních opatření. Díky scanneru se celkově snižuje riziko útoku, jelikož jsou podchycena slabá a zranitelná místa, která se v systému vyskytují. Aby hledač zranitelných míst správně fungoval, je potřeba neustále aktualizovat databázi, která slouží jako znalosti daného scanneru.

K monitoringu neodlučitelně patří i **penetrační testy**. Penetrace je stav, kdy útočník úspěšně vnikne do systému či zařízení, za jeho bezpečnostní hranice. Penetrační testy tedy vznikají za účelem zabránit útočníkovi ve vniknutí do systému a způsobení jakékoliv škody. K takovýmto testům jsou speciálně najímány zkušené týmy odborníků, kteří se snaží narušit bezpečnostní opatření, jež brání systém a v něm ukrytá data. Cílem je nalezení slabých a zranitelných míst za pomoci hrubé síly, či speciálně vytvořenými programy, jež se snaží o vniknutí. Rozdíl mezi penetračním testem a skutečnou penetrací útočníka je v tom, že pokud se v testu nalezne slabina, vývojáři se okamžitě snaží dané místo posílit. Takovéto testy probíhají na odloučených sítích, aby

nedocházelo k oslabení či k vyvolávání falešných zpráv o útoku, kterými by správce byl zahrnut, nebo aby nebyla ohrožena produktivita firmy.[49]

3.3.4 Firewall

Firewall neboli ohnivá stěna, slouží k obraně proti útoku z vnějšku. Jelikož je velice náročné hlídat všechny počítače, které mají přístup k internetu, je snadnější hlídat pouze jeden počítač, ke kterému se ostatní zařízení připojují. Hlídáním tohoto počítače, který představuje jakousi vstupní bránu, je zaúkolován právě Firewall. Ten má různé podoby, ať je to softwarové, nebo hardwarové vypodobení. Software, který hlídá příchozí a odchozí data, nebo hardware, který je zapojený mezi sítí a internetem.[50]

Filtrování paketů je jedním z nejstarších opatření, které má chránit přístup k síti. Princip je takový, že podle identifikačních údajů příchozího datového balíčku neboli paketu se rozhodne, zda má vstoupit či vystoupit ze sítě. Důležité je ještě vysvětlit, jak mezi sebou systémy komunikují. Aby byl zaručený bezproblémový přenos, je potřeba, aby si systémy mezi sebou vzájemně rozuměly. Tuto komunikaci zajišťuje TCP/IP protokol, který slouží jako jakýsi dorozumívací jazyk. Aby komunikace byla zvládnutelná, tak se příchozí a odchozí informace musí rozdělit na menší části. Těmto částem se říká pakety. Každý paket pak obsahuje svou identifikaci, která se označuje jako hlavička paketu. Pakety jsou po síti odesílány podle informací v nich zapsaných. Mimo jiné tedy paket ještě obsahuje svůj původ (zdrojovou adresu) a svůj cíl (cílovou adresu). Filtrování je tedy založeno na principu, že pokud k nám dorazí určitý paket, dojde k přečtení jeho hlavičky a podle vyšší instrukce se rozhodne, zda se takový paket má pustit, či zakázat. Tato technologie je však velice zastaralá a velice špatně kontrolovatelná. Pokud k nám totiž dorazí škodlivý paket a my o něm zrovna nevíme a není v seznamu zákazů, tak nám pronikne do sítě. Tudíž se filtrování používá spíše na blokování hostitelských systémů. Tato blokace funguje na základě IP adresy, tedy adresy, kterou má každý systém unikátní. Můžeme tedy libovolně zakazovat či povolovat komunikaci mezi systémy a hostiteli.[51]

Stavové Firewally pracují na základě stavové tabulky. Tato tabulka slouží k určování pravidel, které slouží k propuštění paketů. Například když jsou odeslány pakety z firemní sítě ven do internetu, stavový firewall následně propustí všechny

[49] HUB, M. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice, 2013. s. 41.
[50] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 116.
[51] NORTHCUTT, S., ZELTSER, L., et al. *Bezpečnost počítačových sítí*. Brno, 2005. s. 27-30.

pakety, které směrují zpět jako odpověď. Stavová tabulka tedy obsahuje záznamy, které identifikují komunikační relace, které jsou pro zařízení známé. Záznam zase obsahuje množinu informací. Tato množina dále identifikuje danou relaci, zdrojovou a cílovou IP adresu zařízení, které spolu komunikují, pořadové číslo a další informace. Položka se ve stavové tabulce vytvoří v okamžiku, kdy započne komunikace mezi oběma stranami. Jedna ze stran tedy vyšle požadavek na komunikaci, a pokud druhá strana odpoví, jsou příchozí pakety porovnány dle stavové tabulky. Pokud pakety odpovídají zadání v tabulce, jsou propuštěny dále do sítě. Informace ve stavové tabulce musí být co nepřesnější a nejpodrobnější, aby nedocházelo k lehkému vytvoření zdánlivě platného paketu, kterého by útočníci využili k vniknutí do systému. Stavová inspekce zaručuje kvalitnější ochranu, než je pouhé filtrování paketů.[52]

Proxy firewally jsou nejpokročilejší, ale i nejnáročnější řešení. Jsou to specializované aplikace, které umožňují komunikaci mezi vnitřní a vnější sítí (internetem). Jejich výhodou je, že vnitřní IP adresy jsou skryté před vnějšími uživateli. Proxy služba, totiž nedovoluje přímou komunikaci mezi externími servery a interními počítači. Administrátor má kontrolu nad zabezpečením a může snadno sledovat narušení zásad. Proxy server dále umožňuje snazší monitorování provozu v síti. Bohužel, díky tomu ale vzniká velké zatížení. Proxy firewally mají však i své slabé stránky. Například díky jejich rozšířenějším možnostem kontroly paketů, jsou značně pomalejší než předchozí dva druhy firewallů. Dále se také naskýtá potřeba, že pro každou novou aplikaci, která má firewallem projít, se musí vytvořit nový proxy server.[53]

Na trhu dnes dominují dva druhy firewallů. Jedním z nich je proxy firewall a druhým je paketové filtrování. Je však ještě možné najít kombinaci obou těchto ochran. Za nejbezpečnější je považován proxy, ale kvůli svým nárokům na výkon a velkému omezování sítě, je používán hlavně na ochranu odchozí síťové komunikace než na ochranu serveru. Paketové filtry či stavové firewally jsou využívány ve větších firmách. Jsou ceněny hlavně pro svůj výkon, díky němuž zvládají oboustranné filtrování komunikace. Firewall je skvělá ochrana, chránící spousty sítí před vandaly. Bohužel však neexistuje firewall, který by byl stoprocentně spolehlivý. Tomu také nepřispěje ani možnost špatného nastavení. Pokud si špatně nakonfigurujeme naši ochrannou zeď, stává se přímým tunelem do našeho počítače. Pokud však útočník narazí na dobře

[52] NORTHCUTT, S., ZELTSER, L., et al. *Bezpečnost počítačových sítí*. Brno, 2005. s. 55-56.
[53] NORTHCUTT, S., ZELTSER, L., et al. *Bezpečnost počítačových sítí*. Brno, 2005. s. 81-87.

navržený, nastavený a spravovaný firewall, nemá takřka žádnou šanci na úspěšné prolomení. Proto se útočníci spíše snaží ochranu nepřímo obejít. Využívá se k tomu útok na slabé články sítě, útok na vytáčené spojení, nebo zneužitím důvěry mezi sítěmi.[54]

3.3.5 Antivirový program

Antivirový program je dnes nepostradatelnou záležitostí při ochraně dat před škodlivým softwarem. Jedná se zejména o viry přenášené v souborech, červy anebo lidi, kteří se snaží přes software dostat do systému a například ho dálkově ovládat, nebo mít přístup k citlivým datům. Antivirový program by měl čelit těmto hrozbám jako jakýsi detektor a léčitel. Pod pojmem léčení se skrývá odstraňování škodlivých virů a tím vyléčení zasaženého programu. Detekce virů pracuje na základě vyhledávání známých rysů, podle kterých se daný vir chová, nebo podle oblasti, do které se škodlivý software dostal. Existují totiž oblasti, jako jsou například systémová nastavení, do kterých nemá přístup jen tak nějaká autorita. Do takovýchto míst mají vstup povolený pouze správci a jimi povolené programy.[55]

Antivirový program je jednou z dalších vrstev posilující bezpečnost sítě a systému. Bohužel jak už tomu u všech obranných mechanismů bývá, má i antivir své kladné a záporné stránky. Přednostmi antivirového programu jsou například:[56]

1. Díky historii antivirů a škodlivého softwaru mají dnes velkou zásobu charakteristik konkrétních virů. Detekce virů tedy probíhá poměrně rychle a dokáže zjišťovat velké množství známých nákaz.
2. Ochranný software běží na pozadí systému, tedy nijak nenarušuje práci uživatele. Díky dokonalosti vylepšování ani neobtěžuje zbytečnými falešnými poplachy, či různými vyskakovacími okny s informacemi. Antivir běží na pozadí v reálném čase a dokáže tedy kontrolovat veškerou činnost uživatele. Události, které potřebují zásah vyšší autority, tedy obsluhu zařízení, se vyskytují jen výjimečně.
3. Postupem času se antivirový software stal běžnou součástí všech zařízení. Díky tomu je jeho pořizovací cena dostupná i běžným uživatelům a malým firmám.

[54] McCLURE, S., SCAMBRAY, J., KURTZ, G. *Hacking bez záhad*. Praha, 2007. s. 369-370.
[55] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 123-124.
[56] NORTHCUTT, S., ZELTSER, L., et al. *Bezpečnost počítačových sítí*. Brno, 2005. s. 238-239.

Omezení antiviru vznikají v závislosti na velikosti databáze, která tvoří známé viry a jejich chování (projevy) v systému. Jedná se zejména o to, že pokud do sítě vnikne vir, který zaútočí na velké organizace či na většinu systémů, obrana ze strany vývojářů antivirových programů se vyburcuje poměrně rychle. Nicméně i to, že než se začne pracovat na obraně proti viru, uběhnou cenné hodiny, kdy si vir může beztrestně putovat po síti a to znamená v některých případech velké ztráty. Dalším problémem se jeví malé viry, u kterých objevení trvá poměrně déle a s tím roste i doba, po kterou páchají škodu. Pokud je vir objeven, tým specialistů začne okamžitě zpracovávat charakteristiku a projevy daného viru, aby mohlo dojít k zařazení do databáze. Pokud však uživatel či firmy nemají povolenou automatickou aktualizaci takovéto databáze, dochází opět k prodlužování doby aktivity škodlivého softwaru.[57]

Jedním z dalších omezení antiviru je jeho malá účinnost při nalézání mutovaných škodlivých kódu. Tedy pokud je detekován vir, jehož charakteristika je zavedena v databázi, antivirová ochrana zareaguje a snaží se s virem vypořádat. Bohužel však stačí u stejné nákazy změnit jeden konkrétní bajt, například v textovém editoru, který je dostupný ve všech počítačích a detekce virů již nákazu nezaznamená. Pokud se najde uživatel znalý a ví co v nákaze přepsat, dokáže změnit charakteristiku viru, na jejímž základě antivirus vyhodnocuje přítomnost škodlivého softwaru.[58]

I přes všechna omezení, která antivirus má, je jednou z nejúčinnějších ochran před nákazou systému. Viry jako jsou trojské koně, červy a jiné, se velice špatně blokují skrze běžná filtrovací zařízení. Hlavním důvodem je to, že škodlivý software má spousty cest, jak se do systému dostat. Může se jednat o útok ze sítě, přes e-mailovou poštu, disketu, CD disk nebo dnes již i přes USB porty. Pokud se stane, že nákaza pronikne do systému, je komunikace mezi virem a autorem poměrně jednoduchá. Samozřejmě tedy záleží s jakým účelem a jakou charakteristikou byl vir vyroben. Firewall je často proti tomuto útoku bezmocný, jelikož komunikace funguje skrze odchozí spojení. Autor má tedy moc podnikat další plánované útoky, či dále infikovat systém. Z těchto důvodu se zavádějí hostitelsky orientované firewally, které slouží ke snížení rizik, jež antivir nedokáže potlačit.[59]

[57] NORTHCUTT, S., ZELTSER, L., et al. *Bezpečnost počítačových sítí*. Brno, 2005. s. 240.
[58] NORTHCUTT, S., ZELTSER, L., et al. *Bezpečnost počítačových sítí*. Brno, 2005. s. 240.
[59] NORTHCUTT, S., ZELTSER, L., et al. *Bezpečnost počítačových sítí*. Brno, 2005. s. 242.

4 Aktuální problematika bezpečnosti informací

V této kapitole bude podrobně rozebrána problematika útočníků a útoků na data, informace a systémy. Dojde také k vysvětlení několika pojmů z IT slovníku, jako jsou například hacker, spam, počítačový vir a škodlivý kód.

4.1 Základní pojmy

Zranitelné místo je charakterizováno jako slabina, která se vyskytuje v informačním systému. Takovéto místo může vést k cílenému útoku za účelem odcizení či poškození dat. Slabá místa lze rozdělit do základních skupin:[60]

- Chybné umístění informačního systému, tedy na místo, kde je lehce přístupný eventuelním útočníkům a sabotérům.
- Nedostatečné zajištění proti živelným pohromám (požár, blesk, povodeň, atd.)
- Chybné řešení ochrany při komunikaci připojených zařízení (pokud dochází k připojování ze vzdálených zařízení atd.)
- Největším zranitelným místem je však lidský faktor.

Zranitelná místa mají za následek další vznik negativních vlastností na informační systém. Tyto vlastnosti pak v důsledku vlivů prostředí nechávají prostor k rozvinutí hrozeb na informační systém.[61]

Hrozba je využití zranitelných míst, která se vyskytují v daném systému. Hrozba jako taková může mít mnoho podob. Může se jednat například o povodně, požáry, ale také o odposlechy skrze elektromagnetické záření, které vyzařuje každé zařízení a k jejichž ochraně se používá různé stínění a pomocná zařízení, která tolik nevyzařují. Hrozbou je i porucha paměťového zařízení, či tvůrcem vytvořená zadní vrátka, která jsou uschována v programu. Jedná se také o neúmyslné hrozby, jež se můžou vyskytnout díky neškoleným zaměstnancům a jejich náhodným chybám. Nebo se také může jednat o úmyslný útok, ať z vnějšku či vnitřku organizace, který je veden zkušenými útočníky.[62]

[60] HUB, M. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice, 2013. s. 35.
[61] HUB, M. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice, 2013. s. 35.
[62] HUB, M. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice, 2013. s. 35.

Útok nebo také bezpečností incident je úmyslné či neúmyslné využití zranitelného místa, jež vede k poškození či zničení dat. Útoky mají mnoho podob, jak již bylo řečeno, může se jednat o útok vedený s cílem způsobit ztrátu anebo se může stát prostě jen chyba, která je zapříčiněna nezkušeným uživatelem. Dále se útoky dělí na způsobenou škodu, kde dochází buďto k velkým, malým či zanedbatelným ztrátám. Je potřeba ještě rozlišit, jak je útok veden. Lze totiž útočit na data, uložená v nějakých paměťových zařízeních, nebo na software, jež brání data či s nimi jinak manipuluje. Posledním možným útokem je fyzický útok. Ten je veden rovnou na hardwarové zařízení, které by mělo být dobře ukryto v prostorách firmy.[63]

Hacker je člověk, který své vědomosti používá k nabourávání do systémů a hledá bezpečnostní díry a nezabezpečené mezery v programech. Pokud najde nějaký nedostatek, poslušně ho nahlásí správci sítě či systému a doporučí, jak chybu opravit a zabezpečit lépe. Existují dokonce jakési hackerské kodexy, které určují chování hackerů. Bohužel i v této skupině se najdou jedinci, kteří se řídí příslovím: *pravidla jsou od toho, aby se porušovala.* Tak se tedy stává, že pokud hacker najde slabinu v systému, tak místo aby ji nahlásil správci, vystaví ji na nějakém z hackerských fór a chlubí se svým úspěchem. Dochází tedy k šíření a zneužívání chyby, která může firmu či organizaci stát značné náklady. Hackeři jsou často organizovaná skupina, jež je dobře informována a znalá nejnovějších trendů.[64]

Cracker, podle jedné z definic, je člověk, který boří protipirátské ochrany programů. Například získává licenční klíče, které jsou potřeba k plnému fungování nějakého programu, aniž by si ho zákazník koupil. Dále také upravuje programy, na které vytvoří crack soubor, který po implementaci do programu zajistí, aby program plnohodnotně fungoval bez zakoupení jakékoliv licence. Další definice zase crackera popisuje jako osobu, která zneužívá chyb, které byly objeveny hackerem. Tyto chyby využívá k vlastnímu obohacení či vydírání, terorismů a jiné počítačové kriminalitě.[65]

Útoky a útočníci se dají rozdělit do různých skupin z hlediska škod, které mohou svou aktivitou způsobit**.** ***Amatéři*** se většinou do systému nebo k objevení chyby dostanou náhodným způsobem. Jejich síla útoku se řadí mezi ty slabé. Jde například o objevení chyby při běžné práci v programu. Většinou jsou tyto útoky náhodné a

[63] HUB, M. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice, 2013. s. 35-37.
[64] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 156.
[65] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 156-157.

neúmyslné. Útočníci z této skupiny se vyznačují omezenými znalostmi a prostředky. K ochraně před těmito škůdci stačí zejména slabá a nenáročná protiopatření. ***Hackeři***, jak už bylo řečeno v předchozím odstavci, se snaží svými útoky dokázat svoje schopnosti nabouráváním se do systému. Útoky hackerů jsou klasifikovány jako střední hrozba a tudíž na jejich odražení stačí ochrana a opatření střední úrovně. Jedná se o běžné útoky na data. ***Profesionálové*** jsou v podstatě zločinci, který útočí „neomezenými prostředky". Jsou to osoby, které pracují pro mafii, špionážní organizace nebo silné konkurenční podniky. Jejich útoky jsou velmi silné z hlediska jejich zkušeností a znalostí. Jsou to vlastně počítačoví zločinci z řad počítačových profesionálních znalců. Charakterizují se neomezenými znalostmi, finančními prostředky a časem. Proti jejich útokům se přijímají velice silná protiopatření, jelikož jejich nabourávání se do systémů se vymyká běžným způsobům.[66]

Viry a škodlivé kódy jsou programy, které se do počítače dostávají skrze přenosná zařízení, elektronickou poštu či internet. Běží na pozadí, tedy uživatel o nich v mnoha případech vůbec neví. Jednou z dalších charakteristik je jich množení. Pokud se dostanou do počítače, dokáží pak následně migrovat na zařízení, která se k danému počítači připojí, nebo útočí jen na další programy v infikovaném počítači. Jejich hlavním cílem je napadení co největšího množství programů a dat a provádět na nich záškodnické činnosti. V lepších případech jsou škodlivé kódy vytvořeny pouze k žertu a napálení uživatele infikovaného zařízení. Však i tato akce je velice nežádoucí z hlediska nabourání osobního pohodlí či ohrožení rozpracovaných dat. Virus, který se infiltruje do programu, se snaží změnit sled instrukcí tak, aby se do něj mohl začlenit a s programem pracovat. Některé viry se mohou projevit až po dlouhé době po proniknutí do systému.[67]

Spam je název pro nevyžádanou elektronickou poštu, která je většinou reklamního charakteru. Spam jako takový není nebezpečný, ale jeho frekvence zatěžuje komunikační přenosy a výpočetní techniku. Nehledě na to, že velice obtěžuje uživatele, jež musí neustále mazat hromady reklamních e-mailů, které se jen těžko blokují. Jde tedy o zneužití digitální komunikace, která je využívaná k nevyžádané reklamě na mnohdy velice pochybné produkty. Nejde však jen o nabídku produktů, ale jedná se i o různé fiktivní příležitosti k rychlému zbohatnutí, šíření pornografických stránek nebo zprávy typu „pošli dál, jinak budeš mít X let smůlu". Výhoda pro spammera je zřejmá a

[66] POŽÁR, J. *Základy teorie informační bezpečnosti.* Praha, 2007. s. 40-41.
[67] POŽÁR, J. *Informační bezpečnost*. Plzeň, 2005. s. 215.

tou je šíření reklamy bez jakýchkoliv nákladů. Další z výhod pro něj činí skrytí identity, jelikož falšování hlavičky e-mailu, je velice jednoduchou záležitostí.[68] Spam jako takový má mnoho škodlivých okolností pro uživatele, který musí řešit nejčastěji tyto problémy:[69]

- Mazat došlý spam a zbytečně dlouho vyčkávat na stažení nové došlé pošty, se kterou přichází i mnoho dalšího spamu
- musí neustále rozlišovat v poště co je a co není spam
- v hromadách nevyžádané pošty může dojít k přehlédnutí důležitého e-mailu
- neustálé upozorňování na nově došlou poštu
- velké zatížení serveru a počítačových linek
- pokud je zapnuta automatická detekce spamu, může lehce dojít k omylu při vyhodnocování
- dochází ke zpožďováním e-mailů, které jsou pozastavovány kvůli antispamové kontrole.

Spyware, charakterizován jako program, který krade data z infikovaného zařízení a odesílá je na předem určené úložiště, aby mohlo dojít k následnému přečtení od útočníka. Spyware pracuje na pozadí počítače a tedy bez vědomí uživatele. Tento škodlivý program se do zařízení většinou dostává skrze stažené free (volně stažitelné) nebo shareware (zkušební verze) programu. Pokud dojde k instalaci zmíněných aplikací, spyware se nainstaluje spolu se staženým programem. Bez detailnější analýzy nejde tento škodlivý kód objevit.[70] Je využíván hlavně na sledování uživatele a jeho zvyklostí vyhledávání na internetu. Tyto údaje jsou pak využívány hlavně k marketingové činnosti. Antivirové programy jsou většinou proti spywaru bezbranné a proto k ochraně před jejich účinky vznikly programy nazývané antispyware.[71] Úspěšným útokem spyware může ze zařízení dostat data, jako jsou:[72]

- IP adresu nakaženého zařízení
- údaje o připojení, tedy jaký poskytovatel zaštiťuje internetové připojení a dle toho lze zjistit zemi, ve které se uživatel nachází

[68] POŽÁR, J. *Informační bezpečnost*. Plzeň, 2005. s. 240-242.
[69] HUB, M. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice, 2013. s. 32.
[70] POŽÁR, J. *Informační bezpečnost*. Plzeň, 2005. s. 247.
[71] HUB, M. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice, 2013. s. 34.
[72] POŽÁR, J. *Informační bezpečnost*. Plzeň, 2005. s. 247-248.

- seznam programů, které se nacházejí v počítači
- veškerá aktivita, kterou uživatel na internetu provádí, (navštívené stránky, záznamy stahování, otevřené reklamy atd.)
- může také stahovat obrazy pořízené z aktuálního stavu obrazovky.

4.2 Útoky a útočníci

Ze studií útoků na data vychází, že nejslabším článkem v ochraně dat a informací je lidský faktor. Zejména se jedná o nespokojené zaměstnance, kteří vynášejí data konkurenčním firmám za účelem vlastního obohacení. Jde však také například o pouhou pomstychtivost nebo zlobu vůči firmě. Riziko úniku dat se zvyšuje s pravomocemi udělenými danému zaměstnanci. Proto často dochází k nekalým praktikám v přetahování zaměstnanců mezi firmami. Stačí si například najít nespokojeného pracovníka u konkurenční firmy a díky jeho pravomocem se dostat k utajovaným datům. Dalším způsobem je nastrčit špióna, který se k firmě dostane zejména na základě podvodného výběrového řízení. Kvůli těmto případům si firmy na příjem zaměstnanců do důležitých pozic dávají velký pozor. Zejména si dávají pozor, zda zájemce nepracoval pro konkurenční firmu, nebo jestli nepracuje někdo z jeho příbuzných. Informace také mohou unikat na základě neopatrnosti či pouhé nevědomosti. Jedná se například o dokumenty v tištěné formě, které jsou jen tak položeny na stole, či bez skartace vyhozeny do koše. Může také jít o poznámky, které si zaměstnanec pořídí a neomaleně je nechá na očích neoprávněných osob, které mohou kolem jeho pracoviště procházet. Dalším způsobem úniku dat je například pouhá nevědomost, že i pokud je disketa či DVD v zařízení nečitelná, i tak se z daných přenosných prvků dají data získat. Proto je zaměstnanec odloží či jen tak vyhodí do koše s vědomím, že médium je dále nepoužitelné.[73]

Útoky na systémy za účelem získání dat mohou mít různé důvody. Dokonce i v kriminalistice se informatika hojně využívá. Jelikož je potřeba data shromažďovat a z různých míst k nim znovu přistupovat. Může se jednat o systémy k evidenci hledaných osob, či provozovaných automobilů. Odcizení těchto dat by tedy mohlo mít fatální důsledky pro společnost. Díky těmto evidencím se dá o člověku zjistit první poslední.[74]

[73] KALAMÁR, Š., POŽÁR, J. *Vybrané aspekty informační bezpečnosti*. Praha, 2010. s. 33-34.
[74] STRAUS, J. a kolektiv. *Kriminalistická taktika*. Plzeň, 2008. s. 267-280.

Samotní útočníci se pak dělí do skupin podle útoků, které provádějí a také podle míst, z kterých je útok veden. O hackerech, crackerech, profesionálech atd., bylo řečeno již v úvodu této kapitoly. Proto zde bude rozebráno dělení z hlediska polohy útočníka.[75]

Vnitřní útočník je osoba, která útočí ze sítě organizace. Většinou jde o samotného zaměstnance dané firmy či organizace. Buďto se jedná o osobu, která je k činu donucena, nebo se jedná o nespokojeného zaměstnance, který chce firmě škodit. Bohužel většina vnitřních útoků je zapříčiněna špatnou kvalifikací pracovníků. Tím tedy dochází k nechtěnému smazání souboru, který nebyl zálohován a dochází tedy k nenávratným škodám, nebo k nákladné obnově smazaných dat. Ochrana před útoky z vnitřku organizace leží v rukách bezpečnostního managementu firmy. Jejich úkolem je zvyšovat loajalitu zaměstnanců k jejich zaměstnavateli a školit pracovníky, aby byli dostatečně kvalifikováni a nedocházelo tak k nechtěným zničením dat.

Vnějším útočníkem je ten, který nemá přístup z vnitřku firmy, ale musí prolomit zabezpečovací ochrany a programy, které chrání vnitřní sít organizace před vnějším vniknutím. O tuto ochranu se stará správce sítě, který udržuje v provozu a aktualizaci ochranné programy, kterými jsou například firewally či zabezpečovací protokoly, bránící komunikační kanály. Jednou z výhod vyplývajících z útoku z vnějšku, je potencionální nepostihnutelnost útočníka. Jelikož taková osoba může být kdekoliv na zeměkouli, je její stíhání velice náročné a těžko prosaditelné. Útočníci mají ještě jednu výhodou a tou je skrytá identita. Osoba tedy může do systému vniknout, nebo se pokusit o útok, aniž by kdokoliv zjistil, o koho se jedná.

4.3 Útoky proti celistvosti dat

Útoky na data, která jsou prezentována v elektronické podobě, mohou přijít z různých oblastí internetu či programu. Jednou z možností, kterou lze zaútočit jsou takzvaná **zadní vrátka (trapdoors)**. Jde o softwarový kód či hardwarové zařízení, jež může být zneužito k útoku na systém. Zadní vrátka se tomuto vstupu říká proto, že většinou vzniká úmyslným vytvořením tvůrce programu. Ten vytvoří tento tajný vstup za účelem pozdějšího získávání dat, či převzetím vlády nad programem. Ve většině případů jsou však zadní vrátka vytvářena za účelem snazšího ladění programu při vývoji. V tom případě musí být po dokončení práce na programu tyto vstupy ošetřeny a uzavřeny, aby nedocházelo k pozdějšímu narušování funkčnosti. Trapdoor lze také

[75] KALAMÁR, Š., POŽÁR, J. *Vybrané aspekty informační bezpečnosti*. Praha, 2010. s. 35-36.

charakterizovat jako příkaz, který je vložen do kódu programu, který vykonává některé jinak nevyvolatelné operace. Jedná se například o přístup k jiným zařízením, které se nacházejí v síti a ke kterým ve finále budou mít přístup vyšší autority. Aby tedy vývojář mohl tuto skutečnost ladit a zkoušet, daným kódem se k přístupu dostane. Může se ale také jednat o chybně ošetřené vstupy do programu, díky kterým lze za použití vstupní syntaxe do programu vniknout.[76]

Trojský kůň neboli (trojan horse) je program, který vykonává určité funkce útoku. Mimo jiné však ještě ukrývá funkce, jež se aktivují po splnění zadané podmínky. Jedná se zejména o mazání dat a souborů, formátování zařízení či se může jedna o nevinné akce. Trojský kůň může také zjišťovat informace o programech, které uživatel používá a zasílat je jejich tvůrcům. Nebo se jedná o monitorování aktivity a pak na základě získaných poznatků uživatele zahlcuje reklamou. Nalezení tohoto viru v kódu, který má miliony řádků je vcelku obtížné. K tomu má trojský kůň tu vlastnost, že se do kódu může zařadit až po otestování a zařazení do provozu.[77]

Salámový útok (salami attack) je technika, která se používá zejména k podvodům ve finančním sektoru. Jednou z vlastností této techniky je například to, že zneužívá chyb a číselných zbytků, které vznikají při zaokrouhlování čísel a jsou na hranici přesnosti počítače. Tato technika je funkční za podmínky velkého množství operací. Program převádí na útočníkovo konto tyto chyby vzniklé při zaokrouhlování, například při výpočtu úroků. Způsob tohoto útoku je velice špatně zjistitelný, protože nečiní velké škody a tak je jeho odhalení spíše zásluhou náhody.[78]

Skryté kanály (covert channels) vznikají zejména za pomoci programátorů. Ti tyto kanály vytvářejí proto, aby mohli přistupovat ke zpracovaným datům po ukončení vývoje programu. Díky tomu je umožněna nepovolená komunikace mezi procesy operačního systému a je otevřena jakási cesta k úniku dat a informací. Skryté kanály, ale mohou také vznikat na základě chyby v systému, nebo díky trojskému koni, který může vytvořit kanál ke skryté špionáži. Jelikož skrze tento způsob útok se přenášejí spíše menší množství dat, je zjištění aktivity toho škůdce velice náročné.[79]

[76] POŽÁR, J. *Základy teorie informační bezpečnosti.* Praha, 2007. s. 44-45.
[77] POŽÁR, J. *Základy teorie informační bezpečnosti.* Praha, 2007. s. 45.
[78] POŽÁR, J. *Základy teorie informační bezpečnosti.* Praha, 2007. s. 46.
[79] POŽÁR, J. *Základy teorie informační bezpečnosti.* Praha, 2007. s. 46.

Hladové programy (greedy programs) jsou programy, které zaberou svou činností velkou část operačního výkonu počítače či systému. Může se jednat o případy, kdy program vykonává zdlouhavé a složité výpočty, které následně zatěžují operační paměť počítače. Tím dochází ke zpomalení jiných operací a k celkovému poklesu výkonu zařízení. Může tedy docházet ke kolabování a zahlcování. Dalším znakem hladového programu je odvozování spuštěných programů. Díky tomuto jevu může nastat chyba celého programu. Dochází také k nekonečné smyčce, tedy k tomu, že spuštěné aplikace běží stále a stále v neukončitelném cyklu.

Červi neboli worms, mají s virem mnoho společného. Jedna z věcí, která je však odlišuje, je skutečnost, že vir běží na pozadí zařízení a způsobuje v něm nějakou škodu. Kdežto červ je síťovým dvojčetem viru. Tento způsob nákazy má schopnost šířit se skrze komunikační kanály z jednoho zařízení na druhé. Problémy, které červ může způsobit, jsou totožné s možnostmi viru. Rozdíl je v tom, že worm je mnohem rychleji šiřitelný a tedy díky internetu je jeho expanze vypočtena v řádech minut. Jeho dopady jsou tímto mnohem závažnější a větší než u virů. "Škody, které způsobily virové nákazy, se pouze odhadují. Např. v roce 1998 – 6 mld. US dolarů, v roce 1999 – více jak 12 mld. dolarů, v roce 2000 – asi 17 mld. dolarů, v roce 2001 – odhad na více než 17 mld. dolarů." [80] To je důkazem jejich vysoké úrovně nebezpečí a vzniká tedy potřeba se před tímto druhem nákazy kvalitně chránit. Jednou z obran je kvalitní péče o programové vybavení.[81]

4.4 Útoky na kryptografické algoritmy

Kryptoanalýza je oborem, který se zabývá luštěním zašifrovaných textů. Kryptoanalytik je zase osoba, jež se pokouší o prolomení šifry či šifrovaného textu. Cílem takovéhoto luštitele je získat text, který je zašifrovaný, nebo zjistit šifrovací klíč. Nejlepším stavem jakého může kryptoanalytik dosáhnout, je získání či vymyšlení algoritmu, který dokáže dešifrovat text bez znalosti klíče, nebo dokáže získat klíč, který bude platit ve všech případech šifrování.[82] Pokud luštitel alespoň přibližně ví, v jakém jazyce je šifrovaný text, nebo pokud se jedná například o nějaký text písně, dokáže

[80] POŽÁR, J. *Základy teorie informační bezpečnosti.* Praha, 2007. s. 47.
[81] POŽÁR, J. *Základy teorie informační bezpečnosti.* Praha, 2007. s. 47.
[82] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 31.

skrze programy, které určí četnost slov či písmen v daném textu, rozluštit šifru dle získaných statistik.[83]

1) Útok hrubou silou

K tomuto útoku je zapotřebí dostatečně výkonného výpočetního systému, který dovolí rozluštit skrytý text. Jedná se o nejzákladnější dešifrovací systém, který zkouší všechny kombinace klíče. Metoda však ztrácí na efektivitě ve chvíli, kdy šifrovací klíč je dlouhý. Proto existuje pravidlo, že klíč musí být tak dlouhý, aby útok hrubou silou zabral delší dobu, než která je potřeba k utajení informace.[84]

- 56 bitů dlouhý klíč zajistí utajení v řádech hodin a je vhodný pro kódování rychlé komunikace.
- 56 – 64 bitový klíč slouží k utajení obchodních informací, které potřebují zabezpečit informace v řádech týdnů.
- 64 bitů stačí pro průmyslový sektor, kde ochrana průmyslových tajemství je chráněna v řádech let.
- 128 bitů slouží k ochraně diplomatických informací a dat, jelikož zde se informace utajují až stovky let.

Zastavení luštícího programu probíhá na základě hledání kontrolního součtu. Tedy vyzkoušíme klíč na základě kontrolního součtu s otevřeným textem, a pokud součet souhlasí, nalezli jsme daný klíč. Ve většině případů otevřeného textu však kontrolní součet neobsahuje a tak je potřeba postupovat podle jiné metody a tou je vyhledávání známých slov. Hledají se smysluplná slova, která se vyskytují ve většině textů.[85]

2) Luštění se znalostí šifrovaného textu

Pokud má útočník k dispozici několikero zašifrovaných zpráv, které jsou šifrované stejným algoritmem a stejným klíčem, pak lze takovýto text rozluštit. Pokud jsou odchycené zprávy zašifrované pomocí jednoho stejného klíče, lze ho na základě

[83] KALAMÁR, Š., POŽÁR, J. *Vybrané aspekty informační bezpečnosti*. Praha, 2010. s. 47.
[84] KALAMÁR, Š., POŽÁR, J. *Vybrané aspekty informační bezpečnosti*. Praha, 2010. s. 48.
[85] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 31-32.

analýzy zjistit. Dále už je luštění zpráv velice jednoduché a umožňuje čtení dalších a dalších zpráv.[86]

3) Luštění se znalostí otevřeného textu

Útočník má v tomto případě k dispozici šifrované zprávy, ale také otevřené texty těchto zpráv. Pak už je jen jeho dalším krokem hledání klíče a to se považuje již za snadnou cestu k získání informací. Lze použít například metodu porovnávání otevřeného textu se šifrovanou zprávou, kde se na základě rozdílů v algoritmu snažíme najít hledaný klíč.[87]

4) Luštění se znalostí vybraných otevřených textů

Analytik si vybere nějaký otevřený text a ten zašifruje. Má tedy k dispozici otevřený text a jeho zašifrovanou podobu. Díky této metodě dokáže získat informace o klíči, na základě porovnávání textu šifrovaného a otevřeného.[88]

5) Luštění se znalostí vybraných šifrovaných textů

Takovýto druh luštění není zcela typický. Jedná se o případ, kdy luštitel vlastní zašifrovaný text a má přístup k dešifrovacímu zařízení. Dokáže si tedy přečíst jakýkoliv získaný zašifrovaný text, ale nemůže otevřený text dostat do podoby zašifrovaného textu skrze dané zařízení.[89]

6) Luštění pomocí kompromitace uživatelů

Tato metoda je založena na základě získání klíče od uživatele. Jedná se zejména o korupční či přesvědčovací metodu, kdy je uživateli nabídnuta například finanční částka, nebo je klíč získán na základě vydírání, mučení a jiných nekalých metod. Někdy tento způsob bývá tou poslední možností, jak prolomit šifru. Tato metoda je považována za velice efektivní a někdy za nejméně náročnou.[90]

7) Frekvenční kryptoanalýza

Metoda, jež je závislá na daném jazyku. Základem je tudíž zjistit, v jakém jazyce se šifrovaný text nachází. Poté dochází k analýze četnosti písmen. Jde tedy o to, že

[86] KALAMÁR, Š., POŽÁR, J. *Vybrané aspekty informační bezpečnosti*. Praha, 2010. s. 48.
[87] POŽÁR, J. *Základy teorie informační bezpečnosti.* Praha, 2007. s. 53.
[88] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 32.
[89] POŽÁR, J. *Informační bezpečnost*. Plzeň, 2005. s. 196.
[90] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 33.

v různých jazycích je různý výskyt konkrétních písmen. V českém jazyce se například písmeno E vyskytuje mnohem častěji než písmeno W. Hlavním úkolem je zjistit frekvenci písmen v daném jazyce a poté porovnat se zašifrovaným textem. Tato metoda se nejvíce používá na prolomení Caesarovi šifry, kdy je díky tomu snadné zjistit posun abecedy, který byl k zašifrování zprávy použit.[91]

4.5 Útoky na autentizační zabezpečení

Autentizace jako taková, musí být před spuštěním dobře otestována a detailně prozkoumána. Hlavně z hlediska útoků, které můžou autentizační protokoly postihnout. Tímto úkolem se zabývá návrhář protokolu, jehož úkolem je bezpečné fungování. Útoky na autentizační protokoly se řadí do skupin, dle jejich provedení:[92]

Opakování neboli replay attack je útok, jenž využívá principu odposlechu nějaké části komunikace, která probíhá mezi dvěma stranami. Mezi těmito stranami právě probíhá proces autentizace a útočník se snaží odposlechnout část, nebo nejlépe celou zprávu. Tato zpráva obsahuje autentizační heslo, nebo pokud se podaří odposlech celé relace, která je následně opětovně vyslána, dojde k odcizení celé relace. Odposlech se jeví jako velice nebezpečný útok. Jeho hlavní výhodou je složité zjištění a poměrně jednoduché provedení. Data, která se dostanou na internet a putují tedy po nezabezpečených cestách (kanálech), se dají skrze zařízení třetí strany, dobře odposlouchávat. Protože pokud data procházejí přes směrovač, může dojít k odposlechu daného směrovače, který právě vlastní třetí strana.

Útok **ze středu**, nebo také zrcadlový útok, je založen na principu vniknutí, které je vedeno na obě komunikační strany. Útočník tak získává pod kontrolu celou komunikaci. Jsou odposlouchávány obě strany a je postupně navazováno spojení s oběma z nich. Jde tedy o to, že se útočník chová jako strana A a odpovídá straně B a naopak.

Jedním z dalších útoků na autentizační protokol, je **útok skrze heslo**. Tento druh útoku se neřadí vyloženě mezi autentizační útoky, jelikož jeho obsahem je získání uživatelova hesla. Takováto krádež hesla může proběhnout například na základě zcizení po síti, kdy heslo putuje k verifikaci na daný server. Velkou motivací k útoku jsou velká databázová úložiště, kde se shromažďují veškeré přístupové kódy. Jelikož je výpočetní

[91] HUB, M. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice, 2013. s. 50.
[92] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno, 2004. s. 69-71.

technika stále v rozvoji a každou chvíli vznikají výkonnější a výkonnější zařízení, dostává se do popředí i možnost získání přístupového kódu na základě útoku hrubé síly. Tedy že dojde k vyzkoušení veškerých kombinací hesel.

4.6 Hacking skrze webové prostředí

Webového klienta lze brát jako pouhou zobrazovací jednotku, která vyvolá určitý obraz dle našeho zadaného požadavku. Vizuální reprezentace je zastoupena HTML jazykem, jež je určen k zobrazování statického pohledu na vyvolanou webovou stránku. Takovéto řešení však po čase začalo zaostávat za rychle se vyvíjející dobou a byl vznesen požadavek na jakýsi aktivní obsah na stránce. Tím se myslí přítomnost spustitelných souborů, kterými lze kupříkladu uzpůsobit stránku dle požadavků vstupujícího klienta. Pokud tedy vstoupíme na stránku, dostává se nám dynamického chování zobrazené webové stránky. K tomuto účelu byly vyvinuty různé nástroje. Zde budou uvedeny nejčastěji používané, kterými jsou: [93]

JavaScript je jazyk, jež umožňuje webovým aplikacím spuštění přímo na klientovi. Dává tudíž vývojářům mnoho nových možností, které se dají využít na webových stránkách. Hlavní výhodou JavaScriptu je však jeho bezpečnostní model. Disponuje totiž integrovanou transparentní správou paměti, umožňující absolutní kontrolu nad spouštěním kódu, což napomáhá k zabraňování nežádoucích akcí, které mohou script postihnout. Proto když je na web umístěna aplikace, její narušení je velice obtížné. JavaScript je tedy používán ke spojování komponentů, které se na webu nacházejí a slouží ke zpracování vstupu, jež uživatel zadává. Bohužel se tento nástroj dá využívat i k nekalým praktikám na uživatelích. Jelikož JavaScript má tu schopnost, umožňující běžet na pozadí bez vědomí uživatele, naskýtá se mnoho možností ke zneužití. Pokud uživatel vstoupí na stránky, kde je implementovaný útočný kód, dokáže o uživateli zjistit citlivé informace. Může se jednat o věci jako zjištění poskytovatele internetu, jeho pevné IP adresy a dalších věcí, dle kterých si lze pak dohledat identitu uživatele. Bohužel však umožňuje i závažnější akce, kterými jsou nahlížení do systémových složek, či hledání specifických dat uvnitř uživatelova zařízení. Na takovéto útoky však existují různé obrany, jež poskytují webové prohlížeče, kde se například dají povypínat různá vylepšení stránek. Ukázkové příklady útočení na klienta Internet Explorer 6 se dají naleznout na stránce Internet Explorer Fun Run Page.

[93] SCAMBRAY, J., SHEMA, M. *Hacking bez tajemství: webové aplikace*. Brno, 2003. s. 241-256.

Obdobným nástrojem jsou i takzvané **cookie**. Toto rozšíření HTTP serveru slouží k uchování určitého stavu, který se nezmění při různě probíhajících dotazech a odpovědích mezi protokolem HTTP a klientem. Cookie umožňuje zachování různých stavů. Pokud tedy navštívíme určité webové stránky a provedeme na nich registraci, která nám umožní zvláštní pravomoce či vylepšení, využitelné na serveru, získáváme stav, kdy jsme hodnotným uživatelem webových stránek. Když se po nějakém čase vrátíme na zmiňované stránky, server může uchovat náš stav přihlášení a tudíž ví, kdo jsme a rovnou nám poskytne profil, který jsme si nastavili. Cookies mají dva různé stavy. Buďto se jedná jen o dočasné nastavení určité relace, kdy zavření prohlížeče znamená, že cookies se vymažou a dále nejsou využitelné. Druhým stavem se vyznačují perzistentní cookies, které jsou uložené na pevném disku uživatele a je tedy možné je kdykoliv vyvolat na dotaz HTTP serveru. Tím se nám ukazuje i velká nevýhoda, jelikož stačí, aby došlo k odcizení těchto takzvaných cookies a může dojít ke snadnému odcizení identity vlastníka. Jako ukázkový příklad lze využít program Achilles, jenž umožňuje nahlížení do odesílaných cookies na server. Pokud tedy přejdeme na některé amatérské stránky, či stránky vytvořené ne zrovna znalým vývojářem, lze si povšimnout, že při příchodu na HTTP nám byl skrze cookies udělen ID = USER. Tento fakt znamená, že si o nás nastavení daných stránek myslí, že jsme uživatelem. Díky programu Achilles však můžeme editovat odchozí parametry, které jsou na webu zpracovávány. Není na škodu tedy zkusit přepsat webem přiřazené ID = USER na ID = ADMIN. Je možné, že si vývojář stránek tento vstup ošetřil, ale v mnoha případech jsou to spíše vrátka ke snadnému zneužití.

Google sloužící jako mocný nástroj při vyhledávání veškerých informací na internetu, se ve zkušených rukách stává silným nástrojem k zjišťování či kradení informací. Tento vyhledávací pomocník totiž dokáže najít na internetu úplně vše, ať se jedná o čísla karet, aktivních webkamer či kořenových adresářů. Webové stránky, fungují jako soubor složek, ve kterých jsou například uloženy přílohy, obrázky a jiné. Tyto složky také slouží k omezenému přístupu, tedy do určitých složek webu, mají přístup jen určití či žádní uživatelé. Google však dokáže najít i tyto složky a může dojít k jejich lehkému zneužití. Pokud tedy útočník ví, co hledá, může si to nechat snadno zobrazit. Jak už bylo řečeno, webové stránky mají svůj adresář, ze kterého čerpají své informace, stačí tedy zadat hledaní kořenového adresáře a získáme všechny složky. Pokud tedy do vyhledávače zapíšeme příkaz *intitle:index.of images,* dostane se nám následujícího výsledku. Po projetí veškerých internetových stránek, dostaneme

kořenové adresáře všech, ve kterých se nachází složka *images*. Jako bonus se ještě dostaneme do celého kořenového adresáře dané stránky. Lze se pohybovat po všech složkách, dokonce i v těch, které by měli být přístupné jen samotným administrátorům. Pokud také například někdo neopatrný uloží do dokumentu jako je *word, pdf*, či do složky jako *zip* důležité informace, kupříkladu rozpočet obce, lze tento archiv nebo dokument lehce vysledovat zadáním klíčového dotazu *.doc* do vyhledávače a máme, co potřebujeme. Takovéto hackování je však značně omezené, ale pokud je uživatel dostatečně zkušený, může si řadou cest získat informace, které potřebuje a ty pak zneužít k získání dalších a dalších.[94] Lze uvést tento ukázkový příklad:[95]

Útočník se snaží na internetu nalézt tajné či ukryté složky na webových stránkách. Zadání příkazu *intitle:index.of admin,* kde se snaží najít administrátorskou složku, však nefunguje. Je tedy pravděpodobné, že správce nazval tuto složku jinak kvůli ochraně před tímto vyhledáváním. Útočník však není amatér a ví, že když chce tvůrce stránek ukrýt některé složky, lze použít googlovský trik robots.txt. Vše co se nachází v tomto textovém dokumentu, je na daných stránkách skryto před smysly vyhledávače. Tudíž nám tedy stačí nechat si vyhledat tento textový dokument a rázem máme k dispozici složky, jež měly být ukryty před zraky uživatelů. Pak již stačí standardně vyhledat ony složky.

K ochraně před Googlem slouží různé triky, jako jsou například ukrývání různých částí kódu již při tvorbě, skrze různé skriptovací kódy. Jako ochranu lze také použít pojmenovávání složek tak, aby nikoho nenapadlo takový název vyhledávat a hledat v něm důležité informace anebo si vyjednat vyřazení z google indexu.

[94] BEAVER, K. *Hacking for dummies.* Indianapolis, 2010. s. 277-287.
[95] JOBABROAD. *Průvodce hackováním pomocí Google.* [online]. 2013 [cit. 13. února 2014]. Dostupné na WWW: <http://jobabroad.sweb.cz/google.htm>.

5 Právo v informačních technologiích

Jak tomu již bývá, se vznikem nových technologií, které jsou určené ke zvyšování lidské úrovně, přichází i spousta možností, jak tyto vymoženosti zneužít k trestné činnosti. Proto se vznikem počítačů vznikla i lavina počítačové kriminality. V době, kdy se počítače staly dostupnými i pro obyčejné lidi, vzniká prudký nárůst těchto spotřebičů, jež jdou ruku v ruce s rozvojem počítačových sítí. V tomto bodě byli zákonodárci donuceni k rychlému jednání. První výskyt ustanovení, která mají chránit elektronická data, byla v trestním zákoně zavedena na počátku 90. let. Novým nástrojem na ochranu elektronických dat se tedy stal nový trestní zákoník, *Zákon č. 40/2009 Sb., trestní zákoník*. Mezi nejzajímavější ustanovení patří:[96]

Uvedení někoho v omyl a využití něčího omylu prostřednictvím technického zařízení (Srov. § 120 trestního zákoníku). Zde se pojednává o trestných činech, které jsou vyvolány něčím omylem, nebo využitím takového omylu. Jedná se například o podvody, obchodování s lidmi, poškozování cizích práv. Bylo tedy ujednáno, že tuto trestnou činnost lze vykonávat i skrze počítačové sítě.

Porušení tajemství dopravovaných zpráv (Srov. § 182 trestního zákoníku). Skutková podstata tohoto trestného činu chrání i jiné druhy komunikace a ne jen komunikaci elektronickou. Pachatelem trestného činu je ten, kdo úmyslně porušuje datové tajemství, zasílané pomocí elektronické komunikace, kde je prokazatelná identifikace účastníka či příjemce zprávy. Však pachatelem se stává i osoba, která vyzradí takové tajemství, o němž se dozvěděla prostřednictví takto získané zprávy a obsah zprávy vyzradí za účelem obohacení se či získání jiného prospěchu pro sebe, nebo za účelem způsobení škody druhé straně. V tomto případě může být pachatelem každý, kdo si přečte jakoukoliv zprávu například na cizím e-mailu, či aplikaci sloužící ke komunikaci jako jsou ICQ, Skype a jiné. Jde tedy hlavně o to, zda je z dané zprávy možná identifikace odesílatele a adresáta. V takovémto případě, by asi byla polovina národa již za mřížemi. Proto přísnější tresty jsou vztahovány na pachatele, kteří jsou zaměstnanci nějakého provozovatele telekomunikačních služeb či počítačových systémů.

Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (Srov. § 231 trestního zákoníku). Trestní zákoník

[96] MAISNER, M. *Základy softwarového práva*. Praha, 2011. s. 115-122.

postihuje již přípravu k činům směřujícím k porušení dopravovaných zpráv či neoprávněnému přístupu k počítačovému systému. Nejedná se sice o všechny případy, ale jen o případy, které jsou zvláště závažné a pokud je to zákonem výslovně ustanoveno. Pokud je pachatel těchto trestných činů uznán vinným z dokonání, nelze ho též odsoudit za přípravu k tomuto trestnému činu. Jinak řečeno, nelze uznat souběh těchto trestných činů. Trestný čin lze spáchat vyrobením, dovezením, vyvezením či jiným držením zařízení, které umožňuje neoprávněný přístup.

Dále by bylo také vhodné, přiblížit české právo, které upravuje bezpečnost v prostředí informačních technologiích:[97]

Antispamový zákon by měl být známý každému uživateli e-mailové schránky. Jak už bylo řečeno v předešlých kapitolách, spam je označení pro nevyžádanou poštu, která zaplavuje e-mailové schránky uživatelů. Některé spamy mohou mít obchodně zaměřený obsah, jenž je vztahován na pochybné produkty či ne zrovna legální nabídky na zbohatnutí. Proto v roce 2004 vchází v účinnost zákon *č. 480/2004 Sb*., který se stává antispamovým zákonem, který problematiku spamů upravuje. Tento zákon však není zaměřený pouze na spam samotný. Jeho snahou je regulovat příchozí spam tím, že je povolené ho zasílat pouze s výslovným souhlasem adresáta. Tedy nevyžádaná obchodní sdělení jsou zákonem zakázána. Zákon nezakazuje rozesílání spamu jako takového, ale pouze nevyžádanou obchodní poštu. Taková pošta je definována jako sdělení k přímé či nepřímé podpoře zboží či služeb. Za takovéto obchodní sdělení je považována i reklama. Zákon též vymezuje i co obchodní sdělení není. Pokud tedy právnická či fyzická osoba mění své údaje či sídlo a tuto skutečnost oznamuje svým zákazníkům či klientům, není toto sdělení hodnoceno jako obchodní. Tedy k takovému rozesílání není potřeba souhlasu příjemců.

Jelikož dnes žijeme v době informačních technologií a veškeré údaje o nás a naší osobě jsou shromažďovány po sítích úřadů a zaměstnavatelů, není na škodu znát **zákon o ochraně osobních údajů**. *Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů*, pojednává o tom, co to vlastně osobní údaj je a jak ho lze chápat v právním podání. Osobní údaj je tedy jakákoliv informace, která se týká určitého subjektu. Na základě této informace jde identifikovat přímo či nepřímo daný subjekt. Jedná se například o číslo, kód, nebo určité prvky charakterizující fyzickou,

[97] LUDVÍK, M., ŠTĚDROŇ, B. *Právo v informačních technologiích.* Kralice na Hané, 2008. s. 7-15.

psychickou, ekonomickou nebo sociální identitu. Pokud je tedy osoba v pracovněprávním vztahu, vznikají jeho zaměstnavateli následující povinnosti k ochraně osobních údajů:

- Zaměstnavatel shromažďuje pouze takové údaje, které odpovídají danému účelu, který je nezbytný pro naplnění stanoveného účelu.
- Lze uchovávat osobní údaje jen po dobu nezbytně nutnou. Pokud tato doba uplyne, mohou být údaje uschovány jen pro účely vědecké, nebo pro účely archivnictví. Dále je třeba ochraňovat data před neoprávněným zásahem a údaje prezentovat jen v anonymním podání, jak nejlépe je to možné.
- Osobní údaje lze zpracovávat jen za souhlasu zaměstnance. Pokud nelze využít zákonné výjimky, která dovoluje za určitých pravidel zpracování bez souhlasu zaměstnance.
- Zaměstnavatel je povinen ochránit údaje před neoprávněným přístupem, tedy takovým přístupem, kdy by mohlo dojít ke ztrátě, zničení nebo změně jakýchkoliv chráněných údajů. Tuto povinnost je udělen dodržet i po zpracování daných údajů.

26. července 2004 nabývá účinnosti novela zákona o osobních údajích *č. 439/2004*, která upravuje informační povinnosti správce osobních údajů. Je psáno, že pokud vlastník osobních údajů požádá o informace o svých zpracovaných datech, správce je povinen mu tuto informaci předat.

Know-how, tedy jakýsi soubor poznatků a zkušeností, které slouží k nějaké činnosti. Většinou je know-how charakterizován jako určitý postup k výrobě hmotných věcí a je brán jako nehmotný statek. Know-how jako takové, není zákonem speciálně chráněno. Je tedy na podnikateli, jak ho ochrání. Lze totiž charakterizovat jako obchodní tajemství a tím zajistit zákonnou ochranu, či zajistit ochranu smluvní. Toto však nelze využít v případě, pokud se jedná o postupy, informace či poznatky, které jsou všeobecně známé, jen nebyly doposud využity proto, že nikoho nenapadly.[98]

[98] MAISNER, M. *Základy softwarového práva*. Praha, 2011. s. 138.

6 Splnění cíle práce

Cíl charakteristiky bezpečnosti informací, byl splněn v úvodní kapitole, kdy dochází k objasnění oboru bezpečnosti informací a základních kritérií při jejich tvorbě. Závažnost a dopady zcizování a chránění informací, jsou poukazovány na různých metodách a příkladech, ať se již jedná o kryptologii, či zabezpečovací mechanismy, jak fyzické, tak logické.

Vyhodnocení nejúčinnějších metod ochrany citlivých dat proběhlo na základě dostupných informací z literatury, či internetových zdrojů. Bylo poukázáno na slabá a silná místa těchto metod a proběhlo seznámení s jejich principiálním fungováním. Také bylo poukázáno, jakým směrem se bezpečnost informací posouvá. Tedy z ochrany základních fyzických dokumentů či komponentů, k digitální formě a ukládání dat a informací. Tímto byl zadaný cíl splněn.

Cíl návrhu a možností rozvoje do budoucnosti z hlediska techniky a nových prostředků nebyl možný. Jelikož se již defakto zlepšuje pouze technika a princip ochrany se drží stále stejných pravidel. Jde již tedy pouze o výpočetní náročnost, která je na různé šifrovací algoritmy kladena.

Závěr

Obor bezpečnosti informací je velice obsáhlé a aktuální téma. Je vyžadována hluboká znalost informačních technologií v doprovodu s nejrůznějšími kritérii, kterých je potřeba ke správnému fungování zabezpečovacích mechanismů. Nejedná se tedy jen o směr informačně technologický, ale jsou zde zahrnuty i různé metody fyzických ochran. Nutná je i znalost trestního práva a prevence proti kriminalitě. V práci jsou shrnuty informace, které byly získány z dostupných literárních a internetových zdrojů. Dotazník, jakožto zdroj výsledků získaných pomocí analýzy nebyl v práci zahrnut, kvůli odborné náročnosti. Z hlediska složitosti tématu by tedy dotazník nebyl efektivním zdrojem informací a bylo tedy využito pouze rozboru literárních zdrojů.

Teoretická část bakalářské práce uvádí historický vývoj bezpečnosti informací, jelikož je to poměrně mladá disciplína, je zacházeno do hlubšího rozboru. Je zde hlavně poukazováno na změny ve vývoji kritérií bezpečnosti informací a hlavně v jakých zemích se tyto změny vyskytly, či kdo působil jako podnět ke změně. Zaznamenán je počátek vzniku těchto kritérií z roku 1983 v USA, až do roku 2008, kdy byla schválena společná kritéria.

Teoretická část dále pokračuje a zaměřuje se na druhy a možnosti zabezpečovacích systémů. Dochází k detailnímu rozboru oboru kryptologie, kde je poukázáno i na principiální fungování. Tomuto tématu je věnována větší část kapitoly, jelikož pochopení těchto principů, je klíčem k dalšímu porozumění ostatních zabezpečovacích praktik. Další část poukazuje hlavně na softwarové a hardwarové vybavení, o kterém by měl uživatel mít alespoň povrchové znalosti, jelikož podcenění těchto ochran, se může stát fatálním důsledkem ztráty dat, či následně ztráty internetové identity.

Poslední úsek bakalářské práce rozebírá útoky, které mohou být na systémy či jednotlivce vedeny. Cílem bylo hlavně poukázat, jak snadno jde zneužít chyb při podcenění situace, ohledně bezpečnosti dat. V některých případech jsou doplněny i ukázkové příklady, které slouží jako demonstrace závažnosti problému. Byla zvolena hlavně ta témata, které by měl běžný uživatel znát a se kterými přichází do styku, ať v práci, či ve svém volném čase, který může trávit na různých moderních zařízeních, jako jsou počítače, přenosné telefony, tablety a jiné.

Cílem bylo hlavně seznámení s oborem bezpečnosti informací a jeho principiálním fungováním. Nebylo zacházeno příliš do hloubky, kvůli znalostní náročnosti. Hlavní důraz byl kladen na celkové pochopení, jak data fungují a jak je lze ochránit bez vysoké IT znalosti. Proto se v práci nevyskytují zdrojové kódy a tudíž vysvětlení bezpečnostních prvků a útoků je pouze teoretické. Další vývoj tohoto oboru se dá očekávat již jen ve zkvalitňování hardwarové techniky. Používá se stále stejných algoritmů, na které je kladen větší a větší výpočetní nárok. Uživatel může svá data uchovávat v bezpečí díky uvedeným softwarovým programům, jakožto i firmy, které používají různé kombinace zabezpečovacích prvků. Jde tedy hlavně o nepodcenění jakékoliv situace a udržování svých zabezpečení ve stále aktuálním stavu.

Seznam zkratek

CD - Compact Disc

DVD - Digital Versatile Disc

PC - Personal Computer

ICQ - I Seek You

USB – Universal Serial Bus

WWW - World Wide Web

HTTP – Hypertext Transfer Protocol

FTP – File Transfer Protocol

ID – Identification

Bit – Binary Digit

TCP – Transmission Control Protocol

IP – Internet Protocol

CPTED - Crime Prevention Trough Enviromental Design

UPS – Uninterruptible Power Supply

ISO – International Organization for Standardization

AES – Advanced Encryption Standard

DES – Data Encryption Standard

IT – Informační technologie

Použité zdroje

Literární zdroje:

1. DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* 1. vy. Brno: Computer Press, 2004. 186 s. ISBN 80-251-0106-1.
2. DOUCEK, P., NOVÁK, L., SVATÁ, V. *Řízení bezpečnosti informací*. 1. vyd. Praha: Professional publishing, 2008. 239 s. ISBN 978-80-86946-88-7.
3. HUB, M. *Bezpečnost a ochrana informací v prostředí internetu.* 1. vyd. Pardubice: Univerzita Pardubice, 2013. 89 s. ISBN 978-80-7395-701-8.
4. KALAMÁR, Š., POŽÁR, J. *Vybrané aspekty informační bezpečnosti*. Praha: Policejní akademie České republiky, 2010. 192 s. ISBN 978-80-7251-339-0.
5. KURTZ, G., McCLURE, S., SCAMBRAY, J. *Hacking bez záhad*. Praha: Grada Publishing, 2007. 520 s. ISBN 978-80-247-1502-5.
6. LUDVÍK, M., ŠTĚDROŇ, B. *Právo v informačních technologiích.* Kralice na Hané: Computer Media, 2008. 132 s. ISBN 978-80-86686-36-3.
7. MAISNER, M. *Základy softwarového práva.* Praha: Wolters Kluwer Česká republika, 2011. 339 s. ISBN 978-80-7357-638-7.
8. NORTHCUTT, S., ZELTSER, L., et al. *Bezpečnost počítačových sítí*. Brno: CP Books, 2005. 589 s. ISBN 80-251-0697-7.
9. PETERKA, J. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. 430 s. ISBN 978-80-904248-3-8.
10. PORADA, V. a kolektiv. *Kriminalistika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2007. 309 s. ISBN 978-80-7380-038-3.
11. PORADA, V., HOLCR, K. a kolektiv. *Policejní vědy.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011. 345 s. ISBN 978-80-7380-314-8.
12. POŽÁR, J. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. 311 s. ISBN 80-86898-38-5.
13. POŽÁR, J. *Základy teorie informační bezpečnosti.* Praha: Policejní akademie České republiky, 2007. 219 s. ISBN 978-80-7251-250-8.
14. SCAMBRAY, J., SHEMA, M. *Hacking bez tajemství: webové aplikace*. Brno: Computer Press, 2003. 328 s. ISBN 80-7226-769-8.

15. STRAUS, J. a kolektiv. *Kriminalistická taktika*. 2. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2008. 291 s. ISBN 978-80-7380-095-6.

Zahraniční literatura:

1. BEAVER, K. *Hacking for dummies*. Indianapolis: Johny Wiley & Sons, 2013. 390 s. ISBN 978-0-470-55093-9.

Elektronické zdroje:

1. JOBABROAD. *Průvodce hackováním pomocí Google*. [online]. 2013 [cit. 13. února 2014]. Dostupné na WWW: <http://jobabroad.sweb.cz/google.htm>.