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

BAKALÁŘSKÁ PRÁCE

POČÍTAČOVÁ BEZPEČNOST

Autor práce: Michal Kobrle

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Prezenční

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2016

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v této práci.

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 vedoucí bakalářské práce RNDr. Růženě Ferebauerové za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

Kobrle, M. *Počítačová bezpečnost : bakalářská práce*. České Budějovice: Vysoká škola evropských a regionálních studií, o. p. s., 2016. 61s. Vedoucí bakalářské práce : RNDr. Růžena Ferebauerová.

Klíčová slova: počítačová bezpečnost, informační bezpečnost, ochrana informací, počítačové a informační hrozby, bezpečnostní opatření, kybernetické hrozby.

Bakalářská práce vysvětluje základní pojmy a termíny týkající se počítačové a informační bezpečnosti. Dále se práce zaměřuje na bezpečnostní hrozby, charakteristiku jejich vlastností, dopady a opatření pro zvýšení bezpečnosti. Práce také popisuje hrozby v kyberprostoru, s hlavním zaměřením na kybernetickou kriminalitu a její popis, pomocí legislativních dokumentů. Dále je práce zaměřena na nejčastější typy protiprávního jednání v kyberprostoru. Jednotlivá nelegální jednání jsou analyzována pomocí legislativních dokumentů. V poslední části práce jsou porovnány nejčastější typy incidentů, které byly v letech 2013 - 2015 řešeny pracovníky Národního centra kybernetické bezpečnosti ČR.

ABSTRACT

Kobrle, M. *Computer Security: Bachelor thesis.* České Budějovice: The College of European and Regional Studies, 2016. 61s. Supervisor : RNDr. Růžena Ferebauerová.

Key words: computer security, information security, information protection, computer and Information threats, security measure, cybernetic threats.

The bachelor thesis explains the basic concepts and terms related to computer and information security. The thesis also deals with the security threats, characterization of their features, impacts and measures to increase safety. The thesis also describes threats in cyberspace with main focus on cyber crime and its description by using legislative documents. The thesis is also focuses on the most common types of wrongful conduct. Individual wrongful conduct are analyzed by legislative documents. In the last part of thesis are compared the most common types of incidents that were solved by employees of National Cyber Security Centre of the Czech Republic in 2013 - 2015.

Obsah

Úvod

Svět informačních technologií a především internetu se stále vyvíjí a zdokonaluje neskutečně rychle. To vede ke stále větší nutnosti ochrany dat a informací. Informační technologie a především internetové sítě se staly součástí běžného života a jsou na nich závislé prakticky všechny obory. Bohužel mnoho uživatelů stále podceňuje zabezpečení počítačů a vystavuje je tak různým nebezpečím. Počítačová a informační bezpečnost je díky zvyšujícímu se využívání těchto technologií velmi důležitá, je nutné brát na vědomí bezpečnostní rizika, která mohou nastat, a nebrat je na lehkou váhu.

Při ochraně dat a informací je potřeba definovat mnohem více hrozeb, jako různé poruchy, výpadky sítě, hrozby z kyberprostoru, neoprávněný přístup a zneužívání důležitých informací. Využívání informačních technologií vyžaduje, aby nedocházelo k chybám nebo ztrátám důležitých dat při přenosu, ukládání a opětovném využívání dat.

Informační zabezpečení vyžaduje spoustu opatření, různých technik, přístupů a metod, neboť data a informace je třeba chránit nejen proti neúmyslnému narušení, nedbalosti, selhání techniky, živelným pohromám, chybám programů nebo škodlivému softwaru, ale také proti úmyslnému narušení, nelegálním aktivitám a kybernetickým hrozbám. K dosáhnutí určité míry bezpečnosti je zapotřebí stanovit specifická opatření, která je nutné zavést do praxe.

1 Cíl a metodika bakalářské práce

Hlavní cíl bakalářské práce je zaměřen na definici pojmu počítačové a informační bezpečnosti, popsání bezpečnostních hrozeb a opatření, která by vedla ke zvýšení bezpečnosti nebo alespoň ke snížení následků, a to jak proti neúmyslnému, tak proti úmyslnému narušení.

V rámci vedlejšího cíle jsou popsány hrozby v kyberprostoru, kde se autor zaměřil především na kybernetickou kriminalitu, kterou definoval z velké části pomocí legislativních dokumentů. Dále se autor zaměřil na nejčastěji páchanou nelegální činnost v souvislosti s počítačovou a informační bezpečností. Jednotlivé druhy nelegální činnosti jsou také popsány pomocí legislativních dokumentů, kde se autor pokusil co nejlépe popsat u jednotlivých jednání zda jsou v rozporu se zákonem a zda se jedná o trestný čin.

Informace a podklady pro tuto bakalářskou autor čerpal z knižních a internetových zdrojů. Z těchto zdrojů jsou čerpány informace především pro definici počítačové a informační bezpečnosti, bezpečnostních hrozeb a škod, které způsobují. Dále tato práce vycházela z legislativních dokumentů pro popis kybernetické kriminality a nelegálních činností. Autor pro řešení kapitol bakalářské práce využíval metod analýzy, komparace a rešerše.

Bakalářská práce je strukturována do devíti základních kapitol. První kapitola definuje cíle a metodiku bakalářské práce. Ve druhé a třetí kapitole jsou popsány pojmy týkající se počítačové a informační bezpečnosti.

Čtvrtá a pátá kapitola se věnuje hrozbám a rizikům v informační bezpečnosti. Popsány jsou hrozby přírodního původu, technického selhání, škodlivého softwaru, ale i úmyslné a neúmyslné hrozby plynoucí z lidského faktoru. V šesté kapitole poté autor vybral a popsal nejčastější opatření pro zvýšení bezpečnosti.

Sedmá a osmá kapitola je zaměřená na hrozby a typy protiprávního jednání v kyberprostoru. Tyto kapitoly jsou zaměřeny především na kybernetickou kriminalitu a její popis pomocí legislativních dokumentů. V deváté kapitole jsou porovnány nejčastější typy útoků v ČR v letech 2013 - 2015 pomocí grafů a měsíčních výpisů bezpečnostních incidentů Národního centra kybernetické bezpečnosti ČR.

2 Počítačová bezpečnost

Počítačová bezpečnost nebo též **ICT bezpečnost** (anglicky **computer security**, **IT security**, **ICT security**, **cyber security**) je součást informační bezpečnosti a zabývá se tou částí bezpečnosti, která souvisí s informačními a komunikačními technologiemi. Do **počítačové bezpečnosti** patří síťová bezpečnost, internetová bezpečnost, bezpečnost koncových zařízení, kryptografie (PKI a certifikační autority, e-podpis, e-archivace), speciální prostředky (odposlech, sledování).[1]

Počítačová bezpečnost se postupem času stává problémem, který je nucen řešit stále větší počet uživatelů. Zatímco dříve se tento problém příliš neřešil nebo byl doménou odborníků, dnes se těmito problémy musí zabývat i koncový uživatel.[2]

Cílem počítačové bezpečnosti je předcházet počítačovým útokům a zajistit bezpečný provoz a tedy omezit pravděpodobnost výskytu rizik. Počítačová bezpečnost se týká návrhu pracovních postupů od základu tak, aby splňovali požadavky na bezpečnost tzv. **Secure by Design**, dále **prevence bezpečnosti**, **detekce útoků a hrozeb** a následná **náprava škod** (disaster recovery).[3]

2.1 Počítačová bezpečnost v praxi

Počítačová bezpečnost se týká jak koncových zařízení, (osobní počítače, mobilní zařízení) tak všech ostatních částí IT infrastruktury, zejména **serverů** a **počítačových sítí.** Často spadá do odpovědnosti IT manažera, ve velkých organizacích ve spolupráci s manažerem informační bezpečnosti. V praxi se realizuje použitím **bezpečnostního software**, nebo pomocí různých hardwarových opatření. Na počítačovou bezpečnost má také vliv pravidelná aktualizace **systémového** nebo **aplikačního software** (zejména operačního systému).[4]

[1] Počítačová bezpečnost. *Management mania*. [online]. 12.01.2016 [cit. 2016-02-06]. Dostupné z WWW: <https://managementmania.com/cs/pocitacova-bezpecnost>.
[2] Lukáš Rychnovský. Počítačová bezpečnost. *Zpravodaj ÚVT MU*. [online]. 2005 [cit. 2016-02-07]. Dostupné z WWW:< http://ics.muni.cz/bulletin/articles/342.html >.
[3] Počítačová bezpečnost. *Management mania*. [online]. 12.01.2016 [cit. 2016-02-06]. Dostupné z WWW: <https://managementmania.com/cs/pocitacova-bezpecnost>.
[4] Počítačová bezpečnost. *Management mania*. [online]. 12.01.2016 [cit. 2016-02-06]. Dostupné z WWW: <https://managementmania.com/cs/pocitacova-bezpecnost>.

3 Informační bezpečnost

Informační bezpečnost je souhrnné označení pro aktivity směřující k ochraně informací. Jejím cílem je zejména ochrana informací a dat před negativními událostmi, jako je jejich ztráta, odcizení, únik, zneužití, zničení, narušení či změny, tedy jakékoliv porušení **integrity**, **důvěryhodnosti** nebo **dostupnosti**. Informační bezpečnost je součástí celoorganizačního řízení bezpečnosti. Zahrnuje práci s informacemi jako celek. Její součástí je **počítačová bezpečnost**, která se zabývá bezpečností na úrovni IT technologií.[5] Světlík[6] definuje informační bezpečnost jako: "Vzájemně provázaná opatření organizační, administrativní, personální a fyzické bezpečnosti a opatření bezpečnosti informačních a komunikačních technologií pro zajištění dostupnosti, důvěryhodnosti a integrity informací".

Termín "informační bezpečnost" nahradil v teorii dříve používaný termín "ochrana informací", který je spíše termínem právním vycházející ze zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších změn a doplňků. Tento zákon upravuje zásady pro stanovení informací, jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.[7]

Vacca[8] ve své publikaci uvádí: "Bezpečnost není pouze o hardwaru a softwaru. Mnoho majitelů společností se domnívá, že koupí dostatku vybavení mohou vytvořit bezpečnou infrastrukturu. Firewally, systémy detekce narušení bezpečnosti, antivirové programy jsou jen některé z dostupných nástrojů při ochraně sítě a dat. Žádný produkt ani kombinace produktů nevytvoří bezpečnou společnost sám. Bezpečnost je proces". Bezpečnost se také nedá zúžit pouze na informační systémy nebo informační a komunikační technologie, musí řešit všechny aspekty, včetně organizačních procedur a chování jednotlivců.[9]

---

[5] Informační bezpečnost. *Management mania*. [online]. 09.07.2015 [cit. 2016-02-08]. Dostupné z WWW: <https://managementmania.com/cs/informacni-bezpecnost>.

[6] SVĚTLÍK, M. Informační bezpečnosti: část 1 - 4, *Softwarové noviny*, 2002, č. 2-5, s. 5 - 6. Dostupné z: <http://www.rac.cz/rac/homepage.nsf/CZ/Download/$FILE/inf_bezp.pdf>.

[7] ČESKO. Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších změn a doplňků: In: *Sbírka zákonů, Česká republika*. 2005, částka 143, s. 7526. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=4741>. ISSN 1211-1244.

[8] VACCA, J. R. *Computer and information security handbook*. Second edition. Amsterdam: Morgan Kaufmann, an imprint of Elsevier, 2013. s. 5.

[9] POŽÁR, J. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, s. 17.

Informační systémy jsou používány nejen pro správu informací a práci s nimi, ale i pro řízení a správu jiných systémů. Součástí každého systému není pouze hardware, software a vlastní data, ale i lidé, kteří informační systémy provozují a spravují. Z hlediska bezpečnosti mají informační systémy zajišťovat utajení důležitých dat, jejich dosažitelnost pro autorizované subjekty a jejich integritu. Dalším prvkem bezpečnosti může být třeba nepopiratelnost provedené operace s daty nebo vzniku datové či programové jednotky, její autentičnost nebo pseudonymita či anonymita autora.[10]

Pod pojmem bezpečnost IT obvykle rozumíme ochranu odpovídajících IS a informací, které jsou v nich uchovávány, zpracovávány a přenášeny. Součástí takto obecně chápané bezpečnosti IT je i komunikační bezpečnost (ochrana informace přenášené mezi počítači), fyzická bezpečnost (ochrana před přírodními hrozbami a fyzickými útočníky) a personální bezpečnost (ochrana před vnitřními útočníky).[11]

Důležitost informační bezpečnosti roste zároveň s důležitostí informací. Pokud o ně přijdeme nebo naše klíčové informace získá konkurence, může to také znamenat konec našeho podnikání nebo fungování. Můžeme o ně přijít v místě uložení (na svém počítači, na serveru nebo v šanonu) nebo někde po cestě k nám.[12]

Čermák[13] popisuje bezpečnost jako ochranu něčeho před poškozením, zničením, ztrátou nebo zcizením. Informační bezpečnost se potom dle výše uvedené definice popisuje jako ochranu informace před poškozením, zničením, ztrátou nebo zcizením. V odborné literatuře se však místo **poškození informace** používá pojem **narušení integrity**, o **zničení informace** se hovoří jako o **narušení dostupnosti** a **ztráta nebo zcizení informace** zase bývá označována jako **narušení důvěrnosti**. Čermák dále zdůrazňuje, že informace musí být odpovídajícím způsobem chráněny během celého jejich životního cyklu (information lifecycle), a to jak v úložišti, tak během přenosu, tak i při samotném používání, neboť hrozí, že by mohlo dojít k narušení jejich důvěrnosti, integrity a dostupnosti. Odpovídající způsob ochrany vyplývá z jejich kritičnosti a citlivosti.

---

[10] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, s 20.

[11] CHLUP, M . BEZPEČNOST ICT . *Český institut informační bezpečnosti*. [online]. [cit. 2016-02-07]. Dostupné z: http://www.cimib.cz/ors/fileadmin/user_upload/dokumenty/CIMIB_Bezpecnost_ICT.pdf

[12] Informační bezpečnost. *Management mania*. [online]. 09.07.2015 [cit. 2016-02-09]. Dostupné z: <https://managementmania.com/cs/informacni-bezpecnost>

[13] ČERMÁK, M. Informační bezpečnost. *Clever and Smart*. [online]. 20.05.2010 [cit. 2016-02-27]. Dostupné z:< http://www.cleverandsmart.cz/informacni-bezpecnost/>.

Proti informačnímu systému mohou být vedeny útoky, jejichž výsledky v případě úspěšného narušení bezpečnosti závisejí na charakteru systému. Výsledkem takového útoku můžou být drobné nepříjemnosti působené uživatelům, v horších případech může docházet i k velkým finančním ztrátám. V praxi můžeme porušení dostupnosti chápat například jako krátkodobý výpadek webové stránky, znemožnění přístupu k elektronické poště, výpadek elektrického proudu v postižené oblasti nebo zasažení jiného energetického zdroje. Ztráta utajení umožní útočníkovi číst utajovanou elektronickou poštu, seznamy kontaktů nebo čísla bankovních účtů. Porušení integrity se neobejde bez ztráty, nebo obnovení poškozených dat. Pokud se útočníkovi podaří nepozorovaný průnik do systému a následná modifikace informačního systému, může ho dlouhodobě nepozorovaně zneužívat.[14]

Pravděpodobnost úspěšného útoku lze podle Jirovského[15] snížit lepší ochranou systému, ale každá ochrana znamená vynaložení finanční částky bez okamžitého efektu. Žádný informační systém není absolutně bezpečný a při návrhu ochrany informačního systému je nutno si uvědomit, že cena chráněných objektů nemusí být stejná pro vlastníka informace a pro útočníka. Zvyšování zabezpečení bez znalosti ceny chráněných aktiv může být od určité úrovně ekonomicky neúnosné. Proto je nutné pochopit význam rizik a hrozeb v souvislosti s chráněnými informacemi a informačními systémy.

Celá problematika informační bezpečnosti se tedy týká **informací.** Informace je něco, co se dá zpracovávat na počítačích, může se ukládat na jejich discích, nebo se může přenášet po síťových linkách a putovat po internetu. Na tyto informace útočí hackeři a viry. Ve snaze zabezpečit tyto informace jsou využívány firewally, šifry, elektronické podpisy a patřičná ochrana přístupovými právy. Informace nejsou pouze bity a bajty v počítačích. Není rozhodující, v jaké formě nebo na jakém nosiči se informace nacházejí, pro uživatele je důležitá informace samotná. S rozvojem výpočetní techniky je častěji informace prezentována v podobě počítačových dat, ale není to její jediná podoba. Rovněž to nejsou jen osobní počítače, které umožňují práci s informacemi.[16]

[14] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, s 20.
[15] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, s 20 - 21.
[16] SVĚTLÍK, M. Informační bezpečnosti: část 1 - 4, *Softwarové noviny*, 2002, č. 2-5, s. 1-2. Dostupné z: <http://www.rac.cz/rac/homepage.nsf/CZ/Download/$FILE/inf_bezp.pdf>.

Pojem informace pochází z latinského slova "informo - informatio", což znamená sdělení, přenos sdělení, ale též poučení, popis něčeho. V odborné literatuře existuje mnoho definic a vysvětlení tohoto pojmu, ale jen některé vystihují složitost tohoto pojmu. Pojmy informace a data se často se zaměňují. Pro efektivní komunikaci mezi odborníky je třeba tyto pojmy odlišit a vymezit jejich vztah.[17] **Data** jsou získané údaje popisující realitu. Jsou to zaznamenané výsledky pozorování reality, fakta, poznatky, znalosti nebo vědomosti. Data existují a jsou uložena na různých mediích nebo nosičích. Interpretací dat a jejich vztahů za pomoci znalostí vznikají **informace.**[18]

Informace začíná být stejně významným výrobním faktorem jako je půda, kapitál, výrobní prostředky, lidé. 21. století bývá někdy pro svůj globalizační trend a rozvoj informačních technologií, zejména internetu, nazýváno stoletím informatiky a přelom letopočtu charakterizován jako informační revoluce. Informace se staly obchodní komoditou, aktivem, se kterým se ve firmách a organizacích počítá. Rozhodující konkurenční výhodou tak již nemá množství půdy, ale správné a rychlé využití informací. Proto dnes informace řadíme k hlavním faktorům podmiňujících pokrok ve všech oborech lidské činnosti.[19] Drucker[20] uvádí: "Tradiční výrobní faktory jako půda, práce, kapitál nezmizely, ale staly se druhořadými. Hlavním faktorem se staly informace a znalosti".

Podle Čermáka[21] většina firem bezpečnost informací podceňuje. Většina firem si stále neuvědomuje, že jejich nejcennějším aktivem jsou informace, a že by jejich ochraně měly věnovat dostatečnou pozornost. A je jedno, zda se jedná o informace o nových produktech, technologiích, výrobních postupech, klientech nebo marketingové strategii. Pravda je, že tyto informace mají určitou hodnotu, a pokud nejsou odpovídajícím způsobem chráněny, mohou být snadno zcizeny a zneužity. Z tohoto důvodu by měla každá organizace, ve vlastním zájmu a bez ohledu na svou velikost a předmět podnikání, zavést určitá bezpečnostní opatření.

[17] POŽÁR, J. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, s. 11.
[18] Informace. *Management mania*. [online]. 23.05.2013 [cit. 2016-02-22]. Dostupné z WWW: <https://managementmania.com/cs/informace>.
[19] POŽÁR, J. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, s. 9.
[20] DRUCKER, P. *Postkapitalistická společnost*. Praha : Management Press, 1994. s. 15.
[21] ČERMÁK, M. Mýty informační bezpečnosti. *Clever and Smart*. [online]. 24.04.2012 [cit. 2016-02-27]. Dostupné z: <http://www.cleverandsmart.cz/myty-informacni-bezpecnosti-aneb-proc-vetsina-firem-zije-v-bludu/>.

3.1 Národní strategie kybernetické bezpečnosti České republiky

O tom, že informační bezpečnosti je věnována pozornost, svědčí i skutečnost, že vláda České republiky 25. května 2015 schválila **Akční plán** k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 a zprávu o stavu kybernetické bezpečnosti České republiky 2014. Oba materiály vypracoval Národní bezpečnostní úřad (NBÚ). Akční plán, který definuje na příštích pět let konkrétní kroky k naplnění hlavních cílů národní strategie, stanoví u nich kompetentní orgán a termíny plnění, připravil NBÚ ve spolupráci se všemi relevantními partnery. Obsahuje např. činnosti potřebné k zajištění účinnějšího potírání informační kriminality, identifikované ve spolupráci s Ministerstvem vnitra a policií, úkoly v oblasti mezinárodní spolupráce určené s Ministerstvem zahraničních věcí a v neposlední řadě postup vytváření a následného zajišťování kybernetické obrany České republiky, vymezený v součinnosti s Ministerstvem obrany. Za kontrolu plnění Akčního plánu je zodpovědný NBÚ.[22]

Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 představuje základní koncepční dokument vlády České republiky pro příslušnou oblast a je v souladu s bezpečnostními zájmy a východisky definovanými v Bezpečnostní strategii České republiky. Slouží jako výchozí dokument pro tvorbu navazujících právních předpisů, politik či standardů, směrnic a jiných doporučení v rámci ochrany a zabezpečení kyberprostoru. Kybernetická bezpečnost podle Národní strategie kybernetické bezpečnosti představuje souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost. Kybernetická bezpečnost pomáhá identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury.[23]

---

[22] Vláda schválila akční plán k národní strategii kybernetické bezpečnosti české republiky. Národní centrum kybernetické bezpečnosti. 25. 5. 2015 [cit. 2016-03-22]. Dostupné z: <http://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vlada-schvalila-akcni-plan-k-narodni-strategii-kyberneticke-bezpecnosti-ceske-republiky-pro-pristich-pet-let-a-zpravu-o-stavu-kyberneticke-bezpecnosti-ceske-republiky-2014/>.

[23] Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. *Národní centrum kybernetické bezpečnosti*. 16.02.2015 [cit. 2016-02-09]. s. 5 - 6. Dostupné z: <http://www.govcert.cz/download/nodeid-1004/>.

3.2 Hlavní cíle Národní strategie kybernetické bezpečnosti

Na základě hlavních cílů Národní strategie kybernetické bezpečnosti je v koordinaci s ostatními zainteresovanými subjekty vypracován podrobný **Akční plán**, který definuje konkrétní kroky, stanoví u nich zodpovědnost, termíny jejich plnění a kontrolu. Mezi hlavní cíle Národní strategie kybernetické bezpečnosti patří především:

1. Zajištění efektivity a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti.
2. Aktivní mezinárodní spolupráce.
3. Spolupráce se soukromým sektorem.
4. Výzkum a vývoj / spotřebitelská důvěra.
5. Podpora vzdělávání, osvěta a rozvoj informační společnosti.
6. Podpora rozvoje schopností Policie České republiky vyšetřovat a postihovat informační kriminalitu.
7. Právní úprava pro kybernetickou bezpečnost (vytváření právního rámce). Účast na tvorbě a implementaci evropských a mezinárodních pravidel.

NBÚ a jeho specializované pracoviště Národní centrum kybernetické bezpečnosti bude průběžně sledovat, diskutovat a hodnotit plnění jednotlivých cílů ve spolupráci s ostatními zainteresovanými subjekty. V rámci každoroční **Zprávy o stavu kybernetické bezpečnosti** v České republice zajistí zpracování hlášení o stavu naplňování **Akčního plánu** ve formě přílohy. Zpráva bude vládu i širokou veřejnost informovat o efektivitě přijímaných opatření a plnění úkolů definovaných Národní strategií kybernetické bezpečnosti.[24]

[24]Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. *Národní centrum kybernetické bezpečnosti*. 16.02.2015 [cit. 2016-02-09]. s. 17 - 22. Dostupné z: <http://www.govcert.cz/download/nodeid-1004/>.

3.3 Principy Národní strategie kybernetické bezpečnosti

1. **Ochrana základních lidských práv a svobod a principů demokratického právního státu** - Česká republika dodržuje při zajišťování kybernetické bezpečnosti základní lidská práva, demokratické principy a hodnoty. Dbá na dodržování svobody projevu, ochrany osobních dat a soukromí. Při zajišťování kybernetické bezpečnosti proto usiluje o maximální otevřenost přístupu k informacím a minimalizaci zásahů do práv občanů a soukromých subjektů.

2. **Komplexní přístup ke kybernetické bezpečnosti založený na principu subsidiarity a spolupráce** - celá strategie dodržuje princip nedělitelnosti bezpečnosti, kde kybernetickou bezpečnost České republiky nelze oddělovat od kybernetické bezpečnosti globální, respektive v euroatlantické oblasti. Česká republika na ni tedy nahlíží komplexně, jako na úzce propojený fenomén.

3. **Budování důvěry a spolupráce mezi veřejným a soukromým sektorem a občanskou společností** - za zajišťování kybernetické bezpečnosti nemůže být odpovědný pouze stát a orgány veřejné správy, ale je nutná i aktivní spolupráce občanů České republiky, soukromých právnických a podnikajících fyzických osob.

4. **Rozvoj kapacit k zajišťování kybernetické bezpečnosti** - vzhledem ke značné závislosti společnosti na informačních a komunikačních technologiích a neustálým změnám povahy současných kybernetických hrozeb a rizik závisí kybernetická bezpečnost České republiky nejen na neustálém budování robustnější, odolnější informační infrastruktury, ale i na společnosti jako celku.[25]

[25] Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. *Národní centrum kybernetické bezpečnosti*. 16.02.2015 [cit. 2016-02-09]. s. 9 - 11. Dostupné z : <http:// www.govcert.cz/download/nodeid-1004/>.

4 Druhy hrozeb v počítačové a informační bezpečnosti

Pojmem hrozba označuje Staudek a Hanáček[26] jako možnost využít zranitelné místo informačního systému k útoku na něj - ke způsobení škody na aktivech. Určuje se úroveň zranitelnosti, která se liší dle **citlivosti**, **zranitelnosti, náchylnosti, kritičnosti** a **důležitosti** aktiva.

Velmi obecně definuje hrozbu Jirovský[27], podle něj pod hrozbou můžeme chápat cokoliv, co nějakým způsobem může vést k nežádoucí změně informace, chování systému nebo ovlivnit jeho parametry. Dále uvádí, že hrozby mohou být klasifikovány jako **úmyslné**, tedy např. průnik útočníka do systému, a **neúmyslné**, kdy ohrožení systému vzniká chybou operátora, uživatele nebo samotného systému. Úmyslné hrozby můžeme dále rozdělit na **pasivní** a **aktivní**. Příkladem pasivní hrozby je monitorování provozu, při kterém je zjišťován obsah předávaným informací, aniž by byl měněn. Útok, což je vlastně realizace aktivní hrozby, zahrnuje změnu přenášené informace.

Podle Požára[28] jsou předmětem mnoha hrozeb aktiva. Hrozba má schopnost způsobit nežádoucí incident, který může mít za následek poškození informačního systému nebo organizace a jejích aktiv. Hrozby mohou být přírodního charakteru nebo mohou hrozit od vlastních zaměstnanců či ze strany vnějšího útočníka. Hrozby mohou být náhodné nebo úmyslné. Škoda způsobená incidentem může být dočasné povahy nebo může být trvalá, jako je tomu v případě zničení nebo nevratného poškození aktiv. Dále Požár pojmem hrozba označuje jakoukoliv okolnost či událost působící na zranitelné místo, která může způsobit potenciální škodu na aktivu. Podle Požára jsou zranitelná místa součástí informačního systému, jejichž existence způsobuje, že některé vlivy prostředí, ve kterém se informační systém provozuje, představují pro něj hrozby.

[26] HANÁČEK, P, STAUDEK, J. *Bezpečnost informačních systémů. Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. 1. vyd. Praha: Úřad pro státní informační systém, 2000, s 39-40.
[27] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, s 20.
[28] POŽÁR, J. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, s 23.

4.1 Hrozby přírodního původu (vyšší moc)

Prevence přírodních hrozeb je podle Požára[29] obtížná a je třeba řešit spíše minimalizaci dopadů vhodným plánem obnovy. Čermák[30] uvádí, že v případě působení vyšší moci nelze s nějakým snížením pravděpodobnosti hrozby většinou počítat, protože frekvence výskytu určité hrozby je nezávislá na naší vůli a zůstává v dané lokalitě stejná. Daleko spíše můžeme hovořit o snížení míry zranitelnosti nebo dopadu. Hrozbě jako je povodeň, požár, výpadek dodávky vody nebo elektřiny nemůžeme dost dobře zabránit, ale může snížit zranitelnost daného aktiva vůči působení těchto hrozeb nebo alespoň jejich následky. Podle Doseděla[31] se dá proti všem přírodním hrozbám bránit duplikací důležitých částí systému a pravidelným zálohováním dat, dále by nosiče dat měly být uloženy v prostředí, které důsledky takové přírodní hrozby co nejvíce minimalizuje. Doseděl dále shrnuje hlavní přírodní katastrofy a navrhuje vhodná preventivní opatření:

- **Požár** - vhodná je instalace samočinných požárních hlásičů a komplexních systémů pro hlášení vzniklých požárů. Zde je třeba upozornit, že elektrická zařízení nelze hasit vodou. Disky s citlivými daty by měly být uloženy v nehořlavých skříních, pokud možno vodotěsných a prachotěsných, aby nedocházelo k vniknutí hasící látky.
- **Zemětřesení** - vhodná je již zmíněná prachu vzdornost, pevnost skříně, odolnost proti mechanickým nárazům, upevnění disku i skříně počítače, aby se zabránilo nežádoucím pádům a nárazům.
- **Klima** - počítačové komponenty jsou poměrně náročné na kvalitu prostředí. Škodí jim prach, velké kolísání teplot, vlhkost atd. Při činnosti vyvíjejí také teplo, proto potřebují určitý druh chlazení, takový problém vyřeší kvalitní klimatizace.
- **Voda** - hlavním protipovodňovým opatřením je vhodná poloha. Servery je vhodné instalovat do vyšších pater budov, dalším nutným opatřením je izolace místnosti, ve které jsou servery umístěny.

[29] POŽÁR, J. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, s 23.
[30] ČERMÁK, M. Bezpečnostní opatření. *Clever and Smart.* [online]. 18.11.2012 [cit. 2016-02-27]. Dostupné z WWW: <http://www.cleverandsmart.cz/snizuje-bezpecnostni-opatreni-hrozbu-zranitelnost-nebo-dopad/>.
[31] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. s. 54 - 55.

4.2 Technické selhání

Technické poruchy, např. v síti, mohou zničit dostupnost jakékoliv informace, která je uchovávána nebo zpracovávána v této síti. Mezi nejčastější příčiny selhání hardware patří například nedostatečná údržba, nejasné postupy při údržbě HW, nevhodné prostředí umístění HW (vlhkost, prach, výkyvy teploty apod.).[32] Podle Čermáka[33] pravděpodobnost selhání HW nebo SW v naprosté většině případů přímo souvisí s jeho fyzickou životností. Dále je podle Čermáka jediným opatřeními ke snížení hrozby výměna daného HW nebo SW, dále pak monitoring a včasný upgrade, který snižuje zranitelnost daného systému.

4.3 Neúmyslné hrozby plynoucí z lidského faktoru

Nejslabším článkem celé sítě je právě uživatel. Zájmem každého uživatele by mělo být seznámení s pravidly bezpečného provozu a poctivě je dodržovat. Podle Matyska[34]si bezpečnou síť nelze představit bez spolupráce dostatečně poučených uživatelů. Současný trend ve vývoji programového vybavení i samotných operačních systémů směřuje k tomu, aby počítače mohl používat i naprostý laik, s prakticky nulovou znalostí principů funkce.

Aby bylo možno považovat informační systém z hlediska lidského faktoru za zabezpečený, musí být definované konkrétní personální pravidla. Mezi tato pravidla patří zejména přesně stanovená odpovědnost jednotlivých uživatelů systému (včetně jejich oprávnění pro přístup do systému) a postupy schvalování mimořádných požadavků a událostí.[35] Nejjednodušší řešení je ve správném nastavení přístupových práv, kdy každý uživatel má přístup pouze do svého domovského adresáře a nikam jinam. Je vhodné, aby existoval společný adresář, do kterého mají přístup všichni uživatelé.[36]

---

[32] CHLUP, M . BEZPEČNOST ICT . *Český institut informační bezpečnosti*. [online]. [cit. 2016-02-07]. Dostupné z: http:<//www.cimib.cz/ors/fileadmin/user_upload/dokumenty/CIMIB_Bezpecnost_ICT.pdf>.

[33] ČERMÁK, M. Bezpečnostní opatření. *Clever and Smart.* [online]. 18.11.2012 [cit. 2016-02-27]. Dostupné z: <http://www.cleverandsmart.cz/snizuje-bezpecnostni-opatreni-hrozbu-zranitelnost-nebo-dopad/>.

[34] Matyska, L. Bezpečnost na Internetu. *Zpravodaj ÚVT MU*. [online]. 2002 [cit. 2016-02-28]. Dostupné z: <http://webserver.ics.muni.cz/bulletin/articles/242.html>

[35] Tomek, M. Lidský faktor v bezpečnosti IS. *System Online*. [online]. 2004 [cit. 2016-02-28]. Dostupné z: <http://www.systemonline.cz/clanky/lidsky-faktor-v-bezpecnosti-is.htm>.

[36] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. s. 56 - 57.

4.4 Úmyslné hrozby plynoucí z lidského faktoru

Do této kategorie hrozeb patří především záměrné útoky na informační systém, nejčastěji se pak jedná o hackerské útoky, pasivní útoky, znehodnocení či modifikace dat a informací, krádeže dat a citlivých informací atd.[37]

Na počítačový systém může (s velkou pravděpodobností dříve či později) z různých důvodů zaútočit člověk se zlými úmysly. Takovou osobu označujeme jako útočníka. Z hlediska odbornosti útoků je možné dělit útočníky do několika skupin. Další dělení může být založeno na druhu útoku - jinak označíme útočníka, který napadá počítačový systém pomocí internetu, a jinak označíme útočníka prolamujícího počítačové programy. Podle místa, odkud jsou vedeny útoky, je možné útočníky rozdělit na vnitřní a vnější.[38]

4.4.1 Vnitřní útočník

Doseděl[39] označuje vnitřního útočníka jako osobu připojenou do vnitřní komunikační sítě organizace. Pachatelem ve většině útoků zevnitř bývá současný nebo bývalý zaměstnanec konkrétního napadeného subjektu, nebo někdo jiný, kdo má přístup do nitra organizace. Útočník při svém postupu vychází ze znalosti vnitřního uspořádání organizace či prostředí, ve kterém je systém umístěn. Většina bezpečnostních incidentů způsobených vnitřními útočníky má povahu nechtěných zásahů a nehod, které způsobuje nízká kvalifikace pracovníků organizace v oblasti informačních technologií. Jedná se např. o smazání souborů, opomenutí provedení zálohování atd. Vyskytují se však i případy, kdy se pracovník mstí zaměstnavateli či kolegovi z různých důvodů. Může se také jednat o poskytování citlivých informací konkurenční organizaci. Proti tomuto jednání se dá bránit zvyšováním loajality k zaměstnavateli, kdy vyloučíme úmyslné útoky, nebo zvyšováním spolehlivosti, kdy vyloučíme neúmyslné chyb zaměstnanců. Požár[40] uvádí, že nejrizikovějším faktorem úniku informací jsou vlastní zaměstnanci. Pokud se přidá jejich nespokojenost, riziko se ještě zvyšuje. Zaměstnanec ve výpovědi nebo ten který je nespokojený s jednáním zaměstnavatele, může pak způsobit velké škody. Často se v takových případech zaměstnanec mstí tím, že vynáší citlivé informace nebo dokonce přechází i s informacemi ke konkurenci.

[37] POŽÁR, J. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, s 41.
[38] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. s. 153.
[39] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. s. 154.
[40] POŽÁR, J. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, s 37.

Díky informačním technologiím a množstvím informací, které firmy denně potřebují pro svůj provoz, se objevila nová skupina hrozeb označovaná jako "**nespokojený zaměstnanec**" nebo v širším pojetí se používá pojem "**insider**". Nespokojený zaměstnanec nebo insider je pro firmu v mnohém nebezpečnější něž útok zvenku, zejména pro jeho vědomosti o chodu firmy, které nashromáždil během své pracovní činnosti, mnohdy disponuje i klíčovými informacemi o zabezpečení. Cizí útočník musí před zahájením útoku najít bezpečnostní slabiny v systému, ale současný či bývalý zaměstnanec určitě prošel bezpečnostním školením, které mu zcela jistě pomůže v identifikaci slabých míst systému. Dále bude disponovat znalostí přihlašovacích jmen a hesel, které velmi ulehčí případný útok.

Metody útoku nespokojeného zaměstnance se liší podle toho, jestli je stále v pracovním poměru nebo byl jeho pracovní poměr ukončen. Zásadní rozdíl je v dostupnosti prostředků a v chování potencionálního pachatele. Současný zaměstnanec se bude více obávat prozrazení, protože k němu lze nalézt stopy snadněji něž k někomu kdo společnost již opustil.

Ve většině protizákonného jednání je motivem finanční zisk. Spokojenost zaměstnance ve firmě je ovlivněna celou řadou faktorů, ale výše částky na výplatní pásce je pro většinu rozhodující, neboť pro mnohé mzda vyjadřuje míru uznání jejich schopností. Mnohé zaměstnance však k útoku proti zaměstnavateli nevede potřeba zisku, ale jiné lidské pohnutky. Pro propuštěné zaměstnance to může být touha po pomstě, demonstrace vlastních schopností, kdy chce zklamaný jedinec bývalému zaměstnavateli ukázat, jak dobrého zaměstnavatele se zbavil. Tento motiv bývá častý u vysoce kvalifikovaných profesí. Nelze pominout ani motiv soupeření, kdy prostřednictvím pracovních nástrojů soupeří se svými kolegy v zaměstnání nebo se svými bývalými kolegy. Typickými nástroji takového soupeření je demonstrace slabin bývalých kolegů prostřednictvím útoku na jejich práci, či proniknutí do systému jako důkaz propustnosti zabezpečení počítačové sítě nebo neschopnosti nového správce sítě, který nastoupil na místo propuštěného pracovníka.[41]

[41] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. s. 114-115.

4.4.2 Vnější útočník

Vnější útočník je osoba, která nemá fyzický přístup k vnitřní komunikační síti. Při svém útoku musí překonat všechny nástrahy a bezpečnostní opatření, které mu klade správce sítě. Takovému útočníkovi může jít pouze o pasivní sběr informací, může se pokusit do probíhajících procesů aktivně zasahovat z důvodů modifikace či poškození dat. Nevýhodou těchto útočníků je poměrně špatná vystopovatelnost, vzhledem k tomu, že se útočník může nacházet kdekoli. Proti takovému útočníkovi je obtížné prosadit a zahájit jeho trestní stíhání. Jedinou ochranou proti takovému útočníkovi je důkladné zabezpečení počítačového systému. Útočníky můžeme rozdělit podle znalostí a nebezpečnosti takového útoku do několika kategorií. Ne každý je schopný realizovat sofistikovaný útok, velká část útočníků se omezí na využití dostupných nástrojů internetu.[42]

- **Amatéři**

Amatéři jsou nejméně nebezpeční útočníci. Jedná se o náhodné útočníky. Do této skupiny patří počítačově nepříliš vzdělaní lidé, studenti atd. Nemají dostatek času, znalostí ani vybavení k provedení sofistikovaného útoku. K ochraně informačního systému proti jejich útokům postačí poměrně levná a jednoduchá bezpečnostní opatření. Většinou jen zkouší, zda dokážou využít nějakou bezpečnostní díru v systému popsanou na internetu. Motivací útoku je tedy většinou zvědavost.

- **Hackeři**

Do této skupiny spadají osoby s velmi dobrými znalostmi v oblasti výpočetní techniky, často se jedná o vysokoškolské studenty informačních technologií. Dokážou provést značně nepříjemné útoky. Jsou však značně limitováni prostředky. Motivací útoku je jednak zvědavost, ale také snaha dokázat své kvality. Proti těmto útočníkům je chráněna většina informačním systémů.[43]

Definice hackera v dnešní době, kdy je pohled na hackerství médii značně zkreslen, není jednoduchá. Podle internetového souboru Jargon File: The New Hackers Dictionary je hacker člověk, kterého baví zkoumat detaily programovatelných systémů a hledat metody jak je vylepšit. Další rysy uvedené v tomto souboru hackera označují jako člověka, který s nadšením programuje, nebo je programováním posedlý.

[42] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. s. 154.
[43] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. s. 155.

Policie definuje hackera jako osobu, která proniká do chráněných systémů, přičemž jejím cílem je prokázat vlastní kvality bez toho, aby měla zájem v získávání nebo zničení informací v systému. Za nejdůležitější je překonání ochranné bariéry, což je považováno za zábavu, dobrodružství či "sportovní nadšení" a to bez nároku na veřejné uznání. Hackerům postačí, když se o jejich činech hovoří alespoň ve vlastní komunitě.

Sami hackeři se většinou vidí jako uživatelé, velmi dobře vybavení technologickými znalostmi, které z pravidla získávají samostudiem. Uspokojení nacházejí v objevování skrytých detailů informačních a telekomunikačních systémů, především v oblastech jejich bezpečnosti a zranitelnosti. Milují praktické, rychlé a sofistikované programování, které bývá ve většině případů nepřehledné a neuspořádané. Jsou to lidé s kreativním myšlením, kteří odmítají stereotypní práci s počítačem.

Nejhorší představu o hackerovi však prezentují média. Ty představují hackera jako kriminální individuum nabourávající se do cizích informačních systémů bez ohledu na důvod nebo cíl takové činnosti. Podle médií je hacker člověk, který ničí internetové stránky, snaží se narušit informační systémy nebo získat choulostivé osobní údaje. Tato představa, vycházející z novinářské nevědomosti, než ze skutečného hackerského světa, však stvořila neblahou představu hackera v očích prostých lidí. Média zcela zkreslila úlohu hackerů ve vývoji informačních technologií, představila ho jako vetřelce a zloděje. Zapomněla, že se jedná o inteligentní osobnosti, které mají snahu dokazovat svoji zručnost v oboru.[44]

- **Profesionálové**

Tento druh útočníků většinou pochází z řad počítačových profesionálů, jsou vybaveni značnými znalostmi a dostatkem prostředků. Jejich útoky patří mezi nejnebezpečnější, často se vymykají všem známým postupům. Zabezpečení proti takovému útoku je velmi nákladné a složité. Motivace takového útočníka může být různá. Do této skupiny spadají jak najmutí zločinci, tak teroristé snažící se poškodit svůj cíl za každou cenu.[45]

[44] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, s. 51.
[45] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. s. 155-156.

4.5 Škodlivý software

Mezi lidmi pohybujícími se v oblasti počítačových virů panuje nejednotnost týkající se terminologie. Všechny druhy programů, které nějakým způsobem uživateli škodí, se označují souhrnným názvem škodlivý software, anglicky **malware** (malicious software).[46]

4.5.1 Viry

Pravděpodobně nejrozšířenější odrůdou škodlivého softwaru jsou počítačové viry. Počítačový virus je nežádoucí program, který se šíří a infikuje další počítače bez vědomí uživatele. V současné době se počet škodlivých programů pohybuje v řádech tisíců, například seznam virů, které se šíří mezi uživateli obsahuje přibližně 600 různých virů.

Oblíbeným médiem pro přenos virů na další počítače jsou USB flash disky. Mohou škodit různými způsoby. V minulosti se viry na napadeném počítači projevovaly různými zvukovými nebo obrazovými efekty, dále pak škodily ničením souborů a dat. V současnosti se naopak snaží chovat co nejméně nápadně a případně stahovat další nežádoucí a škodlivé programy do napadeného počítače. Označení virus je zvoleno, protože je tu jistá podobnost s biologickými viry. Počítačový virus totiž ke svému šíření také potřebuje hostitele.[47]

Základním úkolem viru je šíření, aby se ale virus mohl šířit, musí být aktivní v paměti. Aktivní virus může bojovat proti svému odhalení uživatelem, nebo antivirovým programem. Používá techniky nazývané "stealth" (neviditelný), která spočívá v nejrůznějším maskování svojí činnosti. Například pokud virus napadne soubor, tento soubor se zvětší o velikost viru, aby tuto činnost uživatel neodhalil snadno, napojí se virus na příslušnou službu operačního systému. Poté, když se některý program zeptá na velikost napadeného souboru, vir mu podstrčí správnou velikost.[48]

[46] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. s. 128.
[47] KRÁL, M. *Bezpečný internet: chraňte sebe i svůj počítač*.Vyd. 1. Praha: Grada Publishing, a.s., 2015. Průvodce (Grada). s. 14 - 15.
[48] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. s. 135.

4.5.2 Červ

Dalším velmi rozšířeným škodlivým softwarem jsou červi. Jedná se o program šířící se pomocí počítačové sítě. Červi většinou plní více škodlivých úkolů. Nespokojují se pouze s mazáním souborů z pevného disku, ale navíc se ještě šíří. Červ se může šířit pomocí jinak nevinného programu, ke kterému přidá nežádoucí funkci (sám sebe).[49] Ke svému šíření může používat řadu cest, pravděpodobně nejrozšířenější jsou ale červi šířící se pomocí e-mailů. Ke své práci využívají bezpečnostních chyb či pokročilých funkcí, které například umožní skupinové rozesílání e-mailů. Mnoho červů spoléhá na neznalost a naivitu uživatelů. Připojují se k dokumentům s lákavým názvem či popisem, který přímo vyzývá, aby byl otevřen.[50]

Prvního červa vypustil roku 1988 do počítačové sítě student americké univerzity. Původním záměrem bylo pouze šířit červa, ale díky chybě kódu došlo k poškození řady systémů a vyřazení části internetu z provozu.[51]

Erbschloe[52] popisuje počítačového červa jako škodlivý program, který vzniká na jednom počítači a vyhledává další počítače přes lokální síť (LAN) nebo pomocí připojení k internetu. Poté co červ najde jiný počítač, replikuje sám sebe do tohoto počítače a pokračuje v hledání dalších připojených počítačů, na nichž se může dál replikovat.

Pravděpodobně nejznámějším případem je červ s názvem **ILOVEYOU**, nazývaný také Love letter nebo The Love Bug. Šíří se přes elektronickou poštu a při svém spuštění zapisuje sám sebe do systémového adresáře.[53] V roce 2000 ILOVEYOU infikoval přes dva miliony stanic a poškodil na nich databáze obrázků, filmů a zvuků. Především znemožnil postiženým komunikovat přes počítač s okolím. Škody vznikaly jak zahlcením e-mailových serverů, tak druhou činností viru, kterou bylo přemazání souborů uložených v napadeném počítači a jejich nahrazení sebou samým.[54]

---

[49] PETROWSKI, T. *Bezpečí na internetu pro všechny*. Vyd. 1. Liberec: Dialog, 2014. s. 33.
[50] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. s. 134-135.
[51] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. s. 127.
[52] ERBSCHLOE, M. *Trojans, worms, and spyware: a computer security professional's guide to malicious code*. Burlington: Elsevier Butterworth Heinemann, 2005. s. 23.
[53] HOWARD, M. a LEBLANC, D. *Bezpečný kód*: *techniky a strategie tvorby bezpečných webových aplikací*. Vyd. 1. Brno: Computer Press, s. 221.
[54] Zákeřný virus I love you napadl před deseti lety desítky miliónů počítačů. *Idnes.cz*. [online]. 3.5.2010 [cit. 2016-03-05]. Dostupné z: <http://www.novinky.cz/internet-a-pc/software/199149-zakerny-virus-i-love-you-napadl-pred-deseti-lety-desitky-milionu-pocitacu.html>.

4.5.3 Trojský kůň

Dalším druhem škodlivého softwaru jsou trojské koně. Počítačová obdoba trojského koně je program, který kromě svých funkcí vykonává ještě další skryté funkce. Tato skrytá část může vykonávat různorodou činnost. Trojský kůň dokáže např. sbírat hesla zadávaná uživatelem z klávesnice a pak je odeslat po internetu, nebo může zjišťovat jaké stránky jsou navštěvovány. [55]

Petrowski[56] označuje trojského koně jako dva programy v jednom. Kdy uživatel po stažení údajně užitečného programu, který si zdarma stáhne z internetu, obdrží "užitečný" program, který dělá co má a "záludný" program, který bez vědomí uživatele provádí jinou činnost.

Erbschloe[57] definuje trojského koně jako základní typ škodlivého softwaru, který má za úkol především poskytování přístupu hackera do systémových souborů. Tento přístup umožňuje hackerovi možnost změnit nastavení souborů, krást soubory nebo hesla, poškozovat soubory nebo sledovat aktivity uživatele v jiných počítačových sítích.

Trojské koně se vyskytují hlavně ve dvou kategoriích programů a to buď ve formě "**freewaru**" zdarma, nebo jako **ukradené programy**, které se šíří internetem. V případě freewarů s trojskými koňmi se jedná o programy zdarma, které jsou většinou vyvinuty soukromými nadšenci, kteří je dávají na internetové servery k dispozici. Běžný uživatel těžko posoudí, zda je takový program bezpečný a užitečný. Další variantou jsou již zmíněné ukradené programy obohacené o trojské koně. Tento typ funguje tak, že hacker, či skupinka hackerů prolomí kódy, obejdou autorská práva a dají původně drahý produkt bezplatně k dispozici všem uživatelům internetu. Hackeři poté k ukradenému zboží přidají také malware, např. trojského koně.[58]

[55] POŽÁR, J. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, s 45.
[56] PETROWSKI, T. *Bezpečí na internetu pro všechny*. Vyd. 1. Překlad Tomáš Kurka. Liberec: Dialog, 2014. s. 38.
[57] ERBSCHLOE, M. *Trojans, worms, and spyware: a computer security professional's guide to malicious code*. Burlington: Elsevier Butterworth Heinemann, 2005. s. 22.
[58] PETROWSKI, T. *Bezpečí na internetu pro všechny*. Vyd. 1. Liberec: Dialog, 2014. s. 39.

4.5.4 Spyware

Další klasická podoba internetových hrozeb jsou špionážní programy, které sledují činnost uživatele na počítači a získávají různé údaje. Charakteristikou spywaru je, že se do počítače dostane zcela nepozorovaně, škodí v tichosti a uživatel o ničem neví. Spyware od uživatele shromažďuje informace, například seznamy webových stránek, které navštěvuje, nebo citlivé informace jako jsou uživatelská jména a hesla.

Spyware je často spojen se softwarem, který zobrazuje reklamy (adware). Někteří zadavatelé reklamy mohou skrytě instalovat adware na uživatelův počítač a vygenerovat tok nevyžádaných reklam. Pokud je v pozadí operačního systému spuštěno nadměrné množství spywaru, dochází ke znatelnému snížení výkonu.

Spyware nebo adware programy se běžně dostanou do uživatelova počítače pomocí instalace jiného softwaru. Kdykoliv uživatel instaluje nějaký program, měl by si pečlivě prostudovat všechny údaje a sdělení, včetně licenční smlouvy a prohlášení o nakládání se soukromými informacemi. Někdy je instalace nežádoucího programu popsána v instalační proceduře, ale může se objevit třeba až na samém konci licenční smlouvy.

Bohužel vynalézavost některých tvůrců spywaru zašla tak daleko, že spywarem či adwarem může nic netušící uživatel obohatit svůj počítač, při pouhém procházení internetových stránek. [59]

Na první pohled by se mohlo zdát, že se jedná o užitečný program, zdání však klame. Spyware prohledává počítač a zneužívá údaje, jež nalezne. Nejvíce se zaměřuje na přístupové údaje a hesla k emailovým službám, internetovému bankovnictví, údaje o kreditních kartách či osobní informace. Získané informace dává spyware dohromady a následně je po internetu pošle svému tvůrci.[60]

[59] KOCMAN, R. a LOHNISKÝ, J. *Jak se bránit virům, spamu, dialerům a spyware*. Vyd. 1. Brno: CP Books, 2005.s. 113 - 114.
[60] PETROWSKI, T. *Bezpečí na internetu pro všechny*. Vyd. 1. Překlad Tomáš Kurka. Liberec: Dialog, 2014. s. 35 - 36.

4.5.5 Key-logger

Jedná se o aplikace, které dokážou zaznamenávat stisknuté klávesy a nepozorovaně běžet v pozadí. Aplikace tohoto typu jsou oblíbeny převážně začátečníky, kteří jsou díky nim schopni dosáhnout dobrých výsledků s minimem zkušeností. Především protože je možné zaznamenat vše, co je zadáno na klávesnici. Tedy nejen hesla, ale i e-maily či celé dokumenty. Podobné monitorovací nástroje používají i profesionálové, ale ti si je většinou programují sami, mohou tak implementovat další funkce, které v běžně dostupných aplikacích tohoto typu chybí.

Podobných monitorovacích programů je celá řada, proto je efektivní ochrana proti tomuto druhu útoku téměř nemožná. Lze provést řadu opatření, aby útočník nemohl podobné škodlivé programy nainstalovat. Přesto je velmi obtížné útočníkovi zabránit, aby takový program při nejmenším nespustil, což může stačit k tomu, aby získal potřebné informace.

Mezi nejúčinnější metodu ochrany proti tomuto programu je kontrola seznamu běžících procesů. Každý uživatel by měl pravidelně kontrolovat, jaké procesy mu na počítači běží a okamžitě zpozornět, když nějaký přibude. Stačí stisknout kombinaci kláves Ctrl+Alt+Delete a hledat podezřelý proces, pokud je přítomný je zřejmé, že činnost na počítači je monitorována. Uživatel se pak může pokusit najít spouštěcí soubor programu.

Monitorovací programy vypadají jako nebezpečné a zákeřné programy, ale na tento druh programů se nesmí pohlížet pouze jako na škodlivý software. Právě naopak. Původně byly vytvořeny za účelem monitorování uživatelů, kteří zneužívají počítače jak by neměli. Řada administrátorů a zaměstnavatelů využívá možnost této kontroly, při které mohou zaměstnance přistihnout, jak místo práce brouzdají po internetu nebo dokonce hrají počítačové hry.[61]

[61] ZEMÁNEK, J. *Slabá místa Windows, aneb, Jak se bránit hackerům*. Vyd. 1. Kralice na Hané: Computer Media, 2004. s. 41 - 49.

5 Rizika v počítačové a informačním bezpečnosti

Pravděpodobnost, že se uplatní některá z hrozeb nebo zranitelných míst informačních systémů je vyjádřena hodnotou informačního rizika. Teoretické odhady jsou potvrzovány praktickými zkušenostmi, ze kterých vyplývá, že nejpravděpodobnější riziko pramení z uplatnění hrozby - systém je dodán, instalován nebo používán způsobem, který není bezpečný.[62]

Čermák[63] upozorňuje na skutečnost častého ztotožnění pojmu riziko a hrozba. Je třeba si však uvědomit, že hrozba může být zdrojem pro jedno nebo více rizik, a že hrozba sama o sobě riziko nepředstavuje. Hrozby pouze zneužívají zranitelnosti vedoucí k ohrožení, což je riziko, které lze snížit prostřednictvím opatření chránící aktiva před působením těchto hrozeb.

Riziko se zjišťuje v procesu, který se nazývá **analýza rizik**. Spočívá v odhalení a definici možných hrozeb a v určení pravděpodobnosti, že určitá hrozba bude prostřednictvím slabin uskutečněna. Výsledkem je souhrn doporučených protiopatření k snížení rizika na minimum. Nepodchycené riziko, které přijímáme, se nazývá zbytkové riziko. Jde o riziko, které se nevyplatí odstínit, protože může způsobit jen velmi malou škodu nebo se vyskytuje jen velmi zřídka. Ochrana proti riziku je zejména otázkou ceny - čím vyšší míra zabezpečení, tím vyšší náklady. Při návrhu vhodných protiopatření je základní otázkou cena chráněného aktiva.[64]

Analýza rizik by se měla provádět pravidelně a vybraná rizika by se měla soustavně monitorovat a přezkoumávat. Dále by měla přinést odpověď na otázku, působení jakých hrozeb je společnost vystavena, jak moc jsou její aktiva vůči těmto hrozbám zranitelná, jak vysoká je pravděpodobnost, že hrozba zneužije určitou zranitelnost a jaký dopad by taková hrozba na společnost mohla mít.[65]

---

[62] ČANDÍK, M. *Informační bezpečnost*. [online]. 2010 [cit. 2016-02-10]. s. 3. Dostupné z: <http://www.cybersecurity.cz/data/candik2.pdf>.

[63] ČERMÁK, M. Analýza rizik. *Clever and Smart*. [online]. 20.05.2010 [cit. 2016-02-27]. Dostupné z: dotupné z: <http://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/>.

[64] POŽÁR, J. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, s. 27.

[65] ČERMÁK, M. Ambicí analýzy rizik není předvídat budoucnost. *Clever and Smart*. [online]. 6.4.2014 [cit. 2016-03-04]. Dostupné z: <http://www.cleverandsmart.cz/ambici-analyzy-rizik-neni-predvidat-budoucnost/>.

6 Opatření pro zvýšení bezpečnosti

6.1 Hesla

Hesla představují jeden ze základních způsobů zabezpečení počítače. Aby heslo mohlo plnit svůj účel, tedy zabezpečit počítač či účty před neoprávněným vniknutím a užíváním, nesmí být jednoduché nebo příliš krátké, nemělo by se opakovat a mělo by být dostatečně často měněno.[66] Zemánek[67] přirovnává hesla k základním pilířům zabezpečení systému. Pokud je heslo prolomeno, je porušena statika a dřív nebo později následuje zhroucení veškeré bezpečnosti.

Zaheslované může být cokoliv od spuštění operačního systému, po různé programy. Hesla by měla chránit přístup do operačního systému a všechna důležitá nastavení v systému. Tato hesla zabrání cizím lidem, kteří překonají vstupní heslo, aby zneužili nastavení systému. Každý, kdo má přístup ke změně nastavení, může drobnými úpravami snížit bezpečnost počítače. Chráněn tak musí být například přístup ke změnám nastavení firewallu, antivirového programu atd. Hesla kromě ochrany před nepovolaným přístupem plní i ochranu proti samotnému uživateli nebo dalším lidem, kteří mají přístup k počítači, aby něco omylem změnili.[68] Analytická společnost **SplashData** vydává každoročně seznam nejhorších hesel. Mezi nejhorší používaná hesla patří například 12345, password, baseball, fotball, abc123 atd.[69]

6.2 Bezpečné používání E-mailu

Kromě užitečných e-mailů se objevují i e-maily s nebezpečných obsahem. Většina nebezpečných e-mailů je dílem virů a červů, které se jejich prostřednictvím šíří, většinou jsou ve zprávě jako příloha. Ve většině případů se připojují jako příloha k nějaké rozumně vypadající zprávě a čekají, až je uživatel spustí.[70] Například v televizním magazínu **@online** uvádí, že až 90% všech e-mailů tvoří viry nebo spam.[71]

---

[66] KRÁL, M. *Bezpečný internet: chraňte sebe i svůj počítač*. Vyd. 1. Praha: Grada Publishing, a.s., 2015. Průvodce (Grada). s. 28 - 29.
[67] ZEMÁNEK, J. *Slabá místa Windows, aneb, Jak se bránit hackerům*. Vyd. 1. Kralice na Hané: Computer Media, 2004. s. 14.
[68] DOSEDĚL, T. *21 základních pravidel počítačové bezpečnosti*. Vyd. 1. Brno: CP Books, 2005. s. 6.
[69] Worst passwords of 2015. *SplashData*. [online]. 19.1.2016 [cit. 2016-03-23]. Dostupné z: <https://www.teamsid.com/worst-passwords-2015/>.
[70] DOSEDĚL, T. *21 základních pravidel počítačové bezpečnosti*. Vyd. 1. Brno: CP Books, 2005, s. 12.
[71] *@online*. TV, ČT 24. 9. 1. 2016. 12:32. Dostupné z: <www.ceskatelevize.cz/ivysilani/10659215431-online/316281381880109/obsah/445364-infografika>.

6.3 Antivirový program

Král[72] se ve své publikaci zmiňuje o antivirovém programu jako o zcela základním programu pro zabezpečení počítače. Správně zvolený a aktualizovaný antivirový program je naprostou nutností a je důležité, aby poskytoval ochranu v reálném čase.

Podle Doseděla[73] se dobrý antivirový program skládá z několika částí. První z nich slouží k provádění kompletních testů celého počítače, tzv. **antivirový skener**, který uživatel využije v případě podezření, že jeho počítač obsahuje nějaký druh škodlivého softwaru. Další částí by měl být **rezidentní štít**, který hlídá soubory otevírané jak z disku, tak z internetu.

Antivirové programy vyhledávají a kontrolují data na základě virové databáze. Od zapnutí počítače jsou spuštěny na pozadí a chrání před útokem viru po celou dobu, kdy počítač pracuje. Kontroluje všechny spuštěné soubory a všechny soubory, které přicházejí a odcházejí z počítače. Tuto činnost většinou uživatel nezaregistruje.

Antivirový program spolehlivě rozpozná pouze ty viry, které zná, a jen ty umí bezpečně, bez poškození souborů odstranit. Jsou proto velmi důležité **aktualizace** virové databáze u antivirového programu, protože denně vzniká množství nových virů a jiného malwaru. Tyto aktualizace zajišťují, že je uživatel chráněn proti nejnovějším hrozbám, které by mohly poškodit počítač. Pokud je uživatel připojen k internetu, aktualizace virové databáze proběhnou automaticky bez nutnosti zásahu uživatele. V případě že se objeví velmi agresivní virus, který se ještě navíc dále vyvíjí, aktualizují výrobci antivirových programů virové databáze i několikrát denně.[74]

Mezi kvalitní antivirové programy patří například **ESET Smart Security**, který nabízí víceúrovňové zabezpečení internetu a plně vyhovuje požadavkům kladeným na podobný software. Poskytuje uživatelům ochranu proti hrozbám, virům a útokům z internetu, přičemž nezatěžuje výkon počítače. Jeho součástí je také antispyware, firewall a antispam.[75]

---

[72] KRÁL, M. *Bezpečný internet: chraňte sebe i svůj počítač*.Vyd. 1. Praha: Grada Publishing, a.s., 2015. Průvodce (Grada). s. 63.
[73] DOSEDĚL, T. *21 základních pravidel počítačové bezpečnosti*. Vyd. 1. Brno: CP Books, 2005. s. 17.
[74] KOCMAN, R. a LOHNISKÝ, J. *Jak se bránit virům, spamu, dialerům a spyware*. Vyd. 1. Brno: CP Books, 2005.s. 16 - 17.
[75] KRÁL, M. *Bezpečný internet: chraňte sebe i svůj počítač*.Vyd. 1. Praha: Grada Publishing, a.s., 2015. Průvodce (Grada). s. 72 - 73.

6.4 Firewall

Firewall je technické či programové vybavení, které slouží jako vstupní brána pro komunikaci mezi sítěmi či mezi počítačem a sítí tak, aby data putující směrem ven a především směrem dovnitř byla bezpečná. Firewall brání zejména před neoprávněnými průniky do sítě. Principem jeho práce je povolení komunikace, kterou považuje za nutnou a potřebnou, přičemž ostatní komunikace je zakázána.[76]

Firewall sleduje nejen příchozí, ale také odchozí komunikaci, tzn. sleduje jaké zprávy se systému odcházejí a kam, protože jejich abnormální počet může signalizovat přítomnost škodlivého softwaru.[77]

Operační systém Windows má v sobě zabudovaný firewall, k jeho nastavení se uživatel dostane pomocí ovládacích panelů, v němž je přehled nastavení firewallu. Kromě firewallu vestavěného ve Windows, může uživatel používat i externí firewall. Uživatel by ale neměl zapomínat, že aktivní firewall může být v počítači pouze jeden, proto je nutné před aktivací externího firewallu deaktivovat vestavěný firewall Windows. Jedním z doporučovaných externích firewallů, je například **ZoneAlarm Free Antivirus + Firewall**. Jedná se software, který pomáhá bránit počítač proti útokům z internetu. Program je velmi jednoduchý a stále běží na pozadí operačního systému. Uživatel si sám může určit, který program má mít přístup k internetu a který ne. V placené verzi navíc dokáže sledovat přijímané emaily a vyhledat nebezpečné přílohy, pracovat s cookies, vyhledat zdroj útoku a obsahuje Anti-Spyware atd.[78] Jak vyplývá z názvu, obsahuje i antivirus, proto není vhodné používat ani jiný antivirový program. Více antivirových programů se nedoporučuje, protože mohou způsobovat vzájemné kolize, vzájemně nesprávné funkce, nestabilitu operačního systému a jiných programů apod.[79]

[76] KRÁL, M. *Bezpečný internet: chraňte sebe i svůj počítač*.Vyd. 1. Praha: Grada Publishing, a.s., 2015. Průvodce (Grada). s. 45.
[77] GÁLA, L, POUR, J. a ŠEDIVÁ, Z. *Podniková informatika*. 2., přeprac. a aktualiz. vyd. Praha: Grada, 2009. Expert (Grada). s. 349.
[78] ZoneAlarm Free Antivirus + Firewall. *Stahuj.centrum.cz.* [online]. [cit. 2016-03-06]. Dostupné z: <http://www.stahuj.centrum.cz/utility_a_ostatni/antiviry/kompletni/zonealarm/>.
[79] KRÁL, M. *Bezpečný internet: chraňte sebe i svůj počítač*. Vyd. 1. Praha: Grada Publishing, a.s., 2015. Průvodce (Grada). s. 48.

6.5 Aktualizace

Všechny programy (operační systém není výjimkou) mohou obsahovat (a také obsahují) chyby. Jak již bylo zmíněno v předešlých kapitolách, bezpečnostních chyb v programech využívá útočník k tomu, aby se dostal dovnitř systému (programy typu červ, trojský kůň atd.).

Výrobci jsou si vědomi toho, že programy obsahují chyby, proto všichni postupně zveřejňují opravy, které tyto chyby napravují. Aktualizace mohou být ve formě **hotfixu** (opravují jednotlivé dílčí problémy), **patche** (záplaty) či **service packu** (servisní balíčky, opravují více problémů najednou). Tato opravná vylepšení dávají výrobci programů k dispozici zdarma prostřednictvím internetu. Většina programů je nastavená tak, že opravy se stahují a instalují automaticky (uživatel je může vypnout, nebo přizpůsobit tak, že se ho zeptá před vlastním stahováním a instalací).[80]

6.6 Anti-spyware

Z předchozích kapitol je zřejmé, že používání firewallu, antivirových programů a aktualizace softwaru je jednou ze základních pravidel ochrany počítače. Bohužel pokud uživatel nemá antivirový program či externí firewall, který obsahuje anti-spyware, není zaručenou ochrana před stažením spywaru nebo adwaru. K tomu slouží speciální detekční software, který pomůže při hledání a odstraňování nežádoucího softwaru z počítače.[81]

Na internetu je dostupná celá řada softwaru na odstranění spywaru. Mezi nejznámější patří například **Spybot - Search & Destroy**. Takový program umožní detekci a odstranění spywaru, adwaru a trojských koňů. Další rozšiřující funkce umožňují vyčistit všechny stopy práce na počítači (dočasné soubory, cookies, historie prohlížečů aj.). Spybot dokáže uživatele ochránit i proti programům zaznamenávajícím stisky kláves aj. Samozřejmostí pro správné fungování je možnost jeho časté aktualizace přes internet.[82]

[80] KRÁL, M. *Bezpečný internet: chraňte sebe i svůj počítač*.Vyd. 1. Praha: Grada Publishing, a.s., 2015. Průvodce (Grada). s. 37.
[81] KOCMAN, R. a LOHNISKÝ, J. *Jak se bránit virům, spamu, dialerům a spyware*. Vyd. 1. Brno: CP Books, 2005.s. 116.
[82] Spybot Search and Destroy. *Stahuj.cz.* [online]. [cit. 2016-03-06]. Dostupné z: <http://www.stahuj.centrum.cz/internet_a_site/bezpecnost/ostatni/spybot-search-and-destroy/>.

6.7 Zálohování

Kromě popisovaných nebezpečí v předchozích kapitolách, která počítači hrozí se může stát mnoho jiných katastrof. Jednou z nejčastějších je fyzická únava materiálu. Počítač je jenom stroj, který může kdykoliv přestat fungovat a všechny komponenty počítače včetně pevných disků, mají určitou životnost. Po jejím uplynutí se například u zmiňovaných disků začnou objevovat chyby v uložených souborech. Další katastrofy mají na starosti přírodní živly, krádeže nebo nehody typu pádu počítače ze stolu na zem (který pevným diskům a informacím na nich uloženým rozhodně nesvědčí). Také se může stát, že uživatel smaže něco, co smazat nechtěl. Všem těmto nepříjemnostem lze samozřejmě do jisté míry předcházet, ne vždy jsou ale preventivní opatření úspěšná nebo efektivní.

Velmi efektivní obranou je vytváření kopií důležitých dat, takzvané **zálohování.** Data, o které nechce uživatel přijít, by měla být v jednom okamžiku minimálně na dvou úložištích (v počítači a například na externím disku). Uživatel nemusí zálohovat celý obsah pevného disku. Programy, které jsou na počítači nainstalované, může snadno obnovit instalací, jiné lze snadno obnovit (stáhnout z internetu atd.). Zálohovat by měl uživatel především vlastnoručně vytvářené soubory.[83]

6.7.1 Zálohováni dat na server - Cloud

Cloudové úložiště je prostor někde na serveru, kam si kdokoliv může ukládat data stejně jako na pevný disk. K nahraným souborům pak můžete přistupovat odkudkoliv, z PC, telefonu, tabletu či webu. Cloudové úložiště je služba, kterou nabízí různí poskytovatelé např. **Google, Microsoft, Dropbox** atd. Základní princip je vždy podobný. Na serverech poskytovatele je vyhrazen prostor určité velikosti, kam může uživatel umístit svoje data. Součástí služby jsou pak různé aplikace (pro PC i mobilní telefony), které umožňují s tímto prostorem pracovat (nahrávat na něj data, synchronizovat je, stahovat atd.). Všechny cloudové služby nabízí nějaký základní prostor zdarma, jeho navýšení je pak placené.[84]

[83] DOSEDĚL, T. *21 základních pravidel počítačové bezpečnosti*. Vyd. 1. Brno: CP Books, 2005. s. 24.
[84] LAŠ, J. Cloudová úložiště. *Android.chaputo.cz* [online]. [cit. 2016-03-06]. Dostupné z: <http://android.chaputo.cz/tema-cloudova-uloziste/>.

6.7.2 Zálohování dat na externí disk

Zálohování dat na externí disk je spolehlivý způsob jak ochránit data před havárií celého počítače. S klesajícími cenami externích disků je tento způsob zálohování dat stále oblíbenější.[85] Mezi velmi spolehlivé a dobře hodnocené externí disky patří například **WD My Passport Ultra**, který má kapacitu 1TB a díky modernímu portu USB 3.0 vysokou přenosovou rychlost (3x vyšší než starší technologie 2.0). Vnitřní části disku jsou navrženy tak, aby odolaly běžným nárazům a všem požadavkům na životnost a spolehlivost při každodenním používání. Pomocí nástroje **WD Security** může uživatel nastavit ochranu heslem a hardwarové šifrování, čímž ochrání soubory před neoprávněným přístupem. Citlivé osobní dokumenty či fotografie budou dosažitelné jen pro uživatele. Disk je navíc dodáván se zálohovacím softwarem **WD SmartWare Pro**. Tento disk navíc umožňuje nejen zálohovat soubory na disk, ale zároveň i do cloudového úložiště služby Dropbox. Data tak budou zálohována hned 2x.[86]

6.7.3 Zálohování dat na flash disk

Pro potřebu zálohy pouze několik jednotek GB dat, bude dostačující variantou flash disk. Bude-li s flash disky uživatel zacházet podle pravidel, jedná se o relativně spolehlivá zálohovací média. Bohužel i přes razantní pokles jejich cen jsou stále pro zálohování poměrně drahé (poměr kapacita/cena). Použitelné tedy pouze pro potřebu zálohy malého množství dat.[87]

6.7.4 Zálohování dat na CD a DVD

Stále ještě používaný způsob zálohování dat. Výhodou tohoto způsobu zálohování je bezpochyby cena, která se pohybuje v desítkách korun za jedno CD/DVD. Samotné zálohování je velmi jednoduché, uživatel zvolí data k zálohování, vypálí co nejnižší rychlostí a pečlivě archivuje. Pokud dodrží pravidla správného skladování (tma, optimální vlhkost, teplota, atd.), mohou zálohy vydržet i několik desítek let.[88]

---

[85] Jak a kam zálohovat data. *Servis PC Kupka.* [online]. 9.11.2015 [cit. 2016-03-06]. Dostupné z: <http://servispckupka.cz/jak_a_kam_zalohovat_kam_zalohovat_data.php>.

[86] WD My Passport Ultra 1TB. *Alza.cz.* [online]. [cit. 2016-03-06]. Dostupné z: <www.alza.cz/western-digital-2-5-my-passport-ultra-1000gb-modry-d435598.htm?catid=18843102>.

[87] Jak a kam zálohovat data. *Servis PC Kupka.* [online]. 9.11.2015 [cit. 2016-03-06]. Dostupné z: <http://servispckupka.cz/jak_a_kam_zalohovat_kam_zalohovat_data.php>.

[88] Způsoby zálohování dat. *Forum.viry.cz.* [online]. 6.12.2007 [cit. 2016-03-06]. Dostupné z: <http://forum.viry.cz/viewtopic.php?t=50012>.

6.8 Anonymita

Požadavkem mnoha uživatelů internetu je možnost anonymního používání webu. V podstatě jde o to, aby o uživateli bylo k dispozici co nejméně údajů, protože při prohlížení stránek na internetu za sebou každý uživatel nechává spoustu informací, jedná se o tzv. **digitální stopu**, především jde o identifikační údaje (IP adresa, host name, informace o operačním systému, údaje o prohlížeči, atd.).[89]

6.8.1 Anonymní režimy v prohlížeči

Je možné využívat tzv. anonymní režimy, které ale neposkytují příliš velkou ochranu. Například prohlížení stránek za pomoci anonymního režimu v prohlížeči Google Chrome nezanechává žádné stopy v historii prohlížeče, v úložišti souborů cookie ani v historii vyhledávání. Všechny stažené soubory a vytvořené záložky však zůstanou zachovány. Anonymní režim Google Chromu ale neskryje aktivitu před zaměstnavatelem, poskytovatelem internetových služeb ani webovými stránkami.[90]

6.8.2 Anonymizace internetového připojení

Jednou z možností, kterou lze zajistit vyšší úroveň soukromí jsou specializované anonymizační služby. Hlavním cílem těch služeb je anonymizace internetového připojení. Zjednodušeně lze říci, že tyto služby fungují jako proxy servery zapojené v řadě za sebou, přičemž konkrétní informace, odkud kam data proudí, mají jen dva po sobě následující servery. Data jsou navíc asymetricky šifrována a v rámci této sítě putuje šum paketů znesnadňující odposlech. Tuto metodu anonymizace využívá například síť TOR (The Onion Router). Po přihlášení do sítě TOR jsou data přenášena přes několik počítačů, takže jsou přeneseny přes několik vrstev a v zašifrované podobě, to přináší velmi dobré anonymizační výsledky.[91] Na jednu stranu je dobré poskytnout uživatelům internetu větší soukromí, ale problémem je, že tyto služby začali využívat i uživatelé pro nelegální činnost. Díky anonymitě lze prakticky obchodovat s čímkoliv. Např. zmiňovaný TOR je výborný nástroj pro činnost hackerů, protože zůstávají v naprosté anonymitě.[92]

---

[89] KRÁL, M. *Bezpečný internet: chraňte sebe i svůj počítač*.Vyd. 1. Praha: Grada Publishing, a.s., 2015. Průvodce (Grada). s. 163.

[90] Soukromé prohlížení v anonymním režimu. *Support.google.cz.* [online]. [cit. 2016-03-07]. Dostupné z: <https://support.google.com/chrome/answer/95464?p=incognito&rd=1#incognito>.

[91] KRÁL, M. *Bezpečný internet: chraňte sebe i svůj počítač*.Vyd. 1. Praha: Grada Publishing, a.s., 2015. Průvodce (Grada). s. 165.

[92] KAPLAN J. TOR – totálně anonymní internet. *Ekontech.cz.* [online]. 7.4.2015 [cit. 2016-03-07]. Dostupné z: <http://www.ekontech.cz/clanek/tor-totalne-anonymni-internet>.

7 Hrozby v kyberprostoru

Informační technologie nabízejí svým uživatelům stále více možností efektivní a rychlé výměny dat, zároveň ale poskytují značné výhody i těm, kteří chtějí kyberprostor zneužívat k nelegálním činnostem. Anonymita a prostorová neuchopitelnost internetu způsobují, že se stále větší a větší část kriminálních aktivit přesouvá právě do kybernetického prostoru, který útočníkům umožňuje rychlé a snadné splnění jejich cílů s minimálním rizikem případného postihu.

Kybernetické útoky spolu s **kybernetickou kriminalitou** patří mezi významné hrozby současnosti, už jenom kvůli tomu, že zahrnují širokou škálu negativních jevů různého stupně škodlivosti, ke kterým dochází v kyberprostoru - od hackerství, crackingu či DDoS útoků, přes stále častější internetové podvody, krádeže a další formy kriminálních či nežádoucích aktivit, až po projevy extremismu a zneužívání internetu k teroristickým aktivitám a propagandě.[93]

Mezi další vážnou hrozbu v kyberprostoru patří **kyberterorismus**, jedná se o teroristické aktivity, které jsou realizované v kyberprostoru. Boj proti kyberterorismu se v poslední době stává prioritou demokratických států i mezinárodních společností.

7.1 Kybernetické útoky

Mezi nejčastější kybernetické hrozby patří **kybernetické útoky**, které jsou stále významnějším nebezpečím jak pro podnikání, tak pro běžné uživatele. Mezi nejčetnější kybernetické útoky v dnešní době patří defacementy a DoS útoky, následkem takovýchto útoků je ve většině případů nedostupnost internetové služby nebo stránky.

Kybernetické útoky stály minulý rok celosvětově firmy 315 miliard dolarů. Nejedná se jen o náklady ve finančním smyslu, ale také o vážné poškození pověsti společností, napadený byl přitom každý šestý podnik. Navzdory mediálně známým případům narušení bezpečnosti a stále častějším hackerským útokům se téměř polovina firem nadále vystavuje riziku tím, že nemají žádnou komplexní strategii pro prevenci digitální trestné činnosti.[94]

[93] Bezpečnostní hrozby. *Ministerstvo vnitra České republiky*. [online]. 7.5.2014 [cit. 2016-03-07]. Dostupné z : <www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09Mw%3D%3D>.

[94] Bezpečnost - Kybernetické útoky. *Novinky.cz*. [online]. 6.11.2015 [cit. 2016-02-09]. Dostupné z: <http://www.novinky.cz/internet-a-pc/bezpecnost/385662-kyberneticke-utoky-staly-firmy-za-posledni-rok-315-miliard-dolaru.html>.

7.1.1 Defacement

Defacement neboli znetvoření, přetvoření webových stránek, je označovaný také jako internetové graffiti nebo webový vandalismus. Zjednodušeně řečeno lze říci, že se jedná o jakýkoli neautorizovaný zásah do vzhledu webové stránky. Defacement je technika hackerů, která má za cíl nahrazení originálních webových stránek jiným obsahem. Útoky tohoto typu jsou nebezpečné v případě, když podvržená stránka má stejný nebo téměř stejný vzhled jako původní stránka. Takový útok je většinou určen k získání důvěrných údajů jako jsou například přihlašovací údaje, čísla kreditních karet atd.[95] Některé formy defacementu mohou zahrnovat vložení škodlivého kódu s úmyslem infikovat počítače návštěvníků. Takto znetvořené stránky jsou schopné nejen způsobit nepříjemnosti firmě, nebo organizaci provozující webovou stránku, ale také poškodit jejich návštěvníky.[96]

7.1.2 DoS a DDoS útoky

Zkratka DoS znamená "**Denial of Service**", tento termín se dá přeložit jako odepření či odmítnutí služby nebo též zablokování služeb. Jeho cílem je způsobit nedostupnost poskytované služby. Většinou jde o útok proti softwarové serverové službě, který má za následek přetížení serverového procesu či celého serveru. Takže dojde k přerušení v poskytování služeb. Nejčastějším druhem tohoto útoku je zahlcení serveru velkým množstvím požadavků v krátkém časovém rozmezí, dalším druhem může být např. využití chyby v serverovém softwaru, která způsobí zastavení serverového procesu či jeho nadměrné zatížení pomocí nekorektně formulovaného či příliš velkého požadavku.

Modifikací DoS je "**Distributed Denial of Service**" (DDoS), při tomto útoku je použito velké množství různých počítačů. Útočník nejdřív musí získat co největší počet klientů, tj. proniknout do velkého počtu počítačů a aktivovat v nich proces, který čeká na pokyny útočníka a poté začnou vysílat požadavky na cílový serverů. Takové počítače se označují jako "zombie". Výhodou pro útočníka je fakt, že je velmi obtížné vystopovat zdroj útoku.[97]

---

[95] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 1. vyd. Praha: Grada, 2007, s. 136.
[96] What Is Website Defacement?. *WebSitePulse.com.* [online]. 5.3.2013 [cit. 2016-03-13]. Dostupné z: <http://www.websitepulse.com/blog/what-is-website-defacement>.
[97] POŽÁR, J. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, s. 50.

7.2 Kybernetická kriminalita

Kybernetická kriminalita, označovaná v angličtině jako "**cybercrime**", může zjednodušeně řečeno znamenat jakýkoliv čin směřující k narušení nebo zneužití počítače nebo počítačového systému a informací, které obsahuje.[98]

Termínem kybernetická kriminalita se označují trestné činy proti počítačům nebo trestné činy páchané prostřednictvím počítačů. Obecně ji lze definovat jako trestné činy mířené proti integritě, dostupnosti a utajení počítačových systémů nebo trestné činy při nichž je použito informačních technologií. Někteří autoři definují kybernetickou kriminalitu jako veškeré aktivity, které vedou k neautorizovanému čtení, manipulaci, vymazání či zneužití dat.

Kybernetickou kriminalitu lze definovat jako trestnou činnost, v níž nějakým způsobem figuruje počítač (chápaný jako souhrn technického a programového vybavení, včetně dat) nebo pouze některé jeho části, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět trestné činnosti nebo jako její nástroj. Počítače v podstatě neumožňují páchat novou trestnou činnost, poskytují jen novou technologii a nové způsoby páchání již známých trestných činů, jako je sabotáž, neoprávněné užívání cizí věci anebo špionáž.

Z hlediska kybernetické kriminality jsou nejnebezpečnější skupinou hackeři, kteří do počítačových sítí pronikají profesionálně. Svoje proniknutí do systému většinou maskují tím, že do počítačového systému infikují viry. Někteří pronikají do systému za cílem narušit systém či získat informace, aby dokázali svou nadřazenost v systému, jiní kopírují údaje a prodávají je tomu, kdo zaplatí nejvíce.[99]

Problémem kybernetické kriminality je fakt, že zapojení počítačů do světových sítí umožňuje útok na počítačový systém odkudkoliv. Tato skutečnost značně ztěžuje případné stíhání a dopadení pachatelů.

[98] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 1. vyd. Praha: Grada, 2007, s. 91.
[99] POŽÁR, J. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, s. 129.

V trestním zákoně **č. 140/1961 Sb.** byl **§ 257a**, který byl do trestního zákona přidán zákonem **č. 557/1991 Sb.** Tento paragraf přímo popisoval to, co by se dalo nazvat jako počítačová kriminalita.

§ 257a Poškození a zneužití záznamu na nosiči informací.

(1) Kdo získá přístup k nosiči informací a v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch

a) takových informací neoprávněně užije,
b) informace zničí, poškodí, změní nebo učiní neupotřebitelnými, nebo
c) učiní zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení.[100]

Pro naplnění skutkové podstaty trestného činu poškození a zneužití záznamu na nosiči informací musel tedy pachatel získat přístup k nosiči informací, ať už oprávněný nebo neoprávněný. Dále zde musí být nějaké další jednání, např. neoprávněné užití informací nebo jejich zničení či poškození nebo zásah do technického či programového vybavení v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch. Objekt tohoto trestného činu lze popsat jako ochranu softwaru i hardwaru. Jedná se tedy o ochranu dat uložených na nosiči informací proti neoprávněnému užívání, změnám nebo zničení a ochranu počítače nebo jiných telekomunikačních zařízení před neoprávněnými zásahy.

Nový trestní zákoník **č. 40/2009 Sb**. je rozsáhlejší, co se popisu postihovaných aktivit týče. Původní § 257a trestního zákona nahradil § 230 postihující neoprávněný přístup k počítačovému systému nebo nosiči informací a § 231, který postihuje opatření a přechovávání přístupového zařízení, hesla k počítačovému systému a jiných takových dat. Přibyl i postih za nedbalostní jednání uvedený v § 232.

[100] ČESKO. Úplné znění zákona č. 140/1961 Sb., trestní zákon, jak vyplývá z pozdějších předpisů. In *Sbírka zákonů, Česká republika*. 2002, částka 146, s. 8093. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3965>. ISSN: 1211-1244.

Na rozdíl od zákona **č. 140/1961 Sb.**, trestní zákoník **č. 40/2009 Sb.** vychází pojmově, pokud se týče počítačové kriminality, z **Úmluvy o počítačové kriminalitě**, schválené výborem ministrů Rady Evropy v roce 2001. České republika tuto Úmluvu podepsala v roce 2005 a ratifikovala v roce 2013.[101]

Cílem Úmluvy je vytvořit mezinárodní právní rámec pro účinné potírání počítačové kriminality prostřednictvím harmonizace prvků skutkových podstat v oblasti počítačové kriminality, za účelem zajištění adekvátního postihu pachatelů, stanovení nezbytných vnitrostátních vyšetřovacích pravomocí pro zajišťování důkazů v elektronické formě a vyšetřování počítačové kriminality, jakož i zavedení pohotového a efektivního režimu mezinárodní spolupráce ve vztahu k trestným činům souvisejícím s informačními technologiemi.[102]

Bohužel ani tato Úmluva neobsahuje přesnou definici počítačové kriminality jako takové, ale pouze souhrn činností, které musí členské státy stíhat jako trestný čin. Tato jednání jsou rozdělena v Úmluvě na trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů (jde především o aktivity jako nezákonný přístup, nezákonný odposlech, zasahování do dat nebo systému, zneužití zařízení), trestné činy související s počítačem (padělání pomocí počítače, počítačové podvody), trestné činy související s obsahem (dětská pornografie) a trestné činy týkající se porušení autorského práva. Všechna výše uvedená jednání bylo možné stíhat již dle současného českého trestního zákoníku a účinnost Úmluvy v tomto ohledu pro české občany žádnou významnější změnu neznamenala.[103]

[101] FILIPOVÁ K. Česká republika po osmi letech ratifikovala Úmluvu o počítačové kriminalitě. *Právní rádce.cz*. [online]. 29.8.2013 [cit. 2016-03-11]. Dostupné z: <http://pravniradce.ihned.cz/c1-60516560-ceska-republika-po-osmi-letech-ratifikovala-umluvu-o-pocitacove-kriminalite>.

[102] Úmluva o počítačové kriminalitě, Budapešť. Úmluva byla přijata Výborem ministrů Rady Evropy na jeho 109. zasedání dne 8. 11. 2001 a následně byla dne 23. 11. 2001 v Budapešti otevřena k podpisu., v platnost vstoupila 1. července 2004. Česká republika podepsala v roce 2005. Dostupné také z WWW: http://www.psp.cz/sqw/text/orig2.sqw?idd=139511.

[103] Zahradníček J. Počítačová kriminalita: Mezinárodní úmluva je konečně závazná i pro Česko. *Advokátní kancelář Kocián Šolc Balaštík*. [online]. 4.8.2014 [cit. 2016-03-12]. Dostupné z: <http://www.ksb.cz/cs/novinky-publikace/clanky/2577_pocitacova-kriminalita-mezinarodni-umluva-je-konecne-zavazna-i-pro-cesko>.

7.2.1 Paragrafy zabývající se kybernetickou kriminalitou

Tato kapitola se zaměřuje na samotný trestní zákoník **č. 40/2009 Sb.** Jsou zde popsány důležité paragrafy, které se týkají kybernetické kriminality.

§ 182 Porušení tajemství dopravovaných zpráv

(1) Kdo úmyslně poruší tajemství

a) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá,

b) neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data,

§ 183 Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí

(1) Kdo neoprávněně poruší tajemství listiny nebo jiné písemnosti, fotografie, filmu nebo jiného záznamu, počítačových dat anebo jiného dokumentu uchovávaného v soukromí jiného tím, že je zveřejní, zpřístupní třetí osobě nebo je jiným způsobem použije.[104]

Pokud jde o popis postihovaných aktivit v § 182 a § 183, jedná se především o úmyslné aktivity, spojené s porušováním tajemství dopravovaných zpráv a listin či dokumentů uchovávaných v soukromí. Tyto paragrafy postihují aktivity spojené s pasivními útoky, které jsou realizované např. sledováním (odposlechem), nebo monitorováním sítě, zaměřené na získávání dat a informací z informačního systému.

[104] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In *Sbírka zákonů, Česká republika*. 2009, částka 11, s. 394. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5405>.

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací.

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,
b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,
c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo
d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat.[105]

§ 230 je zaměřen na ochranu informací uložených v počítačovém systému. První odstavec normy upravuje postih překonání bezpečnostních opatření a současně neoprávněného přístupu k počítačovému systému. V tomto případě pro naplnění skutkové podstaty stačí "hacknout" počítač a nemusí ani udělat nic navíc, např. manipulovat s informacemi uloženými v počítači.[106] Tento paragraf postihuje tedy i útoky tzv. hrubou silou, kdy pachatel přes speciální program zkouší možná hesla, dokud nepřijde na správnou kombinaci.[107]

[105] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In *Sbírka zákonů, Česká republika*. 2009, částka 11, s. 406. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5405>.
[106] SOKOL T. Postih počítačové kriminality podle nového trestního zákona. *Právní rádce.cz* [online]. 22.7.2009 [cit. 2016-03-09]. Dostupné z: <http://pravniradce.ihned.cz/c1-37865090-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona>.
[107] POŽÁR, J. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, s. 115.

V druhém odstavci jsou popsané další aktivity hackera nebo toho, kdo získal přístup k počítačovému systému. Není uvedeno, zda přístup musel získat neoprávněně, tedy naplněním skutkové podstaty v odstavci 1 a nebo zda jde o uživatele, který má k systému legální přístup. Podstatné je, že tato osoba naplní některou skutkovou podstatu uvedenou v písmenech a) - d). Ve třetím odstavci je uvedeno, že přísnější trest čeká toho, kdo některé z jednání uvedených v odstavci 1 a 2 spáchal proto, aby tím jinému způsobil škodu nebo sobě získal prospěch či omezil neoprávněně funkčnost systému.

§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo

b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části.[108]

K naplnění skutkové podstaty tohoto trestného činu není zapotřebí získat přístup k informačnímu systému a manipulovat s daty uloženými v tomto systému. Stačí pokud někdo přechovává nebo si opatří výše uvedené, v úmyslu spáchat trestný čin neoprávněného přístupu k počítačovému systému. Je důležité zmínit, že norma nepostihuje jen osobu, která si v daném úmyslu opatří nebo přechovává zmíněné, ale i takové, které něco takového vyrobí, uvedou do oběhu, dovezou, vyvezou, nabízejí, zprostředkují nebo prodávají, což výrazně zvětšuje okruh zakázaných aktivit.

[108] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In *Sbírka zákonů, Česká republika*. 2009, částka 11, s. 407. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5405>.

Již zmíněné paragrafy týkající se počítačových systémů postihovaly výhradně úmyslné delikty, v následujícím paragrafu může být postihována i hrubá nedbalost. V tomto směru jde trestněprávní úprava v České republice nad rámec toho, co je vyžadováno Úmluvou. Důvodem je možnost značného ohrožení při nedbalém nakládání s počítačovými systémy, které jsou dnes součástí každého odvětví lidské činnosti a na jejich bezchybném provozu závisí majetek, zdraví i životy osob.[109]

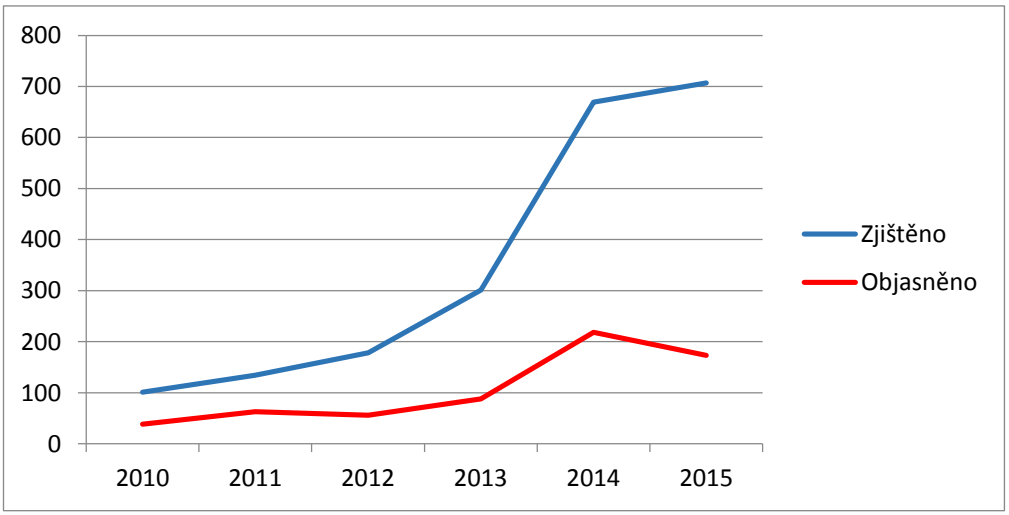
§ 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

(1) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení, funkce nebo uložené podle zákona nebo smluvně převzaté

a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo

b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat, a tím způsobí na cizím majetku značnou škodu.[110]

Graf č. 1 Pošk. a zneuž. záz. na nos. infor. § 230, 231, 232 v letech 2010 - 2015[111]



[109] SOKOL T. Postih počítačové kriminality podle nového trestního zákona. *Právní rádce.cz* [online]. 22.7.2009 [cit. 2016-03-09]. Dostupné z: <http://pravniradce.ihned.cz/c1-37865090-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona>.

[110] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In *Sbírka zákonů, Česká republika*. 2009, částka 11, s. 407. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5405>.

[111] Zdroj: Statistiky kriminality. *Policie České republiky*. [online]. [cit. 2016-03-22]. Dostupné z: <http://www.policie.cz/statistiky-kriminalita.aspx>.

Z grafu je zřejmé, že poškození a zneužití záznamu na nosiči informací je aktuální hrozba a díky rozvoji informačních technologií je stále četnější. Objasněnost tohoto druhu trestného činu je sotva poloviční, a to hlavně kvůli anonymitě internetu, díky které je obtížné odhalit a potrestat pachatele. Dále je zajímavý vývoj škod, způsobený tímto druhem trestné činnosti, v letech 2010-2012 byla finanční ztráta nulová, ale od roku 2013 se škoda začala projevovat i na finančních ztrátách, v roce 2014 byla škoda způsobená těmito trestnými činy téměř 16 mil. Kč. a v roce 2015 více než 12 mil. Kč.

§ 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi

(1) Kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi.[112]

Mezi nejčastější případy porušování autorských práv patří kopírování díla. Specifické pro prostředí internetu je vznik kopií děl při běžném provozu a bez vědomí autora. Klasickým porušením autorského zákona je neoprávněné šíření díla, zejména pomocí internetu (warez).[113]

[112] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In *Sbírka zákonů, Česká republika*. 2009, částka 11, s. 416. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5405>.
[113] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, s. 101.

7.3 Kyberterorismus

Pojem kyberterorismus je nejčastěji definován jako souhrnný název pro teroristické aktivity v kyberprostoru. Obecně je kyberterorismus chápán jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich uložených, za účelem zastrašit, donutit vládu nebo obyvatele k podporování sociálních či politických cílů. I když je tato definice velmi přesná, opomíná fakt, který doprovází veškeré teroristické aktivity v kyberprostoru a tím je psychologický moment napadení sítě jakýmkoli způsobem. Tento efekt, dostatečně znásobený hrozbami a jinými metodami psychologické války, může vést k tomu, že uvnitř napadené strany vyvolá takovou míru strachu, která sekundárně povede k významným fyzickým, ekonomickým nebo jiným škodám značného rozsahu. Kvůli tomuto sekundárnímu efektu je vlastně vedeno velké množství útoků.[114]

Kyberterorismus je možné definovat jako zneužití počítačových technologií proti osobám či majetku, za účelem vyvolání strachu nebo vydírání a vymáhání ústupků, zaměřené proti vládním institucím nebo civilní populaci, případně proti jejich segmentům, pro podporu politických, sociálních, ekonomickým, případně jiných cílů, zaměřené na informační systémy používané cílovým objektem.

Značné možnosti k uplatnění kyberterorismu poskytuje právě prostředí internetu. Umožňuje teroristickým skupinám i jednotlivcům rychlou a utajenou výměnu informací, poskytuje prostor pro šíření jejich ideologií a názorů, umožňuje získávání nových aktivistů i sympatizantů. V jiných případech se internet stává bránou k průniku do počítačových sítí a poskytuje tak příležitosti k vedení kyberteroristických operací.

Boj proti kyberterorismu je díky neustálému vývoji informačních a komunikačních technologií velmi obtížný. Proto je nezbytné se neustále vzdělávat v takových oblastech jako je ochrana dat, informační bezpečnost atd. Toto vzdělání by mělo směřovat nejen na informační specialisty, ale i na politiky, manažery a zaměstnance firem a státních organizací.[115]

[114] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, s. 130 - 131.
[115] POŽÁR, J. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, s. 152 - 153 a 156.

8 Typy protiprávního jednání

V této kapitole jsou vybrány a popsány pouze některé druhy nejčastěji páchané nelegální činnosti v kyberprostoru. Prokazování a klasifikace nelegální činnosti je většinou velmi obtížná. Proto se autor v této kapitole aspoň pokusil co nejlépe popsat u jednotlivých jednání, zda jsou v rozporu se zákonem a zda se jedná o trestný čin.

8.1 HACKING

Podle Hlavenky[116] lze hacking definovat jako nestandardní použití systému či aplikace, při němž uživatel uplatňuje neobvyklé funkce systému a může tak využít některých jeho jinak nepřístupných funkcí.

Dále například Jirovský[117] definuje hacking jako proniknutí do počítačového systému jinou než standardní cestou při obejití nebo prolomení jeho bezpečnostní ochrany. Dále podle Jirovského u hackingu lze jenom těžko vyčíslit škodu, která byla způsobena (zejména proto, že k žádné ani dojít nemusí). Správce systému ani nemusí vědět, že hacker do systému pronikl. Motivací původních hackerů nebylo působení škody, ale pouze radost z osobního vítězství nad technikou, spolu se získaným uznáním od hackerské komunity.

Je jasné, že ne všechny hackerské činnosti jsou legální. Najít ale právní úpravu, která by postihovala hacking jako takový je velmi obtížné. V první řadě by se mohlo jednat o porušení ústavou garantovaných základních lidských práv a svobod. Zde se bude jednat především o **článek 7 odstavec 1**, který pojednává o nedotknutelnosti osoby a jejího soukromí, která může být omezena jen v případech stanovených zákonem, dále se bude jednat o **článek 13**, ve kterém je výslovně zakázáno porušování listovního tajemství a tajemství jiných záznamů, ať již uchovaných v soukromí nebo zaslaných jiným způsobem, také se v tomto článku zaručuje tajemství zpráv podávaných telefonem nebo jiným zařízením.[118]

[116] HLAVENKA, J. *Výkladový slovník výpočetní techniky a komunikací*. 3. vyd. Praha: Computer Press, c1997. s. 179.
[117] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, s. 102.
[118] ČESKO. Listina základních práv a svobod: In *Sbírka zákonů, Česká republika*. 1992, částka 1, s. 18-19. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=22426>. ISSN 1211-1244.

Jednání hackerů dále naplňuje skutkovou podstatu **§ 230** trestního zákoníku. V tomto případě stačí, když hacker překoná bezpečnostní opatření, čímž získá přístup k počítačovému systému. Pokud by ho po získání přístupu do systému ještě neoprávněně užíval, mazal nebo poškodil data uložená v počítačovém systému, byl by poté přísněji trestán. Hacker může naplnit i skutkovou podstatu v **§ 231**, pokud by vytvořil nebo někomu opatřil počítačový program, pomocí něhož by získal neoprávněný přístup k počítačovému systému. Mohlo by se jednat např. o tzv. prolamovače hesel.

8.2 WAREZ

Warez, neboli výroba a rozšiřování pirátského software, označován také jako moderní počítačové pirátství, je stále více využíváno díky rozmachu informačních technologií a internetu. Warez scéna je velmi dobře organizovaná, kterou tvoří uzavřená komunita lidí, její členové jsou z celého světa a mnohdy se osobně nikdy nepotkají. Většinou se tedy jedná o skupinovou záležitost, kdy jedna skupina pracuje na odstraňování ochran proti kopírování a nelegálnímu spouštění (cracker), zatímco druhá část se specializuje na jejich šíření přes tzv. warezová fóra, která slouží zejména k šíření cracků, tedy programů umožňující zrušení ochrany u různých programů, čímž umožňují využívání plné verze programu, filmů, hudby atd.

Aktivity warez scény jsou vesměs ilegální, ve většině případů se jedná se o porušování autorských práv, na které se vztahuje **§ 270**, a tak logickou reakcí je aktivita represivních složek projevující se proti členům warez scény. Vzhledem k povaze a dokonalé organizaci warez scény to ale není vůbec jednoduché. Uzavřenost skupin a jejich globální působnost znesnadňuje jak získávání důkazů, tak i možnosti reakce orgánů činných v trestním řízení. Zásahy proti warez scéně jsou proto dlouho připravované a rozsáhlé. Mezi takovou akci patřila operace FastLink, která byla spuštěna 22. 4. 2004 v deseti evropských státech a USA. Tato akce trvala cca 24 hodin a za tuto dobu bylo identifikováno přibližně 100 osob a zajištěno bylo 200 počítačů z čehož bylo 30 serverů obsahujících pirátský software v hodnotě téměř 50 milionů dolarů.[119]

[119] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, s. 73 - 74 a 105 - 106.

8.3 CRACKING

Cracking (z angličtiny crack - lámat), tedy prolamování nebo obcházení ochranných prvků programů s cílem jejich neoprávněného používání. Cracking je často používán při průniku do systému, kde cílem není zprovoznění programu chráněného softwarovým klíčem, ale zjištění informací důležitých pro umožnění neoprávněného přístupu do cílového systému. Nejčastěji se jedná o tzv. "password cracking", kde jde především o zjišťování hesla pro přístup do systému. Password cracking má mnoho technik, mezi nejčastější patří snaha odhalit heslo pomocí slovníku nejčastěji používaných hesel, použití hrubé síly při zkoušení možných kombinací znaků až po složité algoritmy snažící se o sestavení odpovídající kombinace znaků hesla.[120]

Požár[121] popisuje crackera jako člověka, který se z programů snaží odstraňovat ochrany, aby bylo možné program nelegálně šířit. Může se jednat o finanční motivaci nebo také soutěž. Cracker, který dokáže jako první odstranit nějakou novou komplikovanou ochranu, se v jeho komunitě stává uznávaným a respektovaným.

Podle Havelky[122] lze crackera definovat jako osobu využívající některých nedokonalostí nebo nestandardních funkcí systému (programu, aplikace) k neoprávněnému pronikání do jeho jinak nepřístupných částí, a to za účelem zneužití takto zpřístupněných informací (zcizení, modifikace, vymazání).

Trestní klasifikace tohoto činu může mít více podob. Ve většině případů se jedná o porušení autorského práva **§ 270** nebo porušení neoprávněného přístupu k počítačovému systému a nosiči informací **§ 230**, kde se bude jednat především o neoprávněné užití dat z počítačového systému a jejich následného padělání.[123]

[120] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, s. 106.
[121] POŽÁR, J. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, s. 117.
[122] HLAVENKA, J. *Výkladový slovník výpočetní techniky a komunikací*. 3. vyd. Praha: Computer Press, c1997. s. 92.
[123] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In *Sbírka zákonů, Česká republika*. 2009, částka 11, s. 406 a 417. Dostupné z : <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5405>.

8.4 PHISHING

V překladu toto slovo připomíná "rybaření". Phishing je ve skutečnosti složeninou výrazů "pheaking" a "fishing". Zatímco "fishing" opravdu znamená rybolov, tedy chytání na návnadu, tak "pheaking" je slovo odvozené od "phone freaking", toto slovní spojení se dá přeložit jako nabourávání do telefonních systémů, které kdysi bývalo populární hlavně v USA.[124] Jedná se o podvodnou techniku sloužící k získání údajů uživatele. Útočník vyžaduje po uživateli pod nejrůznějšími záminkami sdělení citlivých údajů (přihlašovací údaje, hesla, PINy ke kartám, bankovní údaje atd.), formou přímé odpovědi (emailem, sms atd.), nebo formou přesměrování na falešné stránky, které vypadají obsahově a graficky stejně jako originál, jsou ale umístěné na jiné internetové adrese. Útočníci se snaží získáním citlivých informací obohatit a to buď prodejem těchto informací nebo je sami zneužijí.

Mezi nejčastější formu phisingu patří rozesílání podvodných e-mailů, vytvářejících dojem, že se jedná o zprávu z důvěryhodné a známé instituce, většinou takový e-mail obsahuje i odkaz na podvodné stránky, které mohou být vizuálně přesnou kopií originálních stránek. Nic netušící uživatel pak do takových stránek zadá své citlivé údaje. Pod odkazem, který e-mail obsahuje, se může také skrývat nebezpečný malware nebo trojský kůň, takový program pak umožní útočníkovi získat citlivé informace (např. sledováním stisknutých kláves).

Základní ochranou proti metodám phishingu je zdravý selský rozum. Žádná instituce, a už vůbec ne bankovní, by po svém klientovi nežádala přihlašovací údaje po e-mailu. Doručené podezřelé emaily by měl uživatel ignorovat a neklikat na žádné odkazy v takovém e-mailu. V případě falešných stránek by uživatel měl použít ruční zadávání adresy přímo do adresního řádku prohlížeče.[125]

Phishing naplňuje skutkovou podstatu trestného činu podvodu podle § 209 trestního zákona. Trestný čin bude dokonán poté, co se útočník obohatí uvedením někoho v omyl a způsobí tím na cizím majetku škodu nikoliv nepatrnou.

---

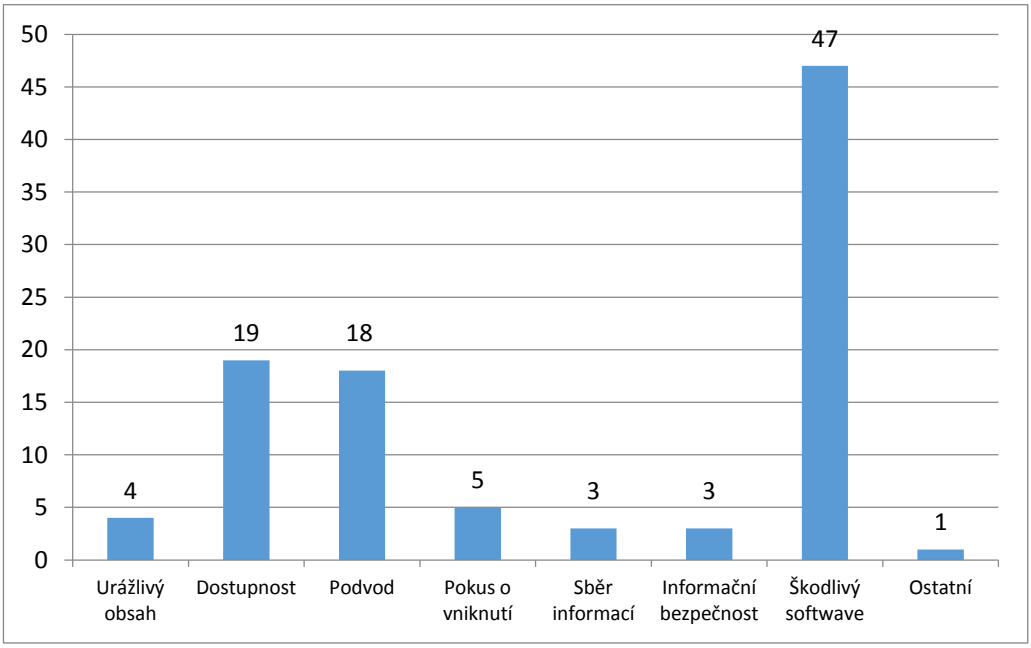
[124] PETROWSKI, T. *Bezpečí na internetu pro všechny*. Vyd. 1. Překlad Tomáš Kurka. Liberec: Dialog, 2014. s. 41 - 42.

[125] PHISHING - stále aktuální hrozba. *Národní centrum kybernetické bezpečnosti*. [online]. 9.10.2013 [cit. 2016-03-21]. Dostupné z WWW: <http://www.govcert.cz/cs/informacni-servis/hrozby/phishing---stale-aktualni-hrozba/>.

9 Nejčastějších typů útoků v ČR v letech 2013 - 2015

Následující grafy znázorňují incidenty, které byly v letech 2013 a 2014 řešeny pracovníky Národního centra kybernetické bezpečnosti ČR.

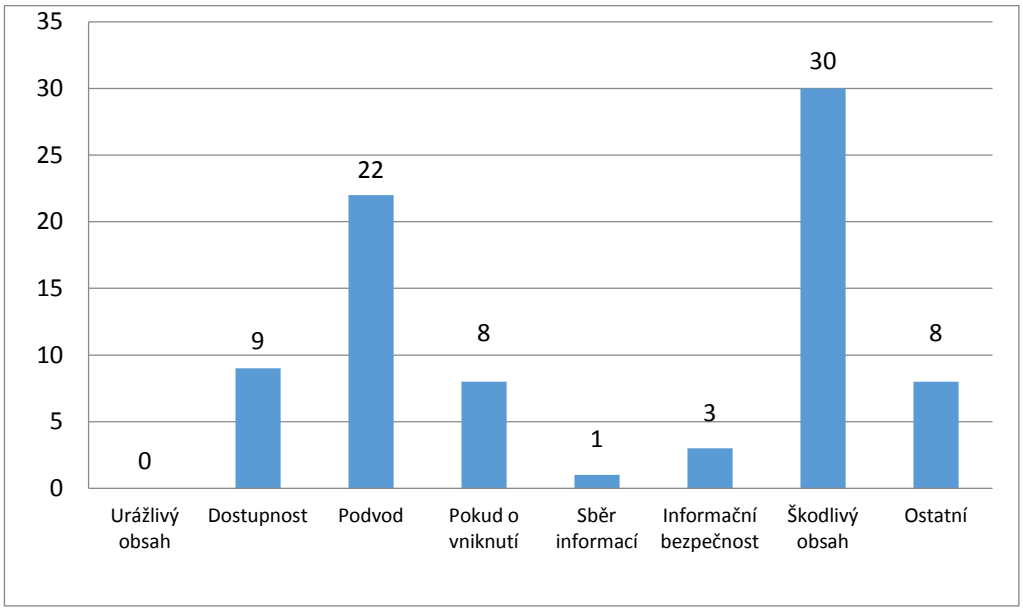
Graf č. 2. Klasifikace incidentů za rok 2013[126]



Mezi nejčastější typy útoků v roce 2013 lze zařadit phishing a DDoS. Většina těchto má za cíl státní organizace nebo organizace s velkým počtem zaměstnanců, případně zákazníků, kde je velká pravděpodobnost, že některý z uživatelů vyzradí tajné informace nebo se nakazí škodlivým softwarem, který umožní útočníkovi získat pro něj užitečné informace. Tyto informace lze následně zpeněžit na černém trhu nebo využít je k dalším útokům. V takových případech je proto důležitá informovanost nejenom zaměstnanců, ale i široké veřejnosti. Důležité jsou také správné sestavená a jedinečná hesla, aby nedocházelo k případům, kdy uživatel má k dvěma různým účtům stejné heslo.[127]

[126] Zdroj: Zpráva o stavu kybernetické bezpečnosti ČR - 2013. *Národní centrum kybernetické bezpečnosti*. [cit. 2016-03-22]. s. 20. Dostupné z: < http://www.govcert.cz/download/nodeid-598/>.
[127] Zdroj: Zpráva o stavu kybernetické bezpečnosti ČR - 2013. *Národní centrum kybernetické bezpečnosti*. [cit. 2016-03-22]. s. 19. Dostupné z: <http://www.govcert.cz/download/nodeid-612/>.

Graf č. 3. Klasifikace incidentů za rok 2014[128]



Po porovnání grafů za rok 2013 a 2014 lze konstatovat, že se charakter útoků páchaných v těchto letech příliš nelišil. Obecně stále platí, že v četnosti útoků je nejvýznamnější phishing. I když se jejich pachatelé snaží používat stále nové a sofistikovanější metody, podstatou útoků zůstává vylákat od uživatelů přístupová hesla, případně distribuovat nebezpečný kód, který útočníkům zajistí přísun užitečných informací. Motivem takových podvodných e-mailů je zpravidla finanční zisk. Rok 2014 je také dokladem dalšího nebezpečného jevu stále častěji se vyskytujícího v kybernetickém prostoru - použití špionážního malwaru. Množství takovýchto škodlivých kódů bylo použito jak proti cílům v Rusku, tak proti Spojeným státům nebo zemím EU. Obvykle se jedná o složitý a sofistikovaný malware navržený ke krádeži důvěrných a citlivých informací státních, vojenských či výzkumných institucí.[129] Pro rok 2015 v tuto chvíli není ještě dostupný graf, který by zobrazoval počet incidentů, které byly zpracovány pracovníky Národního centra kybernetické bezpečnosti ČR. Zatím jsou dostupné pouze měsíční výpisy bezpečnostních incidentů, z kterých je zřejmé, že ani v roce 2015 se charakter útoků příliš nelišil. Jednalo se především o phishing a škodlivý obsah, a to i prostřednictvím sociální sítě Facebook. Mezi nejznámější incident v roce 2015, patřilo napadení účtu premiéra Bohuslava Sobotky na síti Twitter. Hackeři na něm zveřejňovali provolání proti uprchlíkům a vyzývali k bojům proti demokratickým elitám s odkazy na extrémistické webové stránky.

[128] Zdroj: Zpráva o stavu kybernetické bezpečnosti ČR - 2014. *Národní centrum kybernetické bezpečnosti*..[cit. 2016-03-22]. s. 34. Dostupné z: <http://www.govcert.cz/download/nodeid-612/>.
[129] Zdroj: Zpráva o stavu kybernetické bezpečnosti ČR - 2014. *Národní centrum kybernetické bezpečnosti*. [cit. 2016-03-22]. s. 33. Dostupné z: <http://www.govcert.cz/download/nodeid-612/>.

Závěr

Cílem bakalářské práce je definovat pojem počítačová a informační bezpečnost, popsat bezpečnostní hrozby a navrhnout opatření ke zvýšení bezpečnosti. Autor by chtěl zdůraznit, že v této práci nejsou vyčerpány všechny varianty bezpečnostních hrozeb a bezpečnostních opatření, vybral si především takové, o kterých se zmiňuje více autorů a popisují je ve svých publikacích. V práci se autor také zaměřil na hrozby a typy protiprávního jednání v kyberprostoru. Autor se v těchto kapitolách zaměřil především na kybernetickou kriminalitu a její popis pomocí legislativních dokumentů. Pro naplnění cíle této práce autor vycházel především z odborné literatury, ale také z internetových zdrojů a legislativních dokumentu.

Po porovnání bezpečnostních hrozeb je těžké určit, která hrozba je nejnebezpečnější, škody značného rozsahu můžou napáchat hrozby přírodního původu, technické závady, úmyslné i neúmyslné. Každý musí k hrozbám přistupovat individuálně a vycházet z rizika konkrétní hrozby pro něj, nebo jeho organizaci. Hrozba sama o sobě riziko nepředstavuje, ale může se stát rizikem díky využití zranitelnosti. Taková rizika by se měla zjišťovat v procesu, který se nazývá analýza rizik. Výsledkem by pak měl být souhrn doporučených opatření ke snížení rizika. Na druhou stranu bezpečnostní opatření by neměl podceňovat nikdo a měl by je využívat každý, kdo chce minimalizovat případné škody způsobené bezpečnostní incidentem. Především se jedná o používání dostatečně silných hesel, bezpečné používání e-mailu, kvalitní a aktualizovaný antivirus a firewall, aktualizovaný systém, časté zálohování či anonymní používání internetu.

Po analýze hrozeb v kyberprostoru autor dospěl k závěru, že mezi významné hrozby současnosti patří kybernetické útoky, kybernetická kriminalita a kyberterorismus. Autor se spíše zaměřil na kybernetickou kriminalitu, kterou popsal pomocí legislativních dokumentů. Informační technologie mají mnoho možností využití a bohužel k nim patří i nelegální činnost. Autor se proto v závěru práce rozhodl popsat a definovat pomocí legislativních dokumentů nejčastější nelegální činnosti v kyberprostoru. Poté autor porovnal nejčastější typy útoků v ČR za roky 2013 a 2015 pomocí grafů a měsíčních výpisů bezpečnostních incidentů Národního centra kybernetické kriminality a dospěl k závěru, že charakter útoků se moc nelišil a mezi nejčetnější útoky v těchto letech patřil phishing, DDoS a škodlivý software.

Seznam použitých zdrojů

Literární zdroje

1. DOSEDĚL, T. *21 základních pravidel počítačové bezpečnosti*. Vyd. 1. Brno: CP Books, 2005. 52 s. ISBN 80-251-0574-1.
2. DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.
3. DRUCKER, P. *Postkapitalistická společnost*. Praha: Management Press, 1994. 197 s. ISBN 80-85603-31-4.
4. ERBSCHLOE, M. *Trojans, worms, and spyware: a computer security professional's guide to malicious code*. Burlington: Elsevier Butterworth Heinemann, 2005. 232 s. ISBN 0-7506-7848-8.
5. HANÁČEK, P, Staudek Jan. *Bezpečnost informačních systémů. Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. 1. vyd. Praha: Úřad pro státní informační systém, 2000, 127 s. ISBN 80-238-5400-3.
6. HLAVENKA, J. *Výkladový slovník výpočetní techniky a komunikací*. 3. vyd. Praha: Computer Press, c1997. 452 s. ISBN 80-7226-023-5.
7. HOWARD, M. a LEBLANC, D. *Bezpečný kód*: *techniky a strategie tvorby bezpečných webových aplikací*. Vyd. 1. Brno: Computer Press, 895 s. ISBN 978-80-251-2050-7.
8. JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 1. vyd. Praha: Grada, 2007. 284 s. bezpečný internet ISBN 978-80-247-1561-2.
9. KOCMAN, R. a LOHNISKÝ, J. *Jak se bránit virům, spamu, dialerům a spyware*. Vyd.1. Brno: CP Books, 2005. 148 s. ISBN 80-251-0793-0.
10. KRÁL, M. *Bezpečný internet: chraňte sebe i svůj počítač*. Vyd. 1. Praha: Grada Publishing, a.s., 2015. Průvodce (Grada). 184 s. ISBN 978-80-247-5453-6.
11. PETROWSKI, T. *Bezpečí na internetu pro všechny*. Vyd. 1. Překlad Tomáš Kurka. Liberec: Dialog, 2014. 244 s. ISBN 978-80-7424-066-9.
12. POŽÁR, J. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007. 219 s. ISBN 978-80-7251-250-8.

13. VACCA, J. R. *Computer and information security handbook*. Second edition. Amsterdam: Morgan Kaufmann, an imprint of Elsevier, 2013. 928 s. ISBN: 978-0-12-374354-1.
14. ZEMÁNEK, J. *Slabá místa Windows, aneb, Jak se bránit hackerům*. Vyd. 1. Kralice na Hané: Computer Media, 2004. 154 s. ISBN 80-86686-11-6.

Elektronické zdroje

1. Bezpečnost - Kybernetické útoky. *Novinky.cz.* [online]. 6.11.2015 [cit. 2016-02-09]. Dostupné z WWW: <http://www.novinky.cz/internet-a-pc/bezpecnost/385662-kyberneticke-utoky-staly-firmy-za-posledni-rok-315-miliard-dolaru.html>.
2. Bezpečnostní hrozby. *Ministerstvo vnitra České republiky*. [online]. 7.5.2014 [cit. 2016-03-07]. Dostupné z WWW: <www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09Mw%3D%3D>.
3. ČANDÍK, M. *Informační bezpečnost*. [online]. 2010 [cit. 2016-02-10]. s. 3. Dostupné z: <http://www.cybersecurity.cz/data/candik2.pdf>.
4. ČERMÁK, M. Ambicí analýzy rizik není předvídat budoucnost. *Clever and Smart*. [online]. 6.4.2014 [cit. 2016-03-04]. Dostupné z WWW: <http://www.cleverandsmart.cz/ambici-analyzy-rizik-neni-predvidat-budoucnost/>.
5. ČERMÁK, M. Analýza rizik. *Clever and Smart*. [online]. 20.05.2010 [cit. 2016-02-27]. Dostupné z: dotupné z WWW: <http://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/>.
6. ČERMÁK, M. Bezpečnostní opatření. *Clever and Smart*. [online]. 18.11.2012 [cit. 2016-02-27]. Dostupné z WWW: <http://www.cleverandsmart.cz/snizuje-bezpecnostni-opatreni-hrozbu-zranitelnost-nebo-dopad/>.
7. ČERMÁK, M. Mýty informační bezpečnosti. *Clever and Smart*. [online]. 24.04.2012 [cit. 2016-02-27]. Dostupné z: <http://www.cleverandsmart.cz/myty-informacni-bezpecnosti-aneb-proc-vetsina-firem-zije-v-bludu/>.
8. FILIPOVÁ, K. Česká republika po osmi letech ratifikovala Úmluvu o počítačové kriminalitě. *Právní rádce.cz*. [online]. 29.8.2013 [cit. 2016-03-11]. Dostupné z WWW: <http://pravniradce.ihned.cz/c1-60516560-ceska-republika-po-osmi-letech-ratifikovala-umluvu-o-pocitacove-kriminalite>.
9. CHLUP, M. BEZPEČNOST ICT. *Český institut informační bezpečnosti*. [online]. [cit. 2016-02-07]. Dostupné z: http:<//www.cimib.cz/ors/fileadmin/user_upload/dokumenty/CIMIB_Bezpecnost_ICT.pdf>.

10. Informace. *Management mania*. [online]. 23.05.2013 [cit. 2016-02-22]. Dostupné z WWW: <https://managementmania.com/cs/informace>.
11. Informační bezpečnost. *Management mania*. [online]. 09.07.2015 [cit. 2016-02-09]. Dostupné z: <https://managementmania.com/cs/informacni-bezpecnost>.
12. Informační servis. *Národní centrum kybernetické bezpečnosti*. [online]. 25.05.2015 [cit. 2016-02-08]. Dostupné z WWW: <https://www.govcert.cz /cs/informacni-servis/akce-a-udalosti/>.
13. Jak a kam zálohovat data. *Servis PC Kupka*. [online]. 9.11.2015 [cit. 2016-03-06]. Dostupné z WWW: <http://servispckupka.cz/jak_a_kam_zalohovat_kam_ zalohovat_data.php>.
14. KAPLAN, J. TOR – totálně anonymní internet. *Ekontech.cz*. [online]. 7.4.2015 [cit. 2016-03-07]. Dostupné z WWW: <http://www.ekontech.cz/clanek/tor-totalne-anonymni-internet>.
15. LAŠ, J. Cloudová úložiště. *Android.chaputo.cz* [online]. [cit. 2016-03-06]. Dostupné z WWW: <http://android.chaputo.cz/tema-cloudova-uloziste/>.
16. MATYSKA, L. Bezpečnost na Internetu. *Zpravodaj ÚVT MU*. [online]. 2002 [cit. 2016-02-28]. Dostupné z WWW: <http://webserver.ics.muni.cz/bulletin/ articles/242.html>
17. Počítačová bezpečnost. *Management mania* [online]. 12.01.2016 [cit. 2016-02-06]. Dostupné z: <https://managementmania.com/cs/pocitacova-bezpecnost>.
18. Počítačová bezpečnost. *Management mania*. [online]. 12.01.2016 [cit. 2016-02-06]. Dostupné z: <https://managementmania.com/cs/pocitacova-bezpecnost>.
19. RYCHNOVSKÝ, L. Počítačová bezpečnost. *Zpravodaj ÚVT MU* [online]. 2005 [cit. 2016-02-07]. Dostupné z : <http://ics.muni.cz/bulletin/articles/342.html>.
20. SOKOL, T. Postih počítačové kriminality podle nového trestního zákona. *Právní rádce.cz* [online]. 22.7.2009 [cit. 2016-03-09]. Dostupné z WWW: <http://pravniradce.ihned.cz/c1-37865090-postih-pocitacove-kriminality-podle-noveho-trestniho-zakona>.
21. Soukromé prohlížení v anonymním režimu. *Support.google.cz*. [online]. [cit. 2016-03-07]. Dostupné z WWW: <https://support.google.com/chrome/answer/ 95464?p=incognito&rd=1#incognito>.
22. Spybot Search and Destroy. *Stahuj.cz*. [online]. [cit. 2016-03-06]. Dostupné z WWW: <http://www.stahuj.centrum.cz/internet_a_site/bezpecnost/ostatni/spy bot-search-and-destroy/>.

23. SVĚTLÍK, M. Informační bezpečnosti: část 1 - 4, *Softwarové noviny*, 2002, č 2-5, s. 5 - 6. Dostupné z: <http://www.rac.cz/rac/homepage.nsf/CZ/Download/$FILE/inf_bezp.pdf>.
24. TOMEK, M. Lidský faktor v bezpečnosti IS. *System Online*. [online]. 2004 [cit. 2016-02-28]. Dostupné z WWW: <http://www.systemonline.cz/clanky/lidsky-faktor-v-bezpecnosti-is.htm>.
25. WD My Passport Ultra 1TB. *Alza.cz.* [online]. [cit. 2016-03-06]. Dostupné z WWW: <www.alza.cz/western-digital-2-5-my-passport-ultra-1000gb-modry-d435598.htm?catid=18843102>.
26. What Is Website Defacement?. *WebSitePulse.com.* [online]. 5.3.2013 [cit. 2016-03-13]. Dostupné z WWW: <http://www.websitepulse.com/blog/what-is-website-defacement>.
27. Worst passwords of 2015. SplashData. [online]. 19.1.2016 [cit. 2016-03-23]. Dostupné z: <https://www.teamsid.com/worst-passwords-2015/>.
28. ZAHRADNÍČEK J. Počítačová kriminalita: Mezinárodní úmluva je konečně závazná i pro Česko. *Advokátní kancelář Kocián Šolc Balaštík*. [online]. 4.8.2014 [cit. 2016-03-12]. Dostupné z WWW: <http://www.ksb.cz/cs/novinky-publikace/clanky/2577_pocitacova-kriminalita-mezinarodni-umluva-je-konecne-zavazna-i-pro-cesko>.
29. Zákeřný virus I love you napadl před deseti lety desítky miliónů počítačů. *Idnes.cz*. [online]. 3.5.2010 [cit. 2016-03-05]. Dostupné z WWW: <http://www.novinky.cz/internet-a-pc/software/199149-zakerny-virus-i-love-you-napadl-pred-deseti-lety-desitky-milionu-pocitacu.html>.
30. ZoneAlarm Free Antivirus + Firewall. *Stahuj.centrum.cz.* [online]. [cit. 2016-03-06]. Dostupné z WWW: <http://www.stahuj.centrum.cz/utility_a_ostatni/antiviry/kompletni/zonealarm>.
31. Způsoby zálohování dat. *Forum.viry.cz.* [online]. 6.12.2007 [cit. 2016-03-06]. Dostupné z WWW: <http://forum.viry.cz/viewtopic.php?t=50012>.

Legislativní dokumenty

1. ČESKO. Listina základních práv a svobod: In *Sbírka zákonů, Česká republika*. 1992, částka 1, s. 18 - 19. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=22426>. ISSN 1211-1244.
2. ČESKO. Úplné znění zákona č. 140/1961 Sb., trestní zákon, jak vyplývá z pozdějších předpisů. In *Sbírka zákonů, Česká republika*. 2002, částka 146, s. 8093. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3965>. ISSN: 1211-1244.
3. ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In *Sbírka zákonů, Česká republika*. 2009, částka 11, s. 406. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5405>.
4. ČESKO. Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších změn a doplňků: In: *Sbírka zákonů, Česká republika*. 2005, částka 143, s. 7526. Dostupné z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=4741>. ISSN 1211-1244.

Ostatní zdroje

Kromě výše uvedených zdrojů byly při zpracování bakalářské práce využity následující materiály:

- *@online*. TV, ČT 24. 9. 1. 2016. 12:32. Dostupné z: <www.ceskatelevize.cz/ivysilani/10659215431-online/316281381880109/obsah/445364-infografika>.
- Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. *Národní centrum kybernetické bezpečnosti*. 16.02.2015 [cit. 2016-02-09]. Dostupné z: <http://www.govcert.cz/download/nodeid-1004/>.
- Zpráva o stavu kybernetické bezpečnosti ČR - 2013. *Národní centrum kybernetické bezpečnosti*. [cit. 2016-03-22]. Dostupné z: <http://www.govcert.cz/download/nodeid-598/>.
- Zpráva o stavu kybernetické bezpečnosti ČR - 2014. *Národní centrum kybernetické bezpečnosti*. [cit. 2016-03-22]. Dostupné z: <http://www.govcert.cz/download/nodeid-612/>.
- Měsíční výpisy bezpečnostních incidentů Národního centra kybernetické bezpečnosti za rok 2015.

Seznam tabulek a grafů