KYBERKRIMINALITA

Cybercriminality

Bc. Pavel Pokorný

Diplomová práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Pavel Pokorný**
Osobní číslo:	**A14504**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Kyberkriminalita**
Téma anglicky:	**Cybercrime**

Zásady pro vypracování:

1. **Vytvořte literární rešerší na téma kybernetický zločin.**
2. **Specifikujte základní pojmy. Kyberkriminalita versus kyberterorismus.**
3. **Popište typické projevy kybernetického zločinu, výběr cíle, průběh útoku, použité prostředky a závažnost dopadů.**
4. **Věnujte se legálním možnostem ochrany a preventivních opatření.**
5. **Zaměřte se na oblast bankovnictví a prezentujte metody z možných útoků a popište jejich specifika.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **HOWARD, Michael a David LEBLANC. Bezpečný kód: [techniky a strategie tvorby bezpečných webových aplikací]. Vyd. 1. Brno: Computer Press, 2008, 895 s. ISBN 978-80-251-2050-7.**
2. **MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. Hacking bez tajemství. 3. aktualiz. vyd. Brno: Computer Press, 2003, xxiv, 612 s. ISBN 80-7226-948-8**
3. **JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.**
4. **Windows server 2003, kapesní rádce administrátora, William R. Staněk, computer press, ISBN: 80-7226-839-2**
5. **DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 2., aktualiz. vyd. Brno: Computer Press, 542 s. ISBN 978-80-251-2619-6.**

Vedoucí diplomové práce: **doc. Ing. Martin Sysel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **5. února 2016**

Termín odevzdání diplomové práce: **16. května 2016**

Ve Zlíně dne 5. února 2016

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

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato práce se zabývá problematikou kyberkriminality. V teoretické části jsou popsány základní metody útoků v kyberprostoru, jejich kategorizace, používané technologie a možné následky těchto kriminálních činností. Samostatná kapitola je věnována útokům v bankovnictví. V práci jsou uvedeny motivy útočníků, možnosti ochrany a prevence a legislativní opatření. V praktické části diplomové práce je proveden rozbor bankovního malware „HESPERBOT“ a navržena základní bezpečnostní pravidla jako preventivní opatření, kterými by se měli klienti bank řídit.

Klíčová slova: Kyberkriminalita, kyberterorismus, malware, phishing, DoS, BotNet, CSIRT, Anonymous, OWASP, ČNB, ISMS, ISO/IEC 27001, keyloger.

ABSTRACT

This thesis deals with the issue of cybercrime. The theoretical part describes the basic methods of attacks in cyberspace, their categorization, the technology used and the possible consequences of these criminal activities. A separate chapter is devoted to attacks on the banking sector. The paper presents the motives of the attackers, the possibilities for protection and prevention and legislative measures. In the practical part of the thesis is an analysis of banking malware "HESPERBOT" and designed the basic safety rules as a preventive measure, which bank clients should follow.

Keywords: Cybercriminality, cyberterorism, malware, phishing, DoS, BotNet, CSIRT, Anonymous, OWASP, ČNB, ISMS, ISO/IEC 27001, keyloger..

PODĚKOVÁNÍ

Tímto bych chtěl poděkovat vedoucímu mé práce doc. Ing. Martinovi Syslovi, Ph.D. za odborné vedení, cenné rady, věcné připomínky a vstřícnost při konzultacích a vypracování diplomové práce.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Počítač, mobilní telefon, Internet, elektronická data, software, IP adresa. To jsou jen některá ze slov, která ačkoliv se začala používat až ve druhé polovině 20. století, patří dnes, na začátku 21. století, snad k nejvíce skloňovaným. Staly se nedílnou součástí našeho života, stejně jako ostatní prvky informačních a komunikačních technologií (ICT). Staly se našimi pomocníky, pracovními nástroji, předměty každodenního používání. Bez nich si neumíme dnes už život ani představit. Postupem času pronikly do každé sféry našeho života. Pomocí nich ukládáme nejen veškeré informace o nás, ale i naše vzpomínky v podobě digitálních fotografii a filmů. Vše je dnes digitalizované. Noviny, časopisy, televize, stejně tak i hudba a pošta. Digitálně dnes téměř vše vytváříme, zálohujeme, komunikujeme, dokonce se i podepisujeme. Bez prostředků ICT se prostě neobejdeme. Ale stejně tak to, co umíme využít ve prospěch nás všech, umí někteří zneužít i v neprospěch, respektive za účelem prospěchu jedince nebo zájmové skupiny. Od pradávna lidstvo každý vynález a objev dokázalo zneužít k vojenským nebo kriminálním účelům. Ať to byl oheň, pazourek, kolo, či elektřina. Nejinak je tomu i u počítačů a všemu co s nimi souvisí. Již od jejich samých začátků se objevovali jedinci, kteří hledali jejich slabiny. Nikoliv však k jejich zdokonalování, ale k jejich ovládnutí. Z prvních nesmělých pokusů o převzetí kontroly nad některým počítačem nebo systémem se postupem času staly organizované a cílené útoky, a to nejen vůči jedinci, ale dokonce i proti vládám nebo státům. Ruku v ruce se tak objevila vedle počítačů i kybernetická kriminalita. V běžné kriminalitě lze prostředky v jednu chvíli použít jen proti jedinci, případně proti malé skupině lidí. Takovými nástroji může být třeba kámen, nůž nebo jakýkoliv jiný předmět denní potřeby. Rozhodně s těmito předměty ale nemůžeme provést v jednu chvíli útok na velkou skupinu lidí. Aby byl veden útok s dopadem na velkou skupinu, byly by potřeba sofistikovanější zbraně, případně skupina útočníků a hovořilo by se v takovém případě o teroristickém útoku, případně válečném konfliktu. V kybernetickém prostoru je ale všechno jinak. Nejen že nemá pevné hranice, tudíž nelze vždy předem dopředu vědět, kdo všechno bude zasažen. To je typické například u malware. Ale díky globální síti lze z jednoho místa v jednu chvíli a jedním člověkem provést útok na obrovské množství lidí, respektive jejich data, informační technologie, případně jejich prostřednictvím na další elektronické systémy, které jsou jimi ovládané, což může v praxi znamenat například přístupové

systémy budov, ale též i prvky kritické infrastruktury, jako je řízení dopravy, energetické systémy a jiné. V běžném životě je tedy možné a v praxi i právně definováno, co je trestný čin, přečin, přestupek, teroristický útok, či válečný konflikt. Zásadními kritérii jsou zde počet poškozených, způsobená škoda, respektive následky, které se dají zdokumentovat a vyčíslit. Jak již bylo zmíněno, v kybernetickém prostoru je tomu jinak. Počet zasažených obětí, ani množství způsobené škody nelze jednoznačně identifikovat, vyčíslit, natož pak odškodnit. Těžko lze vyčíslit například, jakou ztrátu mají osoby či organizace, kterým byla po nějakou dobu znepřístupněna nějaká služba, nebo jakou hodnotu měla data uložená na jejich mediích. A vzhledem k tomu, že dopady mohou být na velkou skupinu lidí, není zde ani dokonce jednoznačná hranice mezi kyberkriminalitou a kyberterorismem. Některé kriminální činy v kyberprostoru tak mohou být považovány i za teroristický čin. Zablokovat možnost komunikace může být považováno za trestný čin, ale když teroristé zablokují možnosti komunikace v době nějakého fyzického útoku a znemožní tak dorozumívání, volání o pomoc a organizaci záchranného zásahu, je to stále jen trestný čin? Rozšiřování viru může být taky jen neškodná aktivita pro některé chuligány, ale co když je s virem do počítačů rozšiřován škodlivý kód, který pomáhá teroristům získávat informace? Definice terorismu říká, že jeho cílem je vyvolat paniku a strach na civilním obyvatelstvu. Nesplní náhodou tento cíl i správně vymyšlený Hoax, ničivý malware nebo cílený útok na sociální sítě? O kybernetickém útoku na kritickou infrastrukturu ani nemluvě. Koneckonců, jedna z vizí války v budoucnosti je útok na elektronické a komunikační systémy. Proto v kyberprostoru nelze jednoznačně ani rozlišit, zda se jedná o trestný čin nebo terorismus. To, co na první pohled vypadá jako banalita, může mít pro mnoho lidí vážné dopady, a svým způsobem i navodit strach a paniku. Tím spíš, že kybernetický prostor poskytuje útočníkům anonymitu, která jim dodává odvahu a příležitosti. Ve své podstatě nemusí být pomocí ICT ani podniknut žádný útok, stačí, když jejich prostřednictvím dochází k verbování, navádění, radikalizaci a organizaci. I v takovém případě přispívají ICT teroristům a kriminálním živlům v jejich činech.

Cílem této práce je zmapovat, jakými způsoby lze provádět trestné nebo teroristické činy, jejichž cílem jsou ICT nebo činy, které jsou prováděny jejich prostřednictvím a uvést metody, jak se těmto činům bránit, eliminovat následky nebo provádět preventivní opatření. V praktické části bude provedena analýza bankovního malware „HESPERBOT“ a navržena vhodná bezpečnostní opatření a prevence při používání internetového a mobilního bankovnictví.

I. TEORETICKÁ ČÁST

1 KYBERKRIMINALITA VS. KYBERTERORISMUS

1.1 Kyberterorismus

Termín „kyberprostor“ poprvé použil William Gibson v roce 1984 ve své knize Neuromancer [1]. Jeho původní literární definice již v současnosti neplatí. Dnes existují desítky definic tohoto slova, nicméně žádná z nich dosud nebyla uznána za oficiální. Definice TRADOC z roku 2010, označuje kyberprostor jako *„globální doména uvnitř informačního prostředí sestávající se z propojených sítí informačních infrastruktur, včetně internetu, telekomunikačních sítí, počítačových systémů a včleněných procesorů a řídících jednotek"* [2]. Naproti tomu, slovo terorismus má jednoznačnější definice. Na stránkách Ministerstva vnitra české republiky (MVČR) je uvedena tato definice *„Terorismus je plánované, promyšlené a politicky motivované násilí, zaměřené proti nezúčastněným osobám, sloužící k dosažení vytčených cílů.“* [3]

Podle Dorothy E. Denningové *„Kyberterorismus je konvergencí terorismu a kyberprostoru obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaných v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů.“* [4] D. E. Denningová ale pojímá kyberterorismu pouze jako útoky vedené proti kritické infrastruktuře, jejichž cílem je získání informační nadvlády. Podle ní kyberútoky nemají primárně za cíl fyzické zničení objektu. Realita v posledních letech nám však ukazuje jiný směr, kdy většinou dochází k narušení funkcí některé služby nebo její součásti a útok tak není veden proti vládě za určitým konkrétním účelem. Její definice tedy nezahrnuje typické nejčastější formy útoků.

Přesnější definice, zahrnující všechny možné aspekty a varianty kybernetických útoků, cílů a motivací je opět uvedena na stránkách MVČR *„Souhrnný název pro teroristické aktivity, jejichž cílem útoku, použitým prostředkem nebo přenašečem je tzv. „kyberprostor“, neboli jde o teroristické aktivity zaměřené proti a prováděné prostřednictvím počítačové sítě a touto sítí řízených systémů („informační elektronické síťové struktury).“* [5]

1.2 Kyberkriminalita

Kyberkriminalita, neboli informační kriminalita, je nejdynamičtějším typem kriminality současnosti a kybernetické incidenty patří dnes mezi nejzávažnější hrozby pro společnost ve vyspělých zemích. Při značném zjednodušení se kyberkriminalitou rozumí ty formy kriminality, které jako nástroj využívají nebo jako cíl směřují na moderní informační a komunikační technologie. Prioritami v potírání kyberkriminality v České republice je v současné době zejména boj proti dětské pornografii, majetkové trestné činnosti na internetu, porušování autorských práv, aktivitám směřujícím k vylákání zneužitelných osobních údajů [6]

Vzhledem k velice blízkým definicím obou pojmů a nejasné hranici mezi nimi bude pro účely této práce nadále používáno výhradně pojmu kyberkriminalita

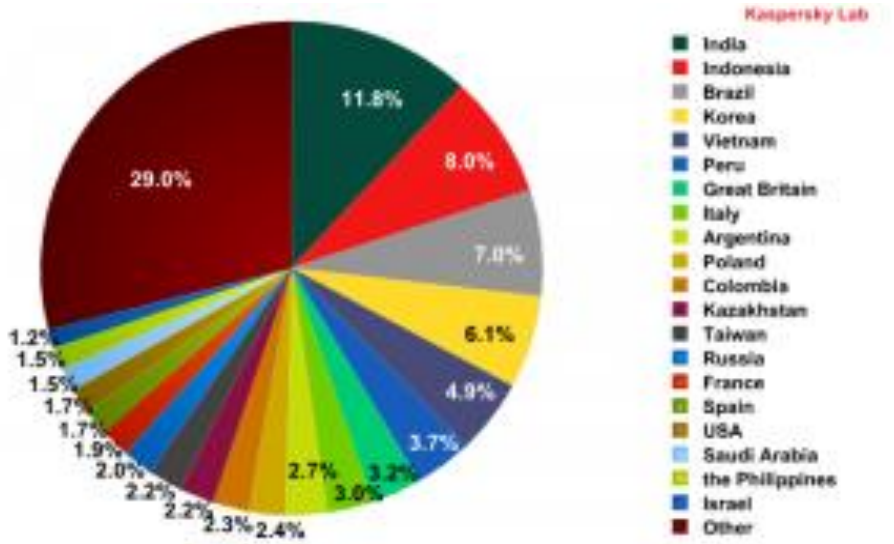
1.3 Co vše je kyberkriminalita

Jak již bylo řečeno v úvodu, je těžké rozlišit, kde jsou hranice mezi kyberkriminalitou a kyberterorismem. Vezmeme-li v úvahu, že neexistuje ani jednoznačná oficiální definice, můžeme zařadit pod tyto pojmy veškeré škodlivé a trestné činnosti, které jsou páchány v kyberprostoru a prostřednictvím ICT. Tímto vyloučíme činy, jež jsou provedeny fyzickým násilím na výpočetní technice nebo fyzickým zcizením nosičů dat.

V této kapitole bude uveden seznam a popis nejběžnějších činů, kterých se útočníci a pachatelé v kyberprostoru dopouštějí.[7]

1.3.1 SPAM

Snad nejméně závažným činem, který se dá zařadit spíše do kategorie „obtěžující“ je spam. Ten v podobě nevyžádané elektronické pošty obtěžuje snad každého uživatele PC a vlastníka emailové schránky. I když se zdá být spamová aktivita nehodna většího zájmu, je potřeba si uvědomit, že obrovské množství spamu zatěžuje přenosové linky, snižuje jejich kapacitu a bere čas jejich příjemcům při jejich probírání a odstraňování.



Obrázek 1: Spam ve světě

(Zdroj: http://svet-hostingu.cz/2012/05/24/podil-spamu-poklesl-a-ceske-e-maily-jsou-pomerne-bezpecne/)

1.3.2 Defacement

Pod tímto pojmem se skrývá pozměňování obsahu webových stránek. Důvody mohou být různé. Běžné vandalství, dokazování si svých schopností, upozornění administrátora na špatné zabezpečení, protesty a projevování názorů.

1.3.3 Porušování autorských práv

Mnoho uživatelů ICT také podceňuje trestné činy páchané na nelegálním používání autorskými právy chráněných dílech. Řeč je v tomto případě převážně o nelegálním používání licencovaného software a multimediálních dílech. Autoři těchto děl a SW přicházejí ročně o milionové zisky. (zde doplnit statistiku). Kromě samotného používání je nelegální i jeho další sdílení a šíření. Díky volně dostupným crackovacím nástrojům je může používat v podstatě kdokoliv. U hudebních a filmových děl není dokonce nutné je ani crackovat. Na tomto místě je vhodné uvést jednu zásadní informaci o které málokterý uživatel torrentových sítí ví. Zapojením do torrentu, a stahováním nějakého „díla“, což samo o sobě nemusí být trestné, dochází současně ale i k jeho sdílení dále, což již trestné je, nebo může být a ne každý uživatel torrentu to zná.

BSA: Evidence případů softwarového pirátství v ČR – statistika obsahuje pouze případy členů BSA

období: 2004–2006

pořadí	kraj	počet případů	škoda (mil. Kč)	podíl (v %)
1.	Praha	78	6,4	25
2.	Jihomoravský	39	0,7	13
3.	Ústecký	37	4,7	12
4.	Středočeský	28	1,5	9
5.	Olomoucký	27	3,2	9
6.	Plzeňský	20	1,9	6
7.	Královéhradecký	17	3,6	5
8.	Jihočeský	11	0,6	4
9.	Pardubický	11	7,3	4
10.	Liberecký	10	1,2	3
11.	Vysočina	10	0,2	3
12.	Moravskoslezský	9	1,0	3
13.	Karlovarský	7	0,4	2
14.	Zlínský	7	0,6	2
CELKEM:		311	33,4 mil. Kč	

Policie ČR: Zjištěné a objasněné případy porušování autorského práva – § 152 trestního zákona

období: 2003–2006

kraj	zjištěno případů	objasněnost (v %)	podíl v %
Praha	824	95	41
Jihomoravský	313	97	16
Severočeský	253	94	13
Středočeský	228	99	11
Západočeský	146	93	7
Severomoravský	92	59	5
Východočeský	80	95	4
Jihočeský	70	97	3
CELKEM:	2006	94	

Obrázek 2: Statistika softwarového pirátství
(Zdroj: http://strategie.e15.cz/prilohy/marketing-magazin/zaplaceni-pokuty-piratsky-software-nelegalizuje-470077)

1.3.4 Kyberšikana

Společensky velmi nebezpečným činem je kyberšikana. Má mnoho forem. Od obtěžování, pronásledování, až po ponižování a zesměšňování. Jde o obdobu fyzické formy. V prostředí ICT však nabývá jiných rozměrů. Díky anonymitě útočníka se stírají fyzické, sociální i věkové rozdíly. K vydírání a obtěžování není zapotřebí převahy nebo skupinového zastání. Takto se mohou dopouštět šikany i jinak neprůbojní a mnohdy i frustrovaní jedinci a to již od mladistvého věku. V některých případech vedly již takovéto útoky i k tragickým následkům, kdy oběti nesnesly míru ponižování a ostudy a spáchaly sebevraždu. Mezi nejznámější takové případy patří vystavování záběrů obětí

v choulostivých situacích na internet. Do této kategorie patří i krádež elektronické identity a vydávání se za někoho jiného.

1.3.5 Zdroj dat pro majetkovou kriminalitu

Důvěra a neopatrnost lidí, obzvláště dětí a seniorů je příčinou uveřejňování informací o sobě a svých blízkých na internetu, převážně sociálních sítí. Ty jsou neuvěřitelným zdrojem informací pro podvodníky všeho druhu. Díky nim tak získávají informace o stylu života, osobního majetku, zvyklostech jedinců i rodin a o jejich přítomnosti či nepřítomnosti v domovech během dovolené. Mají k dispozici podrobné informace o odjezdu na dovolenou, době návratu, mnohdy i o formě zabezpečení majetku a jejich cennostech.

Jiní podvodníci lákají peníze přes internet od lidí prostřednictvím falešných e-shopů, nabízených služeb, inzerátů. I zde hraje velkou roli anonymita. Do podobné kategorie se dají zařadit podvodníci, kteří vydírají peníze například registrováním internetových domén na názvy, které v reálném světě patří jiným vlastníkům, nebo si registrují domény, jejichž název je na první pohled stejný jako název jiné domény, jehož klienty se tak snaží nalákat na jeho falešné stránky.

1.3.6 Malware

Typickým nebezpečím číhajícím na každém kroku v internetu je malware. I ten má mnoho forem. Od virů, jejichž úkolem je poškodit systém nebo data, přes trojany (trojské koně), kteří jsou přenašeči škodlivého kódu, zatímco se tváří jako jiný software a spyware, který získává informace na svém hostiteli a předává je svým tvůrcům až po ransomware, který znepřístupní systém nebo data oběti, kterou následně jeho tvůrce vydírá tím, že požaduje pro obnovení čitelnosti dat finanční obnos. Malware je tak původcem další trestné činnosti, která využívá jeho účinků. Jako příklad lze uvést vybírání bankovních účtů na základě získaných přístupových údajů nebo průmyslovou špionáž. [7] K těmto účelům obvykle slouží keylogger, který zaznamenává stisknuté klávesy a tyto informace předává útočníkovi, který tento nástroj do hostitelského zařízení podstrčil. Tím dokáže zjistit autentizační údaje, jako jsou uživatelská jména, hesla, PIN, atd. Některé formy malware se umí i samy šířit na další zařízení umístěná ve stejné síti.

Obrázek 3: Nárust malware
(Zdroj: http://mobilenet.cz/clanky/mobilni-malware-jiz-dle-avastu-dosahl-1-milionu-vzorku-a-dale-roste-17340)

1.3.7 Blokování služeb

Velmi nebezpečné jsou útoky na různé služby, servery, nebo jejich prostřednictvím na elektronické systémy, jež jsou jimi řízeny. Takové útoky se snaží tyto systémy znepřístupnit, nebo vyřadit z provozu. Takovým typem je třeba DDoS. Při něm je zneužito k útoku velké množství počítačů, jejichž majitelé o této aktivitě nemají tušení. U těchto útoků se může zdát na první pohled účinek bezvýznamný, ale pro mnoho uživatelů je mnohdy daná služba kritická. Navíc, u počítače, který vzdáleně ovládá nějaký útočník k distribuovanému útoku na jiný cíl, je pravděpodobné, že díky instalovanému malware a zapojenému do nějakého BotNETu, je zřejmě využit i k jiným nelegálním účelům.

1.3.8 Ovládnutí serveru/PC

Ovládnutí a převzetí kontroly nad zařízením. V takovém případě útočníci mohou zneužít dat a informací, případně je pozměnit, nebo po nějakou dobu administrovat daný systém dle jejich instrukcí. Variabilita možných scénářů je zde široká. Od krádeže dat, po řízení dopravních systémů nebo bezpečnostních systémů, včetně systémů kritické infrastruktury. I jaderné reaktory v elektrárnách jsou řízeny prostřednictvím ICT. Dalším možným zneužitím může být využití takto ovládaného zařízení pro páchání další trestné činnosti.

„V roce 2010 byl široce diskutován případ útoku Stuxnet. Byl napaden systém odstředivek k obohacování uranu v Íránu pomocí cíleného počítačového viru. V r. 2012 byl kyberútokem postižen německý producent elektřiny 50Hertz Transmission GmbH. V rámci tohoto prvního útoku na evropského provozovatele elektrosítě byly jeho internetové komunikační systémy pro vzdálenou podporu kompletně vyřazeny. Teprve v letošním roce sdělilo Ministerstvo vnitřní bezpečnosti Spojených států amerických (Department of Homeland Security), že tzv. trojan Havex patrně napadl průmyslové řídicí systémy. Bylo oznámeno, že hodlají prověřit 1000 energetických podniků v celé Evropě a Severní Americe na infekci škodlivým kódem. Získávání informací / krádež dat“[8]

Krádež autentizačních údajů, získávání osobních údajů a osobních dat, odposlech komunikace, atd. je společným průvodním jevem mnoha trestných činů. Například vydírání, krádeže duševního vlastnictví, převzetí identity, kyberšikany, bankovních fraudů, atd. Bankovnímu malware je věnována samostatná kapitola č.7.

Všechny tyto odposlechem nebo stažením získané informace, mohou být nejen cílem útočníka nebo prostředkem pro další způsobu útoků, ale též dobrým a ceněným prodejním artiklem.

Existuje velké množství způsobů a metod pro jejich získání. Od sociálního inženýrství, přes malware, keylogery, sniffing, phishing, až po exploity.

1.3.9 Doprovodná a nepřímá kriminalita nebo terorismus

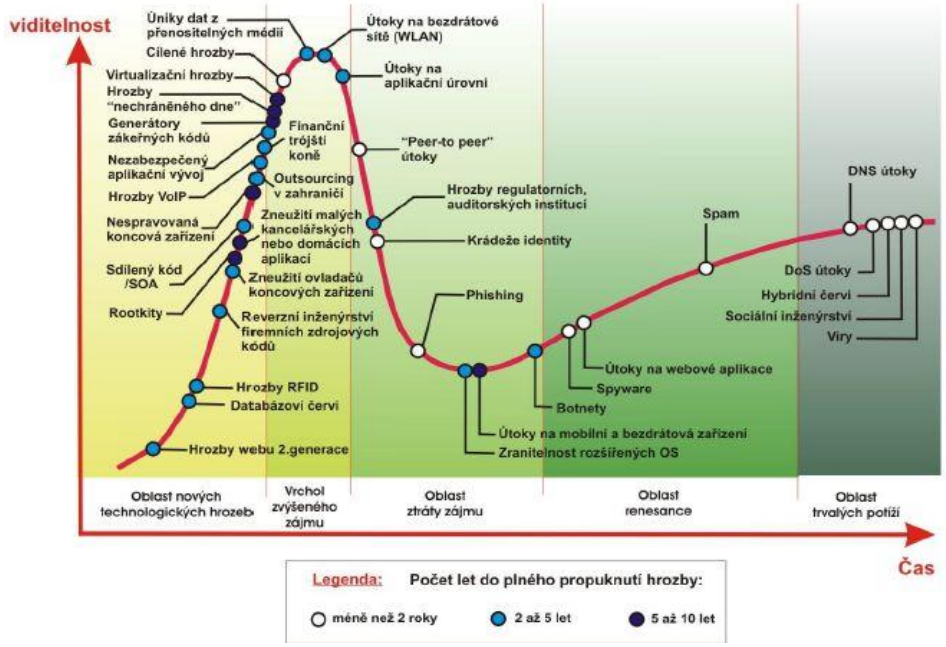
Kybernetické útoky nemusí být pouze hlavním a jediným útokem. Může být použit souběžně s jiným útokem jako podpora hlavního útoku ke zvýšení účinku nebo dopadů. Při bombovém útoku může jít třeba o vyřazení nejbližší BTS či internetové linky. Nebo zasílání dezinformací v době poplachu.

I samotné využívání internetu teroristy či jiných aktivistů a kriminálních živlů k náboru členů, propagaci jejich myšlenek a názorů, k propagaci terorismu, násilí, rasismu, šíření výzev, radikalismu, k organizování a dorozumívání členů při plánování a provádění teroristických činů, je nutno brát v úvahu jako hrozbu ve spojení terorismu a kriminality s kyberprostorem a jeho negativními dopady.

1.3.10 Interní fraudy

Tímto způsobem se označují podvody, které páchají zaměstnanci ve firmách. S rostoucím podílem automatizace a kybernalizace ve firmách, se samozřejmě přesouvá váha těchto činů i do oblasti ICT. Jde především o krádeže dat a informací, poškozování dat či jejich modifikace, nebo jejich zneužívání.

Motivy jsou prosté. V podstatě stejné jako u interních fraudů páchaných před zavedením ICT ve firmě. Hlavními motivy je pomsta nebo osobní zisk. Někdy je možné k těmto motivům počítat i průmyslovou špionáž. Nutno však podotknout, že s nástupem ICT, je mnohdy provedení incidentu jednodušší. Hlavně z důvodu provádění kopii, odposlouchávání, čtení korespondence, přístupu k datům a v neposlední řadě i dostupnosti interních dat z vnějšího prostředí. Zaměstnavatelé dnes v rámci zvýšení efektivity a úspor dávají možnosti vzdáleného přístupu svým zaměstnancům. Tím se rozšiřuje i potencionální okruh útočníků, neboť zneužít takového vzdáleného přístupu tak nemusí jen samotný zaměstnanec, ale i rodinní příslušníci nebo hackeři, kteří mají pod kontrolou jeho domácí PC nebo síť.



Obrázek 4: Vývoj typů kybernetických útoků (zdroj: http://www.internetprovsechny.cz/pocitacova-kriminalita-a-bezpecnost/)

2 KYBERKRIMINALITA V PRAXI

Kyberkriminalita může mít projevy od nenápadné či „neškodné“ aktivity až po obrovské hrozby nebo dopady. S tou mírnější formou se určitě již setkal každý z nás. Například takový SPAM. Otravuje nás, ale většina z nás si na tuto skutečnost již zvykla. Mnohem horší dopady by byly, kdyby se někdo dostal k našim osobním nebo autentizačním údajům. Zde již tyto aktivity hraničí s kriminální činností. Velkým nešvarem sociálních sítí především je týráni či ponižování obětí na základě skryté identity, kterou útočníci využívají díky anonymnímu prostoru zvaném „INTERNET“. Další známou formou kyberkriminality jsou útoky na prostředky ICT. Tady jde především o jejich vyřazení z provozu alespoň na určitou dobu nebo jejich ovládnutí.

Kyberkriminalita je stále na vzestupu. Každým rokem se několikanásobně zvyšuje. Na tiskové konferenci ke dni bezpečnějšího internetu uvedl ministr vnitra Milan Chovanec, že od roku 2011 se zvýšil počet internetových trestných činů trojnásobně. Podle jeho slov bylo v roce 2001, 15 zločinů, v toce 2011 to bylo 1500 zločinů a v roce 2014 již 4300 zločinů. Nejrizikovější skupinou jsou přitom děti a důchodci. V roce 2000 šlo převážně o zločiny porušování autorského práva. V posledních letech se situace změnila a v současnosti jde především o hospodářskou kriminalitu, kyberšikanu nebo šíření dětské pornografie. Přibližně dvě třetiny útoků prostřednictvím internetu cílí na bankovní účty.

2.1 Příklady z praxe

2011

- Hackeři zaútočili na japonskou firmu Mitsubishi Heavy Industries, jež je největším výrobcem zbraní a zbrojních systémů v Japonsku. Ovládli 80 jejich serverů a počítačů. Jejich snahou bylo dostat se k přísně tajným informacím o raketových systémech a ponorkách. [9]
- *Krize ve společnosti SONY se prohlubuje. Firma oznámila, že o osobní data by mohlo přijít až 25 milionů jejích uživatelů. Firma totiž odhalila další masivní útok hackerů na své službyz2012* [10]

2012

- V ČR počítačový pirát nabízel na internetu ke stažení tisíce filmů. Způsobil škodu 80 milionu korun. [11]

2013

- Hacker ovládl v Německu jeden ze serverů firmy Vodafone a ukradl informace o 2 milionech zákazníků [12]
- *Hackeři dnes napadli web UniCredit Bank. Uvedl to server Živě.cz. Útok ale zřejmě nesouvisel se sérií napadení českých webů z minulých dní, byl proveden jiným způsobem. Na rozdíl od předchozích útoků hackeři web nezahltili. Údajně jim pomohlo slabé heslo administrátora stránek, které znělo "Banka123". Na web banky hackeři vyvěsili své prohlášení, stránky vypadly jen na pět minut* [12]
- Španělská policie za pomoci Europolu odhalila skupinu kybernetických útočníků, kteří pomocí ransomware vylákali po svých obětech velké finanční prostředky. V průměru požadovali 100 Eur za to, že stahovali ilegální obsah. Skupina působila ve 30 zemích světa a napadla stovky tisíc obětí. Několik případů se objevilo i v České republice, konkrétně ve zlínském kraji. Hlavou gangu byl 27-letý Rus. [13]

2014

- hackeři ukradli z eBay údaje o všech jeho aktivních uživatelích, což bylo cca 145 milionu uživatelů. [14]

2015

- hackeři zaútočili na providera placené televize, mobilních sítí a internetu, britskou firmu TalkTalk. Útočníci se dostali k datům 4 milionu klientů. Zhostili se nejen kontaktních údajů, jmen a adres, ale i přístupových údajů k bankovním účtům. Hackeři se k činu přihlásili ve jménu „Allaha“. [15]

Toto jsou pouhé střípky případů, které se v české republice a ve světě staly. Jak je z uvedených příkladů vidět, způsoby a motivy mohou být různé. Následující tabulka ukazuje statistiku incidentů, kterou zveřejňuje CSIRT.

	2008	2009	2010	2011	2012	2013	2014	2015	sum
IDS				491	3924	2121	2380	3638	12554
Phishing	65	220	209	144	159	175	368	359	1699
Malware	53	97	42	9	19	44	117	240	621
Spam	47	28	103	26	43	73	159	109	588
Other	1	5	8	62	13	75	101	263	528
Virus		121	178	1	1				301
Trojan	66	6	26	5	5	12	56	90	266
DOS	1	4	2	2	68	72	32	34	215
Probe		3	14	25	12	26	86	42	208
Botnet		3	46	5	8	15		2	79
Portscan	10	4	1	6	1	3	2	5	32
Pharming							18	3	21
Crack	1		4						5
Copyright			1		1				2
sum	244	491	634	776	4254	2616	3319	4785	17119

Obrázek 5: Statistika incidentů
(zdroj: https://www.csirt.cz/files/csirt/statistics/stats.html)

2.2 Typické projevy kyber útoku

Rozpoznat kybernetický útok nemusí být vždy snadné. Jeho projevy mohou být různé. Snahou útočníků je, aby nebyly po určitou dobu rozpoznány. Proto se jednotlivé typy útoků stále vylepšují a i z důvodu edukovatelnosti útočníků se vyvíjí stále nové a sofistikované metody. Mezi ty nejběžnější projevy útoku patří:

- Zatížení procesoru
- Neznámí uživatelé v systému
- Zvýšený sítový provoz
- Snížení volného místa na disku
- Změna webových stránek
- Nedostupnost sítové služby
- Podezřelé či neznámé procesy
- Editace/nepřítomnost logů
- Ztráta dat
- Destabilizace systému

2.3 Průběh útoku

Jak takový běžný útok vypadá? Jaký je jeho nejběžnější průběh? Přestože každý může vypadat jinak, záleží především na formě útoku, i zde se dají vysledovat všeobecné postupy, jež jsou typické pro většinu kybernetických útoků. Obecně lze popsat běžný postup v tomto sledu [16]:

- Sběr informací o cílovém subjektu z veřejných zdrojů
- Sniffing a scanování služeb
- Analýza zjištěných informací a úrovně zabezpečení
- Získání admin přístupu
- Instalace malware
- Zametení stop
- Realizace útoku

2.4 Základní pojmy

- **Bombing** – zahlcování poskytované služby velkým množstvím paketů
- **Defacement** – nahrazení originálních stránek jejich podvrženou variantou
- **DoS** – při tomto útoku je server nebo služba zahlcena velkým množstvím requestů
- **DDoS** – forma DoS útoku prováděna soustředěně z velkého množství stanic
- **MiM** – forma odposlouchávání elektronické komunikace
- **Ransomware** – útok, kdy útočník znepřístupní data jejím majitelům a vyžaduje „výkupné“
- **Sniffing** – útok založený na odposlouchávání paketů
- **Spoofing** – útok založený na falšování identity zdroje
- **Sociální inženýrství** – metoda založená na získávání informací, které jsou následně využity k průniku do systému
- **Malwar**e – souhrnný název pro škodlivý kód. Dělí se na:
    - **Viry** – škodlivý kód likvidující funkce prostředků ICT
    - **Trojské koně** – nosný SW pro infikaci počítačů jiným škodlivým kódem
    - **Adware** – jde o vnucování obtěžující reklamy

    - **Spyware** – SW pro utajené odesílání údajů o uživateli
- **Phishing** – získávání údajů, převážně autentizačních prostřednictvím falešných emailů, webových stránek.
- **Pharming** – metoda přesměrování oběti na podvodnou stránku změnou DNS záznamů
- **Spamming** – metoda zasílání reklamních nebo nevyžádaných zpráv

- **Cracking** – označení metody pro narušení informačního systému zvenčí
- **Cybersquatting/domain grabbing** – zaregistrování doménového jména stejného nebo podobného názvu za účelem záměny za originální doménové jméno
- **Hacking** – narušení bezpečnosti či stability počítačových sítí
- **Phreaking** – bezplatné využívání telefonních linek
- **Phishing** – metody získávání a zneužívání personálních a autentizačních údajů
- **Pharming** – odposlouchávání elektronické komunikace a získávání údajů pomocí změny v DNS záznamech
- **Spam** – nevyžádaná pošta
- **Kyberšikana** – převážně dětí. Cílené útoky, zesměšňování, vyhrožování a zneužívání založené především na anonymitě útočníka a bojácnosti oběti.
    - **Sexting** – šíření textových zpráv, obrázků a videí se sexuální tematikou
    - **Kybergrooming** – zmanipulování osoby a nucení ji k nějakému jednání
    - **Kyberstalking** – pronásledování a obtěžování lidí
- **Warez** – slangové označení pro nelegální nakládání s autorskými díly
- **Malware** – škodlivý kód, sloužící k narušení či ovládnutí funkčnosti a služeb jednotlivých prostředků ICT.
- **Haktivismus – hacking** využívaný k politickým nebo společenským cílům
- **Keyloger** – nástroj sledující stisknuté klávesy
- **Exploit** – nástroj nebo sada příkazů pro využití známé chyby v systému
- **Rootkit** – program, pomocí kterého lze maskovat škodlivý SW v PC
- **Brute force** – útok hrubou silou
- **Backdoor** – škodlivý kód, který umožňuje crackerovi převzít kontrolu nad počítačem
- **Keylogger** – program, který snímá stisknuté klávesy
- **Hoax** – poplašná zpráva

2.5 Rozdělení

Kyberkriminalitu je možné kategorizovat z několika pohledů.

Základní rozdělení vychází přímo z definice kyberkriminality

- **Kriminalita na prostředky ICT** – cílem je napadnout technologie, zařízení a informace. Jejich ovládnutí, zničení, znepřístupnění
- **Kriminalita pomocí prostředků ICT** – cílem jsou uživatelé, nebo technologie a elektronická zařízení ovládaná pomocí ICT nebo služby

Z výše uvedených oblastí je patrné, že kyberkriminalita není jen o tom napadnout informační technologie, získat nad nimi kontrolu či je zničit, ale i o zneužití těchto prostředků proti jedinci či skupině osob. Dle jeho rozsahu a dopadů můžeme kyberkriminalitu rozdělit na:

- **Lokální –** útok na jedince, jednotlivá zařízení nebo konkrétní celky (například organizace)
- **Globální –** útok na neohraničenou skupinu lidí a zařízení. Například nekontrolovatelné šíření virů.

Případně na

- **Zaměřený proti jedinci**
- **Zaměřený na skupinu osob**

V prvním případě by se útok dal kvalifikovat jako kriminální čin, ve druhém případě by mohlo jít již o terorismus v pravém slova smyslu zaměřený na širokou veřejnost.

Podle Jirovského lze rozdělit kyberkriminalitu do 4 základních typů dle hrozeb [7]

- **Únik informace -** je stav, kdy dojde k vyzrazení chráněné informace neautorizovanému subjektu.
- **Narušení integrity -** představuje poškození, změnu, či vymazání dat.
- **Potlačení služby -** znamená úmyslné bránění v přístupu k informacím, aplikacím, či systému. Jde například o útoky typu DoS, DDoS, atd.

- **Nelegitimní použití -** je užití informací neautorizovaným subjektem

Další možností je rozdělit kriminální činy v oblasti kyberprostoru dle její společenské závažnosti.

- **Obtěžující** (například: spam, Defacement)
- **Škodlivé** (například: porušování autorských práv, malware, krádež dat)
- **Nebezpečné** (například: kyberšikana, kyberterorismus, blokace služeb jako DoS, DDoS)

Možné rozdělení se nabízí i podle jejich dopadů. Této problematice je věnována samostatná kapitola č. 4

- **Ekonomické**
- **Politické**
- **Vojenské**
- **Fyzické**
- **Morální**

Kyberkriminalitu, případně kyberterorismus můžeme též rozdělit z pohledu zaměření na:

- **Přímý** – konkrétní útoky na konkrétní cíl
- **Doprovodný** – sem může být zařazen například možnost verbování a propagace pomocí prostředků ICT nebo další činnost na zvýšení účinku hlavního útoku. Viz kapitola 1.3.9

Přičemž dopady mohou být:

- **Primární** – škoda způsobená na samotných datech, ušlý zisk, atd.
- **Sekundární** – následné škody. Například reputační, změna chování, atd.

3 POUŽÍVANÉ TECHNOLOGIE A METODY

Každý útok v kyberprostoru, ať již na prostředky ICT, data nebo jejich majitele, je vedený prostřednictvím jiných prostředků informačních a komunikačních technologií. To znamená, že každý prostředek použitý k útoku se může sám stát cílem útoku. A to bez ohledu na velikost, platformu, použitou technologii nebo výrobce. Kromě původce a cíle může být využit i jako prostředník. V takovém případě většinou o jeho zneužití jeho majitel nemá tušení [16].

3.1 Servery

Servery jsou typickým cílem v oblasti kyberkriminality, případně jeho prostředníkem. Na serverech jsou uložena data, která jsou předmětem zájmu útočníků. Také na nich běží většina poskytovaných služeb, které se snaží útočníci jejich klientům znepřístupnit, proniknout do nich pod jinou identitou nebo pozměnit jejich obsah. Typickými příklady takových útoků, jsou pozměněné webové stránky, zneužití bankovních účtů nebo znepřístupnění služby.

Jako prostředek k útoku se server většinou nepoužívá, jelikož stejnou úlohu plní za nižší cenu obyčejný desktopový počítač nebo laptop. Nicméně existují i případy, ve kterých je nanejvýše vhodné, použít jako prostředek server, a to především v případech, kdy je potřeba využít jeho hardwarového a výpočetního výkonu. Například při lámání hesel.

V mnoha případech je serverů využíváno jako prostředníka. V takovém případě se útočník snaží buďto využít technologii nebo výkon, který nemá sám k dispozici, případně se maskovat tak, aby to vypadalo, že zdrojem útoku je samotný server. Správci se o zneužití jejich serverů dozvídají buď oznámením od obětí nebo zaregistrují tuto událost podezřelým nárůstem výkonu.

3.2 Stanice

Pracovní stanice jsou typickým představitelem všech tří kategorii. Většinu útoků provádí nebo alespoň řídí jejich strůjci právě z pracovních stanic.

Stejně tak bývají velice často cílem útoku. To převážně z důvodu získání dat, která jejich majitelé mají na svých discích uložena a také slouží jako sběr údajů, které jejich majitel zadává. V tomto směru jsou zřejmě nejcennějším zdrojem informací o heslech a jiných autentizačních prvcích.

Velice často bývají pracovní stanice zneužity i jako prostředník. V těchto případech však bývá taková stanice jednou z mnoha, řádově až statisíců, které jsou takto zneužity k rozložení výpočetního výkonu, nebo k distribuovanému útoku, typicky DDoS. Více v kapitole BotNet.

3.3 Mobilní zařízení

Mobilní zařízení jsou mezi uživateli stále více oblíbená. Nejen pro jejich velikost, která majiteli dovoluje mít své zařízení stále u sebe, ale i HW výkony a kapacity dokáží u moderních zařízení směle konkurovat svým desktopovým protějškům. Vzhledem ke své mobilitě umožňují útočníkovi spouštět a řídit svůj útok odkudkoliv, kde existuje nějaké internetové připojení. Takto není závislý na jedné lokalitě, jež by mohla být časem vysledována, naopak mu to umožnuje být v prostředí kyberprostoru více anonymní a hůře vysledovatelný.

Jako cíl útoku se mobilní zařízení stávají předmětem zájmu při odposlechu, a v případě bankovních fraudů jako zdroj zasílaných SMS kódů, použitých při dvou-faktorové autentizaci. [17]

Pod pojem mobilní zařízení se dá zahrnout i další skupina zařízení, u které se ustálil všeobecně používaný pojem „přenosná“ zařízení. Do této kategorie spadají převážně flash disky, USB disky. I ta se používají v rámci kyberkriminality k nekalým účelům. Vzhledem k svému charakteru především jako prostředník pro zanesení malware do počítače.

3.4 Platformy OS

U operačních systémů je situace trochu jiná než u hardware. Zde odpadá kategorie prostředníka a zůstává nám OS jako cíl a OS jako použitá platforma. V obou případech je to však z různých důvodů. U OS použitého jako cíl, se využívá převážně jeho slabin. Naopak u OS použitého jako zdroj se využívá jeho schopností. Nemusí však jít vždy

během útoku o stejnou platformu. Tím je myšleno, že pokud je útok veden například z linuxového stroje, nemusí být jeho cílem jen linuxové koncové stanice.

U cílových operačních systémů využívají útočníci hlavně jejich slabých míst, jako jsou neaktualizované verze systémů, jejich ovladačů, spuštěných služeb, chybné konfigurace, instalovaný SW s bezpečnostními slabinami nebo absence bezpečnostních mechanismů, jako jsou SW firewally, antivirové programy a slabá bezpečnostní pravidla v podobě hesel, uživatelských oprávnění, atd. [18]

OS používaný útočníkem na jeho počítači k programování škodlivého kódu, scriptování a zasílaní instrukcí je otázkou spíše oblíbenosti a sympatie. Velkou míru také hraje dostupnost nástrojů třetích stran pro danou platformu nebo jeho otevřenost pro provádění různých změn a nastavení.

3.5 Sítové prvky

Sítové prvky, na rozdíl od předchozích zařízení, zase mohou být využity buďto jako cíl, nebo prostředník. V případě cíle jde hlavně o jejich zahlcení a odstavení nebo ovládnutí za účelem dalších aktivit, čímž se stávají prostředníkem. V těchto případech jsou využívány hlavně k odposlechu síťové komunikace a získávání informací, případně k přesměrování komunikace na podvržené stránky. Převzetí kontroly nad zařízením je například u firewallu a routerů možné díky nalezeným zranitelnostem nebo nedostatečnému zabezpečení. Někdy umísťují útočníci do sítě i vlastní sítové prvky, které mají ve své správě a pomocí nichž odchytávají síťovou komunikaci nebo ji přesměrovávají. Jsou to typicky nastrčené free WiFi hotspoty, nebo do lan sítě zapojené HUB, které na rozdíl od switch umožňují útočníkovi přesměrovat veškerý provoz přes jeho IP adresu. [19]

3.6 Databáze

Databázové systémy a vlastní databáze jsou vždy jen cílem útočníků. Nikdy nejsou zdrojem útoku nebo prostředníkem. Jako cíl jsou využívány pro svůj obsah dat. A to buď zcizení obsahu nebo jeho pozměnění. Jejich zranitelnost je dána hlavně nedostatečným

zabezpečením nebo špatně napsanou aplikací, která danou databázi využívá. Typickým útokem je SQL injection.[20]

3.7 Bezdrátové technologie

Stejně jako mobilní zařízení jsou oblíbené nejen u legálních uživatelů, ale i útočníků. Obzvláště ve spojení s mobilními prostředky, pro které jsou primárně navrženy, tvoří silný prostředek pro páchání nekalých aktivit v kyberprostoru. Díky nim se útočníci stávají nezávislí na místě a mohou se se svými prostředky přiblížit blíže k cílené skupině.

Stejně tak se stávají i oblíbeným terčem útočníků, kteří převzetím kontroly díky špatnému zabezpečení získávají přístup k veškeré komunikaci, která jimi prochází, jak již bylo popsáno v kapitole 3.5 Síťové prvky. Mezi tyto technologie patří nejen WiFi, ale i Bluetooth, NFC, či radiové technologie.[21] Výhody bezdrátové konektivity jsou vykoupeny nemožností přesného prostorového vyzařování, tudíž jsou náchylné na odposlechy.

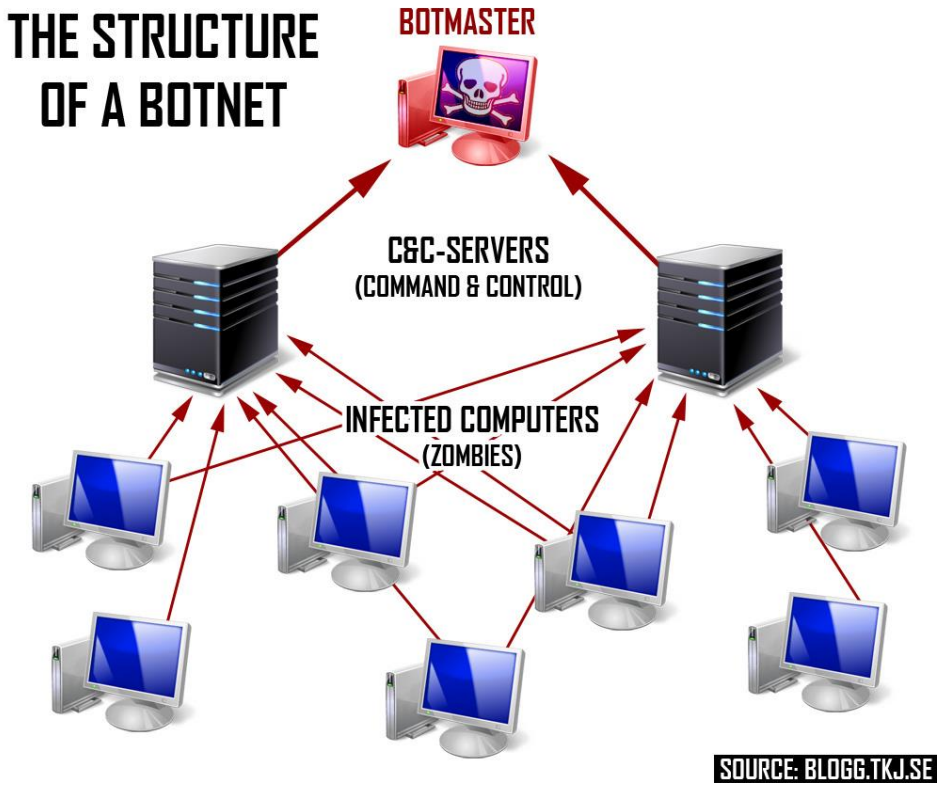
Existuje mnoho dalších technologii a prostředků, které nejsou samy o sobě ani zdrojem, ani cílem útočníků. Jsou spíše prostředníkem, který umožnuje provedený útok vykonat nebo maskovat a zůstat tak v anonymitě. Zde je jeden z nich.

3.8 Botnet

Bot je druh škodlivého kódu, který útočníkovi umožňuje převzít kontrolu nad napadeným počítačem. Boti, kterým se také říká „weboví roboti“, jsou obvykle součástí sítě infikovaných počítačů, tak zvané robotické sítě, která obvykle sestává z napadených počítačů rozptýlených po celém světě (zdroj: http://cz.norton.com/botnet)

Řídícímu počítači se říká command & control server (C&C server). Jeho tvůrce pomocí malware rozšíří agenty na infikované stroje, odkud pak šíří své boty dále. Agenti pak vykonávají pro tvůrce činnosti. Například využívají hostitelských stanic k rozesílání spamu nebo z hostitelských stanic sbírají informace a odesílají je na C&C server. Jejich tvůrci nevyužívají Botnety jen ke svým útokům, ale mnohdy pronajímají své Botnety za finanční

odměnu jiným útočníkům, a to nejen samotný botnet, ale i svoje administrátorské schopnosti. Samozřejmě v takovém případě platí, že čím větší Botnet, tím více se cení.



Obrázek 6: Struktura botnetu
(zdroj: https://www.alienvault.com/blogs/security-essentials/botnet-detection-and-removal-methods-best-practices)

4 HROZBY A NÁSLEDKY

Jak bylo uvedeno v kapitole 1, kybernetických útoků existuje velká řada. Od útoků na osoby, přes data, až po samotný hardware nebo poskytované služby. Podle toho budou vypadat i následky u jednotlivých typů útoků. Dopady mohou být jak na jednotlivé osoby, což je hlavně u cílených personálních útoků, tak mohou postihnout velké skupiny nebo regiony lidí. Dopady a následky nemusí být pouze materiální. V případě útoku na kritickou infrastrukturu může dojít k omezení základních potřeb obyvatel nebo ochromení některé infrastruktury, což může mít pro některé lidi i katastrofální následky. Jako příklad může být uvedeno blokování tísňových linek nebo zablokování dopravního provozu při záchranných operacích. V případě dlouhodobého útoku mohou nastat i sekundární následky, což může být například nedůvěra obyvatelstva ve stát, zajišťovat základní služby a ochranu a mohlo by dojít i na občanské nepokoje. Dlouhodobé výpadky energií, obzvláště elektrické energie by měly za následek nemožnost používání elektronických přístrojů, což by vedlo k zastavení výroby, služeb, zdravotnických výkonů, nemožnosti komunikace, atd. I zde by taková situace vyvolala sekundární následky v podobě rabování, loupeží a jiné trestné činnosti. Při neomezeném kybernetickém boji mohou mít virtuální útoky následky, které jsou reálné, hluboké a dalekosáhlé.[22]

V principu mohou být dopady přímé a nepřímé. Někdy se také označují jako primární a sekundární. V zásadě jde o to, zda byla způsobena nějaká škoda přímo na zasaženém cíli nebo škoda, která vznikla následkem v souvislosti s útokem, nikoliv však na samotném zařízení, datech nebo osobě.

V následujících odstavcích jsou stručně uvedeny dopady rozdělené do základních kategorií:

4.1 Ekonomické

Ekonomické dopady mohou být přímé i nepřímé. Přímé škody mohou být způsobeny například krádeží peněz z bankovních účtů, zničením dat a jejich potřebnou obnovou nebo zablokováním obchodních příležitostí. Nepřímé ekonomické dopady mohou být způsobeny nedůvěrou ve služby i po obnově provozu, potřebou budování záložních center, datových

linek, režimovými opatřeními, atd. Mezi sekundární následky je možné považovat způsobené škody při rabování, krádežích.

4.2 Politické

Jak již bylo uvedeno v úvodu této kapitoly, politické důsledky mohou mít sekundární dopady způsobené nedůvěrou obyvatel ve schopnost zajistit základní potřeby a ochranu. Primární politické důsledky budou v případě napadení serverů a stránek politických stran, vyzrazení jejich interních informací nebo předvolebních internetových propagacích.

4.3 Fyzické

Primární fyzické dopady jsou hlavně na zdraví a životě lidí, závislých na elektronických systémech, nebo lidí v případě ohrožení. Sekundární následky mohou být vyvolány jednáním a chováním lidí v krajních situacích.

4.4 Vojenské

Tento druh dopadů je velmi závažný. Může nejen způsobit ochromení vojenských systémů a tím schopnosti jednat, ale také může ovládnutím vojenských systémů a jejich nepovoleným použitím vyvolat ozbrojené konflikty nebo způsobit škody na zasaženém území. Nepřímým dopadem může být třeba politické napětí mezi dvěma státy nebo vyhrožování použitím síly v případech, kdy může jít i o nedorozumění. Takovými případy mohou být třeba útoky vedené na státní infrastrukturu, výzvědné služby, ozbrojené složky, u nichž není znám jejich původce a může tak snadno dojít k mylným podezíráním nevinných subjektů.

4.5 Morální

Morální úpadek by nastal v situaci, kdy by byly blokovány energetické a zásobovací systémy, jako elektrárny, plynárny, vodárny, zásobování potravinami, atd.

Morální dopad mají i různé propagační a náborové aktivity extrémistů, náboženských nebo protináboženských hnutí a celkově řečeno, jakákoliv masová propagace nemorálních činů, kterou Internet umožňuje. Nejen, že dokáže oslovit širokou veřejnost, ale i ponechat původce v anonymitě.

Na závěr této kapitoly je nutno uvést, že ne všechny dopady musí být hned zřejmé a ne všechny lze finančně vyčíslit. Takovými dopady mohou být ztracené životy, zničené důkazy, poškození autorských práv a jiné. Také nelze vždy u kybernetických útoků zjistit celkový rozsah. Napadeny mohou být systémy, které nebyly primárním cílem, nebo třeba není možné zjistit počty nakažených stanic některým virem.

Obrázek 7: Ilustrační obrázek kybernetické kriminality (zdroj: http://www.internetprovsechny.cz/pocitacova-kriminalita-a-bezpecnost/)

5 ÚTOČNÍCI

Rozdělení útočníků je možné provést z několika hledisek. Například podle jejich motivu, počítačové odbornosti, nebo organizovanosti. Vždy záleží na úhlu pohledu, momentální situaci, použité taktice. [23]

5.1 Rozdělení podle odbornosti

Ne každý kybernetický trestný čin nebo útok je proveden profesionály a odborníky v oblasti informačních technologií. V případě sociálních útoků na osoby, a obzvláště kyberšikany, se v podstatě vůbec nejedná o žádné hackerské metody. Zde se využívá pouze dostupných prostředků, hlavně sociálních sítí, k získávání informací a zesměšňování osob vystavováním citlivých obrázků. I na vytváření virů dnes existují různé generátory. Pomineme-li profesionální hackery, kteří pracují organizovaně a své útoky provádějí na zakázku a za finanční odměnu, existují v rámci kyberkriminality ještě dvě skupiny. Jedna skupina jsou experti, kteří dokáží napsat kód, vytvořit Botnet, exploit, atd. Obvykle však nejsou autory samotného útoku, ale své zdrojové kódy nebo nástroje prodají těm, co mají odvahu útok provést, ale schází jim odborné znalosti. Mezi základní typy útočníků patří:[19]

- **Script kiddies**. Jsou to lidé, převážně mladiství, kteří sami neumí najít slabinu, ale spoléhají se na vyhledané nástroje, které používají k průniku. Převážně tak napadají webové stránky a mění jejich obsah.
- **Hacker**. Počítačový specialista s detailními informacemi o fungování systému, který ho umí výborně ovládat ale též upravit podle svých potřeb. V mediích se často používá ve významu počítačového zločince, kterým se ale správně říká cracker.
- **Cracker.** Synonymum ke slovu průnikář. Hledá slabiny systému, které se snaží využít k prolomení ochrany, převážně za účelem vlastního zisku. Rozdělení hackerů/crackerů.
    - **Black hat**. Je to cracker s úmyslem uškodit nebo provádět nelegální průnik z osobního prospěchu. Tento typ crackera stojí za obecně špatným povědomím lidí o této skupině lidí.

  - **White hat.** Synonymum ethického hackera. Na základě smlouvy hledá slabiny systému s úmyslem je odhalit a opravit.
  - **Gray hat.** Tito crackeři prohledávají internet a hledají slabiny s úmyslem upozornit na ně administrátora, případně mu nabídnout pomoc s opravou.
  - **Blue hat.** Cracker, který se nechává najímat na zlepšování zabezpečení systému před jeho vydáním na trh.
- **Virový tvůrce.** Programátor, který umí napsat škodlivý kód
- **Informační válečník**. Specialista s výbornými znalostmi, obvykle s praxi.
- **Cractivista/haktivista**. Osoba, která pomocí IT technologií prosazuje nebo oznamuje své politické, ideologické, náboženské a sociální názory, přesvědčení nebo sdělení

5.2 Rozdělení podle organizovanosti

Kyberterorismus a kyberkriminalita není doménou jen organizovaných skupin. V mnoha případech jde o činy jednotlivců. Stejně tak nejde jen o činy uskutečněné profesionály v oblasti informačních technologii. Někteří útočníci jsou typičtí samotáři. To se týká především činů sociálních, kyberšikany. Naproti tomu jiné útoky jsou typickým skupinovým činem. Jedná se především o útoky, ke kterým se hlásí nějaké hnutí, například „Anonymous“.

5.2.1 Jedinec

Mezi jedinci, páchajícími trestnou činnost v kyberprostoru, jsou nejen počítačově edukovaní odborníci, ale většina z nich jsou zcela obyčejní uživatelé. Každý uživatel, který někdy nelegálně stáhnul, použil nebo poskytl dále licencovaný software či autorské dílo, se tak stává pachatelem. Na Internetu je také ke stažení mnoho škodlivého kódu, který mohou využít k šíření. Trestné činy sociálního charakteru jsou páchány převážně jedinci. Jejich odvaha a sebevědomí roste s anonymitou, kterou jim poskytují virtuální identity, kterých může každý mít neomezeně.

5.2.2 Skupina (organizovaná, virtuální)

Dva a více jedinců již tvoří skupinu. Pokud se jedná o skupinu s pevnou hierarchií a stejným cílem, můžeme hovořit o organizované skupině. U jedinců organizovaných do

skupin narůstá potencionální riziko globálnějších dopadů, jelikož jednotliví členové mohou působit z různých konců světa. Navíc se mohou doplňovat, co se týče odborností a též i vzájemně krýt. Protikladem jsou skupiny, které vznikají spontánně, nebo jde o organizovaná hnutí s variabilním počtem členů.

Existují dokonce i organizace, které působí v oblasti hackingu oficiálně. Takové firmy, jejichž základnu tvoří profesionální crackeři, si najímají jiné firmy, organizace, či seskupení, někdy dokonce i vlády. Jejich zakázky jsou směrovány do oblasti získávání informací. Ať již odposlechem elektronické a hlasové komunikace nebo získáním dat z jejich osobních zařízení, účtů a profilů. Za svou práci dostávají zaplaceno.[24]

ANONYMOUS

Jak již název napovídá, jde o anonymní, nezávislé a nehierarchické hnutí, proslavené díky svým haktivistickým aktivitám. Nejslavnější jejich haktivistické činy jsou hájení WikiLeaks, nebo útoky proti firmě Sony. V české republice provedli útok například na webové stránky OSA (ochranný svaz autorský), ODS, KSČM. Symbolem anonymous je maska Guye Fawkese.

Obrázek 8: Maska Anonymous
(zdroj: http://www.kirotv.com/news/news/national/fbi-probing-anonymous-hack-clevelands-website/njFcy/)

5.3 Motiv

Stejně jako u jiných trestných činů, i v oblasti kyberkriminality vede jejich pachatele nepřeberné množství motivů k dosažení jejich cílů. Většinu z nich je možné zařadit do jedné z následujících kategorii. [23]

- Internetový exhibicionismus
- Pomsta
- Zábava, nuda
- Zisk
- Publicita, sláva
- Aktivismus (politický, náboženský, rasový, legislativní, atd.)
- Špionáž
- Vnitřní nepřítel
- Konkurence
- Terorismus

Dle jejich motivu je možné definovat i různé kategorie kybernetických útočníků.

- Zloděj
- Profesionální kriminálník
- Kybernetický chuligán
- Politický aktivista
- Frustrovaní lidé (nedocenění zaměstnanci, atd.)

6 OCHRANA

Základními bezpečnostními atributy při ochraně informací jsou:[25]

- Důvěrnost – zajištění autorizovaného přístupu k datům
- Dostupnost – zajištění přístupu k datům
- Integrita – zajištění celistvosti a správnosti dat

Ochrana spočívá především v prevenci. Pokud prevence selže a dojde k překonání ochrany, mluvíme již o záchraně dat. Platí zde zásada, že ochrana musí být přiměřená. To znamená, že investice a vynaložené úsilí do ochrany nesmí překročit hodnotu chráněných aktiv. Velké firmy mají k ochraně svých ICT většinou své specialisty. Ale co běžný uživatel? Zde platí pravidlo, že každý uživatel je odpovědný za své počínání a nakládání s prostředky ICT. Základní bezpečnostní pravidla chování v počítačových sítích a při používání PC by měl znát každý jeho uživatel. Asi nemá smysl dbát zvýšené bezpečnosti a vynakládat finanční prostředky na zabezpečení PC určeného převážně pro hraní počítačových her. Pokud však využíváme své PC nebo smartphone pro přístup do internetového bankovnictví musí každý z nás dodržovat pravidla bezpečnosti. Nelze se spoléhat pouze na technická zabezpečení.

6.1 Osobní a korporátní

Ochrana před kyberhrozbami je široký pojem. Někdy stačí velmi málo ze strany uživatelů, například používat dostatečná hesla, jindy si ochrana vyžaduje sofistikovaná a nákladná řešení, jejíž administraci je nutno svěřit odborníkům. Příkladem může být AFW nebo IDS. I když se výrobci OS a bezpečnostních řešení snaží, aby byly tyto nástroje dostupné každému uživateli nejen cenou, ale i uživatelskou přívětivostí, která nevyžaduje hlubší znalosti ICT, je stále mnoho takovýchto řešení určeno výhradně pro korporátní sféru. Na základě této skutečnosti můžeme rozdělit ochranu na:

- Personální/uživatelská. Tím je myšlena nejen ochrana soukromých zařízení, ale i základní bezpečnostní pravidla každého uživatele ICT, ať již pracuje s osobním nebo firemním zařízením

- Korporátní. Pod tuto kategorii patří obvykle nákladná technická řešení. Velké firmy mají k jejich správě vlastní týmy specialistů, menší firmy využívají služeb externích firem. Patří sem ale i režimová opatření a další formy ochrany, ať již HW, SW, školení zaměstnanců, audity, atd.

6.2 SW ochrana

Kryptování.

Pod tento pojem se řadí metody ochrany dat pomocí šifrování, hash a elektronický podpis. Cílem těchto metod je utajit obsah před neoprávněným uživatelem, zajistit integritu dat a ověřit jejich autora.[18], [19], [26]

Patchování a update

Každá renomovaná společnost vyrábějící SW, včetně OS, která se chce udržet na trhu, musí vydávat nejen nové verze svých produktů, ale i opravy stávajících, mezi něž patří i opravy bezpečnostních chyb. Mělo by být povinností každého uživatele tyto bezpečnostní záplaty pravidelně instalovat.[18], [19]

Autentizace a autorizace/user management

Základním prvkem ochrany dat je řízení přístupu uživatelů k poskytovaným zdrojům. Tyto mechanismy mají za úkol ověřit, zda k dané aplikaci, DB, systému nebo jinému prostředku přistupuje oprávněná osoba a přidělit mu správná oprávnění. Do této kategorie patří nejen autentizace uživatelů, ale i zařízení, například protokolem 802.1x

Logování/monitoring.[18], [19]

Úkolem těchto metod je sledovat aktivity systémů a uživatelů a zaznamenávat důležité události. Tyto záznamy se využívají nejen při analýze problémů, ale slouží i jako důkazní materiál a především jako nástroje pro včasné zjištění problémů.

Zálohování/archivace

Principem zálohování a archivace, je vytvářet kopie dat, aby byly dostupné v případě poškození, ztráty nebo nedostupnosti. Zálohy se musí provádět pravidelně, na media, která mají dostatečnou životnost pro daný účel, a i zde platí stejně jako u zdrojových dat, že i zálohy se musí chránit a zabezpečit. [18], [19]

FireWall

Je síťový prvek, jehož úkolem je řízení a ochrana sítového provozu mezi dvěma sítěmi s různou důvěryhodností. Existují jak v HW variantě, tak i SW variantě. [18]

Antivir

Tyto nástroje mají za úkol detekovat a případně odstranit škodlivý kód. Měly by být automatickou součástí každého zařízení s OS. Důležitá je pravidelná aktualizace jejich virových bází. Detekovat mohou buď v online režimu nebo mohou být kontroly spuštěny ručně, případně automaticky v nastaveném období.[16]

Antispam

V emailové komunikaci nezbytná součást. Může být implementován buď na straně klienta nebo v praxi mnohem častěji na straně emailového serveru. Mezi základní pravidla patří nezadávat emailové adresy do neznámých internetových formulářů a zásadně na spamy neodpovídat. Tím se pouze potvrdí platnost takovéto adresy a spadá tak do seznamu ověřených funkčních adres, na které jsou cíleny další spamy.

Se spam je šířeno také množství phishingových emailů, které obsahují přílohy se škodlivým kódem nebo odkazy na zavirované či podvodné webové stránky. Základním pravidlem, při podezření na phishingový email, je tento email neprodleně smazat a v případě otevření jeho přílohy okamžitě počítač odvirovat nebo přeinstalovat.

IDS/IPS

Intrusion detection systém a Intrusion prevention systémy jsou síťové nástroje pro sledování podezřelého chování stanic a operačních systémů v síti. IDS takové chování dokáže detekovat a upozornit na něj. IPS je rozšířením IDS, kdy při detekci anomálního chování dokáže udělat i preventivní opatření, například přerušit danou komunikaci, blokovat IP adresu nebo filtrovat škodlivé pakety. [19]

DLP

Data loss prevention jsou řešení pro identifikaci, monitorování a ochranu dat. Důležitým předpokladem pro jejich práci je správná klasifikace dat. Dokážou sledovat, jak zaměstnanci nakládají s citlivými daty a případně jim v tom i zabránit.

6.3 HW ochrana

Jejím principem je spíše než samotná ochrana zařízení, jejich samotná dostupnost. Dostupnost dat a internetových služeb je stejně důležitá jako ochrana samotných dat. Data, případně služby, které jsou v bezpečí, ale nedostupné jsou k ničemu. Někdy je jejich dostupnost téměř klíčová. Jako příklad můžeme uvést dostupnost bankovních služeb, elektronické komunikace, telekomunikace nebo DNS serverů. Jejich dostupnost se většinou řeší duplikací zdrojů. Mezi základní taková řešení patří

- Záložní zdroje
- DRC
- Clustering
- RAID

Na tomto místě je však nutné podotknout, že za každým HW a SW stojí jisté schopnosti uživatelů tyto prostředky používat a nastavovat. Nedílnou součástí procesu ochrany jsou vzdělávání, režimová opatření, principy utajení informací, atd.

6.4 Režimová a objektová

Jedná se především o prvky fyzické ochrany. Tím mohou být různé zabezpečovací systémy dveří, oken, kamerové systémy, alarmy, detektory pohybu, atd. Samozřejmostí jsou i režimová opatření, a to nejen objektů s výpočetní technikou, ale i režimová opatření v souvislosti s používáním samotných zařízení. [27] [28]

6.5 Fyzická ochrana

Řeší převážně ochranu zařízení před jejich neúmyslným poškozením. Například přepěťová ochrana, odolnost proti mechanickému poškození, pádu, povětrnostním vlivům, ale i například ochrana disků proti poškrábání u přenosných zařízení zaparkováním hlavičky pevného disku do výchozí polohy při pádu.

6.6 Personální ochrana

Pod tímto pojmem je myšleno, dodržování pravidel bezpečnosti samotným uživatelem. Jeho rozumné chování, zdravá nedůvěřivost atd. Každý uživatel ICT by se měl chovat při práci s ICT a na Internetu zvlášť ostražitě. Měl by dbát bezpečnostních pokynů zaměstnavatele, správců systémů, neotvírat přílohy z neznámých zdrojů, nevystavovat svá data a informace o sobě a svých blízkých na veřejných stránkách. Zabezpečovat svoje profily vhodnými a bezpečnými metodami, provádět pravidelně zálohy, používat pouze legální a licencovaný SW, pravidelně aktualizovat veškerý SW a HW (tímto je myšlen firmware), nepřipojovat se k neznámým sítím, používat šifrované kanály a protokoly, atd.

6.7 Prevence

Prevence je obecný pojem, ale jeho význam je obrovský. Bez prevence není možná žádná účinná ochrana proti útokům ani v reálném světě ani v kyberprostoru. Bez prevence usnadňujeme útočníkům jejich práci. V praxi se osvědčuje více menších ochran, než jedna velká. Bez prevence nejsme připraveni na útok, ani jeho následky. Prevencí se rozumí nejen technická, ale i režimová, edukativní opatření a především chování samotných uživatelů.

6.8 Edukace

I když se základy používání ICT učí již i na základních školách, pravidla bezpečnosti zná málokterý uživatel. Většina z nich se spoléhá na technická opatření, která jsou součástí OS, nebo výrobců HW. U zaměstnanců používajících firemní techniku převažuje názor, že za bezpečnost odpovídá jejich provozovatel, respektive IT oddělení. Klienti bank se zase spoléhají na opatření, která má zavedena banka. Málokdo si však uvědomuje, že i oni sami jsou součástí bezpečnostního řetězce, a že bezpečnost je pouze tak silná, jak jeho nejslabší článek.

6.9 Etický hacking

Metody a nástroje, které používají hackeři, lze v dobrých rukou použít i k zjišťování slabin. Jinak řečeno, mluvíme-li o hackerovi, který pracuje na straně výrobce nebo poskytovatele služby, aplikace, říkáme mu etický hacker a práci, kterou pro svého klienta či zaměstnavatele odvádí, etický hacking. V principu jde o stejnou práci, kterou vykonává hacker, ovšem s tím rozdílem, že nalezené slabiny nevyužívá ke svému prospěchu, ale informuje o nich poskytovatele služeb a vlastníky aplikací a spolupracuje na jejich odstranění. Principem je tedy nalézt stejné slabiny a opravit je dříve než budou zjištěny a zneužity neeticky smýšlejícími osobami.[29]

Aby byly slabiny odhaleny včas, je potřeba provádět bezpečnostní a penetrační testy dříve, než bude daná služba či aplikace k dispozici veřejnosti. Tj. před jejím uvedením do provozu, nebo prodeje. Testy by se měly provádět v odděleném a uzavřeném testovacím prostředí. Po provedení náprav zjištěných slabiny musí být provedeny retesty. Stejně tak se musí testy opakovat i při každém novém release.

Testovat rozsáhlé aplikace, sítě a systémy je časově náročné. Proto vzniklo mnoho nástrojů, které pomáhají provádět velkou část testů automatizovaně. Nicméně stále se bez manuální práce žádný hacker, ani ten etický, neobejde. Obzvláště u aplikací s komplikovanou logikou. Stejně tak i výsledky automatizovaného testování se musí následně manuálně prověřovat.

6.9.1 OWASP

Je zkratka Open Web Application Project. (owasp.org) Jedná se o komunitu a projekt zabývající se bezpečností webových aplikací. V posledních letech se jejich zájem rozšiřuje i na mobilní aplikace. OWASP založili Mark Curphey a Dennis Groves dne 9.září 2001. Owasp foundation je organizace, která byla založena v USA roku 2004 a jejím cílem je poskytovat podporu OWASP a jejich projektů. Po světě má přibližně 100 lokálních poboček a několik tisíc účastníků projektu.

Obrázek 9: Logo OWASP

(zdroj: http://dunnesec.com/test-standards/owasp-open-web-application-security-project/)

Činnost OWASP spočívá především ve sdílení znalostí a osvětě v oblasti bezpečnosti webových aplikací. Jejím prostřednictvím je pořádáno mnoho konferencí. Její členové se podílí na vývoji několika nástrojů pro testování webových aplikací, tréningové weby, nástroje pro ověřování kódu, atd. OWASP vydal také několik dokumentačních projektů. Například Testing Guide, což je průvodce testerů při testování webových aplikací, nebo Top Ten, což je dokument popisující nejrizikovější chyby. Takovýchto projektů je však více.

6.9.2 OWASP Top Ten

Je dokument licencovaný dle Creative Commons Attribution Share Alike 3,0. Na jeho uvedení se podílelo mnoho odborníků v oblasti bezpečnosti a popisuje 10 nerizikovějších chyb ve webových aplikacích. Vedoucím tohoto projektu je Dave Wichers.

Dokument OWASP Top Ten byl již několikrát aktualizován. Poslední verze je z roku 2013. Jejich 10 nerizikovějších chyb je: [20]

- **A1: Injection**

Ke zranitelnostem injektováním, např. injektováním SQL, OS a LDAP dochází, když se jako součást příkazu nebo dotazu odesílají do interpretu nedůvěryhodná data. Útočníkova nepřátelská data mohou lstí přimět interpret k provedení nezamýšlených příkazů nebo k umožnění přístupu k datům bez řádné autorizace.

- **A2: Broken Authentication and Session Management**

Funkce aplikací, které se vztahují k ověřování a správě relace často nejsou provedeny správně, což útočníkům umožňuje kompromitovat hesla, klíče nebo tokeny relací anebo zneužít jiné slabiny v implementaci k tomu, aby převzali identitu jiných uživatelů.

- **A3: Cross-Site Scripting (XSS)**

Chyby typu XSS nastávají tehdy, když aplikace přijme nedůvěryhodná data a odešle je webovému prohlížeči bez řádného ověření nebo escapování. XSS útočníkům umožňuje spouštět skripty v prohlížeči oběti, které mohou unést uživatelské relace, přetvořit webové stránky nebo přesměrovat uživatele na nebezpečné stránky.

- **A4: Insecure Direct Object References**

Přímý odkaz vznikne, když vývojář vystaví odkaz na vnitřní objekt implementace, například soubor, adresář nebo databázový klíč. Bez kontroly řízení přístupu nebo jiné ochrany mohou útočníci manipulovat s těmito odkazy a získat tak neoprávněný přístup k datům.

- **A5: Security Misconfiguration**

Dobré zabezpečení vyžaduje mít definováno a nasazeno bezpečné nastavení aplikace, frameworků, aplikačního serveru, webového serveru, databázového serveru a platformy. Bezpečnostní nastavení by měla být definována, prováděna a udržována, protože výchozí hodnoty jsou často riskantní. Navíc by měl být software průběžně aktualizován.

- **A6: Sensitive Data Exposure**

Mnoho webových aplikací nechrání náležitě citlivá data, jakými jsou kreditní karty, daňová ID *(pozn.: v USA)* a autorizační údaje. Tato slabě chráněná data útočníci mohou krást či modifikovat, aby mohli provádět podvody s kreditními kartami, krádeže identity nebo jiné zločiny. Citlivá data si zaslouží zvláštní ochranu, např. šifrování dat v klidu nebo v pohybu, stejně tak i zvláštní bezpečnostní opatření pro data v prohlížeči.

- **A7: Missing Function Level Access Control**

Většina webových aplikací ověří úroveň přístupových oprávnění k funkcím před tím, než je tato funkcionalita viditelná v uživatelském rozhraní. Přesto je zapotřebí, aby se při přístupu ke každé funkci prováděla stejná kontrola přístupu na serveru. Jestliže požadavky nejsou verifikovány, útočníci budou moci vytvořit požadavky na získání přístupu k funkcionalitě bez řádného povolení.

- **A8: Cross-Site Request Forgery (CSRF)**

Útok typu CSRF donutí prohlížeč přihlášené oběti odeslat zranitelné webové aplikaci podvržený požadavek HTTP, včetně cookie relace oběti a jiných automaticky vkládaných autentizačních informací. To útočníkovi umožňuje donutit prohlížeč oběti generovat požadavky, které zranitelná aplikace považuje za legitimní požadavky oběti.

- **A9: Using Known Vulnerable Components**

Komponenty, např. knihovny, frameworky a další softwarové moduly, téměř vždy běží s nejvyššími oprávněními. Jestliže je zranitelná komponenta zneužita, útok může usnadnit závažnou ztrátu dat nebo ovládnutí serveru. Aplikace používající komponenty se známými zranitelnostmi mohou zmařit ochranu aplikací a umožnit řadu útoků a dopadů.

- **A10: Unvalidated Redirects and Forwards**

Webové aplikace často přesměrovávají a předávají uživatele na jiné webové stránky a používají k určení cílové stránky nedůvěryhodné údaje. Bez řádného ověření mohou útočníci přesměrovat oběti na phishingové nebo malwarové stránky nebo použít předání k získání přístupu k neoprávněným stránkám.

6.10 Ochrana dle typu útoku

V kapitole 1.3 jsou uvedeny základní typy útoků v kyberprostoru. V této kapitole budou uvedeny k těmto útokům vhodná opatření.

- **SPAM**

V první řadě prevence formou rozumného sdělování svých emailových adres. Uživatelé by měli pro registraci na neznámých serverech mít separátní emailové adresy. Vždy platí, že na SPAM se zásadně neodpovídá. V dnešní době je samozřejmou součástí každého emailového serveru kvalitní ANTISPAM a ANTIVIR.

- **Defacement**

Zde především ochrana webového serveru a samotné webové stránky nebo aplikace. Důležitý je FW, případně AFW, opravené nalezené zranitelnosti dle metodiky OWASP, omezený a řízený přístup do administrace serveru a aplikace.

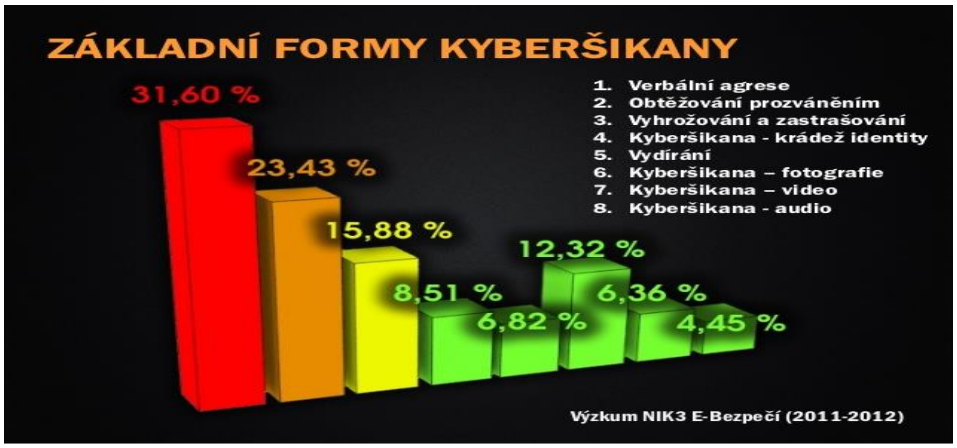
- **Porušování autorských práv**

Možným řešením jsou technická opatření na omezení kopírování nebo opatření formou registrace. [30] Primárním opatřením je však edukace a trestní stíhání. V české republice zastupuje vlastníky autorských práv několik organizací. Mezi hlavní patří:

  - **BSA** - mezinárodní protipirátská organizace zastupující práva výrobců software
  - **OSA** – zastupující autory hudebních děl
  - **INTEGRAM** – zastupující výkonné umělce
  - **OOA-S** – zastupující autory výtvarných děl
  - **DILIA** – zastupující autory literárních děl

- **Kyberšikana**

Z principu jejího zaměření je nejdůležitější ochranou vzdělávání a prevence. Ta spočívá hlavně v dostatečně zabezpečených osobních profilech a mailboxech, nesdělováním osobních informací, nevystavováním fotografii a preventivním chováním před jakýmkoliv způsobem vydírání. Důležité je nepoužívat pro práci na internetu neznámá zařízení a ta osobní mít dostatečně zabezpečena proti odposlechu elektronické komunikace a převzetí kontroly nad zařízením.



Obrázek 10: Základní formy kyberšikany

(zdroj: http://www.slideshare.net/kopeckyk/prevence-kyberikany-pohledem-ebezpe)

- **Zdroj dat pro majetkovou kriminalitu**

Zdrojem dat bývají stejné chyby, kterých se dopouštějí oběti v případě kyberšikany. Proto zde platí i stejná opatření.

- **Malware**

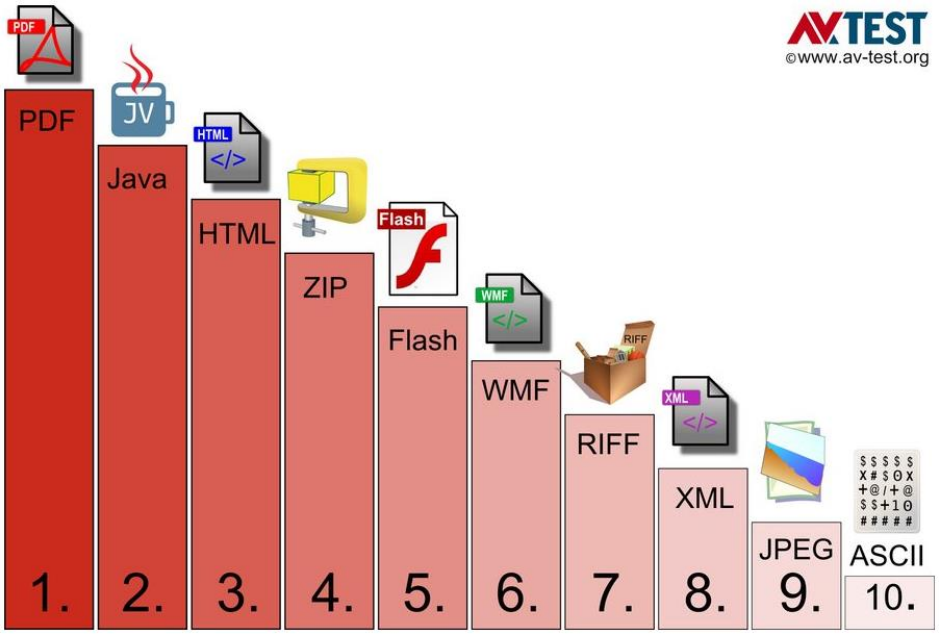
Základním pravidlem je mít vždy aktualizovaný operační systém, veškeré aplikace, firmware a antivirový software, anspyware, antiadware a dobře nakonfigurovaný FW. Preventivním opatřením je nenavštěvovat webové stránky s pravděpodobným výskytem malware, neotvírat přílohy od neznámých odesílatelů a prověřovat antivirem veškerá vyměnitelná média. Dobrou praxí je v případě zasílání elektronických příloh tyto soubory zaheslovat a heslo zaslat příjemci jiným kanálem, třeba SMS. Takto má příjemce větší jistotu, od koho soubor pochází nebo emailovou korespondenci podepsat elektronickým podpisem.[18]

- **Blokování služeb**

Jedná se o velkou množinu různých typů útoků. Prvním předpokladem je zabránění převzetí kontroly nad zařízením, systémem, či aplikací. Druhým předpokladem je zajistit síťovou bezpečnost prostřednictvím IPS, FW, proxy serverů a routerů. V sítové bezpečnosti je též důležité mít dostatečně dimenzované a záložní datové linky. Pro případ dlouhodobých výpadků je zapotřebí mít redundantní veškeré prostředí a zdroje.[19], [16]

- **Ovládnutí serveru/PC**

Útočníci, kteří se snaží prolomit ochranu počítače s cílem převzít na jistou dobu jeho kontrolu nebo ukrást či poškodit data, využívají nejčastěji nalezených slabin v operačních systémech, zranitelných neaktualizovaných aplikacích, nedostatečném zabezpečení nebo využívají technik sociálního inženýrství.[7] Ochranou tedy jsou základní pravidla bezpečného používání PC, technická opatření v podobě FW a utajení informací, převážně autentizačních údajů.



Obrázek 11: Nejrizikovější aplikace a nástroje
(Zdroj: http://www.viry.cz/wp-content/uploads/2013/12/diry.png)

- **Získávání informací / krádež dat**

Data a informace lze získat přímo z napadnutého zařízení nebo prostřednictvím odposlechu elektronické komunikace. Zabezpečení samotného zařízení je popsáno v předchozí kapitole. Ochrana proti snifování provozu je v šifrování komunikace a v navazování důvěryhodných spojení, například tunelování. Dobrou praxí by mělo být nepoužívat neznámá free připojení. Důležité informace je také možné rozdělit a každou část předat jiným kanálem. Šifrovat lze i telefonní hovory. Jako preventivní opatření může být uvedeno vypnutí nepoužívaných služeb, například WIFI, Bluetooth, NFC.[21]

- **Doprovodná a nepřímá kyberkriminalita**

U kyberkriminality, jako je třeba blokování služeb, již byly ochrany popsány v předcházejících odstavcích. U formy, která spočívá ve využívání k propagaci a organizaci teroristů nebo jiných nelegálních organizací, je možné pouze blokování obsahu správci webů, sociálních sítí nebo diskusních fór, případně blokování obsahu na straně příjemce pomocí proxy serverů nebo webových filtrů. V případě, že je některá doména či IP adresa označena jako nebezpečná, mohou být tyto adresní rozsahy blokovány prostřednictvím národního bezpečnostního úřadu, nebo organizace CSIRT.

- **Interní fraudy**

Interní fraudy jsou založeny na všech předchozích principech. Větší riziko a pravděpodobnost úspěchu je dána znalostmi z interního prostředí, zabezpečení, existence oficiálních přístupů útočníka a jiných okolnostech založených na fyzické přítomnosti útočníka v daném prostředí. I technika sociálního inženýrství je pro takové útočníky mnohem snadnější. Technická ochrana je stejná jako u jiných zařízení. Ve firemním prostředí se však musí dbát i na pravidelné kontroly, procesní a režimová opatření, sledování logů, rozdělení pravomocí.

7 LEGISLATIVA

Boj proti žádné formě kriminality není možný bez opory v legislativě. Česká republika je demokratický stát, což neznamená, že ani zde si nemůže každý dělat, co chce. V boji proti kyberkriminalitě pomáhá několik zákonů a některá vládní opatření a instituce pro boj s kybernetickým zločinem. K dispozici jsou i doporučení v podobě norem, která pomáhají stanovovat úroveň bezpečnosti a doporučují vhodná opatření pro zajištění bezpečnosti v oblasti ICT.[31]

7.1 Zákon o ochraně osobních údajů 101/2000sb.

Ochranou osobních a citlivých údajů se zabývá zákon 101/2000 sbírky. V něm jsou kromě definic uvedeny i podmínky jejich zpracování a sankce při jejich nedodržování.

Na základě paragrafu 2 tohoto zákona byl zřízen úřad pro ochranu osobních údajů (ÚOOÚ) se sídlem v Praze. Tento úřad je ústředním správním úřadem pro oblast ochrany osobních údajů v rozsahu stanoveném tímto zákonem, mezinárodními smlouvami, které jsou součástí právního řádu, a přímo použitelnými předpisy Evropské unie. Úřad vykonává působnost dozorového úřadu pro oblast ochrany osobních údajů vyplývající z mezinárodních smluv, které jsou součástí právního řádu.
Nejdůležitější definice jsou tyto:

Pro účely tohoto zákona se rozumí
a) osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu,
b) citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů,

c) anonymním údajem takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů,
d) subjektem údajů fyzická osoba, k níž se osobní údaje vztahují,
e) zpracováním osobních údajů jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace,
f) shromažďováním osobních údajů systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování,
g) uchováváním osobních údajů udržování údajů v takové podobě, která je umožňuje dále zpracovávat,
j) správcem každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak,
k) zpracovatelem každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.[32]

7.2 Zákon o kybernetické bezpečnosti 181/2014 Sb.

Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Nevztahuje se na informační nebo komunikační systémy, které nakládají s utajovanými informacemi

Pojmy definované v §2 tohoto zákona

a) kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací,

b) kritickou informační infrastrukturou prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti [33]

orgány a osoby, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, jsou dle definice v paragrafu 3 tyto:

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací1), pokud není orgánem nebo osobou podle písmene b)

b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem komunikačního systému podle písmene d),

c) správce informačního systému kritické informační infrastruktury,

d) správce komunikačního systému kritické informační infrastruktury a

e) správce významného informačního systému [34]

Pod pojmem významná informační síť se rozumí systém, který má zásadní význam pro fungování veřejné správy (dle stávajícího návrhu vyhlášky např. informační systém základních registrů ISZR, samotné základní registry ROB, ROS, RÚIAN a RPP, informační systém datových schránek ISDS, editační agendové IS atd.). Určující kritéria, resp. konkrétní systémy jsou definovány vyhláškou č. 316/2014 Sb., o kybernetické bezpečnosti.[35]

Povinnosti pro organizace, na které se vztahuje zákon o kybernetické bezpečnosti, jsou uvedeny na následujícím obrázku:

Subjekty spravující/zajišťující: Povinnosti:	elektronické komunikace[2]		významné sítě[3]		informační systémy KII[4]		Komunikační systémy KII[5]		Významné IS[6]	
hlásit kontaktní údaje	✔	✖	✔	✖	✔	✖	✔	✖	✔	✖
detekovat kybernetické bezpečnostní události			✔	✖	✔	✖	✔	✖	✔	✖
hlásit kybernetické bezpečnostní incidenty			✔	✖	✔	✖	✔	✖	✔	✖
zpracovávat bezpečnostní dokumentaci a zavádět bezpečnostní opatření					✔	✖	✔	✖	✔	✖
provádět opatření vydaná NBÚ		✖		✖	✔	✖	✔	✖	✔	✖

Obrázek 12: Povinnosti organizace
(Zdroj: http://www.kybernetickyzakon.cz/)

Všechny prováděcí předpisy k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti, jsou uveřejněny ve Sbírce zákonů v částce 127 pod tímto označením:

- 317/2014 Vyhláška o významných informačních systémech a jejich určujících kritériích

- 316/2014 Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
- 315/2014 Nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

S kybernetickým zákonem dále souvisí nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. [36]

7.3 Autorský zákon 121/2000 sb.

Celý název je Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon). [37]

Tento zákon zapracovává příslušné předpisy Evropské unie a upravuje

- práva autora k jeho autorskému dílu,
- práva související s právem autorským:
    - práva výkonného umělce k jeho uměleckému výkonu,
    - právo výrobce zvukového záznamu k jeho záznamu,
    - právo výrobce zvukově obrazového záznamu k jeho záznamu,
    - právo rozhlasového nebo televizního vysílatele k jeho vysílání,
    - právo zveřejnitele k dosud nezveřejněnému dílu, k němuž uplynula doba trvání majetkových práv,
    - právo nakladatele na odměnu v souvislosti se zhotovením rozmnoženiny jím vydaného díla pro osobní potřebu,
- právo pořizovatele k jím pořízené databázi,
- ochranu práv podle tohoto zákona,
- kolektivní správu práv autorských a práv souvisejících s právem autorským

Dle § 2 tohoto zákona je za autorské dílo považováno

(1) *Předmětem práva autorského je dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně*

vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam (dále jen "dílo"). Dílem je zejména dílo slovesné vyjádřené řečí nebo písmem, dílo hudební, dílo dramatické a dílo hudebně dramatické, dílo choreografické a dílo pantomimické, dílo fotografické a dílo vyjádřené postupem podobným fotografii, dílo audiovizuální, jako je dílo kinematografické, dílo výtvarné, jako je dílo malířské, grafické a sochařské, dílo architektonické včetně díla urbanistického, dílo užitého umění a dílo kartografické.

(2) *Za dílo se považuje též počítačový program, je-li původní v tom smyslu, že je autorovým vlastním duševním výtvorem. Databáze, která je způsobem výběru nebo uspořádáním obsahu autorovým vlastním duševním výtvorem a jejíž součásti jsou systematicky nebo metodicky uspořádány a jednotlivě zpřístupněny elektronicky či jiným způsobem, je dílem souborným. Jiná kritéria pro stanovení způsobilosti počítačového programu a databáze k ochraně se neuplatňují. Fotografie a dílo vyjádřené postupem podobným fotografii, které jsou původní ve smyslu věty první, jsou chráněny jako dílo fotografické.*

(3) *Právo autorské se vztahuje na dílo dokončené, jeho jednotlivé vývojové fáze a části, včetně názvu a jmen postav, pokud splňují podmínky podle odstavce 1 nebo podle odstavce 2, jde-li o předměty práva autorského v něm uvedené.*

(4) *Předmětem práva autorského je také dílo vzniklé tvůrčím zpracováním díla jiného, včetně překladu díla do jiného jazyka. Tím není dotčeno právo autora zpracovaného nebo přeloženého díla.*

(5) *Sborník, jako je časopis, encyklopedie, antologie, pásmo, výstava nebo jiný soubor nezávislých děl nebo jiných prvků, který způsobem výběru nebo uspořádáním obsahu splňuje podmínky podle odstavce 1, je dílem souborným.*

(6) *Dílem podle tohoto zákona není zejména námět díla sám o sobě, denní zpráva nebo jiný údaj sám o sobě, myšlenka, postup, princip, metoda, objev, vědecká teorie, matematický a obdobný vzorec, statistický graf a podobný předmět sám o sobě.* [37]

7.4 Zákoník práce a trestní zákoník

Tento zákon, kromě běžných pracovně právních vztahů, upravuje také práva a povinnosti jak zaměstnance, tak zaměstnavatelů, které lze uplatnit při sledování zaměstnanců v souvislosti s interními fraudy. A to nejen při jejich vyšetřování, ale i jako prevence. [38], [39], [40], [41]

7.4.1 Zákoník práce

§ 316

(1) *Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.*

(2) *Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.*

(3) *Jestliže je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů podle odstavce 2, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.*

§ 301

Zaměstnanci jsou povinni
a) pracovat řádně podle svých sil, znalostí a schopností, plnit pokyny nadřízených, vydané v souladu s právními předpisy a spolupracovat s ostatními zaměstnanci,
b) využívat pracovní dobu a výrobní prostředky k vykonávání svěřených prací, plnit kvalitně a včas pracovní úkoly,

c) dodržovat právní předpisy vztahující se k práci jimi vykonávané; dodržovat ostatní předpisy vztahující se k práci jimi vykonávané, pokud s nimi byli řádně seznámeni, d) řádně hospodařit s prostředky svěřenými jim zaměstnavatelem a střežit a ochraňovat majetek zaměstnavatele před poškozením, ztrátou, zničením a zneužitím a nejednat v rozporu s oprávněnými zájmy zaměstnavatele.

§ 302

Vedoucí zaměstnanci jsou dále povinni

a) *řídit a kontrolovat práci podřízených zaměstnanců a hodnotit jejich pracovní výkonnost a pracovní výsledky,*
   b) co nejlépe organizovat práci,
   c) vytvářet příznivé pracovní podmínky a zajišťovat bezpečnost a ochranu zdraví při práci,
   d) zabezpečovat odměňování zaměstnanců podle tohoto zákona,
   e) vytvářet podmínky pro zvyšování odborné úrovně zaměstnanců,
   f) zabezpečovat dodržování právních a vnitřních předpisů,
   g) zabezpečovat přijetí opatření k ochraně majetku zaměstnavatele.

7.4.2 trestní zákoník - § 220

(1) Kdo poruší podle zákona mu uloženou nebo smluvně převzatou povinnost opatrovat nebo spravovat cizí majetek, a tím jinému způsobí škodu nikoli malou, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.
(2) Odnětím svobody na šest měsíců až pět let nebo peněžitým trestem bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 jako osoba, která má zvlášť uloženou povinnost hájit zájmy poškozeného, nebo

b) způsobí-li takovým činem značnou škodu.

(3) Odnětím svobody na dvě léta až osm let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu.

7.5 Směrnice Evropského parlamentu a rady 2013/40/EU

Cílem této směrnice je sblížit ustanovení trestního práva členských států v oblasti útoků na informační systémy prostřednictvím stanovení minimálních pravidel týkajících se definice trestných činů a příslušných sankcí a zlepšit spolupráci mezi příslušnými orgány, včetně policie a dalších specializovaných donucovacích orgánů členských států, jakož i mezi příslušnými specializovanými agenturami a institucemi Unie, jako je Eurojust, Europol a jeho Evropské centrum pro boj proti kyberkriminalitě a Evropská agentura pro bezpečností sítí a informací (ENISA).[42]

7.6 Úmluva o počítačové kriminalitě, 104/2013 sb. m. s.

Tato úmluva byla otevřena k podpisu v Budapešti 23. 11. 2001. Tuto úmluvu ratifikoval prezident České republiky 22. 8. 2013 a od 1. 12. 2014 vešla v platnost. [43]

7.7 EBA/ČNB

I česká národní banka a evropská bankovní asociace se snaží zavedením pravidel a podmínek zajistit bezpečnost klientů bank. Dva z jejich závazných předpisů jsou tyto:

- Úřední sdělení ČNB k výkonu činností na finančním trhu – operační riziko v oblasti informačního systému. Ze dne 27. 5. 2011
- Obecné pokyny k bezpečnosti internetových plateb.

7.7.1 Úřední sdělení ČNB

V Úředním sdělení ČNB jsou v bodě 9 uvedeny základní povinnosti v oblasti bezpečnosti IS [44]

9. Při provozování informačního systému poskytovatel finančních služeb zabezpečí zejména:

a) *aby jeho změnu bylo možno provést až po vyhodnocení vlivu této změny na bezpečnost informačního systému,*

b) *aby bylo používáno pouze otestované programové vybavení, u kterého výsledky testů prokázaly, že bezpečnostní funkce jsou v souladu se schválenými bezpečnostními zásadami informačního systému; testovací prostředí musí být logicky i fyzicky odděleno od prostředí produkčního a výsledky testů musí být zdokumentovány,*

c) *aby servisní činnost byla organizována tak, aby bylo minimalizováno ohrožení bezpečnosti informačního systému,*

d) *zálohování informací a programového vybavení, významných pro jeho fungování; zálohované informace a programové vybavení jsou uloženy tak, aby byly zabezpečeny proti poškození, zničení a krádeži,*

e) *připojení své interní sítě k externí komunikační síti, která není pod jeho kontrolou tak, aby byla minimalizována možnost průniku do jeho informačního systému,*

f) *aby při přenosu důvěrných informací externí komunikační sítí byla zajištěna přiměřená důvěrnost a integrita informací a dále spolehlivá autentizace komunikujících stran, včetně ochrany autentizačních informací,*

g) *pravidelné prověřování a vyhodnocování bezpečnosti informačního systému.*

7.7.2 Obecné pokyny k bezpečnosti internetových plateb

Tento dokument je platný od 1. 8. 2015. Dle tohoto dokumentu je v hlavě I – „Oblast působnosti a definice“ definována oblast působnosti takto: [45]

Tyto obecné pokyny stanoví soubor minimálních požadavků v oblasti bezpečnosti internetových plateb. Obecné pokyny vycházejí z pravidel směrnice 2007/64/ES1 (dále jen „směrnice o platebních službách“), které se týkají požadavků na informace o platebních službách a povinností poskytovatelů platebních služeb (PPS) v souvislosti s poskytováním

platebních služeb. Čl. 10 odst. 4 směrnice dále vyžaduje, aby měly platební instituce zavedeny spolehlivé mechanismy pro správu a řízení a odpovídající vnitřní kontrolní mechanismy.

Obrázek 13: Logo EBA
(zdroj: https://commons.wikimedia.org/wiki/File:EBA_logo.png)

7.8 NBU

Národní bezpečnostní úřad je orgánem výkonné moci, který byl zřízen na základě zákona č. 148/1998 sb. , což je zákon o ochraně utajovaných skutečností. Vláda České republiky ustanovila v říjnu 2011 NBU gestorem problematiky kybernetické bezpečnosti a současně národní autoritou pro tuto oblast. [46]

7.8.1 Národní centrum kybernetické bezpečnosti

NBU tuto činnost zajišťuje prostřednictvím Národní centra kybernetické bezpečnosti, jehož součástí je Vládní CERT. Úlohou centra je koordinovat spolupráci na národní i mezinárodní úrovni při prevenci kybernetických útoků, i při návrhu a přijímání opatření na řešení incidentů a proti probíhajícím útokům. Hlavní oblasti činnosti centra jsou:[47]

- provozovat Vládní CERT České republiky (GovCERT.CZ)
- spolupráce s ostatními národními CERT® týmy a CSIRT týmy
- spolupráce s mezinárodními CERT® týmy a CSIRT týmy

- příprava bezpečnostních standardů pro jednotlivé kategorie organizací v ČR
- osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti
- výzkum a vývoj v oblasti kybernetické bezpečnosti

7.8.2 Vládní CERT

Vládní CERT (GovCERT.CZ) a týmy typu CSIRT hrají klíčovou roli při ochraně kritické informační infrastruktury a významných informačních systémů podle zákona o kybernetické bezpečnosti (181/2014 Sb.) a jeho prováděcích předpisů. Každá země, která má své kritické systémy připojeny do internetu, musí být schopna efektivně a účinně čelit bezpečnostním výzvám, reagovat na incidenty, koordinovat činnosti při jejich řešení a účelně působit při předcházení incidentům.[48], [49]

Úlohou těchto týmů je zároveň působit jako prvotní zdroj bezpečnostních informací a pomoci pro orgány státu, organizace i občany. Neméně důležitou roli hrají při zvyšování vzdělanosti v oblasti bezpečnosti na internetu.

Orgány a osoby, na které se vztahuje zákon o kybernetické bezpečnosti, musí plnit určité povinnosti vůči vládnímu CERT týmu a orgány a osoby podle § 3 písm. a) a b) plní povinnosti zejména vůči národnímu CERT týmu. Národní CERT tým zaštiťuje organizace CZ.NIC (citace http://www.govcert.cz/cs/vladni-cert/)

7.8.3 Rada pro kybernetickou bezpečnost

Vládním usnesením č. 781 ze dne 19. října 2011 byla ustavena Rada pro kybernetickou bezpečnost. Je poradním orgánem předsedy vlády pro oblast kybernetické bezpečnosti. Jejím cílem je zároveň podpora výkonu gesční a koordinační role Národního bezpečnostního úřadu v oblasti kybernetické bezpečnosti vyžadující součinnost státních institucí a subjektů kritické infrastruktury.

Hlavními úkoly Rady jsou: [50]

- *koordinace činnosti státních institucí v oblasti kybernetické bezpečnosti a přispívání k zajištění plnění závazků meziresortní povahy,*
- *koordinace státních institucí při plnění závazků v oblasti kybernetické bezpečnosti, které vyplývají z členství České republiky v mezinárodních organizacích a*

koordinace zastupování České republiky v mezinárodních organizacích a v dalších zahraničních aktivitách souvisejících s kybernetickou bezpečností,

- *aktivní vytváření podmínek pro hladké fungování spolupráce mezi členy Rady,*
- *řešení aktuálních otázek kybernetické bezpečnosti a předkládání odborných návrhů a doporučení vládě,*
- *sledování plnění závěrů z jednání Rady jejími členy,*
- *shromažďování, analýza a vyhodnocení údajů o stavu zajištění kybernetické bezpečnosti poskytovaných členy Rady,*
- *příprava návrhu zprávy o stavu zajištění kybernetické bezpečnosti České republiky, která je pravidelně předkládána předsedou vlády vládě jako výchozí dokument, který stanovuje priority a z nich vyplývající úkoly v oblasti kybernetické bezpečnosti pro nadcházející období,*
- *spolupráce s externími odbornými subjekty a využívání jejich výstupů v zájmu zajišťování kybernetické bezpečnosti České republiky*

7.8.4 CSIRT.CZ

CSIRT je zkratka Computer Security Incident Response Team. CSIRT.CZ je národním týmem České republiky a je bezpečnostním týmem pro koordinaci řešení bezpečnostních incidentů v počítačových sítích provozovaných v České republice.

Bezpečnostní tým CSIRT.CZ provozuje sdružení CZ.NIC, správce české národní domény, a to na základě veřejnoprávní smlouvy uzavřené v prosinci 2015 s Národním bezpečnostním úřadem jako gestorem problematiky kybernetické bezpečnosti.

Role CSIRT.CZ jsou následující: [49]

- Udržování zahraničních vztahů se světovou komunitou CERT/CSIRT týmů a organizacemi, které tuto komunitu podporují.
- Spolupráce se subjekty v rámci ČR - ISP, poskytovateli obsahu, bankami, bezpečnostními složkami, akademickým sektorem, úřady státní správy a dalšími institucemi.
- Poskytování služeb v oblasti bezpečnosti:
  - Řešení a koordinace řešení bezpečnostních incidentů

- Osvětová a školící činnost
- Proaktivní služby v oblasti bezpečnosti

CSIRT.CZ také pomáhá předávat hlášení o bezpečnostních incidentech správcům těch sítí nebo domén, ze kterých incidenty pocházejí a které na stížnosti nereagují. V takovém případě slouží jako "institut poslední záchrany" v případech, kdy jiné metody kontaktování správců selžou.

Obrázek 14: Logo CSIRT.CZ (zdroj: https://csirt.cz/)

7.9 ISO/IEC 27XXX

Série norem ISO 27XXX je pro oblast bezpečnosti informací.

- ISO/IEC 27000 Systémy řízení bezpečnosti informací – Přehled a slovník
- ISO/IEC 27001 Systémy řízení bezpečnosti informací – Požadavky
- ISO/IEC 27002 Soubor postupů pro opatření bezpečnosti informací
- ISO/IEC 27003 Směrnice pro implementaci systému řízení bezpečnosti informací
- ISO/IEC 27004 Řízení bezpečnosti informací – Měření
- ISO/IEC 27005 Řízení rizik bezpečnosti informací
- ISO/IEC 27006 Požadavky na orgány poskytující audit a certifikaci systémů řízení bezpečnosti informací
- ISO/IEC 27007 Směrnice pro audit systémů řízení bezpečnosti informací
- ISO/IEC TR 27008 Směrnice pro audit opatření ISMS
- ISO/IEC 27010 Směrnice pro řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi
- ISO/IEC 27011 Směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002

- ISO/IEC 27013 Návod pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000-1
- ISO/IEC 27014 Správa bezpečnosti informací
- ISO/IEC TR 27015 Směrnice pro řízení bezpečnosti informací pro finanční služby
- ISO/IEC TR 27016 Řízení bezpečnosti informací – Organizační ekonomika

7.10 ISO/IEC 27001

ISO 27001 je hlavní normou pro systém řízení bezpečnosti informací (ISMS). Tato norma poskytuje podporu při ustavování, zavedení, provozování, monitorování a zlepšování ISMS. Též obsahuje požadavky posouzení a ošetření rizik bezpečnosti informací. V Příloze A jsou uvedena opatření k jednotlivým cílům, které jsou:[51]

- Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky týkajícími se činnosti organizace, příslušnými zákony a směrnicemi
- Ustavit rámec řízení pro zahájení a řízení implementace a provozování bezpečnosti informací v organizaci
- Zajistit bezpečnost při použití mobilních zařízení a pro práci na dálku
- Zajistit, aby zaměstnanci a smluvní strany byli srozuměni se svými povinnostmi a aby pro jednotlivé role byli vybráni vhodní kandidáti
- Zajistit, aby si zaměstnanci a smluvní strany byli vědomi a plnili si svoje povinnosti v oblasti bezpečnosti informací
- Chránit zájmy organizace v rámci procesu změny nebo ukončení pracovního vztahu
- Identifikovat aktiva organizace a definovat odpovědnosti k jejich přiměřené ochraně
- Zajistit aby informace získaly odpovídající úroveň ochrany v souladu s jejich důležitostí pro organizaci
- Předcházet neoprávněnému vyzrazení, modifikaci, odstranění nebo zničení informací uložených na médiích
- Omezit přístup k informacím a vybavení pro zpracování informací

- Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k systémům a službám
- Učinit uživatele odpovědné za ochranu jejich autentizačních informací
- Předcházet neautorizovanému přístupu k systémům a aplikacím
- Zajistit řádné a efektivní používání kryptografie k ochraně důvěrnosti, autentičnosti a/nebo integrity informací
- Předcházet neautorizovanému fyzickému přístupu, poškození, a zásahům do informací a vybavení pro zpracování informací organizace
- Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činnosti organizace
- Zajistit správný a bezpečný provoz vybavení pro zpracování informací
- Zajistit, aby informace a vybavení pro zpracování informací byly chráněny proti malwaru
- Chránit proti ztrátě dat
- Zaznamenávat události a vytvářet záznamy
- Zajistit integritu provozních systémů
- Zabránit využívání technických zranitelností
- Minimalizovat dopady auditních činností na provozní systémy
- Zajistit ochranu informací v sítích a jejich podpůrných prostředcích pro zpracování informací
- Zajistit bezpečnost informací při jejich přenosu v rámci organizace a s externími subjekty
- Zajistit, aby se bezpečnost informací stala nedílnou součástí informačních systémů v jejich celém životním cyklu. To zahrnuje i požadavky na informační systémy, které poskytují služby ve veřejných sítích
- Zajistit, aby bezpečnost informací byla navrhována a implementována v životním cyklu vývoje informačních systémů
- Zajistit ochranu dat používaných pro testování
- Zajistit ochranu aktiv organizace, ke kterým mají dodavatelé přístup
- Udržovat dohodnutou úroveň bezpečnosti informací a dodávky služeb ve shodě s dodavatelskými dohodami

- Zajistit odpovídající a efektivní přístup ke zvládání incidentů bezpečnosti informací zahrnujícímu komunikaci ohledně bezpečnostních událostí a slabých míst
- Kontinuita bezpečnosti informací musí být součástí systémů řízení kontinuity činností organizace
- Zajistit dostupnost vybavení pro zpracování informací
- Vyvarovat se porušení zákonných, předpisových nebo smluvních povinností týkajících se bezpečnosti informací a jakýchkoliv bezpečnostních požadavků

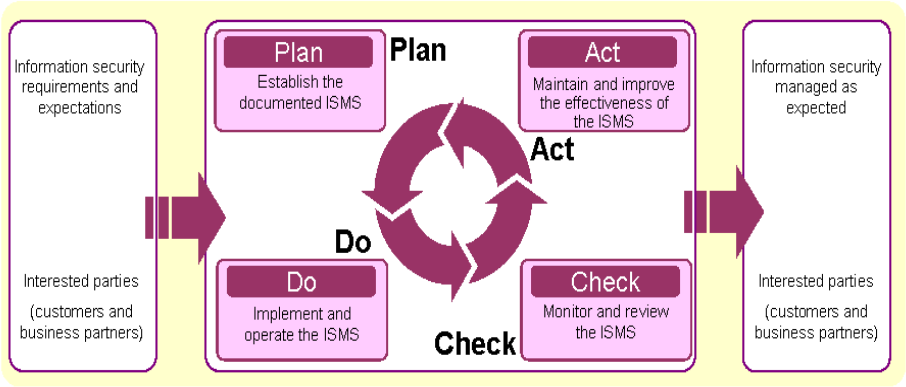
7.11 ISMS

Information security management system. Jde o dokumentovaný systém, jehož cílem je chránit definovaná informační aktiva, řídit rizika bezpečnosti informací a kontrolovat zavedená opatření. Tento pojem prvně zavedla norma ISO/IEC 17799, která byla nahrazena řadou norem ISO/IEC 27000 Přijetí ISMS by mělo být strategickým rozhodnutím organizace a může být použito na organizační složku, informační systém nebo jeho část, nebo na celou organizaci.[25]

Řada norem, kterou ISMS využívá:

- ISO/IEC 27XXX
- ISO 27799:2008 Zdravotnická informatika – Řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002
- ČSN ISO/IEC 15939:2011 (36 9040) Systémové a softwarové inženýrství – Proces měření

Tento systém je založen na modelu známém jako Plánuj-Dělej-Kontroluj-Jednej (Plan-Do-Check-Act nebo zkratkou PDCA).



Obrázek 15: Princip ISMS

(Zdroj : http://www.isms.jipdec.or.jp/en/isms/approach.gif)

Plánuj

ustanovení rozsahu, politiky, cílů, úkolů, opatření, procesů a postupů kontinuity činností, aby vše bylo v souladu s politikami a cíli organizace. Základním předpokladem je podpora ze strany vedení organizace

Dělej

Dalším krokem je zavedení a provozování politiky, opatření, procesů a postupů kontinuity činností. Tento krok zahrnuje provádění analýzy dopadů (Business Impact Analysis, BIA), analýzy a hodnocení rizik, stanovení strategií BCM, zavedení a vývoj plánů BCM a jejich testování a přezkoumávání

Kontroluj

Monitorováním a přezkoumáním ověřujeme výkon ve vztahu k politice, cílům a reportují se výsledky vedení organizace. Úkolem je provést přezkoumání výsledků, definovat a schválit nápravná opatření

Jednej

Tato fáze je o opatřeních přijatých k nápravě a prevenci, založených na výsledku auditu a přezkoumání BCMS vedením organizace tak, aby bylo dosaženo stálého zlepšování BCMS

8 BANKOVNÍ KYBERKRIMINALITA

S krádežemi úzce souvisí specifický druh kyberkriminality, a to krádež peněz z bankovních účtů. Může se jednat o útok na jedince, což je obvykle spojováno s osobami blízkými. Nebo o hromadný útok na několik klientů, což zase bývá spojeno s rozšiřováním malware.

8.1 Způsoby

V praxi se nemusí jednat pouze o běžný výběr peněz, které má oběť na svém kontě, ale může jít i o jiné formy. Například půjčka. Zná-li útočník autentizační údaje oběti do IB a nemá-li na kontě dostatek peněz, může si jeho prostřednictvím vzít hotovostní půjčku, nebo zaplatit za zboží. Peníze se dají získat i pomocí platební karty, a to ne jen jejím fyzickým zcizením. Zde jsou popsány základní způsoby.

8.1.1 Bankovní malware

Typický průběh je následující. Útočníci pomocí botnetu nebo phishingu infikují počítač oběti malwarem. Ve chvíli kdy oběť spouští webovou stránku svého internetového bankovnictví, zachytí malware pomocí keylogeru zadávané autentizační údaje a odešle je útočníkovi. V případě, že má banka implementovanou dvou faktorovou autentizaci pomocí SMS kódů, pozmění oběti při návštěvě některé webové stránky, kterou může být i samotné bankovnictví, její obsah tak, že ji nabídne instalaci falešného SW do jejího smartphonu například pod záminkou většího zabezpečení nutného pro příští přihlášení. Tento škodlivý SW ve smartphonu však zachytává autorizační kódy zaslané bankou a přeposílá je útočníkovi. Ten tak má k dispozici veškeré autentizační údaje potřebné k převedení finanční částky z účtu oběti na účet útočníka. O pár hodin později stačí peníze vybrat například pomocí kreditní karty z ATM. Jelikož jsou všechny bankovní účty svázány s konkrétní osobou, musí útočník řešit ještě jednu podstatnou věc, a to anonymitu svého bankovního účtu. To se provádí dvěma možnými způsoby. Buďto útočník vytvoří bankovní účet s internetovým bankovnictvím online cestou u banky, která nemá dostatečné mechanismy pro jednoznačnou identifikaci zakládající osoby a následné vybrání v ATM se skrytou tváří, neboť ATM pořizují při výběru peněz fotografie vybírajících nebo vytvoří

účet na tzv. bílého koně. Těmi jsou obvykle osoby s nižším intelektem a v obtížné životní situaci. Takovýmto osobám útočník nabídne finanční částku za zprostředkování finanční transakce na účet bílého koně, její vybrání a předání v hotovosti útočníkovi.

Vzhledem k rozvíjející se oblibě mobilního bankovnictví se dá očekávat v dohledné době zaměření útočníků na mobilní aplikace bank.

8.1.2 Interní fraud

Dalším možným způsobem, jak vybrat peníze z klientských bankovních účtů, je interní fraud. Při tomto způsobu dochází ke zneužití pravomocí samotným bankovním zaměstnancem. V takovém případě došlo pravděpodobně k porušení interních procesů, zanedbání interních kontrolních mechanismů nebo k přidělení větších oprávnění jedné osobě. Zaměstnanec tak může fraud provést buď získáním autentizačních údajů oběti a vzdávat se tak při útoku za identitu oběti, nebo zneužít zvýšených oprávnění v systému k provedení operace, která by měla být validována jinou pověřenou osobou.

8.1.3 Sociální inženýrství

Při tomto způsobu neinstaluje útočník žádný SW do klientova počítače. Spoléhá se pouze na jeho důvěru a ochotu. Vydává se za blízkého známého oběti, kterou kontaktuje prostřednictvím ukradené internetové identity. Prostřednictvím sociální sítě osloví oběť s prosbou o pomoc. Ta spočívá v zaslání malého obnosu peněz. K tomuto účelu navede pod falešnou záminkou útočník oběť na podvodnou stránku platební brány. Oběť na ni zadá požadovanou částku a své autentizační údaje do internetového bankovnictví. Jelikož je podvodná stránka ve správě útočníka, ten odchytí zadávané autentizační údaje a použije je pro přihlášení do IB oběti. Nyní již jen potřebuje získat PIN kód pro potvrzení transakce. Ten získá tak, že své oběti sdělí, že nemá u sebe svůj telefon, na který by mu měl dojít kód, takže si ho nechá zaslat na jeho číslo a požádá o jeho přeposlání prostřednictvím sociální sítě. Ve chvíli kdy toto oběť provede, použije zaslaný kód k autorizaci platby, kterou provedl útočník v IB oběti.

8.1.4 Debetní a kreditní karty

Podaří-li se útočníkovi získat informace o platební kartě, může tyto informace využít při placení služeb nebo zboží přes internet. K těmto účelům stačí znát tyto údaje

- Číslo karty
- Platnost
- CVC2/CVV2 kód

Obrázek 16: CVC/CVV2 kód

(zdroj: http://www.eftnedir.org/wp-content/uploads/2015/11/?ND)

Všechny tyto informace jsou vytištěny na kartě. K jejich krádeži ale není nutné mít přístup k fyzické kartě. Stačí pomocí malware v PC oběti, nebo pomocí podvodné webové stránky tyto údaje zachytit, když je oběť sama vyplňuje do formulářového pole webové aplikace při provádění platby. Na takový okamžik může útočník buď čekat, nebo oběť sám donutit tyto údaje zadat, například nabídkou nějakého výhodného produktu.

8.2 Opatření

Opatření, která banky provádějí na ochranu svých klientů je nespočet a není možné je všechna v rozsahu této práce uvést. Bankovní a finanční instituce provádějí tato opatření v rámci svých režijních nákladů, s výjimkou zpoplatnění dvoufaktorové autentizace u některých bank. Mezi ty základní způsoby patří:

- dostatečně zabezpečená interní síťová infrastruktura, která musí zabránit průniku do bankovních systémů zvenčí. Kvalitní AFW, FW, IDS, IPS, nástroje pro behaviorální analýzu sítového provozu.

- SIEM. Sběr, analýza logů a jejich sledování. Nastavení warningů a korelačních pravidel
- Zabezpečené a otestované internetové bankovnictví. Jeho zranitelnost se testuje penetračními testy dle metodiky OWASP
- Dvoufaktorová autentizace
- Šifrovaná komunikace důvěryhodnými certifikáty
- Antifraud nástroje pro sledování chování klienta
- Antifraud nástroje pro sledování pohybů na účtu
- Režimová opatření
- Procesní opatření
- Interní bezpečnost (používání AV, user management, atd.)

Dostupnost je pro případy výpadků a jiných neočekávaných událostí zajištěna ještě navíc těmito opatřeními:

- DRC
- zálohy a archivace
- redundance zdrojů a HW
- clustery
- BCP, DRP

Veškerá uvedená opatření vycházejí z normy ISO/IEC 27001, ISO/IEC 27002, z nařízení ČNB o řízení operačního rizika a z nařízení EBA o bezpečnosti internetových plateb. Jejich nasazení a správné dodržování je prováděno pravidelnými audity. (zde uvést odkazy na literaturu)

Na bezpečnost v bance bdí a za bezpečnost odpovídá útvar IT bezpečnosti, který stanovuje pravidla a hlídá jejich dodržování. Při řízení bezpečnosti vychází z ISMS.

Rozbor jednoho konkrétního bankovního malware je obsahem náplně praktické části této diplomové práce. V kapitole č. 10 je také seznam bezpečnostních opatření, která musí dodržovat samotní klienti.

II. PRAKTICKÁ ČÁST

9 WIN32/SPY.HESPERBOT.D - ANALÝZA TROJSKÉHO KONĚ

Přibližně v polovině srpna 2013 byl detekován nový trojský kůň zaměřený na klienty bank z České republiky, Turecka, Portugalska a Velké Británie. Svým zaměřením se podobá trojským koňům Zeus a SpyEye, nejedná se však o jejich mutaci, ale o úplně novou rodinu trojských koňů.

Nejprve malware cílil na klienty velkých českých bank (ČSOB, Komerční Banka, UniCredit Bank, Česká spořitelna), nicméně později byl trojský kůň modifikován tak, aby byl schopen útočit i na klienty ostatních bank.

Tato analýza trojského koně Hesperbot byla limitována faktem, že k určitým fázím útoku je nutné přihlásit se pomocí platných přihlašovacích údajů do internetového bankovnictví a také, že některé komponenty malwaru (C&C servery) nebyly dostupné po celou dobu analýzy. Z těchto fází útoku je tedy přiloženo alespoň pro ilustraci pár screenshotů, které poskytla firma Eset.

9.1 Použité nástroje

9.1.1 Online nástroje

- malwr.com
  - Online služba pro automatizovanou analýzu malware
  - Založeno na technologii Cuckoo sandbox vyvinuté stejný mi autory
  - Poskytuje behaviorální analýzu
- anubis.iseclab.org
  - Online služba pro automatizovanou analýzu malware
  - Umožňuje i analýzu aplikací pro operační systém Android
  - Poskytuje behaviorální analýzu
- virustotal.com
  - Online služba pro hromadnou antivirovou kontrolu velkým množstvím antivirových systémů
  - Dceřiná společnost Googlu

9.1.2 Offline nástroje

- Oracle VM VirtualBox

    - Multiplatformní virtualizační nástroj
- IDA v5.0 free
    - Interaktivní dissasembler
- Wireshark
    - Paketový sniffer a analyzátor
- BurpSuite
    - MitM proxy a nástroj pro manuální penetrační testování
- Sysinternals TcpView
    - Nástroj pro zobrazení informací o aktivních síťových připojeních a naslouchaných portech
- Sysinternals Process Monitor
    - Nástroj umožňující detailní sledování činností jednotlivých běžících procesů
- Process Hacker
    - Pokročilý správce úloh

9.2 Použité prostředí

Automatizovaná analýza byla provedena s využitím online nástrojů, podrobnosti o jejich prostředích nejsou známy.

Pro manuální analýzu trojského koně byl z důvodu bezpečnosti použit virtualizovaný operační systém Microsoft Windows 7 s využitím nástroje Oracle VM VirtualBox. Systém záměrně neměl nainstalované nejnovější aktualizace, protože jejich nainstalováním by se potenciálně mohly znemožnit některé funkce trojského koně, které mohou využívat zranitelností operačního systému.

Pro analýzu síťové komunikace byly použity nástroje Wireshark a BurpSuite. Mezi virtualizovaným a hostitelským systémem byla vytvořena síť a hostitelský počítač sloužil jako výchozí brána. Pro dešifrování HTTPS komunikace byl na virtualizovaném systému nastaven proxy server směřující do aplikace BurpSuite na hostitelském počítači. BurpSuite zde tedy pracuje jako Man-in-the-middle a také dokáže podvrhnout vlastní certifikáty pro HTTPS provoz. Tímto způsobem lze analyzovat HTTPS provoz.

9.3 Postup analýzy

Pro analýzu bylo nutné nejprve získat vzorek trojského koně. Ten se šířil prostřednictvím odkazu nebo přílohy v podvodných emailech. Předmětem analýzy je vzorek získaný prostřednictvím odkazu v podvodných emailech předstírajících, že jde o informaci o nedoručené poštovní zásilce.

9.3.1 Automatizovaná analýza

Dalším krokem bylo provedení automatizované analýzy pomocí online analyzátorů malwaru. Tímto způsobem lze snadno zjistit základní informace o analyzovaném vzorku, které mohou být cenným vodítkem pro následnou manuální analýzu.

Nevýhodou těchto nástrojů je fakt, že jsou známé i autorům malware, kteří pro znesnadnění analýzy často do svých kódů přidávají mechanismy pro detekci těchto nástrojů a testovaný vzorek se pak při analýze chová jinak než v reálném prostředí, případně nepracuje vůbec. Další nevýhodou je neschopnost dešifrovat HTTPS komunikaci, záznam síťové komunikace, který většina těchto nástrojů poskytuje ke stažení, tak není v čitelné podobě.

Z výsledků analýzy službou Malwr.com je patrné, že soubor je šifrovaný a při jeho spuštění dochází k rozšifrování, tím se autor malwaru pravděpodobně snaží o znesnadnění analýzy a tím i zbrždění reakce na útok.

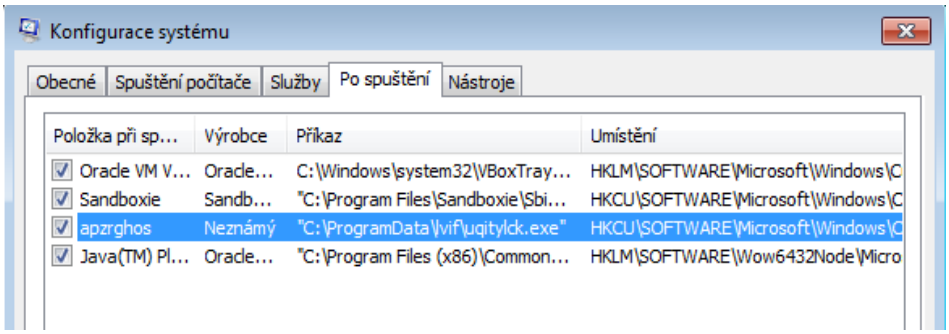
9.3.2 Manuální analýza

Manuální fáze analýzy spočívala především v úmyslném nakažení virtualizovaného systému a následné analýze jeho chování a síťového provozu.

Ještě před nakažením systému byly pomocí nástrojů Process hacker vyexportovány informace o běžících procesech. Před samotným nakažením systému byly také spuštěny nástroje zaznamenávající veškeré aktivity procesů v systému a síťový provoz. Pro monitoring aktivit procesů byl použit nástroj Process monitor ze sady SysInternals. Síťový provoz byl monitorován pomocí nástroje Wireshark a HTTPS provoz pomocí MiM proxy BurpSuite.

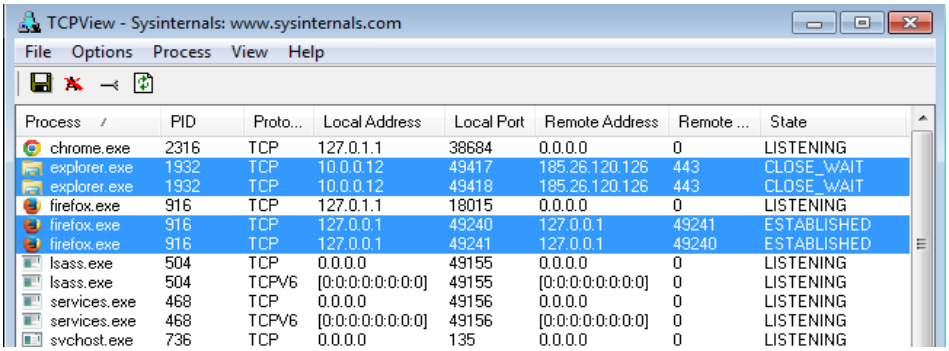
Po infikování počítače spuštěním souboru 11_777_1.exe získaného z podvodného webu pošty, dojde ke stažení aktuálních verzí modulů Hesperbota z mateřského serveru a jejich uložení do náhodně pojmenovaných podadresářů v %PROGRAMDATA% nebo

%APPDATA%. Dále Hesperbot provede změny v registrech, aby se škodlivý kód spouštěl automaticky při každém startu počítače (Obrázek 17). Do těchto adresářů si také ukládá videozáznamy, záznamy stisknutých kláves a další odcizená data.

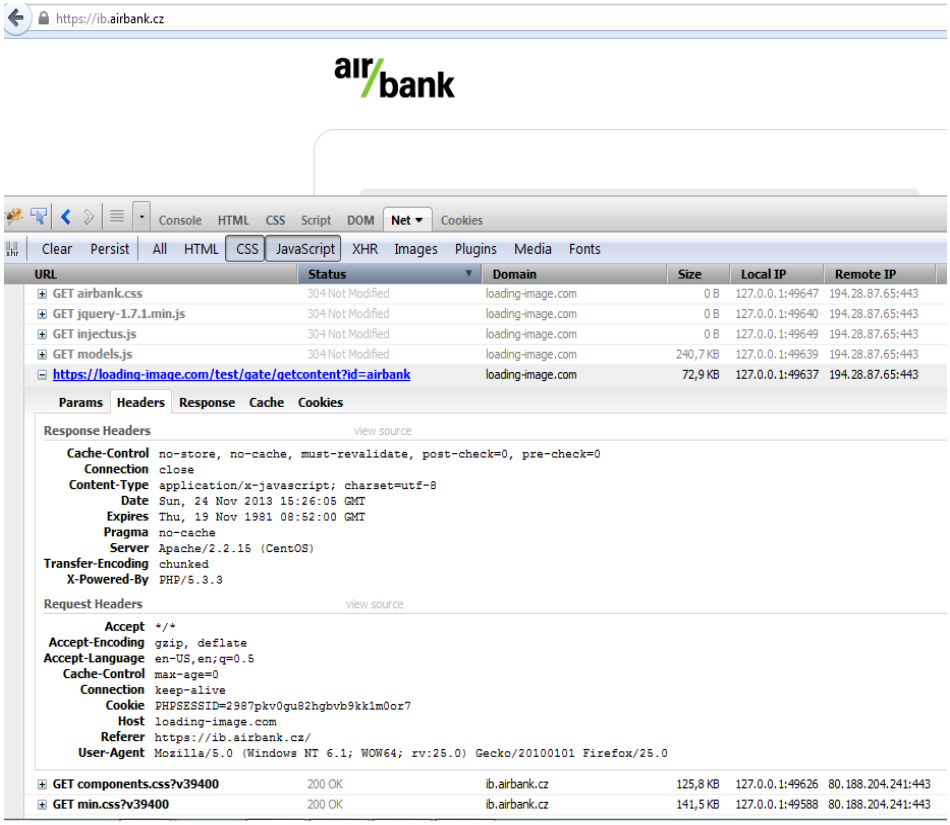


Obrázek 17: Trojský kůň se automaticky spouští po startu systému
(zdroj: autor)

Jedním z modulů Hesperbota je proxy server na modifikaci HTTP a HTTPS provozu. Tento proxy server naslouchá na loopback adrese 127.0.0.1 a 127.0.1.1 a je přes něj směrován veškerý HTTP a HTTPS provoz. Provoz procházející přes proxy je zcela v útočníkově moci, takže pokud uživatel navštíví některý z webů na který Hesperbot cílí, provede se injekce skriptů, pomocí kterých je upraven například vzhled internetového bankovnictví. (Obrázek 19). Na Obrázek 18 je také patrná podezřelá komunikace procesu explorer.exe se serverem s ruskou IP adresou 185.26.120.126. Výpis z databáze whois k této IP adrese je na Obrázek 21.

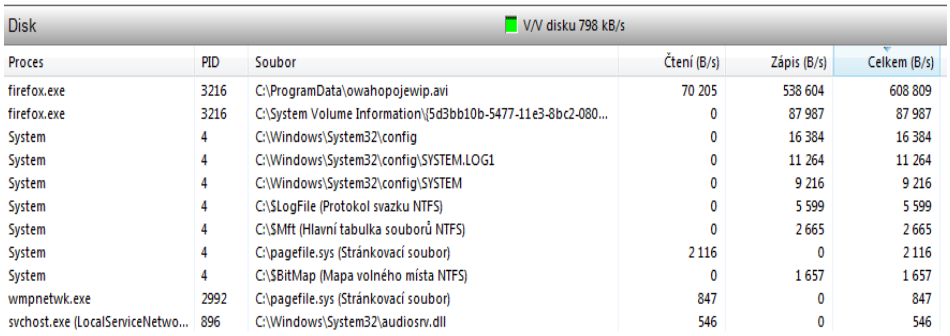


Obrázek 18: TCP komunikace
(zdroj: autor)



Obrázek 19: Injekce CSS a javascriptu

(zdroj: autor)



Obrázek 20: Záznam videa

(zdroj: autor)

Obrázek 21: Podezřelá IP se kterou virus komunikuje

(zdroj: autor)

Za povšimnutí stojí také injektované skripty, lze z nich vyčíst jak přibližně Hesperbot funguje. Skript getcontent.js je ze serveru získán s parametrem ?id=airbank, je tedy přizpůsoben přímo internetovému bankovnictví Air Bank. Z toho je patrné, že virus je univerzální pro více bank, jaký konkrétní skript se použije, závisí na navštíveném webu. Na obrázku 22 je patrné, že pravděpodobně rusky hovořící autor zapomněl komentář k funkci pro zjištění zůstatku na účtu.

```
// Parsim total s glavnoi stranici, gde spisok accov
INJ.parseBalances = function() {
  if(jq('div.mhtAccount').length) {
    var bal1 = parseFloat(jq('div.p:eq(1)').text().replace(/,/g,'.').replace(/[^\d.]/g,''));
    var bal2 = parseFloat(jq('div.p:eq(0)').text().replace(/,/g,'.').replace(/[^\d.]/g,''));
    var totalB = bal1+bal2;
    INJ.sendGateRequest('get_status', {}, function(data){
      if(data.account && data.account != 0) {
        INJ.account_id = data.account;
        INJ.sendGateRequest('save_balances', {balances: totalB}, function(data){});
      }
    });
    INJ.log('Total = ' + totalB);
  } else {
    INJ.log('Balances not found ... ');
  }
};
```

Obrázek 22: Funkce zjišťující zůstatek na účtu

(zdroj: autor)

9.4 Moduly

V této kapitole jsou popsány funkce jednotlivých modulů analyzovaného trojského koně.

9.4.1 Dropper

Tento modul je oběti nabídnut ke stažení na podvodném webu české pošty a po jeho spuštění dojde k napadení počítače a stažení dalších modulů. V tomto případě se jedná o soubor 11_777_1.exe

9.4.2 Keylogger

Jeden z důležitých modulů trojského koně Hesperbot umožňuje zachytávání stisknutých kláves (tzv. keylogger) a následné odesílání zachycených dat útočníkovi. Tímto útočník získá přístup mimo jiné k přihlašovacím údajům do internetového bankovnictví.

9.4.3 Odchyt síťového provozu a vyčítání formulářů

Trojský kůň disponuje také modulem pro odchyt síťového provozu (network interception), který útočníkovi poskytuje širokou škálu možností. Například určit, které weby uživatel navštěvuje a následně z nich vyčítat různé údaje o klientovi (zůstatek a telefonní číslo, osobní údaje, atd).

9.4.4 HTTP/HTTPS injekce

Dalším modulem trojského koně je lokální proxy server umožňující Man-In-The-Middle útoky (MITM). Tento modul naváže HTTPS spojení s legitimním serverem internetového bankovnictví, dešifruje jej, injektuje škodlivý javascriptový kód, dále jej zašifruje svým vlastním certifikátem a odešle do prohlížeče oběti. Protože internetová bankovnictví používají šifrovaný přenos přes HTTPS, v případě MITM útoku detekují internetové prohlížeče neplatný certifikát a varují uživatele před nebezpečím. Hesperbot je však vybaven mechanizmy, které tuto kontrolu dokáží obejít a ve většině prohlížečů se tak žádné varování nezobrazí. Vložený škodlivý javascriptový kód pozměňuje chování internetového bankovnictví z pohledu klienta a je využit například pro zobrazení výzvy k instalaci mobilní komponenty nebo pro vyčítání informace o zůstatku na účtu.

9.4.5 Pořizování snímků obrazovky

Trojský kůň je schopný pořizovat a odesílat útočníkovi také snímky obrazovky, tzv. printscreeny.

9.4.6 Skrytá VNC sezení

Další zákeřnou vlastností Hesperbota je schopnost navázat skryté VNC sezení. Sezení se spouští na skrytém monitoru, takže útočník může libovolně ovládat napadený počítač a uživatel nic nepozná. VNC sezení útočníkovi také poskytuje možnost provádět podvodné transakce přímo z napadeného počítače oběti, aby nebylo tak snadné transakci vyhodnotit jako podvodnou na straně banky.

9.4.7 Videozáznam obrazovky

Hesperbot pořizuje videozáznamy obrazovky (Obrázek 20) a pravděpodobně je odesílá útočníkovi. Nahrávat trojský kůň začne, když uživatel navštíví web, který je pro útočníka zajímavý.

Videa jsou ukládána v plném rozlišení displeje, díky čemuž zabírají poměrně hodně místa na disku a je tedy možné, že se videa útočníkovi neodesílají, ale může je sledovat prostřednictvím skrytého VNC sezení.

9.4.8 Mobilní komponenta

Protože internetová bankovnictví zpravidla používají vícefaktorovou autentizaci pro potvrzení aktivních operací, často ve formě jednorázových potvrzovacích kódů zasílaných pomocí SMS, součástí Hesperbota je i škodlivá aplikace pro mobilní telefony, pomocí které útočník tyto SMS zachytává a přeposílá si je na své telefonní číslo. Útočník má díky podvodné mobilní aplikaci možnost telefon vzdáleně ovládat pomocí SMS příkazů. V této verzi Hesperbota existují mobilní komponenty pro plaftormy Android, Symbian a Blackberry.

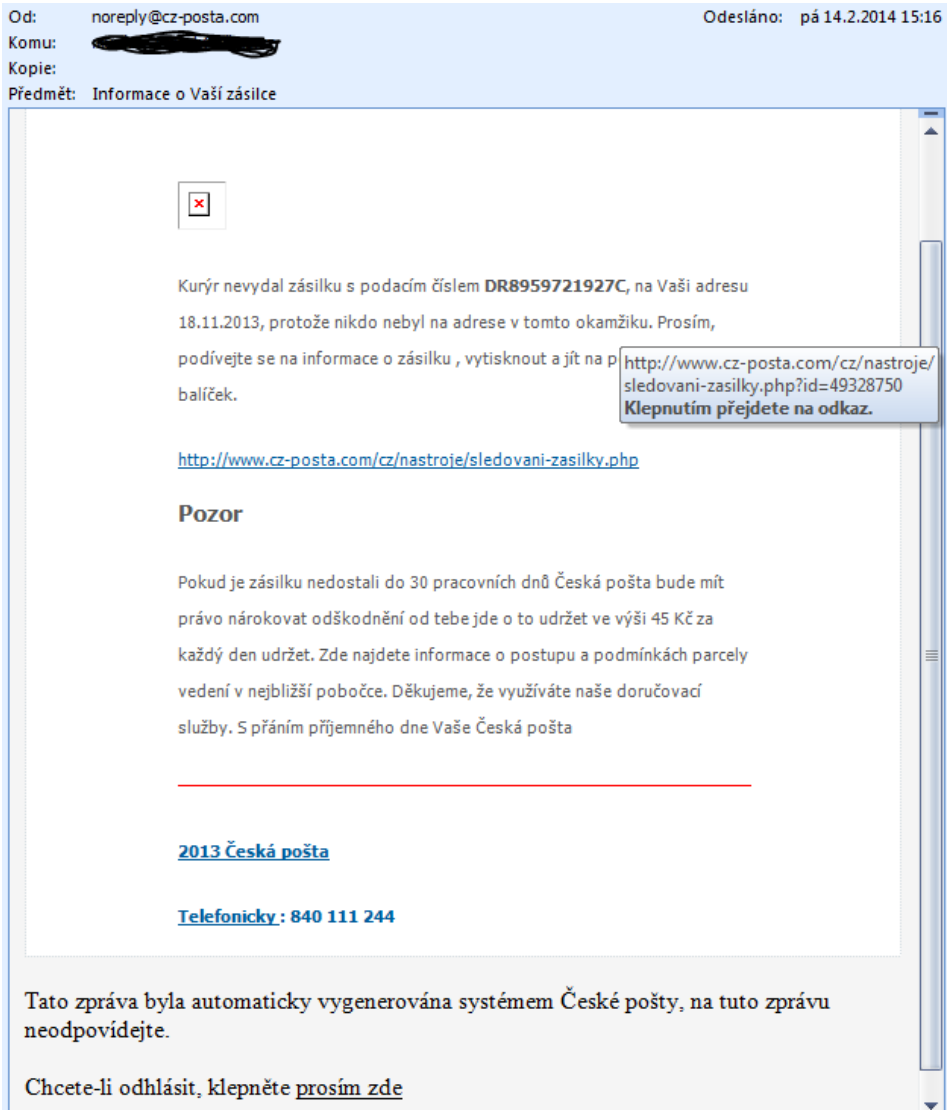
Aby útočník nakazil telefon oběti, vyzve po přihlášení do internetového bankovnictví na nakaženém počítači oběť ke stažení „bezpečnostního software pro chytré telefony“, buď pomocí odkazu zaslaného SMS, nebo přímo. Dokud klient tento krok neudělá, útočník mu znemožní vstup do internetového bankovnictví. (Obrázek 26)

Spárování mobilní komponenty s konkrétní obětí je realizováno prostřednictvím aktivačního kódu, který se zobrazí na napadeném internetovém bankovnictví a po oběti je

požadováno jeho zadání do podvodné mobilní aplikace a opsání dalšího kódu, kterým si útočník ověří, že je aplikace skutečně nainstalována a má tedy smysl se touto obětí dále zabývat.

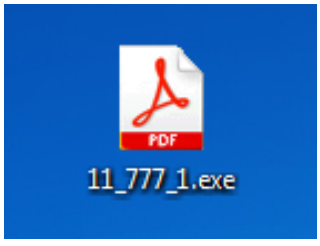
9.5 Způsob šíření

Hesperbot využívá ke svému šíření phishingových e-mailů (viz Obrázek 23). E-mail se tváří jako upomínka k nedoručené zásilce od České Pošty. V textu zprávy je odkaz, na který když uživatel klikne, je mu nabídnut ke stažení soubor. Jedná se o ZIP archiv, ve kterém se nachází soubor 11_777_1.exe s ikonou podobající se PDF dokumentům (viz Obrázek 24). Pokud má uživatel skryté přípony (defaultní nastavení Windows), může snadno nabýt dojmu, že se jedná o neškodný PDF dokument s informacemi o nedoručené zásilce. Když uživatel tento soubor spustí, jeho počítač je nakažen. Text emailu, odesílatel, cílový server a název souboru se mohou lišit v závislosti na verzi trojského koně. Dříve se šířil soubor Zásilka.pdf.exe.



Obrázek 23: Podvodný e-mail

(zdroj: autor)



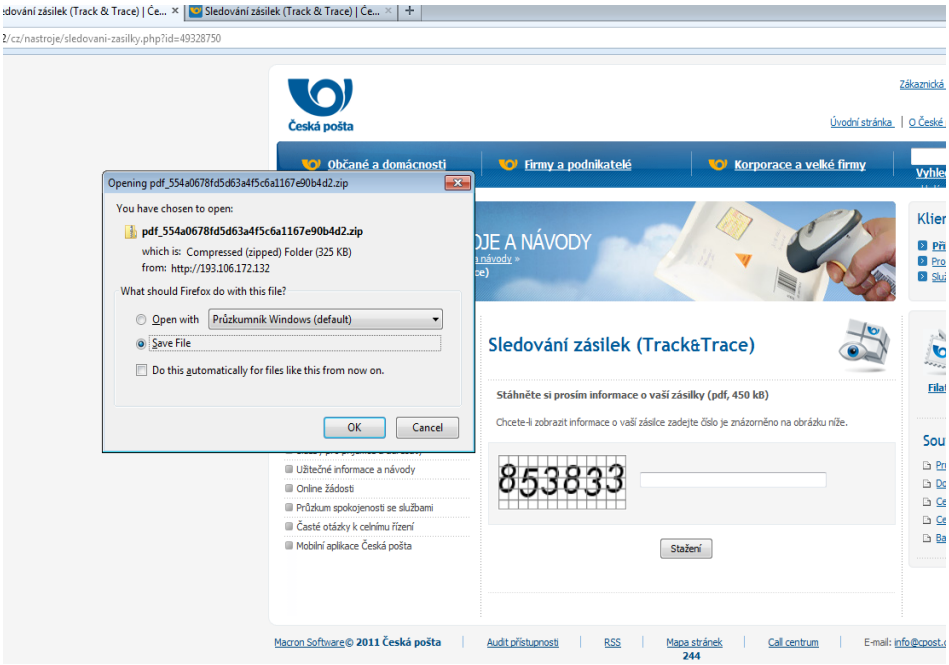
Obrázek 24: ikona

(zdroj: autor)

9.6 Princip útoku

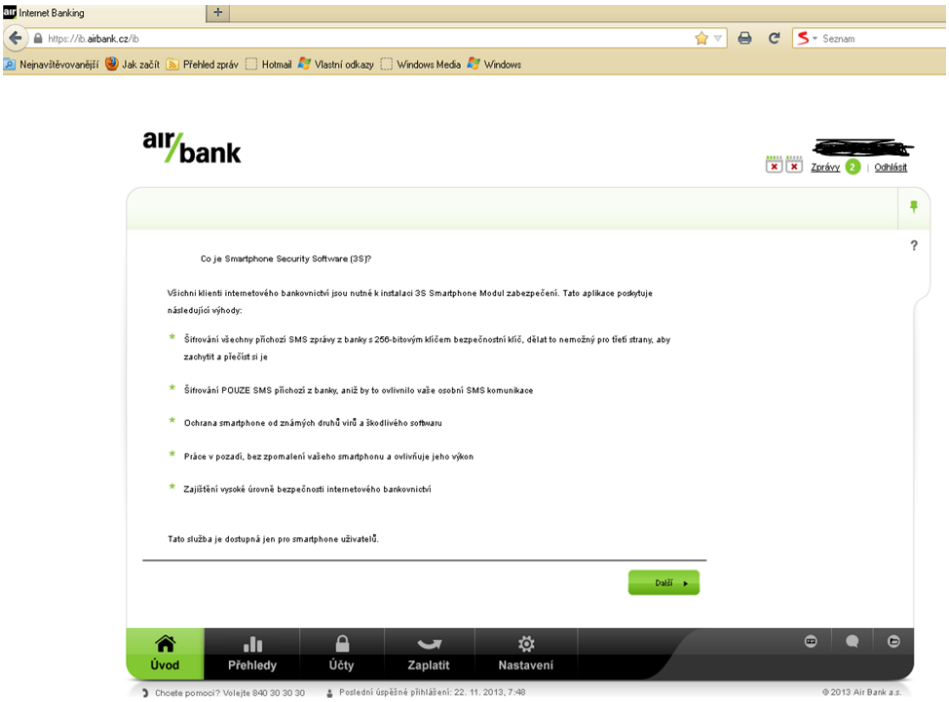
Útok na uživatele internetového bankovnictví prostřednictvím Hesperbota lze rozdělit na následující fáze:

- Nakažení klientova PC
    - Prostřednictvím podvrženého e-mailu, kde klikne na odkaz (Obrázek 23)
    - Klient vyplní captcha kód, následně je mu nabídnut ke stažení ZIP soubor, který rozbalí
    - Klient vidí ikonu PDF dokumentu a soubor spustí v mylném přesvědčení, že jde o PDF dokument s informacemi o nedoručené zásilce (Obrázek 24)
- Získání přihlašovacích údajů klienta do IB
    - Prostřednictvím keyloggeru, odposlechu sítě, atd.
- Modifikace IB a podvržení malwaru pro vyčítání autorizačních SMS z chytrého telefonu
    - Poté, co se oběť přihlásí do IB, zobrazí se výzva k instalaci „bezpečnostního software pro chytré telefony“ (Obrázek 26)
    - Klient si zvolí typ telefonu a je mu nabídnut odkaz pro stažení, případně je mu zaslán přes SMS (Obrázek 27)
    - Klient si aplikaci nainstaluje a potvrdí aktivační kód pro spárování (Obrázek 28)
    - V případě, že klient aplikaci do svého telefonu nainstaluje, útočník získá přístup k ověřovacím SMS a má tedy vše potřebné pro provádění podvodných transakcí



Obrázek 25: Podvodný web s malwarem

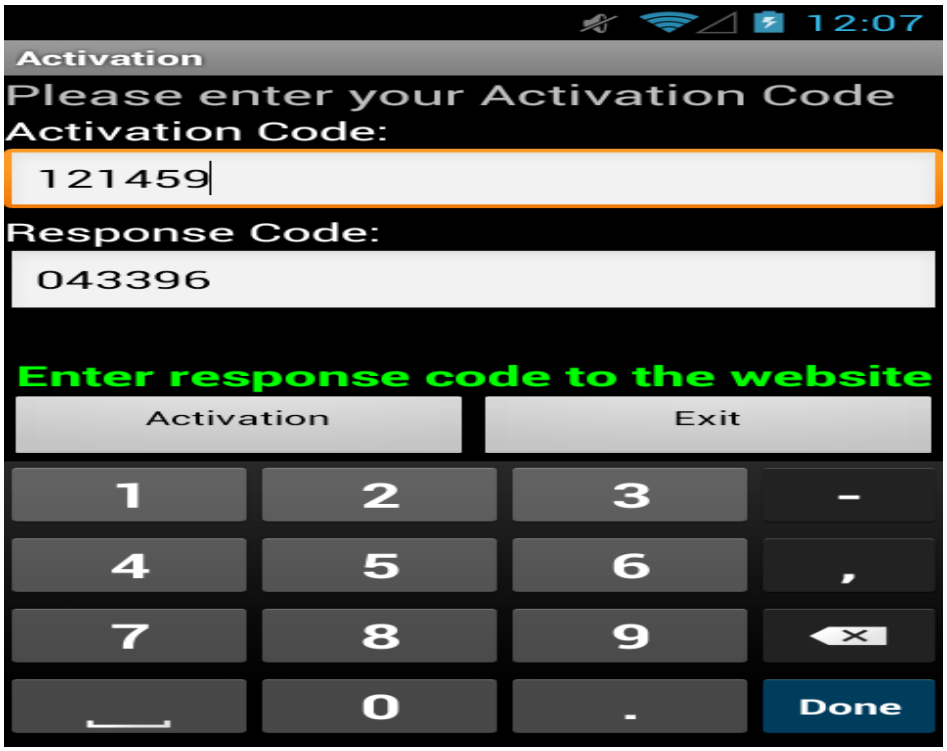
(zdroj: autor)



Obrázek 26: Výzva k instalaci podvodné aplikace pro smartphony

(zdroj: autor)

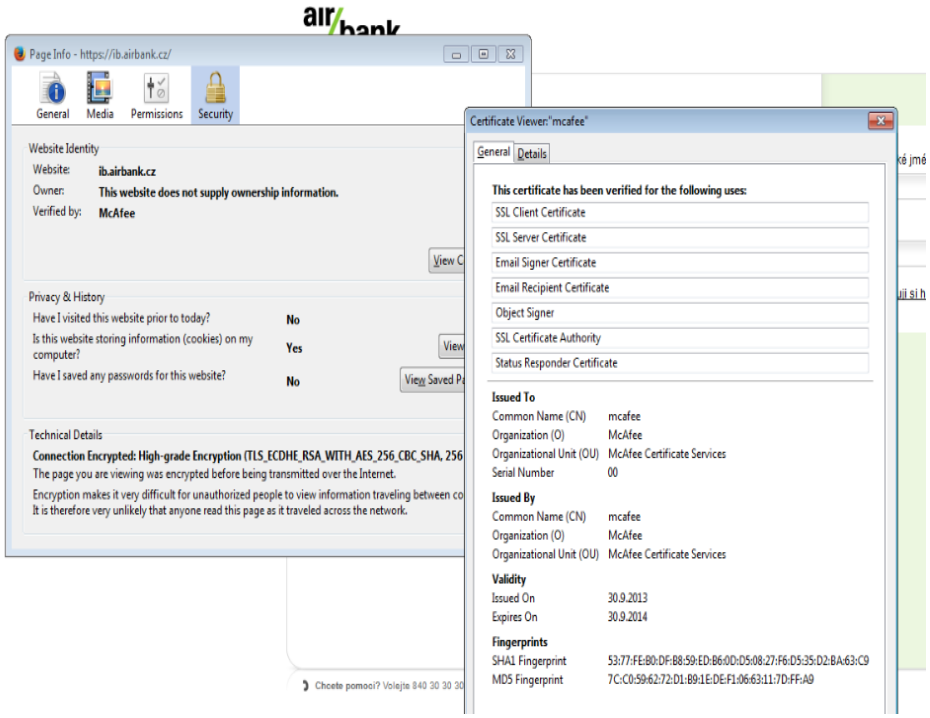
Obrázek 27: Potvrzovací SMS (zdroj: ESET)



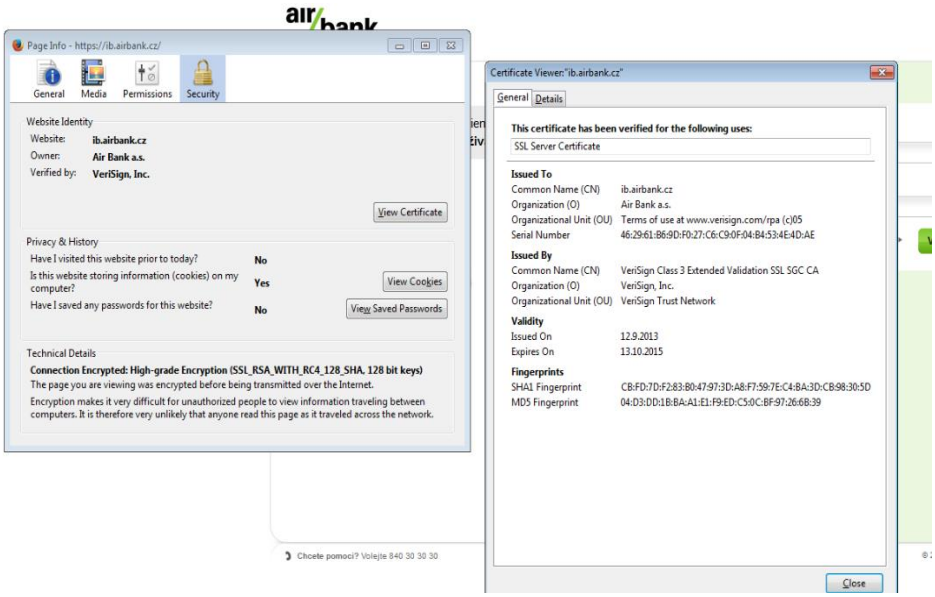
Obrázek 28: Malware pro Android
(zdroj: http://www.welivesecurity.com/2013/09/06/hesperbot-technical-analysis-part-12/)

9.7 Projevy infekce Hesperbotem

Hesperbot je vybaven mechanizmy blokujícími varovná hlášení prohlížeče o neplatném certifikátu a na první pohled se tedy zdá, že je vše v pořádku. Lze si však všimnout, že na nakaženém počítači chybí zelené podbarvení v adresním řádku prohlížeče, které značí platný a tzv. extended validation (EV) certifikát vydaný důvěryhodnou certifikační autoritou (zde VeriSign, Inc.) pro danou doménu (ib.airbank.cz) a pro správnou organizaci (Air Bank a.s.). Mechanismus potlačení kontroly validity certifikátu již nefunguje v nejnovější verzi prohlížeče Google Chrome a je zobrazeno varování. Toto se však může změnit v další verzi Hesperbotu. Nesrovnalosti jsou patrné také v zobrazení detailních informací certifikátu. (Obrázek 29, Obrázek 30)



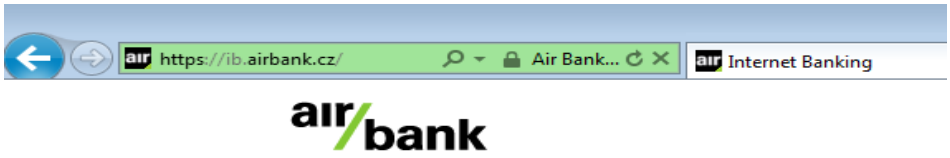
Obrázek 29: Podvržený certifikát
(zdroj: autor)



Obrázek 30: legitimní certifikát

(zdroj: autor)

9.7.1 Internet Explorer 9



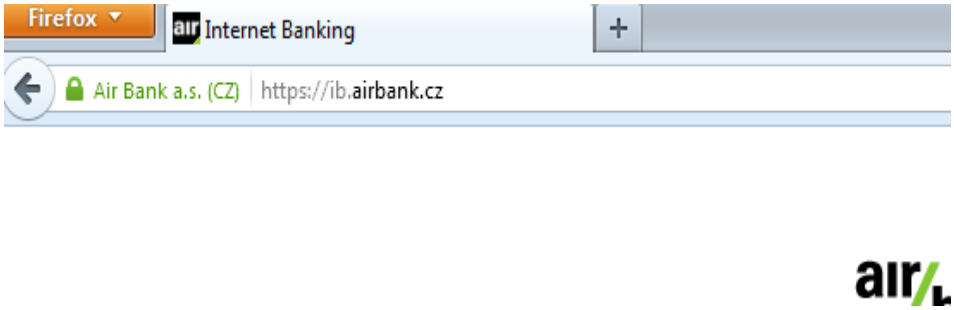
Obrázek 31: IE - čistý PC

(zdroj: autor)

Obrázek 32: IE - nakažený PC

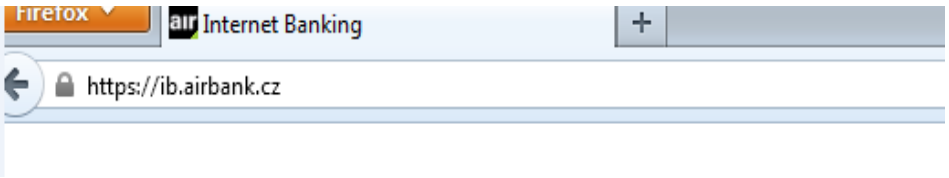
(zdroj: autor)

9.7.2 Mozilla Firefox 25



Obrázek 33: Firefox - čistý PC

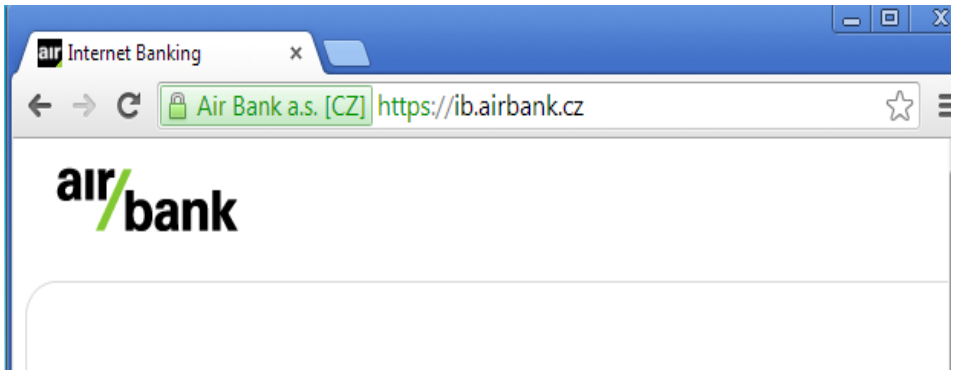
(zdroj: autor)



Obrázek 34: Firefox - nakažený PC

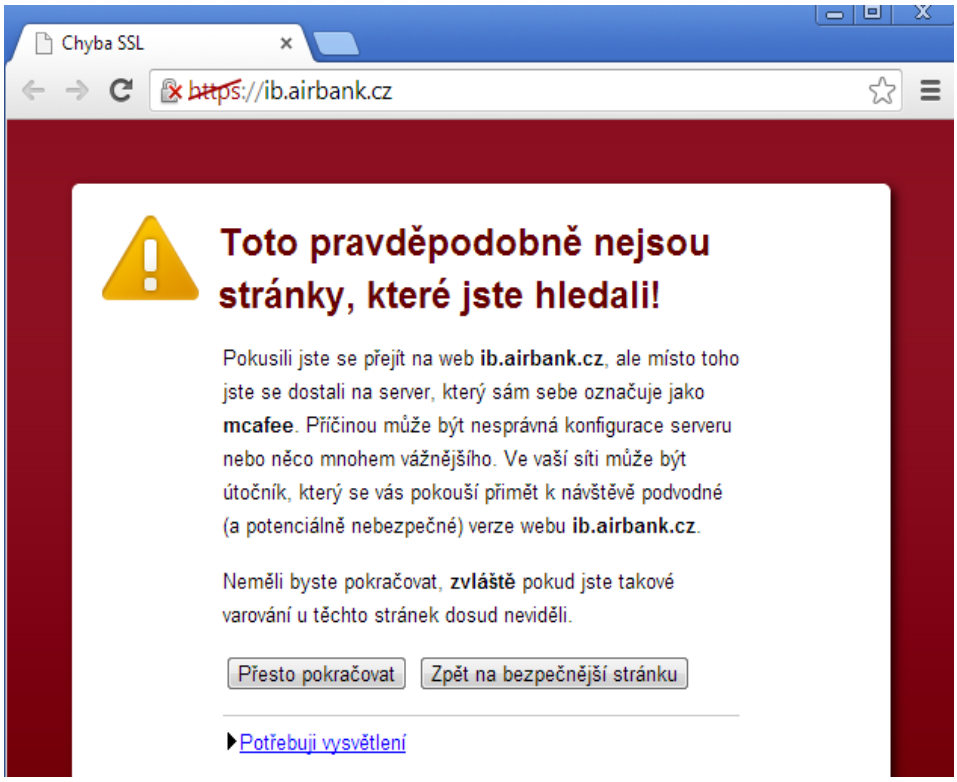
(zdroj: autor)

9.7.3 Google Chrome



Obrázek 35: Chrome - čistý PC

(zdroj: autor)



Obrázek 36: Chrome - nakažený PC

(zdroj: autor)

9.8 Hesperbot a Antivirové systémy

9.8.1 Detekce k datu 27. 11. 2013 (virustotal.com)

ANTIVIRUS	SIGNATURE
Bkav	W32.Clod070.Trojan.db56
MicroWorld-eScan	Trojan.GenericKD.1414298
nProtect	Clean
CAT-QuickHeal	Clean
McAfee	BackDoor-FBLZ
Malwarebytes	Trojan.Ransom.ED
K7AntiVirus	Trojan (098754d80)
K7GW	Clean

TheHacker	Clean
Agnitum	Clean
F-Prot	W32/Trojan3.GOR
Symantec	Trojan.Zbot
Norman	ZBot.FXKB
TotalDefense	Clean
TrendMicro-HouseCall	TROJ_GEN.F47V1121
Avast	Win32:Injector-BNO [Trj]
ClamAV	Clean
Kaspersky	Trojan.Win32.Weelsof.qfr
BitDefender	Trojan.GenericKD.1414298
NANO-Antivirus	Clean
ViRobot	Clean
Emsisoft	Trojan.GenericKD.1414298 (B)
Comodo	Clean
DrWeb	Trojan.PWS.Siggen1.9985
VIPRE	Trojan.Win32.Generic!BT
AntiVir	TR/Agent.cada.26780
TrendMicro	Clean
McAfee-GW-Edition	BackDoor-FBLZ
Sophos	Troj/Zbot-GYV
Jiangmin	Clean
Antiy-AVL	Trojan/Win32.Zbot
Kingsoft	Win32.Troj.Weelsof.q.(kcloud)
Microsoft	VirTool:Win32/CeeInject.gen!KK
SUPERAntiSpyware	Clean
AhnLab-V3	Trojan/Win32.Blocker
GData	Trojan.GenericKD.1414298
Commtouch	W32/Trojan.WSJB-7926
ByteHero	Clean
VBA32	Clean

Baidu-International	Clean
ESET-NOD32	Win32/Spy.Hesperbot.D
Ikarus	Clean
Fortinet	W32/Weelsof.D!tr
AVG	Inject2.HXM
Panda	Generic Malware

Tabulka 1: Detekce antivirovými nástroji dne 27.11.2013

(zdroj: autor)

9.8.2 Detekce k datu 5. 1. 2016 (virustotal.com)

ANTIVIRUS	SIGNATURE
Bkav	Clean
MicroWorld-eScan	Trojan.Agent.BAWC
nProtect	Trojan.Agent.BAWC
CMC	Clean
CAT-QuickHeal	TrojanPWS.Zbot.Gen
ALYac	Trojan.Agent.BAWC
Malwarebytes	Ransom.Agent.ED
Zillya	Trojan.Zbot.Win32.142452
K7AntiVirus	Spyware (0048e8391)
Alibaba	Clean
K7GW	Spyware (0048e8391)
TheHacker	Clean
NANO-Antivirus	Trojan.Win32.Zbot.cqinpc
Cyren	W32/Trojan.WSJB-7926
Symantec	Trojan.Zbot
ESET-NOD32	Win32/Spy.Hesperbot.D
TrendMicro-HouseCall	TROJ_HESPRBOT.SM
Avast	Win32:CeeInject-X [Trj]
ClamAV	Clean

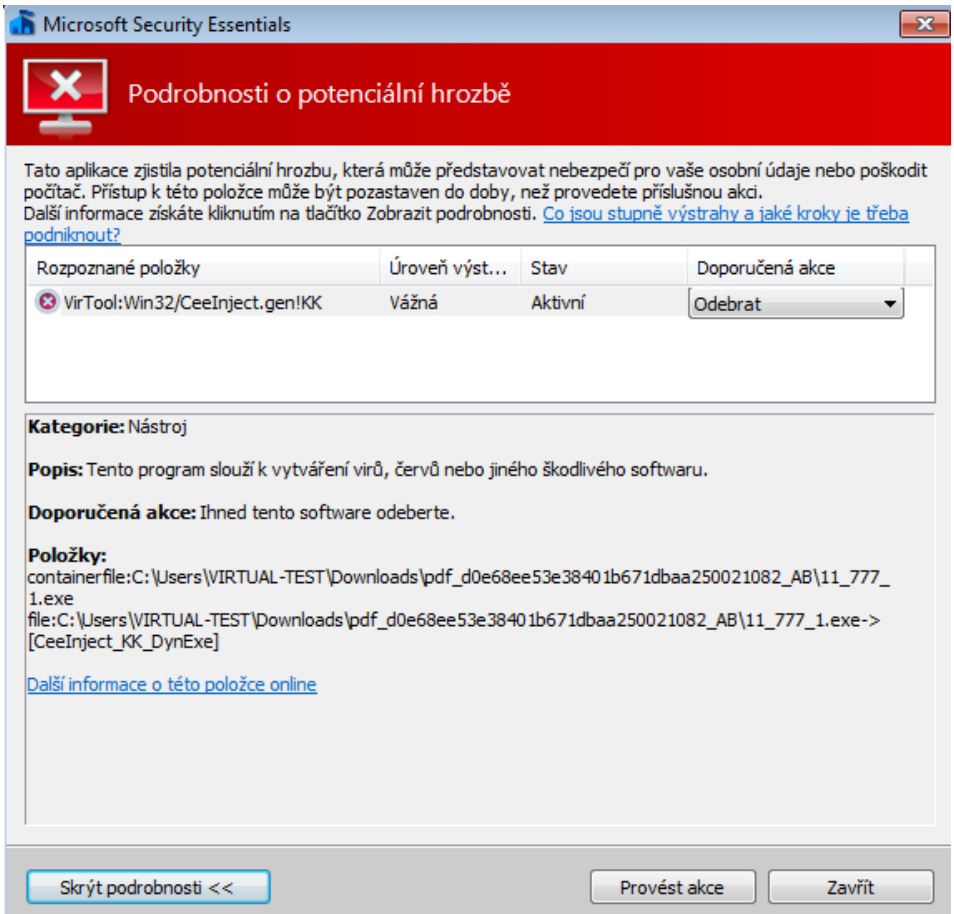
GData	Trojan.Agent.BAWC
Kaspersky	HEUR:Trojan.Win32.Generic
BitDefender	Trojan.Agent.BAWC
Agnitum	Trojan.Weelsof!A5yJJt4kDDc
ViRobot	Trojan.Win32.Z.Zbot.385024.F[h]
AegisLab	Clean
Rising	PE:Malware.Obscure/Heur!1.9E03 [F]
Ad-Aware	Trojan.Agent.BAWC
Emsisoft	Trojan.Agent.BAWC (B)
Comodo	TrojWare.Win32.Spy.Hesperbot.D
F-Secure	Trojan.Agent.BAWC
DrWeb	Trojan.PWS.Siggen1.9985
VIPRE	Trojan.Win32.Fareit.if (v)
TrendMicro	TROJ_HESPRBOT.SM
McAfee-GW-Edition	BehavesLike.Win32.Downloader.fc
Sophos	Troj/Zbot-GYV
F-Prot	W32/Trojan3.GOR
Jiangmin	Trojan/PornoAsset.sjo
Avira	TR/Injector.afd.1
Antiy-AVL	Trojan/Win32.Yakes
Arcabit	Trojan.Agent.BAWC
SUPERAntiSpyware	Trojan.Agent/Gen-Siggen
AhnLab-V3	Trojan/Win32.Blocker
Microsoft	TrojanSpy:Win32/Hesperbot.D
ByteHero	Clean
McAfee	BackDoor-FBLZ
AVware	Trojan.Win32.Fareit.if (v)
VBA32	SScope.Malware-Cryptor.FCM.3913
Panda	Generic Malware
Zoner	Clean
Tencent	Win32.Trojan.Generic.Szvg

Ikarus	Trojan-Spy.Zbot
Fortinet	W32/Kryptik.ARZ!tr
AVG	Inject2.HXM
Baidu-International	Trojan.Win32.Hesperbot.D

Tabulka 2: Detekce antivirovými nástroji dne 5.1.2016

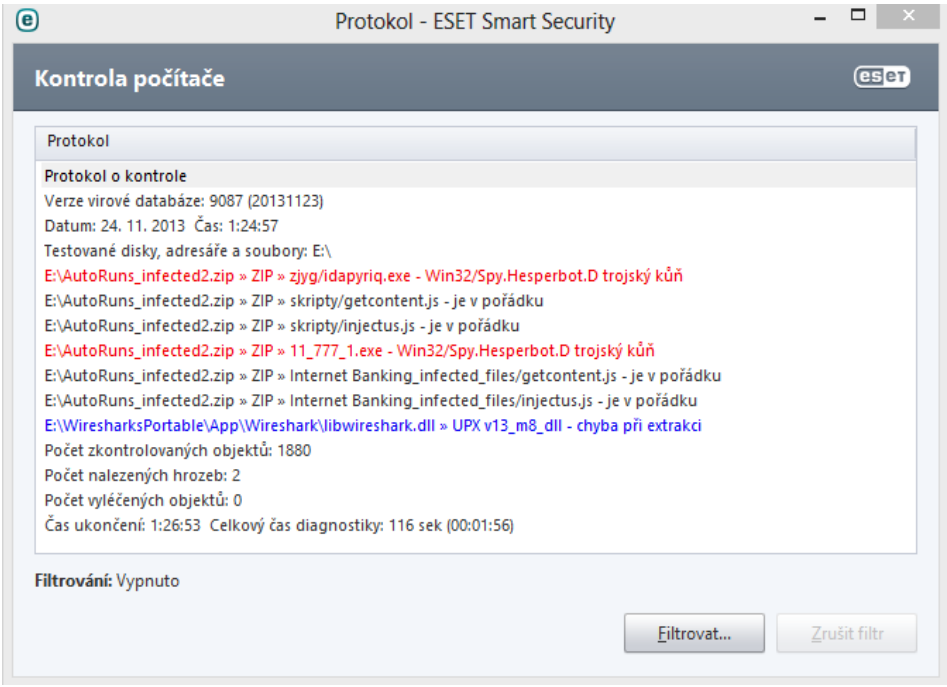
(zdroj: autor)

9.8.3 Zobrazení detekce malware některými antivirovými programy



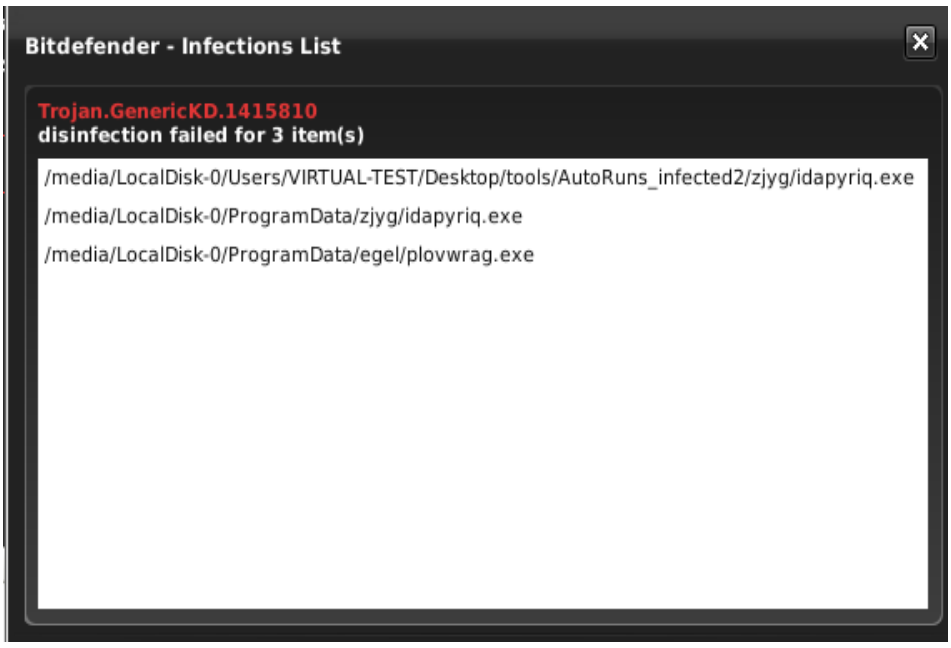
Obrázek 37: Detekce malware – Microsoft Security Essential

(zdroj: autor)



Obrázek 38: Protokol - Esset Smart Security

(zdroj: autor)



Obrázek 39: Protokol – Bitdefender

(zdroj: autor)

Obrázek 40: Protokol – AVG

(zdroj: autor)

10 DOPORUČENÍ

Doména cz-posta.com je dnes již zablokovaná, tím je šíření viru zpomaleno. Hesperbot ale již v minulosti používal více různých domén, lze tedy očekávat, že se objeví modifikace podvodného emailu s novou doménou. Server s IP adresou 193.106.172.132, na kterou doména cz-posta.com směřovala, je stále v provozu.

Trojský kůň Hesperbot je nebezpečnou hrozbou pro neopatrné nebo nedostatečně poučené klienty většiny českých bank. Všechny banky mají na svých webových stránkách vystaveny informace o bezpečném používání IB. V době, kdy byl malware aktivní, byli občané České republiky o riziku informování i prostřednictvím médií a Internetu.

Nebezpečí nespočívá pouze v možnosti napadení bankovního účtu, ale protože se jedná o trojského koně, útočníkovi se do rukou dostávají prakticky všechna hesla, která uživatel na nakaženém počítači používal, nebo je na něm měl uložené. Kromě hesel jsou problém také údaje o kreditních kartách, pokud je uživatel na napadeném počítači používal pro platby na internetu. V případě, že uživatel na nakaženém počítači údaje o kartě zadával, je nezbytná její okamžitá blokace a výměna za novou kartu.

Veškeré informace v tomto dokumentu vycházejí z mého osobního zjištění a jsou poplatné pouze pro jeden konkrétní malware. U jiných klientů, nebo v budoucnu, se mohou vyskytovat jiné modifikované verze, které se mohou méně či více lišit formou provedení, zdrojovými a cílovými adresami, názvy souborů, a samozřejmě i reakcí jednotlivých antivirů.

10.1 Návrh bezpečnostních opatření

Na základě provedené analýzy a znalosti o šíření malware jsou navržena tato obecná pravidla pro minimalizaci rizik při používání internetového a mobilního bankovnictví a platebních karet.

10.1.1 Internetové bankovnictví

- Používat IB pouze na důvěryhodných počítačích (nepoužívat cizí počítače, například v internetových kavárnách)
- Neotvírat přílohy emailů od nedůvěryhodných odesílatelů
- Mít vypnuté skrytí přípon známých typů souborů – kvůli dvojitým příponám

- Nepoužívat webovou verzi internetového bankovnictví na zařízení, na které chodí autorizační SMS – došlo by tím k porušení principu vícefaktorové autentizace.
- Pozorně číst textaci potvrzovacích SMS a v případě podezření se ihned obrátit na banku
- Potvrzovací SMS zadávat výhradně jenom do internetového bankovnictví dané banky
- Na počítači, ze kterého se vstupuje do IB, mít aktualizovaný operační sytém, aktivní a aktualizovaný antivirový SW, nakonfigurovaný FW, aktualizované aplikace třetích stran.
- Nevyužívat k připojení do internetu neznámé sítě, obzvláště pozor na free WIFI.
- Při používání dbát zvýšené opatrnosti
- Do IB přecházet jen z důvěryhodných odkazů (veřejný web banky, přímý zápis URL včetně specifikace protokolu - https://)
- Kontrola adresního řádku. (při použití validního EV certifikátu se zbarví zeleně)
- Kontrola správného certifikátu. Ověřit, zda je vydán pro danou banku
- Neinstalovat do smartphone aplikace z neznámých zdrojů.
- Nepoužívat pro příjem ověřovacích SMS kódů telefony s odstraněnou ochranou. Jedná se o tzv. ROOT nebo Jailbreak
- Používat i na smartphone antivirový SW
- Nikomu nikdy neprozrazovat své autentizační údaje. Po klientovi je nikdy nežádá ani banka, ani policie
- Neukládat hesla v prohlížeči
- Pravidelně měnit autentizační údaje (hesla)
- Dodržovat zásady bezpečných hesel
- Při práci s IB neodcházet od počítače
- Pravidelně kontrolovat historii transakcí
- Kontrolovat v IB poslední přihlášení (pokud to banka umožňuje)
- Nastavit si limity pro internetové platby (lze je kdykoliv změnit)
- Využívat všech dostupných bezpečnostních prvků, které banka nabízí
- Po skončení práce promazat historii prohlížeče, cookies,

10.1.2 Mobilní bankovnictví

- Používat MB pouze na svých soukromých smartphone
- Mít svůj smartphone aktualizovaný
- Mít na smartphone nainstalovaný antivirový SW
- Nevyužívat k připojení do internetu neznámé sítě, obzvláště pozor na free WIFI.
- Při používání dbát zvýšené opatrnosti
- Neinstalovat do smartphone aplikace z neznámých zdrojů.
- Nepoužívat pro MB telefony s odstraněnou ochranou. Jedná se o tzv. ROOT nebo Jailbreak
- Zabezpečit telefon proti nepovolanému použití. Šifrování, PIN, Heslo. Odemknutí obrazovky pomocí gest není bezpečné
- Neinstalovat na smartphone aplikace z neznámých zdrojů
- Instalovat do smartphone aplikaci pro MB pouze z důvěryhodného zdroje. Ideálně získat odkaz na veřejném webu banky
- Nikomu nikdy neprozrazovat své autentizační údaje. Po klientovi je nikdy nežádá ani banka, ani policie
- Neukládat hesla ve smartphone ani v jeho dosahu
- Pravidelně měnit autentizační údaje (hesla)
- Dodržovat zásady bezpečných hesel
- Při práci s MB neodcházet od smartphone
- Pravidelně kontrolovat historii transakcí
- Kontrolovat v IB poslední přihlášení (pokud to banka umožňuje)
- Nastavit si limity pro mobilní platby (lze je kdykoliv změnit)
- Využívat všech dostupných bezpečnostních prvků, které banka nabízí

10.1.3 Pravidla pro bezpečné používání platebních karet

- nikomu kartu nepůjčovat
- opatřit kartu svým podpisem
- nastavit si svůj vlastní bezpečný pin
- nikomu nesdělovat PIN (ani policistům nebo zaměstnancům banky)
- nezaznamenávat PIN a nenechávat ho v blízkosti karty
- přistupovat k ATM jednotlivě

- opticky překontrolovat bankomat, zda na něm nejsou neobvyklé prvky. Obzvláště u štěrbiny pro zasunutí karty
- při zadávání PINu být obezřetní
- vyhýbat se v noci ATM, který není dobře osvětlen
- nevystavovat kartu mechanickým a magnetickým vlivům
- provádět pravidelnou kontrolu výpisů z účtů
- nahlásit ztrátu karty co nejdříve
- žádný personál či obsluha by nikdy neměl odcházet s Vaší kartou
- Vždy zkontrolovat zda Vám personál vrátil Vaši kartu
- při platbě na internetu ověřit důvěryhodnost serveru
- nikdy nezadávat údaje o platební kartě na webu, který není chráněn protokolem HTTPS nebo nemá platný certifikát

10.2 Reakce v případě podezření na bankovní malware nebo únik peněz

Co dělat při podezření na bankovní malware:

- vypnout počítač a odpojit od sítě
- kontaktovat klientské centrum.
- Resetovat autentizační údaje a jejich změnu provést na bezpečném počítači
- Odvirovat nebo přeinstalovat počítač
- Resetovat telefon do továrního nastavení

V případě zjištěného úniku peněz ze svého účtu

- vypnout počítač a odpojit od sítě
- kontaktovat klientské centrum.
- Resetovat autentizační údaje a jejich změnu provést na bezpečném počítači
- Ohlásit událost na policii
- Počítač a telefon do vyšetření policie nepoužívat. Mohou být policií podrobeny šetření a zajištění důkazů

ZÁVĚR

Kyberkriminalita je pojem, který v podstatě nezná hranic. Jak bylo uvedeno v této práci, její rozsah je velmi široký. Od neškodných srandiček v podobě srandovně upravených webových stránek, což ale v samotné podstatě svědčí o slabinách provozovaného webu, které mohou být zneužity i k jiným závažnějším činům, přes vydírání, bankovní krádeže, až po závažné případy s celospolečenskými dopady, hraničící s kyberterorismem.

Kyberkriminalita tu s námi je a pravděpodobně i navždy bude. S touto skutečností je nutné se nejen smířit, ale i se tomu přizpůsobit. V této práci se podařilo popsat základní formy kyberkriminality, definovat její pojmy, ukázat její příčiny a motivy pachatelů. Popsány byly i příznaky, kterými je možné trestné činy v oblasti kyberprostoru rozpoznat a včas zareagovat a klasifikovány následky. V diplomové práci byly uvedeny jednotlivé prostředky ICT a popsány jejich role v rámci kyberkriminality. Samozřejmě, že stejně jako u každé jiné kriminality, je nejdůležitější prevence. Někdy však ani tato nestačí, nebo není v silách běžných uživatelů ICT. Součástí této práce je proto i samostatná kapitola o tom, jak se v takových případech jednotlivým formám kyberkriminality bránit. Uvedeny jsou nejen technické, procesní a softwarové prostředky, ale i legislativní možnosti. Z nich je patrné, že kyberkriminalita jako specifická forma kriminality, je vnímána zákonodárnými orgány velmi vážně. Z tohoto důvodu jsou nejen v rámci České republiky, ale i ostatních národů a společenství vytvářeny nejen normy a zákony, ale i orgány, které mají pravomoc kontrolovat a prosazovat opatření na zajištění bezpečnosti a potírat zločin v souvislosti s ochranou informací, dat, síťové infrastruktury, prostředků ICT a jejich majitelů.

Samostatná kapitola byla věnována bankovní kyberkriminalitě. Uvedeny byly formy možných útoků na finanční prostředky zákazníků. V praktické části pak byla zpracována analýza bankovního malware „HESPERBOT“, který zasáhl většinu bank a jejich klientů v roce 2013 a 2014. Od té doby se objevily další modifikace tohoto malware. Je tedy patrné, že snaha útočníků v tomto sektoru kyberkriminality neklesá, naopak s přibývajícími možnostmi elektronického bankovnictví stále roste. Uživatelská přívětivost a dostupnost správy bankovních účtů a provádění aktivních transakcí odkudkoliv a kdykoliv vede banky samozřejmě v rámci konkurenčního boje k tomu, že se snaží převést váhu poskytování svých služeb z oblasti pobočkové sítě do oblasti elektronických plateb.

Nezanedbatelná je v tomto směru i úspora nákladů. I přesto, že banky vynakládají na zabezpečení elektronického bankovnictví velké úsilí a jsou v tomto směru i pod kontrolou regulátorů, je nutné si uvědomit, že bez spolupráce a odpovědnosti zákazníků není možné bezpečnost zajistit. Z tohoto důvodu je součástí praktické části i návrh klientům používajícím služby elektronického bankovnictví na zabezpečení jejich ICT a doporučená chování při jejich používání.

Jedna rada klientům bank na závěr. Bezpečnost, jako každá jiná služba, něco stojí a nelze ji zajistit bez součinnosti všech zúčastněných stran. S rozvojem služeb elektronického bankovnictví se stávají prioritou bezpečnostní opatření na úkor výše úroků. K čemu vám budou slíbené vyšší úroky a jednoduchost obsluhy, když vám hacker na bankovním účtu žádnou hotovost nezanechá. Čím snadněji se dostanete ke svému účtu vy, tím větší pravděpodobnost je, že se to podaří i neoprávněnému uživateli. Jak kdysi řekl Neil Armstrong „je to sice malý krok pro člověka ale obrovský skok pro lidstvo“. Analogicky je tedy možné říct, že zavede-li se jeden prvek autentizace navíc, je to z pohledu uživatele malý krok, ale obrovský skok pro bezpečnost. To platí nejen u zajištění bankovních účtů, ale i jiných elektronických dat.

SEZNAM POUŽITÉ LITERATURY

[1] *GIBSON, William. Neuromancer*. London: Harper Collins Publishers, 1995. ISBN 0-00-648041-1

[2] *TRADOC. Cyberspace Operations: Concept Capability Plan 2016-2028*. [online] 2010, 80 s. [Cit. 2016-04-01] 16 s. Dostupné z: www.fas.org/irp/doddir/army/pam525-7-8.pdf?

[3] *Ministerstvo vnitra české republiky: Definice pojmu terorismus* [online]. [cit. 2016-03-28]. Dostupné z: http://www.mvcr.cz/clanek/definice-pojmu-terorismus.aspx

[4] DENNING, Dorothy E. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. IWS - The Infornation Warfare site. [online]. [cit. 2016-04-01]. Dostupné z: http://www.iwar.org.uk/cyberterror/resources/denning.htm

[5] *Ministerstvo vnitra české republiky: Kybernetický terorismus, kyberterorismus* [online]. [cit. 2016-03-28]. Dostupné z: http://www.mvcr.cz/clanek/kyberneticky-terorismus-kyberterorismus.aspx

[6] *Policie české republiky: Hlášení kyberkriminality* [online]. [cit. 2016-03-28]. Dostupné z: http://www.policie.cz/clanek/hlaseni-kyberkriminality.aspx

[7] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

[8] *Corpus Solutions: Kyberútoky na kritickou infrastrukturu* [online]. [cit. 2016-03-28]. Dostupné z: http://www.corpus.cz/tiskove-centrum/kyberutoky-na-kritickou-infrastrukturu

[9] *Česká televize: Na hlavní japonskou zbrojovku zaútočili hackeři* [online]. [cit. 2016-03-28]. Dostupné z: http://www.ceskatelevize.cz/ct24/svet/1242032-na-hlavni-japonskou-zbrojovku-zautocili-hackeri

[10] *Nasepenize.cz: Sony odhalila další útok hackerů, ohroženy jsou kreditní karty 100 miliónů lidí* [online]. [cit. 2016-03-30]. Dostupné z: http://www.nasepenize.cz/sony-odhalila-dalsi-utok-hackeru-ohrozeny-jsou-kreditni-karty-100-milionu-lidi-8980

[11] *Zlínsko Online.cz: Nabízením filmů ke stažení způsobil škodu za 80 milionů Kč* [online]. [cit. 2016-03-28]. Dostupné z: http://www.zlinsko-online.cz/aktuality/nabizenim-filmu-ke-stazeni-zpusobil-skodu-za-80-milionu-kc/

[12] *IDNES.CZ: Německý Vodafone napadl hacker. Získal údaje o dvou milionech klientů* [online]. [cit. 2016-03-28]. Dostupné z: http://mobil.idnes.cz/hacker-napadl-vodafone-deutschland-dtt-/mobilni-operatori.aspx?c=A130912_133137_mobilni-operatori_lhr

[13] *LIDOVKY.CZ: Španělé rozbili světovou síť* [online]. [cit. 2016-03-30]. Dostupné z: http://www.lidovky.cz/spanelska-policie-a-interpol-rozbily-svetovou-sit-kyberzlocinu-phc-/zpravy-svet.aspx?c=A130213_173308_ln_zahranici_jv

[14] *Aktuálně.cz: Hackeři ukradli z databáze eBay údaje 145 milionů lidí* [online]. [cit. 2016-03-28]. Dostupné z: http://zpravy.aktualne.cz/ekonomika/technika/hackeri-ukradli-z-databaze-ebay-udaje-145-milionu-lidi/r~5d2dd94ee18111e38a35002590604f2e/

[15] *Hospodářské noviny: Na britského operátora TalkTalk zaútočili hackeři, krádež dat hrozí čtyřem milionům lidí* [online]. [cit. 2016-03-28]. Dostupné z: http://byznys.ihned.cz/c1-64778490-na-britskeho-operatora-talktalk-zautocili-hackeri-kradez-dat-hrozi-ctyrem-milionum-lidi

[16] MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ. Hacking bez tajemství. 3. aktualiz. vyd. Brno: Computer Press, 2003, xxiv, 612 s. ISBN 80-7226-948-8

[17] Bezpečnost a správa mobilních zařízení. BusinessIT [online]. [cit. 2016-03-23]. Dostupné z: http://www.businessit.cz/cz/bezpecnost-sprava-mobilnich-zarizeni-android-apple-mdm.php

[18] Windows server 2003, kapesní rádce administrátora, William R. Staněk, computer press, ISBN: 80-7226-839-2

[19] SMITH, Ben a Brian KOMAR. Zabezpečení systému a sítě Microsoft Windows. 2. vyd. Brno: Computer Press, 2006, 700 s. ISBN 80-251-1260-8.

[20] *OWASP: OWASP Top 10 - 2013* [online]. , 22 [cit. 2016-03-28]. Dostupné z: https://www.owasp.org/images/f/f3/OWASP_Top_10_-_2013_Final_-_Czech_V1.1.pdf

[21] PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: jak zabezpečit wi-fi, bluetooth, GPRS či 3G. Vyd. 1. Brno: Computer Press, 2005, 179 s. ISBN 80-251-0791-4.

[22] *Ministerstvo obrany & Armáda České republiky: Jak čelit kybernetické válce* [online]. [cit. 2016-03-30]. Dostupné z: http://www.army.cz/scripts/detail.php?id=309

[23] Polčák, R. a T. Gřivna. Kyberkriminalita a právo. 1. vyd. Praha: AUDITORIUM, 2008. 220 s. Auditorium. ISBN 978-80-903786-7-4.

[24] *Wikipedia: Hacking Team* [online]. [cit. 2016-03-28]. Dostupné z: https://en.wikipedia.org/wiki/Hacking_Team

[25] Jašek, Roman. *Bezpečnost informačních systémů*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 3.12.2013. ISBN 978-80-7318-889-4.

[26] DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 2., aktualiz. vyd. Brno: Computer Press, 542 s. ISBN 978-80-251-2619-6.

[27] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I*. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. ISBN 978-80-7318-889-4.

[28] IVANKA, Ján. *Mechanické zábranné systémy*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. ISBN 978-80-7318-910-5.

[29] HOWARD, Michael a David LEBLANC. Bezpečný kód: [techniky a strategie tvorby bezpečných webových aplikací]. Vyd. 1. Brno: Computer Press, 2008, 895 s. ISBN 978-80-251-2050-7.

[30] JANSA, Lukáš a Petr OTEVŘEL. Softwarové právo: praktický průvodce právní problematikou v IT. Brno:Computer Press, 2011, 340 s. ISBN 978-80-251-3458-0

[31] Polčák, R. Právní problémy české a evropské kybernetické bezpečnosti. In Haňka, R., Kaplan, Z., Matyáš, V. Mikulecký, J. Říha, Z.. Information Security Summit 2011. 1. vyd. Praha: Data Security Management, 2011. ISBN 978-80-86813-22-6

[32] Zákon č. 101/2000 sb. ze dne 4. dubna 2000, Zákon o ochraně osobních údajů, Část první: Ochrana osobních údajů, Hlava I: Úvodní ustanovení, § 4

[33] Zákon č. 181/2014 sb. ze dne 23. července 2014, Zákon o kybernetické bezpečnosti,Část první: Kybernetická bezpečnost, Hlava I:Základní ustanovení,§2

[34] Zákon č. 181/2014 sb. ze dne 23. července 2014, Zákon o kybernetické bezpečnosti, Část první: Kybernetická bezpečnost,Hlava I:Základní ustanovení,§3

[35] Předpis č. 316/2014 sb. ze dne 15. prosince 2014, Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti

[36] Předpis č. 432/2010 sb. ze dne 22. prosince 2010, Nařízení vlády o kritériích pro určení prvku kritické infrastruktury

[37] Zákon č. 121/2000 sb. ze dne 7. dubna 2000, Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů

[38] Zákon č. 262/2006 sb. ze dne 21. dubna 2006, Zákoník práce, Část třináctá: společná ustanovení, Hlava VIII: ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance, § 316

[39] Zákon č. 262/2006 sb. ze dne 21. dubna 2006, Zákoník práce, Část třináctá: společná ustanovení, Hlava II: základní povinnosti zaměstnanců a vedoucích zaměstnanců vyplývající z pracovního poměru nebo dohod o pracích konaných mimo pracovní poměr, jiné povinnosti zaměstnanců, zvláštní povinnosti některých zaměstnanců a výkon jiné výdělečné činnosti, § 301

[40] Zákon č. 262/2006 sb. ze dne 21. dubna 2006, Zákoník práce, Část třináctá: společná ustanovení, Hlava VIII: ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance, § 302

[41] Zákon č. 40/2009 Sb. ze dne 8. ledna 2009, Trestní zákoník, Část druhá: zvláštní část, Hlava V: Trestné činy proti majetku, § 220 Porušení povinnosti při správě cizího majetku

[42] Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV

[43] Zákon č. 104/2013 Sb.m.s. ze dne 23. prosince 2013, Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě

[44] Úřední sdělení ČNB ze dne 27.5.2011 k výkonu činnosti na finančním trhu – operační riziko v oblasti informačního systému. Věstník ČNB, částka 5/2011 , třídící znak 20811560

[45] EBA, Obecné pokyny k bezpečnosti internetových plateb. EBA/GL/2014/12_rev1 z 19. prosince 2014

[46] *Národní bezpečnostní úřad* [online]. [cit. 2016-03-28]. Dostupné z: http://www.nbu.cz/cs/

[47] *Národní centrum kybernetické bezpečnosti: GOVCERT.CZ* [online]. [cit. 2016-03-28]. Dostupné z: http://www.govcert.cz/cs/vladni-cert/

[48] *Národní centrum kybernetické bezpečnosti: CO JE NCKB* [online]. [cit. 2016-03-28]. Dostupné z: http://www.govcert.cz/cs/

[49] *CSIRT.CZ* [online]. [cit. 2016-03-30]. Dostupné z: https://www.csirt.cz/

[50] *Národní centrum kybernetické bezpečnosti: RADA PRO KYBERNETICKOU BEZPEČNOST* [online]. [cit. 2016-03-28]. Dostupné z: http://www.govcert.cz/cs/rkb/rada-pro-kybernetickou-bezpecnost/

[51] ČSN ISO 27001:2006. Systémy managementu bezpečnosti informací – Požadavky, Praha: Český normalizační institut, 2006

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

802.1x	Protokol umožňující zabezpečení přístupu do počítačové sítě
AFW	Aplikační firewall
ATM	Bankomat
AV	Antivir
AVG	Antivirová společnost
BCM	Business Continuity Management
BCMS	Business Continuity Management Systém
BCP	Business continuity plan
BIA	Business Impact Analysis
BSA	Mezinárodní protipirátská organizace zastupující práva výrobců software
BTS	Systém základnových stanic
C&C	Command and control
CERT	Computer Emergency Response Team
COBIT	Framework pro správu a řízení informatiky
CSIRT	Computer Security Incident Response Team
CSRF	Cross-site Request Forgery
CVC	Card Verification Value
CZ.NIC	Správce české národní domény
ČNB	Česká národní banka
ČR	Česká republika
ČSN	Česká státní norma
ČSOB	Československá obchodní banka
DB	Databáze
DDoS	Distributed Denial of Service
DILIA	Občanské sdružení autorů a dalších nositelů autorských práv
DLP	Data loss prevention

DNS	Domain Name System
DoS	Denial of Service
DRC	Disaster recovery centrum
DRP	Disaster recovery plan
EBA	Evropský orgán pro bankovnictví
ENISA	Evropská agentura pro bezpečností sítí a informací
EV	Extended validation
FW	Firewall
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HUB	Rozbočovač
HW	Hardware
IB	Internetové bankovnictví
ICT	Informační a komunikační technologie
IDS	Intrusion detection system
IDS	Intrusion Detection System
IP	Internetový protocol
IPS	Intrusion prevention systém
IS	Informační systém
ISDS	Informační systém datových schránek
ISMS	Systém řízení bezpečnosti informací
ISO/IEC	Standardization and the International Electrotechnical Commission
ISP	Poskytovatel internetového připojení
ISZR	Informační systém základních registrů
IT	Informační technologie
ITIL	Information Technology Infrastructure Library
JAVA	Programovací jazyk
KSČM	Komunistická strana Čech a Moravy

LDAP	Protokol pro ukládání a přístup k datům na adresářovém serveru
MB	Mobilní bankovnictví
MitM	Man-In-The-Middle
MVČR	Ministerstvo vnitra české republiky
NBU	Národní bezpečnostní úřad
NFC	Near field communication
ODS	Občanská demokratická strana
OOA-S	Organizace zastupující umělce a dědice při hromadné správě práv
OS	Operační systém
OSA	Ochranný svaz autorský
OWASP	Projekt a komunita zabývající se bezpečností webových aplikací
PC	Osobní počítač
PDCA	Plan-Do-Check-Act
PDF	Portable Document Format
PIN	Personal identification number
PPS	Poskytovatel platebních služeb
RAID	Redundant Array of Inexpensive/Independent Disks
ROB	Registr obyvatel
ROS	Základní registr osob
RPP	Registr práv a povinností
RÚIAN	Registr územní identifikace, adres a nemovitostí
SIEM	Security Information and Event Management
SMS	Služba krátkých textových zpráv
SQL	Standardizovaný strukturovaný dotazovací jazyk
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol
ÚOOÚ	Úřad pro ochranu osobních údajů
USA	Spojené státy americké

USB	Universal Serial Bus
VNC	Virtual Network Computing
WiFi	Bezdrátová síť
XSS	Cross-site scripting
ZIP	Souborový formát pro kompresi a archivaci dat

SEZNAM OBRÁZKŮ

SEZNAM TABULEK