ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA ELEKTROTECHNICKÁ

KATEDRA TECHNOLOGIÍ A MĚŘENÍ

BAKALÁŘSKÁ PRÁCE

Vybrané aspekty bezpečnosti informačních a komunikačních systémů

Martin Novák **2016**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martin NOVÁK**
Osobní číslo:	**E13B0379P**
Studijní program:	**B2612 Elektrotechnika a informatika**
Studijní obor:	**Komerční elektrotechnika**
Název tématu:	**Vybrané aspekty bezpečnosti informačních a komunikačních systémů**
Zadávající katedra:	**Katedra technologií a měření**

Zásady pro vypracování:

S použitím odborné vypracujte:

1. Přehled současného legislativního stavu v oblasti bezpečnosti ICT v ČR.
2. Posouzení změn a dopadů v souvislosti s přijetím zákona o kybernetické bezpečnosti.
3. Posouzení vybraných bezpečnostních hledisek z pohledu správce a uživatele informační infrastruktury.

Rozsah grafických prací: **podle doporučení vedoucího**

Rozsah kvalifikační práce: **30 - 40 stran**

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

Seznam odborné literatury:

Student si vhodnou literaturu vyhledá v dostupných pramenech podle doporučení vedoucího práce.

Vedoucí bakalářské práce: **Doc. Ing. Jiří Tupa, Ph.D.**
Katedra technologií a měření

Datum zadání bakalářské práce: **15. října 2015**

Termín odevzdání bakalářské práce: **2. června 2016**

Doc. Ing. Jiří Hammerbauer, Ph.D.
děkan

L.S.

Doc. Ing. Vlastimil Skočil, CSc.
vedoucí katedry

V Plzni dne 15. října 2015

Abstrakt

Předkládaná bakalářská práce je zaměřena na popis a vysvětlení vybraných aspektů informačních a komunikačních systémů v souvislosti s přijetím zákona o kybernetické bezpečnosti. Hlavním cílem práce je posouzení změn a dopadů v souvislosti s přijetím zákona o kybernetické bezpečnosti. Teoretická část popisuje principy fungování Internetu, kybernetickou bezpečnost a možnost obrany proti základním typům útoků a hrozeb na Internetu z pohledu uživatele a správce/administrátora. Praktický část popisuje pokus s veřejnou IPv4 adresou, který zkoumá četnost útoků, které jsou vedeny na zařízení připojená k Internetu.

Klíčová slova

Bezpečnost, kybernetická bezpečnost, kybernetický zákon.

Abstract

The bachelor thesis presents and explains selected aspects of information and communication systems security in connection with the Law on cyber security. The main aim of the thesis is to assess the changes and impact in connection with the Law on cyber security. The theoretical part describes the principles of how the Internet works, cyber security and ways how to defend against basic types of attacks and threats on the Internet from the perspective of user and manager/administrator. The practical part describes the experiment with public IPv4 address, which examines the frequency of attacks, which are conducted on devices connected to the Internet.

Key words

Security, Cyber security, The Law on Cyber Security

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně, s použitím odborné literatury a pramenů uvedených v seznamu, který je součástí této diplomové práce.

Dále prohlašuji, že veškerý software, použitý při řešení této bakalářské práce, je legální.

.....

Podpis

V Plzni dne 31.5.2016 Martin Novák

Poděkování

Tímto bych rád poděkoval vedoucímu bakalářské práce doc. Ing. Jiřímu Tupovi, Ph.D. za cenné profesionální rady, individuální přístup, připomínky a metodické vedení práce.

Obsah

Úvod

Předkládaná práce je zaměřena na popis kybernetické bezpečnosti a nového zákona. Práce je rozdělena na teoretickou a praktickou část. Teoretická část popisuje principy fungování Internetu, kybernetickou bezpečnost a možnost obrany proti základním typům útoků a hrozeb na Internetu.

Cílem této bakalářské práce je zpracovat posouzení tématu bezpečnosti informačních a komunikačních systémů a to v souvislosti s přijetím zákona o kybernetické bezpečnosti. Práce je rozdělena do tří částí. První část se zabývá popisem fungování Internetu, logováním provozu a aktuálním trendem Internetu všeho. Druhá část popisuje legislativu ohledně Internetu v ČR a shrnuje vybrané části vlastního znění zákona o kybernetické bezpečnosti. K vypracování této části bylo použito vlastní znění zákona o kybernetické bezpečnosti č. 181/2014 Sb. a důvodová zpráva k zákonu o kybernetické bezpečnosti. Třetí část popisuje anonymitu na Internetu a možnou obranu proti základním typům útoků a hrozeb. Tato část je rozdělena na pohled správce/administrátora a běžného uživatele.

Tato práce je doplněna o pokus s veřejnou IPv4 adresou, který zkoumá četnost útoků, které jsou vedeny na zařízení připojená k Internetu. K těmto útokům dochází z důvodu možného získání důvěrných informací.

Důvodem pro výběr tohoto tématu byla aktuálnost přijatého zákona, a jak se potvrdilo ve světle nedávných událostí v Evropě, i stále větší potřeba zvyšování kybernetické bezpečnosti a kybernetické obrany České republiky. Zároveň zde existuje možnost rozšířit obzory o problematice tématu bezpečnosti zařízení spadajících do kategorie Internetu všeho potenciálním čtenářům této práce.

Seznam symbolů a zkratek

§	Paragraf
A/D,	Analog/Digital
CERT	Computer Emergency Response Team
D/A	Digital/Analog
DDOS	distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOS	Denial of Service
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IoE	Internet of Everything
IoT	Internet of Things
IPS	Intrusion Prevention System
ISO/OSI	ISO/Open Systems Interconnection
ISP	Internet Service Provider
KŘP	Krajské ředitelství policie
LLC	Logical Link Control
LZPS	Listina základních práv a svobod
MAC	Media Access Control
MMS	Multimedia Messaging Service
NAT	Network Address Translation
NBÚ	Národní bezpečnostní úřad
NetBIOS	Network Basic Input Output System
NIC	Network Interface Controller
PAT	Port Address Translation
POP3	Post Office Protocol 3
RPC	Remote procedure call
SAN	Storage Area Network
SMS	Short Message Service
VPS	Virtual Private Service
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TCP/UDP	Transmission Control Protocol/User Datagram Protocol
Telnet	Telecommunication Network
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
ZKB	Zákon o kybernetické bezpečnosti

1 Komunikační a informační systémy

V dnešní době se našimi životy prolínají ICT technologie více, než si dokážeme představit. Většinou nám tyto technologie přináší užitek. Bohužel občas dojde k zneužití těchto systémů a úniku dat. Většina běžných uživatelů si neuvědomuje morální a právní dopady za své jednání, jež uskutečňují v informačních systémech. Problémem může být i nízká digitální gramotnost a povědomí o fungování Internetu. Pojďme se tedy podívat a vysvětlit si několik základních pojmů.

1.1 Kyberprostor

Kyberprostor je prostor kybernetických aktivit nejčastěji na Internetu. Internet lze chápat jako celosvětovou počítačovou síť. Internet jako síť sítí je složena z velkého množství menších sítí. Vzájemně jsou propojeny páteřní sítí.

1.2 Fungování Intenetu

Celou komunikaci lze popsat pomocí TCP/IP modelu nebo referenčního ISO/OSI modelu.

Pro tuto práci jsem si vybral pro mne přehlednější model a to ISO/OSI. Tento model obsahuje 7 vrstev: [1].

1.2.1 Fyzická vrstva

Fyzická vrstva definuje všechny elektrické a fyzikální vlastnosti zařízení. Obsahuje rozložení pinů, napěťové úrovně a specifikuje vlastnosti kabelů. Definuje, jak probíhá přenos "jedniček a nul". Zjednodušeně hovoříme o službě typu „pošli bit a „přijmi bit“.

Hlavní funkce poskytované fyzickou vrstvou jsou: navazování a ukončování spojení s komunikačním médiem. Řeší aspekty: kódování, časování, synchronizace, modulace a další. Efektivní rozložení šířky pásma mezi všechny uživatele. V rámci fyzické vrstvy rozlišujeme bezdrátový přenos, ať v licenčním pásmu nebo v bezlicenčním pásmu.

1.2.2 Linková (spojová) vrstva

Datová vrstva poskytuje funkce k přenosu dat mezi jednotlivými síťovými jednotkami, jejím úkolem je rozeznávat začátek a konec rámce. Tato synchronizace na úrovni rámců se řeší znakově orientovanými protokoly. Hlavním úkolem je přenos bloků dat, tyto bloky označujeme jako rámce (z anglického frames). Linková vrstva se dělí na dvě podvrstvy a to vrstvu logické řízení linek (Logical Link Control, LLC) a vrstvu řízení přístupu k médiu (Medium Access Control, MAC). Na této vrstvě se pracuje s MAC adresami (vysvětlení níže).

1.2.3 Síťová vrstva

Síťová vrstva zajišťuje funkce k zajištění přenosu dat od zdroje k příjemci skrze jednu případně několik vzájemně propojených sítí a vytváří tzv. end–to-end komunikaci. K tomuto propojení využívá bloky dat (pakety).

Síťová vrstva poskytuje směrovací funkce a podává informace o problémech při doručování dat. K tomuto propojení se používá Směrovač (Router), který směruje pakety do sítích, které má uložené ve své směrovací tabulce.

Nejznámější protokol pracující na 3. vrstvě je Internetový Protokol (IP). Dnes již hovoříme o zastaralém IPv4 popsaném v RFC 791, který je nahrazen IPv6 popsaným v RFC 2460. Základní jednotkou informace je paket. Na této vrstvě se pracuje s IP adresami (vysvětlení níže).

1.2.4 Transportní vrstva

Vrstva č. 4, anglicky *transport layer*. Tato vrstva zajišťuje přenos dat mezi koncovými uzly. Vyšší vrstvy ISO/OSI modelu vyžadují určitou kvalitu přenosu, kterou zajišťuje právě transportní vrstva. Vrstva nabízí spojově (TCP) a nespojově orientované (UDP) protokoly.

1.2.5 Relační vrstva

Vrstva č. 5, anglicky *session layer*. Funkcí této vrstvy je výměna informací mezi vzájemně komunikujícími procesy. Vytváří relační spojení, obnovuje a nastavuje spojení. Do této vrstvy se řadí: NetBIOS, RPC. Pomocí synchronizačních značek je relační vrstva schopna skládat navracející se pakety v pořadí v jakém byly odeslány a nikoliv, ve kterém byly přijaty.

1.2.6 Prezentační vrstva

Vrstva č. 6, anglicky *presentation layer*. Účelem vrstvy je poskytnout potřebné kódování a konverze, které v aplikační vrstvě zajistí čitelnost informací i v aplikační vrstvě jiných systémů. Vrstva transformuje data do tvaru používaného aplikacemi pomocí šifrování, komprimace atd. Vrstva nezkoumá význam jednotlivých dat, funkcí vrstvy je např. modifikace grafického uspořádání, přizpůsobení pořadí bajtů apod.

1.2.7 Aplikační vrstva

Vrstva č. 7, anglicky *application layer*. Definuje, jakým způsobem spolu komunikují v síti aplikace jako např. elektronická pošta. Vrstvu lze definovat jako softwarovou. Využívá předcházejících nižších vrstev a sama je od jejich problémů odproštěna. Do této vrsty spadají protokoly a služby jako:
FTP, DNS, DHCP, POP3, SMTP, SSH, Telnet, TFTP.

1.3 MAC adresa

Vychází z anglického „Media Access Control“, je jedinečný identifikátor síťového zařízení, které používají různé protokoly druhé (spojové) vrstvy OSI. MAC adresa je přiřazována k síťové kartě NIC bezprostředně při její výrobě (u starších karet je přímo uložena do EEPROM paměti) a proto se jí také někdy říká fyzická adresa, nicméně ji lze dnes u moderních karet dodatečně změnit (nedoporučuje se).

Ethernetová MAC adresa se skládá ze 48 bitů a podle standardu by se měla zapisovat jako tři skupiny čtyř hexadecimálních čísel. Standardně se častěji píše jako šestice dvojciferných hexadecimálních čísel oddělených pomlčkami nebo dvojtečkami V odborném textu záleží tedy na struktuře zápisu daného autora.

MAC adresa přidělená výrobcem je vždy celosvětově jedinečná. Z hlediska přidělování je rozdělena na dvě poloviny. O první polovinu musí výrobce požádat centrálního správce adresního prostoru a je u všech karet daného výrobce stejná (či alespoň velké skupiny karet, velcí výrobci mají k dispozici několik hodnot pro první polovinu). Výrobce pak každé vyrobené kartě či zařízení přiřazuje jedinečnou hodnotu druhé poloviny adresy. Jednoznačnost velmi usnadňuje správu lokálních sítí – novou kartu lze zapojit a spolehnout se na to, že bude jednoznačně identifikována.

1.4 IP adresa

V současné době je nejrozšířenější verze Internet Protocol verze 4 (IPv4), která používá 32bitové adresy zapsané dekadicky po jednotlivých oktetech.

Z důvodu nedostatku veřejných IPv4 adres je postupně nahrazován protokolem Internet Protocol verze 6 (IPv6). IPv6 používá 128bitové IP adresy zapsané hexadecimálně. [3]

Adresa se v IPv4 dělí na tři základní části:

Tab. 1 Jednotlivé části IPv4 adresy [3]

adresa sítě	*adresa podsítě*	*adresa počítače*

Rozsahy IP adres a masky sítě

Tab. 2 Rozsahy IPv4 adres [3]

Třída	*1. bajt*	*minimum*	*maximum*	*maska podsítě*
A	*0–127*	*0.0.0.0*	*127.255.255.255*	*255.0.0.0*
B	*128–191*	*128.0.0.0*	*191.255.255.255*	*255.255.0.0*
C	*192–223*	*192.0.0.0*	*223.255.255.255*	*255.255.255.0*
D	*224–239*	*224.0.0.0*	*239.255.255.255*	*255.255.255.255*
E	*240–255*	*240.0.0.0*	*255.255.255.255*	—

1.5 NAT/PAT

Z důvodů nedostatku veřejných IPv4 adres se používají vyhrazené privátní IP adresy v sítích LAN a pro komunikaci v síti Internet se na routerech musí provádět překlad IP adres nebo portů, tzv. NAT nebo PAT.

Network Address Translation (NAT, česky *překlad síťových adres*), také Network Masquerading (*síťová maškaráda*), Native Address Translation (*nativní překlad adres*) nebo IP Masquerading (*IP Maškaráda*) je způsob úpravy síťového provozu přes router přepisem výchozí nebo cílové IP adresy, často i změnou čísla TCP/UDP portu u průchozích IP paketů. Po přepisu je obvykle nutné měnit kontrolní součet datagramu. NAT se většinou používá pro přístup více počítačů z lokální sítě na Internet pod jedinou veřejnou adresou. NAT ovšem může způsobit a působí problémy v komunikaci mezi klienty a snižuje rychlost přenosu. [4]

PAT je podmnožina NAT a těsně souvisí s konceptem překladu síťových adres. PAT je také známá jako přetížená NAT (NAT overload). V PAT je obecně jediná veřejně

odkrytá IP adresa a všechny soukromé počítače/zařízení se připojují pomocí jedné odkryté adresy. Přicházející balíčky dat z veřejné sítě jsou poslány k jejich cílům na soukromé síti pomocí odkazů uložených v tabulkovém seznamu obsaženém uvnitř PAT zařízení, které tímto způsobem udržují komunikaci mezi jednotlivými páry veřejných a soukromých síťových portů. PAT upravuje jak odesílatelovu soukromou IP adresu, tak i číslo portu. PAT zařízení si vybere čísla portů, která budou vidět vzdálenými počítači na veřejné síti. Tímto způsobem PAT operuje ve 3. síťové vrstvě a zároveň 4. transportní vrstvě OSI modelu, zatímco základní NAT operuje jen ve vrstvě 3. [5]

V žádném případě NAT ani PAT nezvyšují bezpečnost a nefungují jako firewall, jak se mnoho běžných uživatelů domnívá.

1.6 Logování provozu

Díky všem těmto identifikátorům jako IP adresa, čísla portů, čas komunikace a dalším, lze snadno provádět záznam provozu tzv. logování. Poté lze určit jednoznačně zařízení v síti, které komunikovalo. A mnohdy je toto logování přímo vyžadováno zákonem.

Zaznamenávají se např. i změny MAC adres, tudíž lze snadno dohledat, kdo měl danou MAC adresu a na jakou si ji v jakém čase změnil.

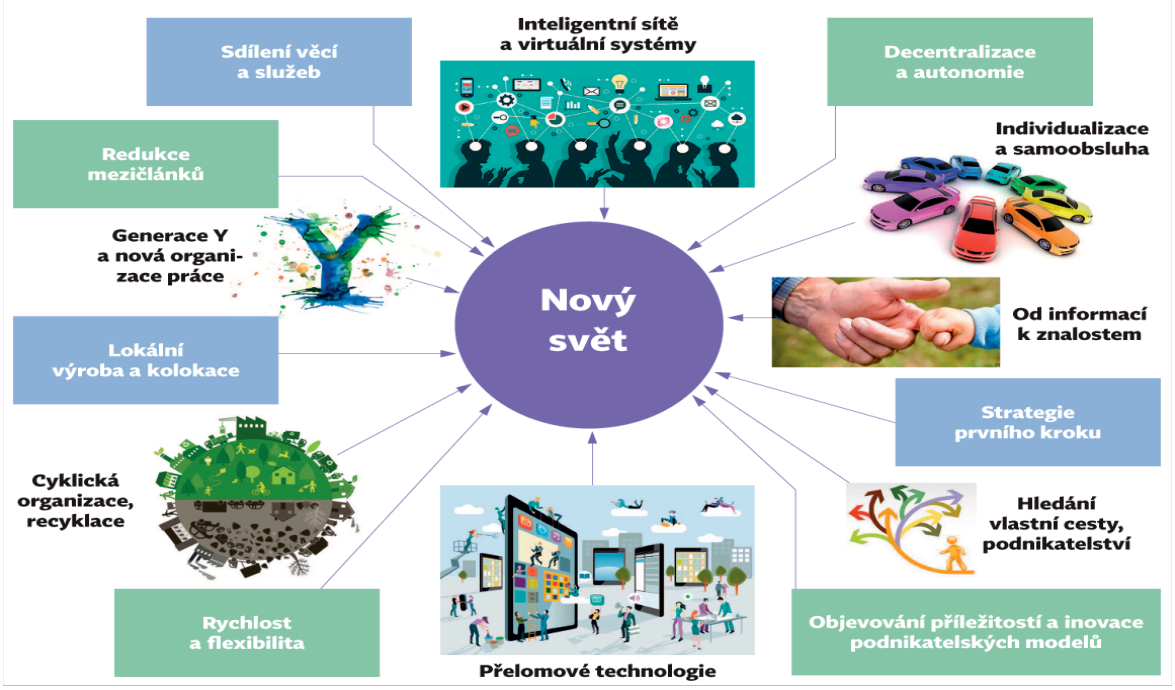
Zaznamenává se nejen odchozí komunikace, ale i příchozí komunikace na dané uzly. Navíc se často používá technologie port mirroringu na switchi, kde se daný celý provoz zaznamenává.

1.7 IoE, IoT a Internet věcí

Novým trendem v oblasti IT je Internet of everything (IoE) a Internet of thing (IoT). Internet všeho (IoE) propojuje dohromady čtyři základní pilíře IoE a to lidi, procesy, data a věci. Tím vytváří síťová propojení, která jsou ještě důležitější a cennější než kdy předtím. Přeměna informací na akce/reakce vytváří nové dovednosti, více zkušeností a bezprecedentní ekonomické příležitosti pro business, jednotlivce a národní hospodářství.

Internet Věcí (IoT) představuje narůstající propojitelnost Lidí a Věcí v takovém rozsahu, který byl dříve nepředstavitelný. Na světě je více připojených zařízení, než je všech lidí na planetě, a to v poměru 1,5 ku 1.

A díky takovému množství zařízení je třeba řešit kybernetickou bezpečnost. Podle odhadů celosvětové výdaje na zabezpečení Internetu věcí přesáhnou 300 milionů amerických dolarů. Do roku 2020 je předpoklad, že čtvrtina všech kybernetických útoků bude směřovat právě na Internet věcí. Předpokladem tohoto čísla je probíhající nasazování IoE v průmyslu (Průmysl 4.0), zemědělství, dopravě a městské infrastruktuře.



Obr. 1.1 Nový svět. Převzato – 4.Průmyslová revoluce, přednáška PREP.

2 Kybernetická bezpečnost

2.1 Přehled současné legislativy

Následující právní normy regulují kyberprostor v ČR: [6, 15]

- Zákon č. 40/2009 Sb., trestní zákoník
- Zákon č. 141/1961 Sb., o trestním řízení soudním
- Zákon č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže
- Zákon č. 121/2000 Sb., autorský zákon
- Zákon č. 127/2005 Sb., o elektronických komunikacích
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 273/2008 Sb., o Policii České republiky
- Zákon č. 89/2012 Sb., Občanský zákoník
- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví
- Zákon č. 441/2003 Sb., o ochranných známkách
- Zákon č. 527/1990 Sb., o vynálezech, průmyslových vzorech a zlepšovacích návrzích
- Zákon č. 227/2000 Sb., o elektronickém podpisu
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Účinný od 1.1.2015

2.2 Legislativa

Rámcové rozhodnutí Rady EU č. 2002/584/JHA o evropském zatýkacím rozkazu označuje za „computer-related crime" takové jednání, které směřuje proti počítači, či jednání, kde je počítač prostředkem ke spáchání trestného činu. [6]

V mezinárodních úmluvách se pro trestnou činnost páchanou prostředky informačních technologií užívá nejčastěji pojem „kybernetická kriminalita" (Cyber Crime) a používání tohoto pojmu se přeneslo do slovníku odborné veřejnosti. Pojem kyberkriminalita má obdobný charakter jako pojmy „násilná kriminalita", „finanční kriminalita", „kriminalita mladistvých" apod. Takto se nazývá skupina trestných činů, které mají společného např. pachatele, počítačový program, síť atd. [6]

Nejobecněji je možné kybernetickou kriminalitu definovat jako jednání namířené proti počítači, případně síti, nebo jako jednání, při němž je počítač použit jako nástroj pro spáchání trestného činu. Neopomenutelnou skutečností pro to, aby bylo možné uplatnit definici kyberkriminality je to, že počítačová síť (zejména Internet) je pak prostředím, v němž se tato činnost odehrává. [7]

Aby bylo možno hovořit o kybernetické kriminalitě, musí být informační prostředky, které byly ke spáchání trestného činu užity zasazeny do určitého kontextu. Kybernetická kriminalita pak tedy představuje takovou kriminalitu, kde jsou prostředky informačních technologií užity jako nástroj pro spáchání trestného činu, jsou cílem útoku pachatele. Přičemž tento útok je trestným činem, za podmínky, že jsou tyto prostředky užity či zneužity v informačním, systémovém, programovém či komunikačním prostředí. [6]

Znaky kyberkriminality:

Virtualita:

- Útočníka
- Hodnot
- Činu

2.3 Anonymita, Internet a právní subjektivita

Internet nemá právní subjektivitu. Není možné ho chápat jako hmotný předmět, věc nebo nehmotný majetek. Je to informační a telekomunikační systém složený ze subjektů, které se musí řídit právem. Jeho účastníci a provozovatelé ať veřejných či neveřejných služeb podléhají právním vztahům ve formě fyzických a právních osob. [8]

Internet jako celek nemá ani nemůže mít vlastníka, existuje však jeho fyzická struktura, která je zpravidla vlastněna a spravována určitými subjekty.

2.4 Úmluva Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. listopadu 2001

Úmluva o kybernetické kriminalitě představuje první mezinárodní dohodu týkající se trestných činů páchaných prostřednictvím informačních technologií, zejména za využití internetu nebo jiných počítačových sítí, vztahujících se k porušování autorských práv, páchání počítačových podvodů, šíření dětské pornografie a k dalším formám útoků proti informační a počítačové bezpečnosti. Jejím hlavním přínosem je sjednocení přístupu signatářů Úmluvy o kybernetické kriminalitě v otázkách postihování nejzávažnějších forem kybernetických útoků. Toho se snaží dosáhnout zejména tím, že smluvním stranám ukládá povinnost zařadit do svých národních právních řádů takové nástroje, které umožní stejný postup proti pachatelům tohoto druhu trestné činnosti bez ohledu na místo spáchání trestného činu, taktéž stanovuje základní principy pro výběr a ukládání trestů za tyto trestné činy. Signatáři této Úmluvy mají rovněž povinnost zřídit kontaktní místo, na které se mohu ostatní státy obrátit, v České republice tuto funkci plní Nejvyšší státní zastupitelství. [9]

2.5 Soukromé právo a ICT

Zákon č. 89/2012 Sb., občanský zákoník Občansko právní odpovědnost za jednání.

§ 2900

„Vyžadují-li to okolnosti případu nebo zvyklosti soukromého života, je každý povinen počínat si při svém konání tak, aby nedošlo k nedůvodné újmě na svobodě, životě, zdraví nebo na vlastnictví jiného.“[10]

§2909

„Pokud škůdce, způsobí poškozenému újmu, úmyslným porušením dobrých mravů, je povinen ji nahradit; vykonává-li však své právo, je škůdce povinen škodu nahradit, jen sledoval-li jako hlavní účel poškození jiného.“ [10]

§ 2912 odst. 1

„Nejedná-li škůdce, jak lze od osoby průměrných vlastností v soukromém styku důvodně očekávat, má se za to, že jedná nedbale.“ [10] Zde je vhodné zmínit, že ten kdo svým jednáním způsobní škodu, má za povinnost tuto škodu uhradit a to i v případě, že jí nezpůsobil vědomě.

2.6 Osobní a citlivá data

Prameny práva na ochranu soukromí (Článek 8 Evropské úmluvy o ochraně lidských práv a základních svobod – právo na respektování soukromého a rodinného života, obydlí a korespondence). Směrnice 95/46/EC zavedla standard ochrany osobních údajů v rámci Evropské unie. Národní legislativa na ochranu osobních údajů může zavést přísnější pravidla. [6]

V ČR toto upravuje zákon č. 101/2000 Sb., o ochraně osobních údajů (ZOOÚ). Vztahuje se na jakékoli zpracování osobních údajů, vyjma: - zpracování osobních údajů fyzickou osobou pro osobní potřebu (§ 3odst. 3 ZOOÚ) a nahodilé shromažďování, pokud nejsou osobní údaje dále zpracovány (§ 3 odst. 4 ZOOÚ). [11,12]

2.7 Osobní údaj

„*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*." [12]

Určeným nebo určitelným subjektem může být výlučně fyzická osoba, a to ta, k níž se osobní údaje vztahují. K určení subjektu údajů může někdy postačit jeden znak (například i fotografie), obvykle je však zapotřebí těchto znaků více, přičemž je třeba, aby jejich prostřednictvím byla osoba určena nebo alespoň určitelná, a to případně i nepřímo. [6]

2.8 Right to be forgotten

Rosudek Soudního dvora EU C-131/12 - spor španělského občana s Googlem

V roce 2010 si úřadu pro ochranu osobní údajů stěžoval Mario Costeja González na výsledky vyhledávání v internetovém vyhledávači Google. Po zadání dotazu na jeho jméno vracel vyhledávač odkazy na novinové články, které byly více než 10 let staré. V těchto článcích autoři popisovali dražbu jeho majetku z důvodu dluhů, které měl vůči státu díky neplacení sociálního pojištění. [13]

Proto v dnešní době lze požádat dle práva o zapomnění o výmaz údajů např. z vyhledávání. Dle statistik je tato služba velice využívána. Existuje i názor, že tímto může docházet k idealizaci a pokřivení vyhledávaných informací.

2.9 Autorská práva, jejich porušování a ochrana EU/ES

Problematice autorského práva jeho ochraně a porušování v EU/ES se věnuje: [6, 15]

- Úmluva Rady Evropy č. 185 o kyberkriminalitě
- Bernská úmluva o ochraně literárních a uměleckých děl (1886)
- Všeobecná úmluva o autorském právu (1952) – Ženeva
- WIPO (World Intellectual Property Organization) – 1967

ČR

- Zákon č. 40/2009 Sb., trestní zákoník
- Zákon č. 121/2000 Sb., autorský zákon
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 40/1964 Sb., Občanský zákoník
- Zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví
- Zákon č. 441/2003 Sb., o ochranných známkách
- Zákon č. 527/1990 Sb., o vynálezech a zlepšovacích návrzích

2.10 Trestně právní postih jednání útočníka

Ve zprávě KŘP Jihomoravského kraje ČR z října 2015 o narůstajícím počtu činů souvisejících s počítačovou kriminalitou hovoří por. Mgr. Lenka Drahokoupilová: [14]

„Uvedenými případy se zabýváme pro podezření z trestného činu neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 trestního zákoníku, viz níže) a po pachatelích pátráme.“

V paragrafu 230 se píše: [14]

„§ 230 (Trestní zákoník) Neoprávněný přístup k počítačovému systému a nosiči informací

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

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

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,

c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo

d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na šest měsíců až čtyři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2 a) v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo b) v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat.

(4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,

b) způsobí-li takovým činem značnou škodu,

c) způsobí-li takovým činem vážnou poruchu v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci,

d) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo

e) způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem.

(5) Odnětím svobody na tři léta až osm let bude pachatel potrestán, a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.,,

2.11 Posouzení změn a dopadů v souvislosti s přijetím zákona o kybernetické bezpečnosti

2.11.1 Účel zákona:

Z důvodové zprávy k zákonu mimo jiné vyplývá, že zákon má sloužit k zajištění bezpečného fungování informační společnosti České republiky, tj. zajištění bezpečné realizace základního práva na informační sebeurčení prostřednictvím informačních systémů, služeb a sítí elektronických komunikací. [15]

Dále se v důvodové zprávě nacházejí informace o přebírání definic subjektů z ostatních právních předpisů. Jedná se o zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. Dále pak o zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). Právní úprava zakládá kategorie správců informačních a komunikačních systémů, kteří jsou zařazeni do kritické informační infrastruktury, správců významných informačních systémů a kategorie subjektů zajišťující významné sítě. [15]

Úprava nezasahuje do provozu informační společnosti, ale má za úkol pouze zabezpečit informační kanály proti cíleným nebo nahodilým kybernetickým útokům.

Právní úprava nezakládá civilní ani trestní právní odpovědnost pachatelů kybernetických útoků. Vytváří systém bezpečnostních opatření, které mají předcházet přítomnosti kybernetických bezpečnostních incidentů. Mají zajistit, že případný kybernetický bezpečnostní incident neohrozí celkový provoz informačních a komunikačních systémů nebo fungování kriticky důležitých společenských informačních systémů. [15]

Cílem zákona je, jak popisuje důvodová zpráva mimo jiné: [15]

- stanovit minimální požadavky na standardní zabezpečení kritické informační infrastruktury a významných informačních systémů,

- zajistit GovCERT.cz v reálném čase přehled o kybernetické bezpečnostní situaci v kritické informační infrastruktuře a ve významných informačních systémech.

- Správcům kritické informační infrastruktury a významných informačních systémů:

nepřetržitý kontakt s vládním CERT umožňující kvalitnější identifikaci kybernetických bezpečnostních rizik s původem mimo příslušný systém, službu nebo síť, efektivnější analýzu kybernetických bezpečnostních událostí a účinnější reakci na kybernetické bezpečnostní incidenty.

- Ostatním subjektům:

povinnost oznamovat kontaktní údaje pro případ vyhlášení stavu kybernetického nebezpečí.

Předpoklad spolupráce těchto subjektů se soukromoprávním národním CERT.

Možnost využívat výhod vzájemné výměny informací o analýze kybernetických bezpečnostních událostí, o řešení kybernetických bezpečnostních incidentů, jakož i získávat metodickou podporu a pomoc odpovídající odborné úrovně.

2.12 Shrnutí vybraných částí vlastního znění zákona o kybernetické bezpečnosti

Zákon vešel v platnost 1. 1. 2015. [16]

Paragraf 1 upravuje práva a povinnosti osob, působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Nevztahuje se na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.

Ve paragrafu 2 je definován kybernetický prostor jako prostředí umožňující vznik, zpracování a výměnu informací, tvořenými informačními systémy, službami a sítěmi elektronických komunikací. Dále definuje:

Kritickou informační infrastrukturu nebo systémy kritické infrastruktury v oblasti kybernetické bezpečnosti. Významné informační systémy spravované orgány veřejné moci, které nejsou kritickými informačními systémy, ale narušení bezpečnosti informací v těchto systémech může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci. A významnou síť elektronických komunikací, která zajišťuje přímé připojení do veřejné komunikační sítě nebo připojení ke kritické informační infrastruktuře.

Pojem významné sítě je definován tak, aby zahrnoval páteřní sítě, jejichž prostřednictvím je kybernetický prostor na území České republiky propojen do zahraničí. Vzhledem k důležitosti kritické informační infrastruktury je jako významná síť označena touto definicí též síť, která sama o sobě není prvkem kritické informační infrastruktury, ale která zajišťuje připojení kritické informační infrastruktury ke kybernetickému prostoru. [17]

Z hlediska významnosti je nutné zmínit zejména paragraf 3, který definuje osoby a orgány, kterých se týká kybernetická bezpečnost.

Definuje orgány a osoby, které mají povinnosti vztahující se ke kybernetické bezpečnosti. Jsou to například: poskytovatel zajišťující elektronickou síť, orgány nebo osoby zajišťující významnou síť, správci informačních systémů kritické informační infrastruktury, správci významných informačních systémů a další.

Paragraf 4 hovoří o nutnosti některých subjektů přijmout bezpečnostní opatření. Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech, dostupnost, spolehlivost služeb a elektronických sítí.

V paragrafu 5 jsou podrobněji popsána a rozdělena bezpečnostní opatření. Tyto opatření se dělí na organizační a technická opatření.

2.12.1 Organizační a technická opatření

Organizační opatření popisují zejména: řízení bezpečnosti informací, řízení rizik, bezpečnost lidských zdrojů. Zvládání kybernetických bezpečnostních událostí, kybernetických bezpečnostních incidentů, audit kritické informační infrastruktury, audit významných informačních systémů a další významná opatření.

Technická opatření popisují zejména: bezpečnost průmyslových a řídících systémů, fyzickou bezpečnost. Dále pak nástroje pro: ochranu před škodlivým kódem, sběr a vyhodnocení kybernetických bezpečnostních událostí, ověřování identity uživatelů, detekci kybernetických bezpečnostních událostí a další.

Uvedená opatření vycházejí ze směrnice ISO 27000 a ISO 27002. Dle zákona teprve vyhlášky stanoví: obsah bezpečnostních opatření, obsah a strukturu bezpečnostní dokumentace, rozsah bezpečnostních opatření pro orgány a osoby uvedené v § 3 a významné informační systémy a jejich určující kritéria. [17]

2.12.2 Kybernetickou bezpečnostní událost a incident

Jde o samotné narušení bezpečnosti informací v informačních systémech, narušení bezpečnosti služeb, bezpečnosti a integrity elektronických sítí. Je tedy myšleno narušení informačního nebo komunikačního systému s negativním dopadem. [17] Orgány a osoby uvedené v § 3 jsou povinny detekovat kybernetické bezpečnostní události.

Hlášení kybernetického bezpečnostního incidentu je popsáno v paragrafu 8. Orgány a osoby uvedené v § 3 jsou povinny hlásit kybernetické bezpečnostní incidenty provozovateli národního CERT Národnímu bezpečnostnímu úřadu (dále jen NBÚ).

2.12.3 Opatření a funkce národního CERT a vládního CERT

Opatřeními se rozumí úkony, jichž je třeba k ochraně informačních systémů, služeb a sítí elektronických komunikací, nebo k řešení již nastalého kybernetického bezpečnostního incidentu.

Národní CERT zajišťuje v rozsahu stanoveném tímto zákonem sdílení informací na národní a mezinárodní úrovni v oblasti kybernetické bezpečnosti. Provozovatel národního CERTu dle § 3 přijímá oznámení kontaktních údajů a hlášení o kybernetických bezpečnostních incidentech. Dále vyhodnocuje kybernetické bezpečnostní incidenty a předává NBÚ údaje o kybernetických bezpečnostních incidentech.

Provozovatelem národního CERT může být pouze právnická osoba, která nevyvíjí ani nevyvíjela činnost proti zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací. Dále je členem nadnárodní organizace působící v oblasti kybernetické bezpečnosti a má technické předpoklady v oblasti kybernetické bezpečnosti.

Vládní CERT jako součást NBÚ poskytuje metodickou podporu dle § 3 a přijímá od osob a orgánů: oznámení kontaktních údajů, hlášení o kybernetických bezpečnostních incidentech, údaje od provozovatele národního CERT, které následně vyhodnocuje. Dále přijímá a vyhodnocuje údaje od zahraničních orgánů působících v oblasti kybernetické bezpečnosti. Mezi významnou činnost patří hodnocení zranitelností v oblasti kybernetické bezpečnosti.

2.12.4 Hlava III zákona o kybernetické bezpečnosti

Definuje stav kybernetického nebezpečí a to jako stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech, bezpečnost a integrita služeb a sítí elektronických komunikací. Ve výše zmíněných případech by mohlo dojít k ohrožení zájmu České republiky.

O vyhlášení stavu kybernetického nebezpečí rozhoduje ředitel NBÚ. Toto rozhodnutí vyvěsí na úřední desce NBÚ, stav kybernetického nebezpečí se vyhlašuje na dobu nezbytně nutnou, nejdéle však na 7 dnů s možností prodloužení na dobu ne delší než 30 dní. Tato informace je pak vyhlášena v celoplošném televizním nebo rozhlasovém vysílání.

Ředitel NBÚ informuje vládu o postupech při řešení stavu kybernetického nebezpečí a o aktuálním stavu hrozeb, které vedly k vyhlášení stavu kybernetického nebezpečí. Stav kybernetického nebezpečí končí uplynutím doby, na kterou byl vyhlášen, pokud ředitel Úřadu nerozhodne o jeho zrušení před uplynutím této doby, nebo vyhlášením nouzového stavu.

2.12.5 Kontrola, nápravná opatření a správní delitkty

2.12.5.1 Kontrola

Národní bezpečnostní úřad vykonává kontrolu v oblasti kybernetické bezpečnosti a zjišťuje dohled nad orgány a osoby uvedené v § 3. Dohled vykonává zejména nad plněním: povinností, rozhodnutí a opatření stanovených tímto zákonem a vydaných NBÚ. Národní bezpečnostní úřad kontroluje jak orgány a osoby uvedené v § 3 plní své povinnosti a dodržují bezpečnostní opatření.

2.12.5.2 Nápravná opatření

Zjistí-li NBÚ při kontrole nedostatky, uloží kontrolovanému orgánu nebo osobě, aby je ve stanovené lhůtě odstranila a popřípadě určí jakým způsobem. Pokud je zjištěn nedostatek v kritické infrastruktuře, může kontrolní orgán zakázat používání této infrastruktury než bude zjištěný nedostatek odstraněn.

2.12.5.3 Správní delikty

Právnická osoba nebo podnikající fyzická osoba uvedená v § 3 se dopustí správního deliktu tím, že nezavede nebo neprovede bezpečnostní opatření, nevede bezpečnostní dokumentaci, neohlásí kybernetický bezpečnostní incident nebo nesplní povinnost uloženou NBÚ. Za správní delikt se uloží pokuta v rozmezí 10000,- až 100000,- Kč. Dopustí-li se fyzická osoba přestupku, bude jí udělena pokuta do výše 50000,- Kč.

Za významný z pohlednu právní odpovědnoti lze považovat § 27, který specifikuje, kdy právnická osoba za správní delikt neodpovídá. A to jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila. Odpovědnost právnické osoby za správní delikt zaniká, jestliže NBÚ nezahájil řízení do 1 roku ode dne, kdy se o něm dozvěděl, nejpozději však do 3 let ode dne spáchání deliktu.

2.13 Celkové shrnutí k poznámkám k ZKB

Z výše uvedeného je znát, že celý zákon se týká pouze velkých sítí/infrastruktur s velkým dopadem a jeho snahou je dostatečná a včasná informovanost o případných problémech. Definuje pojmy jako národní a vládní CERT. Dalším bodem je definice stavu kybernetického nebezpečí.

Zákon definuje také správní delikty, z velké části za neinformování nebo neplnění nařízených opatření. Rozhodně se tento zákon tolik netýká běžných uživatelů, jak bylo v době přijetí a přípravy zákona předkládáno společnosti z médií.

2.14 Přehled nejvýznamnějších incidentů za rok 2014

Shrnutí stavu v ČR za rok 2014 popisuje Zpráva o stavu kybernetické bezpečnosti České republiky 2014, kde se píše: [18]

Závažnější útoky se odehrály v březnu 2014. Za zmínku stojí především tzv. Pony botnet, jak jej nazvala bezpečnostní společnost Trustwave. Ta vydala analýzu, uvádějící, že útočníci zprovoznili botnet za účelem krádeže přihlašovacích údajů k webovým stránkám, sociálním sítím, e-mailovým účtům a jiným službám. Podle zveřejněných údajů byl tento botnet aktivní od září 2013 do ledna 2014. Ve zmíněném období se útočníkům podařilo

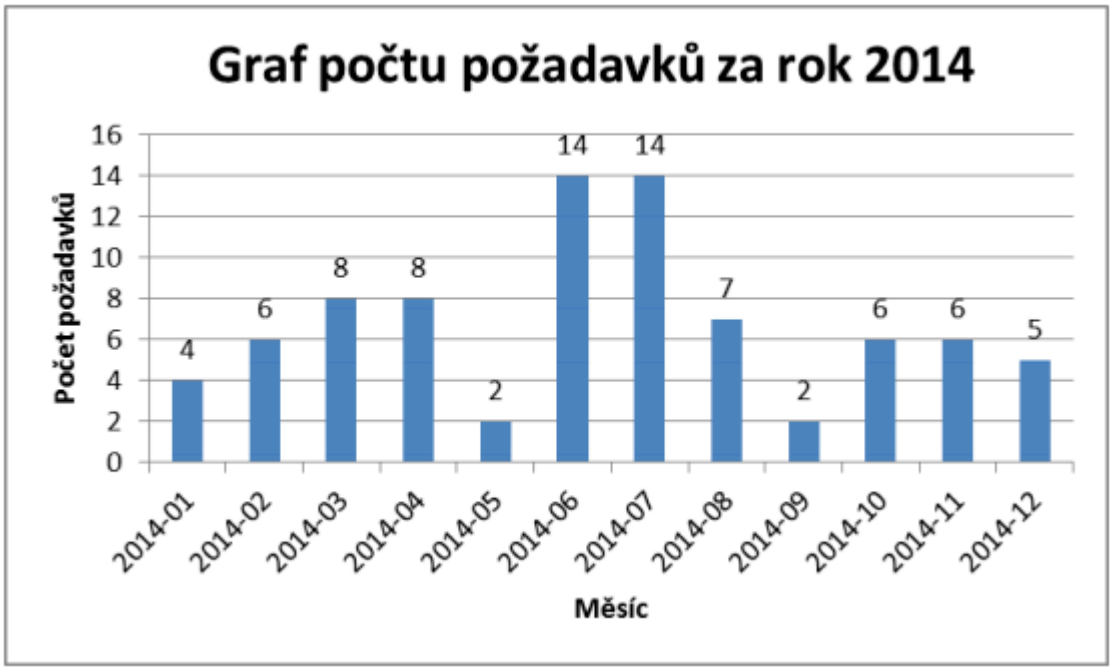
odcizit více než 700 000 uživatelských pověření. Vyjma kompromitace uživatelských účtů se tento botnet zaměřil i na některé virtuální měny.

Kromě phishingu patřily k významnějším červencovým incidentům také DoS útoky na informační systémy Kanceláře prezidenta republiky. Útok byl údajně prováděn z čínské IP adresy.

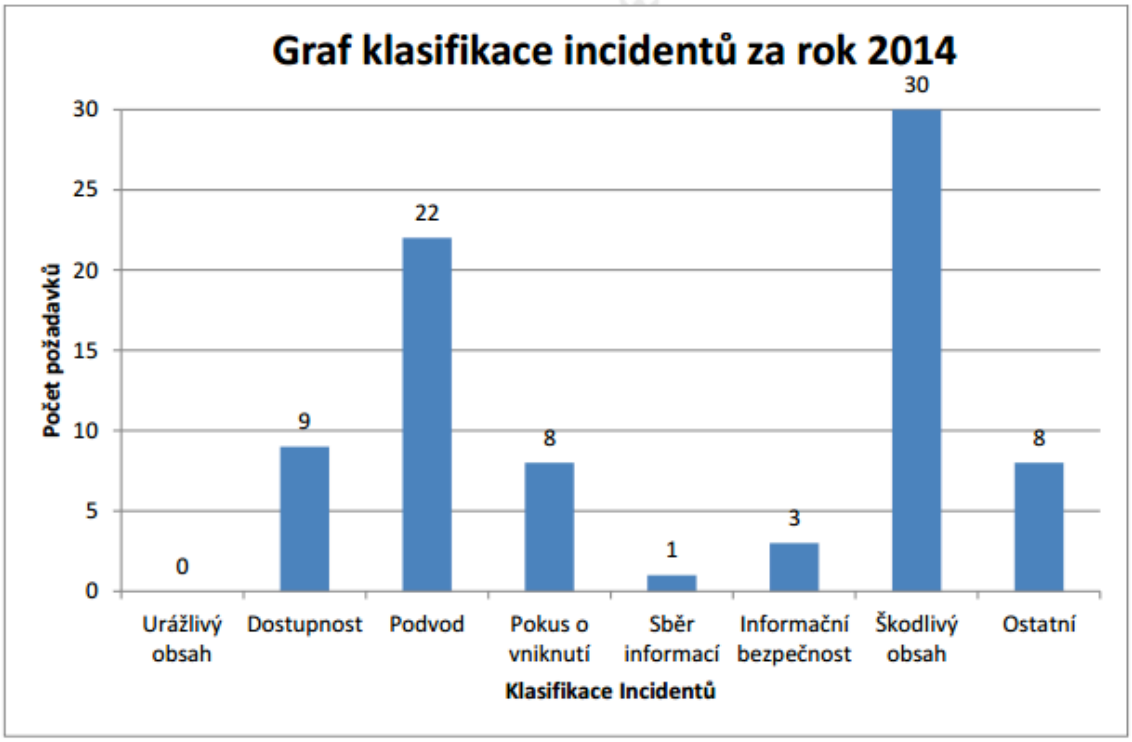
Zatímco v září se Českou republikou šířila v pořadí několikátá etapa falešných e-mailů vyzývající uživatele k zaplacení dlužné částky, říjen byl pozoruhodný pro další z ruských špionážních kampaní. Akce cílila na instituce NATO, ukrajinské vládní instituce, západoevropské vládní organizace, energetické společnosti, telekomunikační společnosti a akademické organizace. V závěru roku probíhalo dořešení některých incidentů, mezi nimi i těch týkajících se phishingových zpráv rozesílaných zákazníkům České pošty.

2.14.1 Statistika kybernetických incidentů v ČR za rok 2014

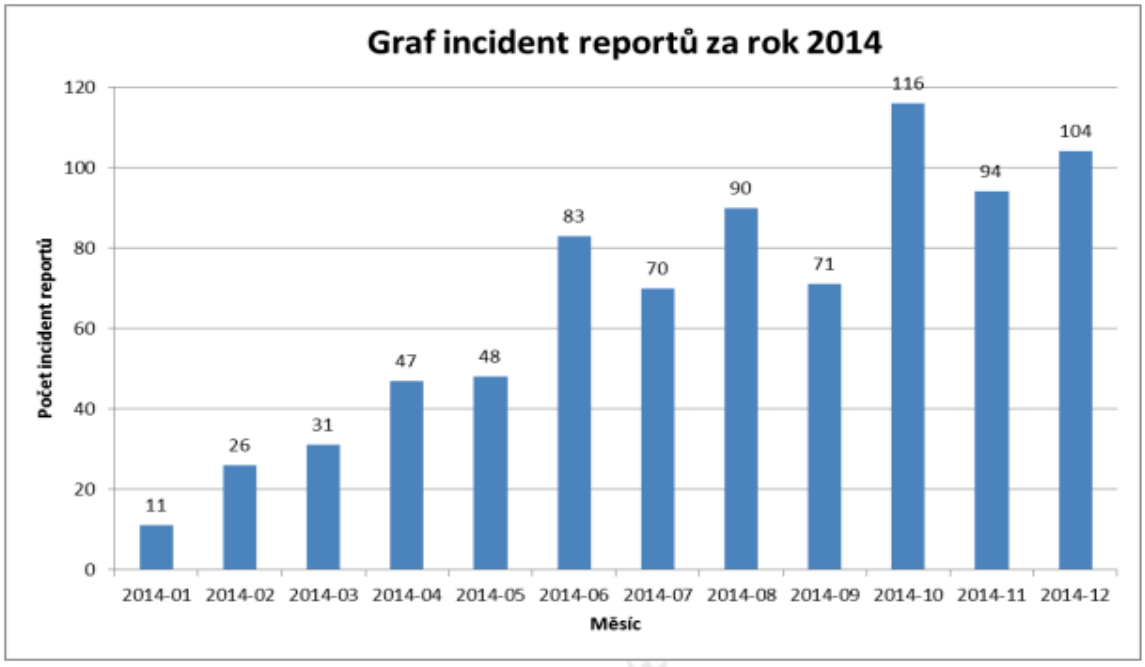
Grafické zhodnocení incidentů řešených pracovníky Národního centra kybernetické bezpečnosti v roce 2014.



Obr. 2.1 množství incidentů přijatých a zpracovaných pracovníky GovCERT.CZ v roce 2014. Převzato - Zpráva o stavu kybernetické bezpečnosti České republiky 2014.



Obr. 2.2 znázornění klasifikace incidentů. Převzato - Zpráva o stavu kybernetické bezpečnosti České republiky 2014.



Obr. 2.3 počet incident reportů za rok 2014 s rozdělením na každý měsíc. Převzato - Zpráva o stavu kybernetické bezpečnosti České republiky 2014.

2.14.2 Shrnutí incidentů za rok 2014

Na základě informací z předchozího roku můžeme vycházet z předpokladu, že charakter útoků páchaných v roce 2013 a 2014 se příliš nemění. Nejvýznamnější složkou útoků tak stále zůstávají útoky z oblasti sociálního inženýrství (phishing, spear-phishing). Přestože se pachatelé těchto útoků uchylují ke komplexnějším metodám, tak podstatou útoků zůstává vylákat od uživatelů přístupová hesla, případně distribuovat nebezpečný kód, který útočníkům zajistí přístup. Motivem takových podvodných e-mailů je zpravidla finanční zisk. Nebezpečným trendem roku 2014 je narůstající počet útoků s použití špionážních malwarů, tedy škodlivých kódů, kterých bylo použito jak proti cílům v Rusku, tak proti Spojeným státům nebo i zemím EU. Obvykle se jedná o velmi složité a komplexní malwary konstruované za účelem krádeže důvěrných a citlivých informací státních, vojenských či výzkumných institucí. [18]

2.15 Systém řízení bezpečnosti informací

Celosvětově uznávaných standardů určených k zavedení systému řízení bezpečnosti není mnoho. Ten nejrozšířenější se celým názvem jmenuje ISO/IEC 27001 – Information Security Management Systems (dále jen ISMS). Do češtiny je překládán jako systém pro řízení bezpečnosti informací. Tato norma ve svém úvodu definuje svůj účel. Tato mezinárodní norma byla připravena proto, aby poskytla podporu pro ustavení, zavedení, provozování, monitorování, udržování a zlepšování systému řízení bezpečnosti informací (Information Security Management Systems nebo ISMS). [19]

V této podkapitole je obecný popis norem využívající ISMS řady ČSN ISO/IEC 27000: [20]

2.15.1 ČSN ISO/IEC 27000

Jedná se o mezinárodní normu, která poskytuje přehled systémů řízení bezpečnosti informací, které tvoří předmět rodiny norem ISMS a definuje související termíny. Termíny a definice uvedené v této normě se týkají termínů a definic obecně použitých v rodině norem ISMS, nikoliv všech termínů a definic. Rodina norem má pomoci organizacím všech typů a velikostí zavést a provozovat systém ISMS.

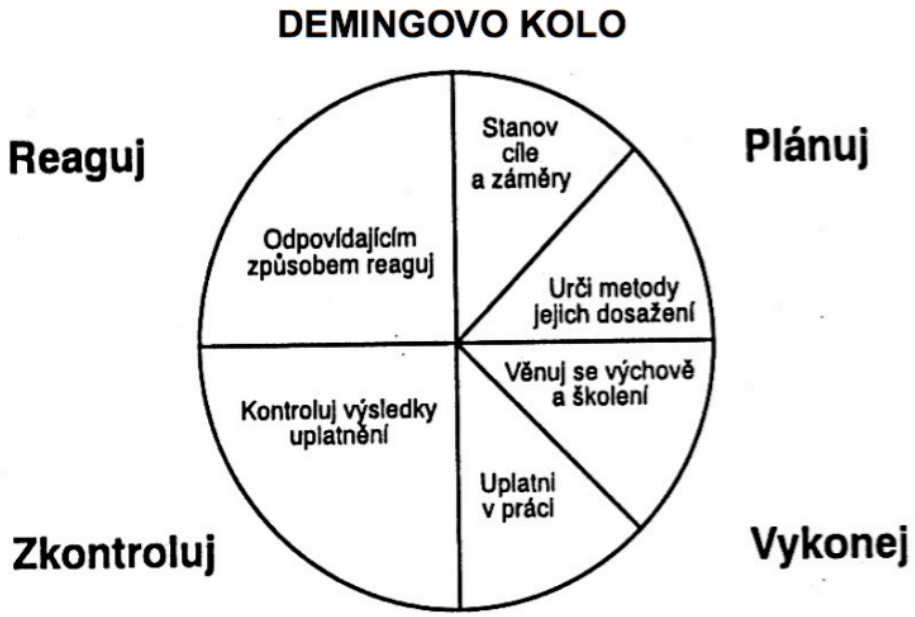
Organizace mohou použitím rodiny norem ISMS vyvinout a využívat rámec pro řízení bezpečnosti svých bezpečnostních aktiv a připravit nezávislé ohodnocení svých ISMS

týkající se ochrany informací, např. finančních informací, duševního vlastnictví a podrobností o zaměstnancích, nebo informací, které jim byly svěřeny zákazníky nebo třetími stranami.

Rodina norem ISMS zahrnuje normy, které definují požadavky na ISMS, normy, které certifikují takové požadavky, normy, které poskytují přímou podporu, podrobné pokyny nebo interpretaci pro všechny procesy „Plánuj-Prováděj (Dělej)-Kontroluj-Jednej", normy, které se zabývají směrnicemi pro ISMS specifickými pro jednotlivé úseky a normy, které se zabývají posuzováním shody ve vztahu k ISMS.

2.15.2 ČSN ISO/IEC 27001

Norma poskytuje doporučení jak používat daná opatření v rámci procesu ustavení, provozu, údržby a zlepšování systému managementu bezpečnosti informací (Information Security Management Systém, ISMS) v organizaci. Pomocí normy se uplatňuje přijetí procesního přístupu k řešení ISMS, zavádí model známý, jako Plánuj-Dělej-Kontroluj-Jednej (Plan-Do-Check-Act nebo zkratkou PDCA), který může být aplikován na všechny procesy ISMS tak, jak jsou definovány touto normou. Norma je propojena a harmonizována s normami ISO/IEC 9001:2000 a ISO/IEC 14001:2004 tak, aby bylo podpořeno jejich konzistentní a jednotné zavedení a provoz.



Obr. 2.4 Demingovo kolo. Převzato – Řízení jakosti, přednáška PREP.

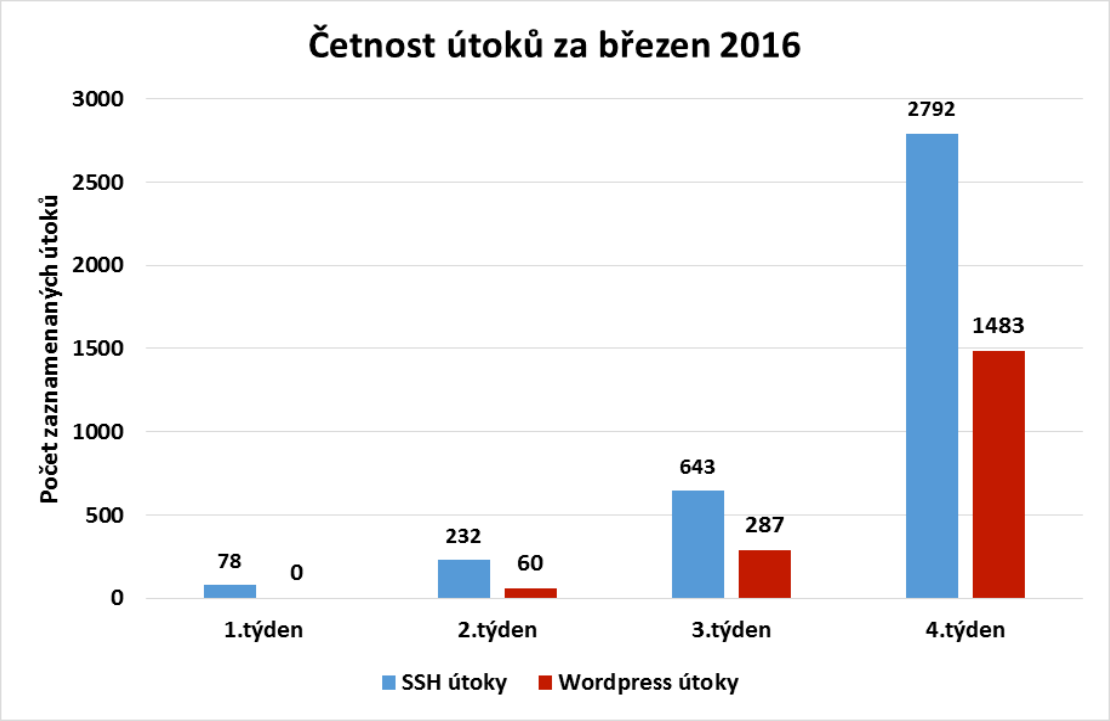
V hlavní části normy jsou upřesněny požadavky na vybudování, zavedení, provoz, monitorování, přezkoumání, udržování, zlepšování a případnou certifikaci zdokumentovaného systému managementu bezpečnosti informací. Jsou zde také specifikovány požadavky na výběr a zavedení bezpečnostních opatření chránících informační aktiva.

2.15.3 ČSN ISO/IEC 27002

Toto nové vydání mezinárodní normy obsahuje více než 133 strukturovaných oblastí doporučení rozdělených do 11 kapitol, ve kterých je uvedeno více než 5000 přímých a odvozených bezpečnostních opatření, podporujících dosahování podnikatelských cílů, přičemž odpovědnost za ně je možné jednoduše přiřadit osobám s odpovídajícími funkcemi. To zajišťuje velmi rychlé jednání při zjišťování bezpečnosti informačního systému organizace a zároveň vytváření východiska pro jeho zlepšení, zejména vymezení oblastí, které nejsou dostatečně zajištěny.

2.16 Pokus s veřejnou IP adresou

Po dohodě s OSVČ Bc. Martinem Prušou byl proveden v březnu 2016 test. Při tomto testu byl použit honeypot postavený na Raspberry Pi. Na tom byl nainstalován: OS Debian, Apache, mySQL, PHP. Dále zde byl nainstalován redakční systém wordpress a SSH server. Účelem tohoto pokusu bylo zjistit množství a typy útoků na tento honeypot. Během prvních dnů docházelo pouze ke slovníkovým útokům na ssh server, poté co stránky zaindexovaly vyhledávací servery (Google, Seznam atd.) začalo postupně docházet i ke slovníkovým útokům na redakční systém wordpress.



Obr. 2.4 počty útoků provedených na honeypot za březen 2016

Výsledkem analýzy těchto útoků je, že jde převážně o zahraniční slovníkové útoky (Čína, Ukrajina, Turecko, Ruská federace) a překvapivě i servery Amazon. Mimo Amazon jde převážně o sítě běžných ISP, což lze vysvětlit zavirovanými koncovými stanicemi zákazníků. U rozsahu Amazon jde pravděpodobně o špatně zabezpečené a napadené VPS.

3 Posouzení vybraných bezpečnostních hledisek z pohledu správce a uživatele informační infrastruktury

3.1 Botnet

Botnety jsou založeny na využívání velkého množství softwarových robotů (tzv. „bots“). Tyto boty pracují v samostatném režimu mimo IT kontrolu napadeného prostředí. Nad tímto cíleně infikovaným počítačem do určité míry převzala neoprávněně kontrolu třetí osoba, a to bez vědomí oprávněných uživatelů. [21]

Takto infikované systémy slouží nejčastěji jako základna pro anonymní připojování útočníka k internetu, k zasílání škodlivých programů, uskutečňování útoků na další cíle, realizace DDosS útoků, k šíření spamu, krádežím identit či jiným kybernetickým útokům.

Jakákoliv manipulace s těmito infikovanými počítači nebo počítačovými systémy nebo využívání takovýchto počítačů, či počítačových systémů bez souhlasu oprávněné osoby je porušením čl. 11 LZPS („Každý má právo vlastnit majetek. Vlastnické právo všech vlastníků má stejný zákonný obsah a ochranu.“) [22], a to nehledě na to, v jaké podobě bude s těmito počítači či systémy manipulováno.

3.2 Sociální inženýrství

Využívá především lidské neopatrnosti, slabosti, neodpovědnosti a hlouposti.

Sociální inženýrství využívá k získávání informací slabosti lidského faktoru. Snaha vylákat za pomoci sociálního inženýrství vnitřní informace prostřednictvím telefonů, mailů nebo osobních kontaktů, infikovaných flash disků a podobně. Využívá mimo jiné i lidské zvědavosti, například rozmístěním cd/dvd nosičů s různými „zajímavými“ popisky jako např. Platy managementu. Na sociální inženýrství doplatil v roce 2015 dnes již zemřelý poslanec Miloslav Ransdorf tím, že došlo k vytvoření falešného Twitterového účtu. [23]

3.3 Malware (Počítačové viry, trojské koně aj.)

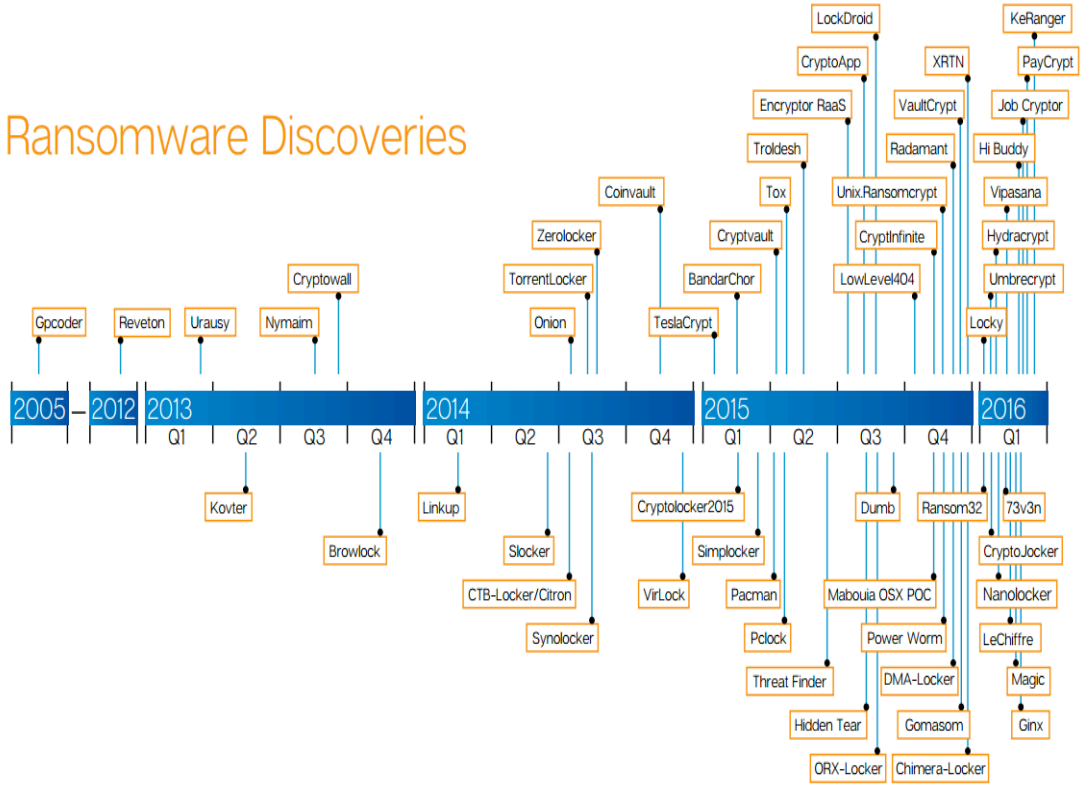
Viry jsou škodlivé kódy šířené jejich tvůrci s různými cíly. Existuje velká řada virů, účelem některých z nich je ničit, jiné naopak mají za úkol usadit se v co největším počtu počítačových systémů a tyto pak využijí k cílenému útoku.

Typické pro tyto programy je schopnost šířit se mezi systémy bez nutnosti zásahu uživatele počítačového systému, jsou schopny se sami automaticky replikovat na přenosná média, připojené síťové jednotky namapované k infikovanému systému. Různé viry se mohou projevovat různě, např. od náhodného přehrávání určité melodie, přes zahlcení systému, úpravu nebo zničení dat, až po celkovou destrukci napadeného systému. Odhaduje se, že každý zhruba 300. zaslaný email v celosvětovém měřítku obsahuje alespoň jeden počítačový vir.

3.4 Ransomware

Za zvláštní druh viru je možno označit tzv. vyděračské viry, označovány jako ransomware (z anglického „ransom“ – výkupné). Tyto programy se projevují tak, že v napadeném systému vyhledají např. soubory tabulkového procesoru (excel), nebo soubory s grafickou příponou např. JPEG, které následně uživateli znepřístupní a žádají po něm odeslání finančních prostředků na účet napadeného souboru.

Od roku 2011 probíhá téměř ve všech státech EU ransomwarový útok na koncové počítače, jehož cílem je zisk finančních prostředků. Podstatou útoku je, že dojde k infiltraci počítače malwarem. Počítač se následně stane součástí botnetu, přes který je šířen „vyděračský vir“. Tento malware následně zablokuje přístup k účtu uživatele operačního systému, v tomto případě Windows a zobrazí upozornění, že počítač byl zablokován policií daného státu. [24]



Obr. 3.1 nárůst nových Ransomware útoků- převzato z CIRT Romania

V tomto případě se útočníci snaží využít důvěřivost lidí a „vzhledu“ oficiální autority k získání peněz od uživatele.

Ze zprávy vydané společností Panda security s názvem „The Hotel Hijackers“ z dubna 2016 vyplývá, že hotelové sítě nejsou vhodným místem k přístupu k internet bankingu a dalším privátním službám, z důvodu odhalených bezpečnostních incidentů jako např.: infikované počítačové systémy a platební terminály. Většina hotelů/řetězců se stala obětí kyberkriminality. Zajímavou informací z pohledu správce/administrátra je informace, že tyto problémy se týkají i známých a luxusních hotelů/řetězců jako: Trump Hotels, Hard Rock Las Vegas, Hilton Worldwide a Starwood, odhalení těchto útoků trvalo v některých případech i více než 12 měsíců.

3.5 Phishing, Pharming, Spear Phishing, Mobilní Phishing

Pojmem phishing se označují různé formy vylákání resp. odčerpání peněžních prostředků z peněžního účtu poškozeného, získání jeho identifikačních údajů, získání údajů o platební kartě apod.

Princip phishingového útoku spočívá nejčastěji v zaslání tzv. phishingového emailu poškozenému, který na první pohled nevzbuzuje u uživatele žádné podezření o podvodnosti tohoto emailu. Součástí takového emailu bývá zpravidla odkaz, na který musí uživatel kliknout. Záminkou je často informace o nové bezpečnostní mezeře nebo kritická aktualizace, kterou je třeba stáhnout a nahrát z daného odkazu. Otevřená webová stránka se následně tváří jako originální podoba původní stránky a svojí věrohodností a funkčností je více či méně zdařilá. Pomocí této stránky je možné realizovat platební styk, vstupovat na zabezpečená konta, taková konta spravovat apod. Takto zadaná data uživatelem jsou automaticky odesílána útočníkovi. Útočník tímto způsobem může získat identifikační údaje uživatelů internetových bankovních služeb. Dále získává přístup k jednotlivým bankovním účtům uživatelů napadených systémů, souborům v napadených systémech a mimo jiné také k citlivým osobním informacím. Další údaje získané touto činností jsou údaje o platebních kartách, s jejichž pomocí je poté v prostředí internetu možné realizovat platební styk apod. [25,26]

Phishing naplňuje skutkovou podstatu trestného činu dle § 209 (Podvod) a § 234 (Neoprávněné opatření, padělání a pozměnění platebního prostředku) Trestního zákona. [6]

Pharming je sofistikovanější formou phishingu. Jde o útok na DNS server, na kterém dochází k překladu doménového jména na IP adresu. Útok začíná ve chvíli, kdy uživatel zadá do svého internetového prohlížeče doménové jméno svého finančního ústavu. Následně nedojde k přesměrování na příslušnou IP adresu originálního serveru, ale na adresu podvrženou. Webové stránky provozované na této podvržené adrese poměrně věrně kopírují originální stránky. Uživatel následně zadá přihlašovací údaje, které získá útočník. [26]

Druhým typickým způsobem pharmingu je napadení počítače koncového uživatele, kde se dá předpokládat menší míra zabezpečení.

Spear phishing je jednou z forem phishingového útoku, který cílí zpravidla na korporátní organizace. Motivy spear phishera jsou různé, od finančního zisku až po poškození dobrého jména. U spear phishingu oproti klasickému phishingu je rozdíl v tom, kdo je rozesílatelem. Spear phisher je tedy pro oběti známou osobou, která má její důvěru. Útok provede pomocí získaných informací z veřejně dostupných míst a to v dnešní době často ze sociálních sítí, kde uživatelé nezodpovědně zveřejňují svoje osobní a firemní informace. [27]

Spear phishera je v případě zisku finančních prostředků možné postihnout dle § 209 (Podvod) a § 234 (Neoprávněné opatření, padělání a pozměnění platebního prostředku) Trestního zákona. Velmi často je za takovýmto útokem např. teroristická organizace. V tomto případě pak není vyloučena odpovědnost pro trestný čin dle § 311 (Teroristický útok) Trestního zákona. [6]

3.6 Sniffing

Zachytávání dat, nelegální odposlech, záznam telekomunikačního provozu sítě. Sniffing je metodou, která zachytává data (volné packety) procházející sítí prostřednictvím tzv. snifferu. Tento sniffer slouží k monitorování a prohlížení si cizí komunikace. [26]

Ve velké většině síťových spojení dochází k nešifrované komunikaci, díky tomu je sniffing reálnou hrozbou. Takto sniffovaný provoz umožňuje „číst“ soukromá data vysílaná a přijímaná v rámci sítě. Takovou činnost můžeme označit jako nelegální odposlech či záznam telekomunikačního provozu. [26]

Mimo „hackerů“ dochází k využití sniffingu i v rámci podnikových sítí, kdy IT oddělení má za úkol sledovat činnost zaměstnanců dané organizace např. s pomocí tzv. keyloggerů, instalací sledovacího softwaru do počítače zaměstnance nebo kontrolou e-mailových schránek zaměstnanců apod. [26]

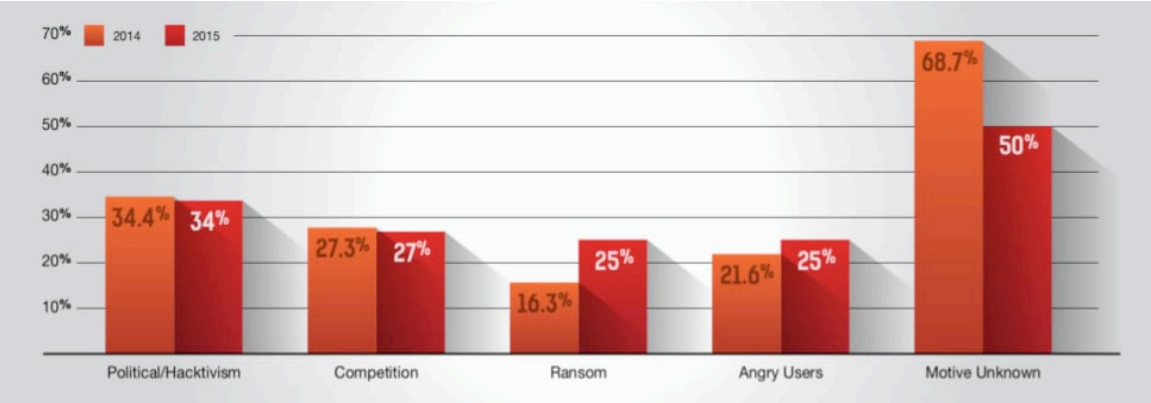
Uvedenou činností jistě dojde k zásahu do základních lidských práv a svobod, zejména se jedná o čl. 13 LZPS, a je zcela lhostejné, zda sniffing provádí externí útočník, či administrátor sítě. [26]

3.7 SPAM

Nevyžádaná elektronická pošta je pošta poškozující/obtěžující uživatele nebo instituci. Nevyžádaný obsah může být mimo jiné vkládán i do internetových diskusních fór, rozesílaný formou SMS, nebo MMS na mobilní zařízení, apod.

3.8 DOS a DDOS

Cílem těchto útoků je poškodit nebo vyřadit určité služby napadeného, například zahlcením velkým množstvím příchozích požadavků na zpracování dat. DoS útoky mohou rovněž využít slabin systémů. DDoS je distribuovaný, což znamená, že je veden z více uzlů.



Obr. 3.2 nejčastější motivace útoků- převzato z www.root.cz

3.9 Možné obrany a postupy proti kybernetickým hrozbám

Mezi další obecná pravidla lze pro správce a administrátory jistě zmínit provádění penetračních testů, nutnost záloh na více nezávislých místech a mít kvalitně zpracovaný recovery plán.

3.9.1 Ochrana proti botnetu/malwaru/virům/sniffingu

Z pohledu uživatele

- Aktuální antivirová ochrana
- Korektně nastavený firewall
- Legální software
- Základní digitální gramotnost uživatele
- Aplikovat bezpečnostní aktualizace

Z pohledu správce/organizace

- Použití IPS/IDS
- Použití kvalitního a korektně nastaveného firewallu
- Monitoring
- Kvalitní personální obsazení správy sítě/administrátorů
- Blokování nevhodných stránek
- Aplikace odzkoušených bezpečnostních aktualizací

3.9.2 Ochrana proti sociálnímu inženýrství

Z pohledu uživatele

- Základní digitální gramotnost uživatele

Z pohledu správce/organizace

- Školení zaměstnanců
- Pravidelná dlouhodobá osvěta

3.9.3 Ochrana proti spamu

Z pohledu uživatele

- Základní digitální gramotnost uživatele

Z pohledu správce

- Korektní nastavení SPAM filtrů na poštovním serveru nebo gateway
- Používání graylistingu
- Používání Blacklistů
- Školení zaměstanců
- Pravidelná dlouhodobá osvěta

3.9.4 Ochrana proti DoS a DDoS

Z pohledu uživatele

- Aktuální antivirová ochrana
- Korektně nastavený firewall
- Základní digitální gramotnost uživatele

Z pohledu správce

- Použití IPS/IDS
- Použití kvalitního a korektně nastaveného firewallu spolu s ochranou proti DoS a DDoS
- Monitoring
- Kvalitní personální obsazení správy sítě/administrátorů

3.10 Anonymita na Internetu

V ČR existuje Zákon o elektronických komunikacích č. 127/2005 Sb., který zavádí tzv. Data retention. Jedná se o povinnost poskytovatelů telekomunikačních služeb (telefony, internet) uchovávat a předávat data o komunikaci každého z nás.

V současné době se sbírají a po dobu 6 měsíců ukládají tyto informace:

- přístup k internetu
- telefonní číslo nebo jiný identifikátor koncového bodu přístupu
- typ připojení (zejména dial-up, ADSL, GPRS, kabelový modem, LAN)
- identifikátor uživatelského účtu
- identifikátor zařízení uživatele služby (zejména adresa MAC, telefonní číslo účastníka u dial-up připojení)
- datum a čas zahájení přístupu ke službě
- datum a čas ukončení přístupu ke službě - přidělená IP adresa statická nebo dynamická (v případě nejednoznačnosti identifikace koncového zařízení z IP adresy také číslo portu, například PAT)
- přístup ke schránkám elektronické pošty
- identifikátor zařízení uživatele služby (IP adresa a číslo portu)
- identifikátor uživatelského účtu
- datum a čas zahájení přístupu ke službě
- datum a čas ukončení přístupu ke službě
- adresa elektronické pošty odesílatele
- adresa elektronické pošty příjemce a označení uživatele, který je příjemcem
- použitá služba (přístup ke schránce, odeslání zprávy)

Z tohoto jasně vyplývá, že na Internetu neexistuje anonymita. Ano můžete se snažit Vaši komunikaci šifrovat, ale jak již bylo několikrát dokázáno i sebelepší šifrovací algoritmy mohou mít bezpečnostní chybu (ať již úmyslnou nebo nechtěnou).

Závěr

Cílem této práce bylo posoudit téma bezpečnosti informačních a komunikačních systémů a to v souvislosti s přijetím Zákona o kybernetické bezpečnosti.

Pro úspěšné zvládnutí této práce bylo využito odborné publikace, Zákona o kybernetické bezpečnosti č. 181/2014, důvodové zprávy k zákonu o kybernetické bezpečnosti a interní dokumenty.

Z pohledu bezpečnosti uživatele je nutné mít alespoň základní digitální gramotnost a mít dostatečné povědomí o možných hrozbách na Internetu. Toho lze dosáhnout jen soustavným a celoživotním vzděláváním uživatelů. Zde je třeba vyzdvihnout práci sdělovacích prostředků, které v případě rozsáhlých útoků všech druhů informují v hlavních vysílacích časech běžné uživatele. Pomocí těchto reportáží dojde k minimalizaci újmy uživatelů a to jak finanční, tak morální.

Jak ukázal pokus s veřejnou IPv4 adresou, tak v případě hromadného přechodu běžných uživatelů na IPv6, kdy každá taková adresa je veřejnou a tento přechod je nevyhnutelný, není otázkou, zda dojde k nárůstu útoků na tyto počítače „vystavené“ na síti Internet, ale jak velký bude dopad těchto útoků. Je tedy otázkou zda budou běžní uživatelé schopni své osobní počítače zabezpečit tak, aby minimalizovali možnost napadení svého systému. Z toho důvodu je třeba dlouhodobě podporovat technické vzdělávání, vychovávat budoucí odborníky, školit běžné uživatele a soustavně zvyšovat počítačovou gramotnost v České republice.

Z pohledu bezpečnosti státu došlo s přijetím Zákona o kybernetické bezpečnosti spolu s nárůstem bezpečnostních hrozeb k rozšíření pravomoci zpravodajských služeb v oblasti ICT. V důsledku těchto událostí dochází na popud premiéra Sobotky k posílení prostředků a personálního obsazení zejména Bezpečnostní informační služby, Vojenského zpravodajství a dalších bezpečnostních složek ČR. Výše zmíněné bezpečnostní složky nyní rozšiřují své řady o odborníky na informační a komunikační technologie, analytiky bezpečnosti a další. Podle připravované novely o tajné službě by se nově věnovalo kybernetické obraně ČR i Vojenské zpravodajství. Kybernetická obrana ČR není

uzákoněna a dle výše zmíněné novely by odpovědnost za kybernetickou obranu neslo právě Vojenské zpravodajství. Problematiku počítačové bezpečnosti má v ČR na starosti NBÚ.

Z pohledu správců a administrátorů jde o dlouhodobé sledování, monitorování sítě, koncových zařízení a vyhodnocování těchto dat. Dále je nutné sledovat aktuální hrozby, trendy a podle toho aplikovat otestované bezpečnostní aktualizace. Optimální je sledovat odborné publikace, být aktivní v komunitě IT odborníků, účastnit se konferencí zaměřených na bezpečnost a dále se aktivně vzdělávat nejen na poli odborných dovedností, ale i sledovat aktuální legislativní situaci.

Vypracování této práce pro mě bylo velkým obohacením v oblasti práce s elektronickými zdroji zabývajícími se odbornou stránkou předkládané bakalářské práce. Z profesního hlediska správce/administrátora jsem si rozšířil obzory v oblasti aktuální i připravované legislativy.

Seznam literatury a informačních zdrojů

[1] Referenční model ISO/OSI. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2016-03-05]. Dostupné z: https://cs.wikipedia.org/wiki/Referen%C4%8Dn%C3%AD_model_ISO/OSI

[2] MAC adresa. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2016-03-06]. Dostupné z: https://cs.wikipedia.org/wiki/MAC_adresa

[3] IP adresa. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2016-03-06]. Dostupné z: https://cs.wikipedia.org/wiki/IP_adresa

[4] Network address translation. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2016-03-06]. Dostupné z: https://cs.wikipedia.org/wiki/Network_address_translation

[5] Port address translation. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2016-03-06]. Dostupné z: https://cs.wikipedia.org/wiki/Port_address_translation

[6] I-Com-Unity z.s, Právo v kyberprostoru, 2015. Interní dokument I-Com-Unity z.s.

[7] *Trestněprávní ochrana před kybernetickou trestnou činností v ČR a SR*. Praha: CESNET-CERTS, 2005, s. 16.

[8] Aktuální trendy v oblasti informační kriminality z pohledu PČR. *Měská policie brno* [online]. [cit. 2016-03-06]. Dostupné z: http://www.mpb.cz/fileadmin/user_upload/Prevence/Souteze/kyber/konference/Aktualni_trendy_v_oblasti_informacni_kriminality.pdf

[9] Počítačová kriminalita: Mezinárodní úmluva je konečně závazná i pro Česko. In: *Patria.cz* [online]. Praha: Patria Online, a.s, 2014 [cit. 2016-04-11]. Dostupné z: https://www.patria.cz/pravo/2694193/pocitacova-kriminalita-mezinarodni-umluva-je-konecne-zavazna-i-pro-cesko.html

[10] Občanský zákoník (nový) | Zákon č. 89/2012 Sb. - Prevence. In: *Měšec.cz* [online]. Milady Horákové 116/109 160 00 Praha 6: Internet Info, 2014 [cit. 2016-04-11]. Dostupné z: http://www.mesec.cz/zakony/obcansky-zakonik-2014/

[11] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 1. ledna 2015. In: *Úřad pro ochranu osobních údajů* [online]. Praha: ÚOOÚ, 2015 [cit. 2016-04-11]. Dostupné z: https://www.uoou.cz/zakon-c-101-2000-sb-o-

ochrane-osobnich-udaju-a-o-zmene-nekterych-zakonu-ve-zneni-ucinnem-od-1-ledna-2015/ds-3109/archiv=0&p1=1261

[12] Pojem osobní údaj. In: *Úřad pro ochranu osobních údajů* [online]. Praha: ÚOOÚ, 2015 [cit. 2016-04-11]. Dostupné z: https://www.uoou.cz/pojem-osobni-udaj/d-1751/p1=1099

[13] Evropský soud ve sporu s Googlem: vyhledávače musí na požádání měnit minulost. In: *Lupa.cz* [online]. Milady Horákové 116/109 160 00 Praha 6: Internet Info, 2014 [cit. 2016-03-06]. Dostupné z: http://www.lupa.cz/clanky/evropsky-soud-ve-sporu-s-googlem-vyhledavace-musi-na-pozadani-menit-minulost/?forceSwitch

[14] DRAHOKOUPILOVÁ, por. Mgr. Lenka. Buďte i ve virtuálním světě obezřetní: § 230 Neoprávněný přístup k počítačovému systému a nosiči informací. In: *Policie ČR* [online]. Znojemsko: Krajské ředitelství policie Jihomoravského kraje Územní odbor Znojmo, 2015 [cit. 2016-04-11]. Dostupné z: http://www.policie.cz/clanek/budte-i-ve-virtualnim-svete-obezretni.aspx

[15] *Důvodová zpráva k zákonu o kybernetické bezpečnosti*. In: . Praha: Poslanecká sněmovna Parlamentu ČR., 2014.

[16] *Zákon o kybernetické bezpečnosti 181/2014*. In: . Praha: Poslanecká sněmovna Parlamentu ČR., 2015.

[17] I-Com-Unity z.s, Poznámky a komentáře zákonu o kybernetické bezpečnosti 181/2014, 2015. Interní dokument I-Com-Unity z.s.

[18] *Zpráva o stavu kybernetické bezpečnosti České republiky 2014* [online]. Praha: Národní centrum kybernetické bezpečnosti, 2015 [cit. 2016-04-12]. Dostupné z: http://www.govcert.cz/cs/informacni-servis/bulletiny/zprava-o-stavu-kyberneticke-bezpecnosti-ceske-republiky-2014/

[19] Zavedení systému řízení bezpečnosti – ISMS - 1.díl. In: *Chrantesidata.cz* [online]. Brno: GiTy, a.s., 2015 [cit. 2016-04-17]. Dostupné z: http://www.chrantesidata.cz/cs/art/472-isms-serial-o-rizeni-bezpecnosti#1dil

[20] ČSN ISO/IEC 27000 - 27002. In: *Portál Kybernetické Bezpečnosti* [online]. Jihlava: GORDIC spol. s r. o., 2016 [cit. 2016-04-17]. Dostupné z: https://www.kybez.cz/bezpecnost/podpora/iso-2700-2

[21] *Potřeba průkazné informatiky* [online]. In: . Praha: Radek Beneš, 2015, s. 38 [cit. 2016-04-19]. Dostupné z: www.cssi.cz/cssi/system/files/all/SI_2015_01_Benes

[22] Listina základních práv a svobod. In: *Poslanecká sněmovna Parlamentu České republiky* [online]. Praha: Poslanecká sněmovna Parlamentu České republiky [cit. 2016-04-21]. Dostupné z: http://www.psp.cz/docs/laws/listina.html

[23] Co je to sociální inženýrství? In: *365tipu* [online]. Daniel Bradbury Dočekal, 2016 [cit. 2016-04-21]. Dostupné z: https://365tipu.wordpress.com/2016/01/01/tip366-co-je-to-socialni-inzenyrstvi/

[24] Ransomware – pokuta za nic. In: *Security.ics.muni.cz* [online]. Brnp: bezpečnostní tým Masarykovy univerzity, 2014 [cit. 2016-04-21]. Dostupné z: https://security.ics.muni.cz/21-Ransomware-pokuta-za-nic

[25] PHISHING - STÁLE AKTUÁLNÍ HROZBA. In: *Národní centrum kybernetické bezpečnosti* [online]. Praha: Národní centrum kybernetické bezpečnosti, 2013 [cit. 2016-04-21]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/phishing---stale-aktualni-hrozba/

[26] Kybernetické útoky. In: *CESNET-CERTS* [online]. Praha: CESNET, z. s. p. o. [cit. 2016-04-21]. Dostupné z: https://csirt.cesnet.cz/_media/cs/documents/kyberneticke_utoky

[27] Spear phishing je cílený phishing, kterému se lze jen těžko bránit. In: *Cleverandsmart* [online]. 2012: cleverandsmart [cit. 2016-04-21]. Dostupné z: http://www.cleverandsmart.cz/spear-phishing-je-cileny-phishing-kteremu-se-lze-jen-tezko-branit/