Acta Informatica Pragensia, 2015, 4(3): 336–348
DOI: 10.18267/j.aip.80
Perspective

Vybrané trendy kybernetické kriminality

Selected Trends of the Cybercrime

Josef Požár*

Abstrakt

V rámci příspěvku je pozornost věnována trendům kybernetické kriminality v budoucím období, věnující se potírání negativních jevů v rámci kyberprostoru. Struktura článku se zabývá definicí kybernetické kriminality, její právní klasifikací a zejména možnými vybranými trendy kybernetické kriminality v budoucím období.

Klíčová slova: Kybernetická kriminalita, kybernetické útoky, trendy, právo.

Abstract

The contribution paid particular attention to trends of the cybercrime in future period dedicated to combating negative phenomena in the context of cyberspace. The structure of article concern of definition of cybercrime, its legal classification especially choosing trends of cybercrime in future period.

Keywords: Cybercrime, Cyber-attacks, Trends, Law.

1 Úvod

V posledních dvaceti letech došlo k rozmachu informačních a komunikačních technologií. Přinesly nám dříve nemyslitelné zrychlení a tedy i zefektivnění pracovních činností, zábavy a komunikací. V posledním desetiletí expandoval vývoj výpočetních systémů obrovským skokem do všech oblastí našeho života. Počítače, výpočetní systémy, nové informační a komunikační technologie, informační sítě se dnes staly samozřejmostí. Díky rozvoji výpočetní techniky je možno lépe a efektivněji provádět sběr informací, jejich třídění a provádět s nimi operace jak analytického, tak i statistického rázu.

Dnes je již používání výpočetní techniky běžné v životě téměř každého člověka. Na druhé straně bouřlivý rozvoj těchto informačních a komunikačních technologií sebou přináší i jisté negativní jevy. Fenomén výpočetní techniky však přinesl nejen zjednodušení práce lidí, ale zároveň se stal zdrojem problémů v oblasti utajení informací a ochrany dat. Zejména se jedná o počítačovou kriminalitu. V souvislosti s počítačovým útokem a zločinem se používají termíny *počítačová kriminalita, informační kriminalita* a nejnověji *kybernetická kriminalita*.

* Faculty of Security Management, Police Academy of the Czech Republic in Prague,
Lhotecká 559/7, P.O.Box 54, 143 01 Praha 4, Czech Republic
✉ pozar@polac.cz

2 Charakteristika kybernetické kriminality

Termínem počítačová kriminalita se obvykle označují trestné činy proti počítačům či trestné činy páchané prostřednictvím počítače. Obecně ji lze definovat jako trestné činy namířené proti integritě, dostupnosti nebo utajení počítačových systémů nebo trestné činy, při nichž je použito informačních či telekomunikačních technologií. Někteří autoři definují počítačovou kriminalitu jako veškeré aktivity, které vedou k neautorizovanému čtení, manipulaci, vymazaní či zneužití dat. Je to tzv. počítačová defraudace jako jedna z metod kybernetické kriminality založená na změně nebo jiné interpretaci dat s cílem získat výhodu, peníze pro vlastní neoprávněnou potřebu. V dnešní době se stále více používán termín kybernetická kriminalita od již uvedeného anglického názvu cybercrime.

Počítačovou kriminalitu lze definovat jako trestnou činnost, v níž figuruje určitým způsobem počítač (chápaný jako souhrn technického a programového vybavení včetně dat), nebo pouze některé jeho části, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti (s výjimkou majetkové trestné činnosti), nebo jako nástroj trestné činnosti. Termín informační kriminalita se užívá při zdůraznění skutečnosti, že trestný čin má vztah k softwaru, k datům, resp. k uloženým informacím, nebo častěji k informačním technologiím. Podobných definic je celá řada, bylo by však nad rámec této práce se jim podrobněji věnovat.

Počítače v podstatě neumožňují páchat novou neetickou a trestnou činnost, poskytují jen novou technologii a nové způsoby na páchání již známých trestných činů jako sabotáž, krádež, neoprávněné užívání cizí věci, vydírání anebo špionáž.

V současné době nemá pojem kybernetická kriminalita žádný oficiálně stanovený obsah ani definici. Existuje však více různorodých pojetí. Velmi jednoduše bychom mohli tvrdit, že se jedná o kriminalitu, kde je hardware nebo software nástrojem pro spáchání, anebo je samotným cílem této kriminality. Avšak nová publikace uvádí kybernetickou kriminalitu jako „trestnou činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostřední (objekty) nebo jako nástroj trestné činnosti“

Kybernetická kriminalita má řadu výrazných charakteristik, které ji odlišují od kriminality klasické. Ve většině případů kybernetické kriminality se neobjevují takové prvky, jako je násilí, použití zbraně, újma na zdraví osob apod. Zatímco však u klasické kriminality se měří doba spáchání trestného činu na minuty, hodiny, dny, trestný čin v oblasti kybernetické kriminality může být spáchán v několika tisícinách sekundy a pachatel ani nemusí být přímo na místě činu.

Další významnou charakteristikou pro kybernetickou kriminalitu jsou v důsledku značné ztráty, ať již přímo v podobě finančních částek, nebo v podobě zneužití získaných údajů. Kybernetickou kriminalitu také provází určitá diskrétnost trestné činnosti. Z uvedeného vyplývá, proč kybernetická kriminalita bývá, pro svou povahu, označována jako kriminalita „bílých límečků“.

3 Právní aspekty kybernetické kriminality

V současné době nemá pojem kybernetická kriminalita žádný oficiálně definovaný obsah, ale existuje více různorodých pojetí, podle toho, z jakého hlediska se autoři na problém dívají.

Kybernetickou kriminalitu je třeba chápat jako specifickou trestnou činnost, kterou je možné spáchat pouze s pomocí výpočetní techniky, a kde je výpočetní technika předmětem trestného činu nebo pachatelovým nástrojem ke spáchání trestného činu.

Aby bylo možno hovořit o kybernetické kriminalitě, musí pachatel ke svému jednání užít nejen výpočetní techniku, ale jeho jednání musí také naplňovat znaky skutkové podstaty některého trestného činu uvedeného v trestním zákoně a nebezpečnost takového jednání musí dosahovat požadovaného stupně nebezpečnosti činu pro společnost.

První případy trestných činů spáchaných pomocí výpočetní techniky se na území někdejšího Československa vyskytly koncem 70. a v průběhu 80. let 20. století. To ještě nebyly v masovém měřítku užívány osobní počítače, nýbrž hlavně velké sálové počítače. Rychlý rozvoj a zvyšování množství osobních počítačů a jejich postupné spojování do sítí v 90. letech vedlo k tomu, že éra kybernetické kriminality začala i u nás.

Na každý jev lze nahlížet z mnoha pohledů a pod různými úhly. Existuje více variant pohledu na kybernetickou kriminalitu. Kybernetickou kriminalitu lze dělit z hlediska postavení počítače při páchání trestné činnosti na tyto základní kategorie:

1. **Trestné činy ve vztahu k počítači, jeho příslušenství a jiným nosičům informací jako věcem movitým**

    - krádež,
    - neoprávněné užívání počítače (cizí věci).

Skutková podstata je táž jako u trestných činů, spáchaných v souvislosti s jinými movitými věcmi. V daném případě může jít zejména o tyto trestné činy uvedené v trestním zákoně:§ 205 – krádež, § 206 – zpronevěra, § 209 – podvod, § 215 a § 214 – podílnictví a § 253 – poškozování spotřebitele § 230 – neoprávněný přístup k počítačovému systému a nosiči informací, § 231 – opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat a § 232 – poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.

Krádež počítače má ovšem odlišné znaky oproti odcizení jiné movité věci. Specifičnost je zde dána faktem, že *počítač* většinou zahrnuje v sobě jednak technické zařízení včetně nosiče informací (hardware) a jednak nehmotný obsah, obecně zahrnující programy (software) a data (informace). Hodnota nehmotného obsahu může výrazně ovlivnit celkovou hodnotu odcizené věci. Ta může několikanásobně převýšit cenu samotného počítače.

2. **Trestné činy ve vztahu k software, datům uloženým informacím, počítač a jeho programové vybavení a data v něm jako cíl útoku, jako předmět trestného činu** (Trestní zákoník, 2009)

    - porušení autorského práva, práv souvisejících s právem autorským a práv k databázi, § 270 trestního zákoníku,
    - útoky viry proti počítačům a informačním systémům,
    - neoprávněné nakládání s osobními údaji, §180 trestního zákoníku,
    - ochrana přenášených zpráv (e-mail),
    - trestná činnost páchaná na internetu,
    - „hacking“ – neoprávněný přístup a průnik.

Jedná se především o jednání pachatelů, které lze postihovat podle ustanovení § 232 trestního zákoníku – poškození a zneužití záznamu na nosiči informací. Podle této úpravy bude potrestán ten, kdo v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch získá přístup k nosiči informací a takových informací

neoprávněně užije nebo informace zničí, poškodí nebo je učiní neupotřebitelnými, nebo učiní zásah do technického či programového vybavení počítače.

Neoprávněný přístup k datům hackerství je možné postihnout podle charakteru získaných informací jako trestný čin vyzvědačství § 316 trestního zákoníku. Aktéři útoků proti programovému vybavení a datům uloženým v informačních systémech se snaží obejít zabezpečení informačního systému a neoprávněně do něj vniknout buďto z důvodu prokázání svých schopností nebo s cílem informace zneužít.

3. Trestné činy, při nichž je počítač prostředkem k jejich páchání

- podvody a padělky, § 250 trestního zákoníku,
- dokladové delikty,
- neoprávněné užívání počítače k vedlejší podnikatelské činnosti – § 249 trestního zákoníku – neoprávněné užívání cizí věci nebo § 170 trestního zákoníku – porušování autorského práva,
- změny údajů v informačním systému.

Nejčastějším případem jsou podvody realizované formou neoprávněného převodu finančních prostředků na účet, který byl k tomu zvlášť založený. Pachateli jsou většinou vlastní zaměstnanci finančních institucí napadající počítačové systémy chráněné identifikací a autorizací.

Technicky zdatní zloději a zaměstnanci firem zcizí miliony až miliardy dolarů ročně. Zloději se neomezují pouze na krádeže peněz z bankovních účtů, ale zajímají se o cenné informace, jako jsou podnikové strategie, specifikace nových výrobků, podrobnosti o smlouvách, data pak nabízejí konkurenci k prodeji. Hlavními cíli útoků jsou velké banky, telekomunikační společnosti a další. Zhruba 70 % narušení systémů má souvislost se zaměstnanci postižených firem.

4. Útoky na nehmotný majetek, trestné činy ve vztahu k programu jako autorskému dílu

Svou charakteristikou by tyto delikty mohly patřit do druhé kategorie trestných činů, vzhledem k jejich četnosti výskytu jsou zařazeny v samostatné skupině.

Toto možné legislativní dělení kybernetické kriminality není samozřejmě konečné a uzavřené. V průběhu technického rozvoje se budou vyskytovat další nové útoky na data a bude nutné nově tyto skutky kodifikovat. Z hlediska technických, technologických a programových přístupů lze popsat kybernetickou kriminalitu podle hrozeb a útoků na data a informace. V současné době se do popředí dostávají případy útoků proti datům, resp. proti uloženým informacím. V tomto případě pachatel vede útok proti uloženým či přenášeným datům. Tento útok může nabýt několika forem. Od nejjednoduššího smazání nebo pozměnění programového vybavení až po zavedení viru do programového vybavení a následné ztráty programů a dat.

Mezi formy takového jednání řadíme již zmíněný hacking. Podstatně jiná situace nastává, když se hacker, který vnikl do databáze, rozhodne, že získané informace nejspíše za určitou protihodnotu použije.

Další formou tohoto druhu kybernetické kriminality je destrukční činnost pomocí virů. Od počátku počítačů jsou průvodním negativním jevem počítačové viry. Počítačový virus je taková forma počítačové infiltrace, která má schopnost vlastního množení a infikování dalších systémů, bez vědomí uživatele. Jedna z definic počítačového viru zní: **počítačový virus je program či část programového kódu, schopný sebereprodukce bez vědomí uživatele**.

Jinými slovy: Vir je počítačový program, který se prostě šíří, aniž by o tom člověk sedící za počítačem věděl (Přibyl, 2015). Škála destruktivní činnosti je samozřejmě velmi široká a bude záviset nejen na skupinovém typu viru, ale i na jeho konkrétním typu, mnohdy variantě či mutaci. Takovými nejobvyklejšími akcemi virů je mazání souborů, zformátování pevného disku, modifikace dat, označování sektorů za vadné atd. Na druhé straně existují i neškodné viry, které jen vyhrožují texty či grafickými efekty na monitoru. Počítačové viry mohou být různého druhu. Například trojské koně, což jsou v podstatě programy, které se chovají jako zcela legální, ve skutečnosti však provádí škodlivé operace. Jedním z velmi rozšířených virů jsou i tzv. červi[1]. Do počítače pronikají většinou elektronickou poštou a otevřením zpravidla souboru v příloze se červi aktivují a rozesílají zavirované e-maily na další adresy, které jsou v adresáři počítače uloženy. Další variantou viru jsou back door čili zadní vrátka. Tento vir se chová podobně jako trojský kůň[2]. Zadní vrátka mohou být do systému nainstalována spolu s dodaným programem, kde může mýt trojský kůň, který je vstupem pro infiltraci. To znamená, že připojený hacker může získat přístup k datům a informacím, může mazat celé soubory, programy, může telefonovat na účet pravého uživatele, nakupovat a čerpat finanční prostředky z tohoto účtu apod.

S rozvojem bezhotovostního platebního styku se objevuje i další forma tohoto druhu kybernetické kriminality, tzv. *carding*. Jím se obecně rozumí zneužití platebních karet. Dochází k němu různými způsoby. Vznik cardingu je spjat s rozvojem internetové komerce. Platební karta se stává převažujícím platebním instrumentem a zabezpečení je v mnoha případech nedostatečné. Pachatelé cardingu získávají osobní údaje majitelů účtů různými pokoutnými způsoby. Pachatelé často využívají tzv. generátorů, což jsou programy, které dokáží vygenerovat číslo kreditní karty na základě zřejmě odcizeného algoritmu. Typický cardingový útok vypadá tak, že na cílovém účtu se začnou objevovat podezřelé pokusy o transakci, kdy jakoby někdo testoval, jaký je na účtu zůstatek, a kolik je ještě banka schopna vyplatit. Toto testování probíhá tak dlouho, až je příkaz k platbě proveden.

Škála protiprávního jednání pachatele s využitím počítače při klasifikaci kybernetické kriminality je velmi široká. Řadíme sem především softwarové pirátství. Mezi základní formy softwarového pirátství je možní zařadit:

- průmyslově vyráběný software bez udělení licence,
- kopírování softwaru bez udělení licence,
- plagiátorství nebo také pozměňování originálního softwaru a vydávání za vlastní,
- nelegální stahování softwaru pomocí sítě Internet,
- vědomé užívání nelegálně vyrobeného softwaru apod.

Crackeři[3] jsou podobná skupina lidí jako hackeři, jen s tím rozdílem, že se svými průniky většinou živí. Specializují se především na užitkový software a hry, u kterých prolomují ochranné mechanismy proti kopírování a pak celé programy a hry vystavují na Internetu k volnému stažení nebo za poplatek. Mezi další formy této kriminality dále patří:

[1] Červ se obvykle šíří bez účasti uživatele, přičemž distribuuje své úplné kopie (případně pozměněné) v rámci sítí. Může spotřebovávat paměť nebo šířku pásma sítě, což může vést ke zhroucení počítače.

[2] Počítačový program, který se jeví jako užitečný, ale při stažení z webu pak později působí škody.

[3] Cracker neoprávněně přistupuje k datům v počítačové síti nebo počítači a slídí v nich, krade je, nebo s nimi jinak manipuluje a také ten, kdo prolamuje zabezpečení programů proti nelegálnímu užívání a kopírování.

- phreaking – zneužívání telekomunikačních služeb, kdy se využívá telefonní linka bez zaplacení za tyto služby provozovateli,
- sniffing [4] – neoprávněné monitorování elektronické komunikace za využití speciálních programů, zpravidla v síti Internet,
- warez [5] – moderní počítačové pirátství, kdy se sdružují skupiny crackerů, za účelem prolomení softwarových ochran programů,
- spamming – zasílání nevyžádané elektronické pošty, nejčastěji s propagačním obsahem,
- dále vydírání, elektronické výpalné, šíření pornografie, extremismus na Internetu apod.

4 Trendy kybernetické kriminality

Kromě běžných uživatelů informačních a komunikačních technologií se bohužel řadí také mnoho profesionálních pachatelů, kteří provádějí latentní, skryté operace. Kybernetickou kriminalitu v současné době rozvíjejí ti, kteří v ní hledají zdroj obživy, což vede k narůstajícímu zapojení organizovaného zločinu. Metody profesionálních pachatelů jsou stále rafinovanější, a proto aktivní ochrana se stává absolutní nezbytností. (Caponi, 2014; Cherry Bekaert, 2014; Ciccatelli, 2013)

Dnešní firmy, organizace a státní instituce jsou na počítačích, počítačových sítích a obzvláště na internetu silné závislé. Počet evropských uživatelů internetu v prosinci 2014 prolomil hranici 100 milionů. Bohužel internetový protokol TCP/IP[6] je velice málo zabezpečený proti útokům zvenčí. Dnes lze kybernetickou kriminalitu charakterizovat následujícími trendy:

1. Nové delikty lze spáchat pouze on-line. Jedná se o trestné činy či pouze přestupky proti integritě, důvěrnosti a dostupnosti počítačových dat a informací. Nejlépe dokumentovanou formou tohoto typu deliktu je hacking.
2. Tradiční útoky na okolní počítače, sítě a informační systémy jsou realizovány prostředky informačních a komunikačních technologií také on-line. Pachatelé využívají k útoku na data a počítačové sítě takové prostředky jako vydírání, podvody a v poslední době jsou realizovány metody tzv. sociálního inženýrství. Před dvěma roky bylo zaznamenáno každý měsíc přibližně 300 škodlivých kódů a dnes je evidováno až 1 500 takových ohrožení. Kybernetická kriminalita zároveň odráží vývoj tradičních off-line kriminálních aktivit. Odhaduje se, že přibližně 70 % veškerých škodlivých kódů vzniká za účelem zisku. Kybernetická kriminalita je v Evropě trestně právní kategorií s nejvyšším nárůstem trestných činů.
3. Vzrůstající ohrožení mobilních komunikačních systémů. Nedávný virus Cabir a jeho následné varianty ukázaly, že ani mobilní zařízení nejsou před útoky zvenčí bezpečná. Celosvětový počet uživatelů mobilních telefonů koncem roku na více než 2,2 miliardy. Sítě 3G přinesou ještě větší konektivitu a vzroste prodej Smartphonů. Podle odhadů vzroste počet útoků na mobilní zařízení v průběhu roku pěti až desetinásobně.

---

[4] Sniffing (čmuchání) – též odposlouchávání přenosových paketů, které hackerovi vůbec nepatří. Pak přijímá a zapisuje obsahy všech paketů s danými vlastnostmi. V těchto paketech, pokud nejsou vedeny šifrovaně, je otevřeně vypsáno uživatelské jméno a heslo. Toho lze pak jednoduše zneužít.

[5] Warez je termín počítačového slangu označující autorská díla, se kterými je nakládáno v rozporu s autorským právem.

Slovo bylo vytvořeno z anglického slova warez (zboží).

[6] Rodina protokolů **TCP/IP** (*Transmission Control Protocol/Internet Protocol* je „primární přenosový protokol/protokol síťové vrstvy“) obsahuje sadu protokolů pro komunikaci v počítačové síti a je hlavním protokolem celosvětové sítě Internet. Komunikační protokol je množina pravidel, která určují syntaxi a význam jednotlivých zpráv při komunikaci.

4. Zneužívání sítí Wi-Fi. Síťoví červi představují nebezpečí pro mobilní telefony a další přenosná zařízení. Bezpečnost sítí Wi-Fi však byla již v roce 2004 rovněž předmětem velkých obav. Viry napadající sítě Wi-Fi mohou přecházet mezi jednotlivými sítěmi a spouštět lokalizované útoky typu Denial-of-Service[7].

5. Masové rozšíření spammingu pomocí trojských koní a botů. Velký nárůst počtu e-mailových červů (mass mailers) upozornil na jejich existenci. Masový spamming, který následně umožňuje stažení trojských virů, nakazí nechráněné počítače, aniž by to jeho uživatel zpozoroval. Takový způsob tajného infikování počítačů umožňuje útočníkům ovládat pomocí „botů" – automatických programů, které z jiného počítače ovládají napadený počítač na dálku. Odborníci odhadují, že počet botů narůstá až o 30 každý den. Jedná se o nesmírně populární způsob napadení, protože infikování se neustále vyvíjí a je velice obtížné je vystopovat. V důsledku toho lze předpokládat, že poroste počet závažných „nárazových" útoků. Jak se tisíce nakažených počítačů začnou spojovat do jedné obrovské sítě (bot network – botnet), umožní provádět rozsáhlé útoky typu Distributed Denial of Service, kde bude kritické úrovně dosaženo během několika minut a dokonce sekund. Pak nastane přetížení a zahlcení napadeného serveru velkým množstvím požadavků na služby a ten přestane vůbec fungovat. Stane se tak nedostupný pro ostatní uživatele.

6. Nárůst phishingu. Podle Anti-Phishing Working Group bylo v listopadu 2014 zaznamenáno 1518 nových jedinečných phishingových útoků, v lednu téhož roku to bylo jen 176 útoků. Phishing znamená rozesílání falešných e-mailových zpráv ze zdánlivě oficiálního zdroje. Tyto zprávy obsahují zpětné adresy nebo odkazy a požadují, aby adresát aktualizoval určité osobní informace, např. hesla, čísla bankovních účtů nebo dokonce PIN. To je právě oblast sociálního inženýrství, která se v poslední době velice rozšiřuje. Vzhledem k tomu, že internetoví podvodníci jsou stále motivováni finančním ziskem, se předpokládá, že počet případů phishingu se každý měsíc zdvojnásobí a bude zejména pro běžné uživatele představovat velmi reálnou hrozbu.

7. Rozšiřování spyware. Spyware jsou programy, které se bez vědomí uživatele zachytí a instalují v jeho systému. Až dosud se jednalo o převážně neškodné programy, které měly hlavně za úkol sledovat, které internetové stránky uživatel otevírá. Spyware využívaly hlavně marketingové a reklamní společnosti. Internetoví pachatelé této trestné činnosti se však stále častěji zaměřují na finanční zisk, a spyware se tak bude stále častěji využívat k zištným a nelegálním účelům. Jedná se například o zcizení identity (identity theft), kdy se takový pachatel vydává za někoho jiného, či k monitorování klávesnice za účelem zachycení osobních údajů.

   Během příštích deseti let dojde k masivnímu rozšíření informačních a komunikačních technologií (ICT), tak jak ho dnes známe. *S nástupem Internetu věcí bude docházet k propojování ICT firem s firmami z oblasti spotřební elektroniky, ale i dalších oborů. V následujícím období tak budeme svědky změn na trhu, bude docházet k vzájemným akvizicím, investicím nebo dohodám o užší spolupráci mezi firmami z oboru ICT a mimo něj.*

   Ve studii Cisco Technology Radar se spojují názory více než osmdesáti předních odborníků a inženýrů jak ze společnosti Cisco, tak mimo ni. V posledních měsících jsme

[7] Denial of Service (DoS) čili odmítnutí služeb, kdy se jedná o útok na přenosové kanály a paměti serveru, kdy je tento zahlcený desítkami tisíc e-mailů a není schopen všechny v daném čase obsloužit. Poté může nastat kolaps, zhroucení serveru.

svědky velmi razantní proměny světa ICT a tak nástup internetu věcí a Internet of Everything přináší na ICT prostředí zcela nové nároky a to se tomu musí přizpůsobit. Dobrým příkladem je například zjednodušování síťové infrastruktury směrem k softwarově definovaným sítím, které bude příští rok rozhodně jedním z nejviditelnějších trendů.

8. Posun ke cloudovým úložištím. Od mobility a videa se bude svět ICT posouvat stále více ke cloudovým technologiím a programovatelným či dynamickým sítím. Stále více zařízení bude připojeno k internetu a stále více služeb či technologií bude k dispozici prostřednictvím internetového prohlížeče z cloudu.[8] To s sebou přinese vyšší nároky na bezpečnost, ale také na dostupnost a rychlost doručení.

9. Nástroje pro vzdálenou spolupráci a komunikaci v reálném čase se přesunou do cloudu. Technologie WebRTC umožňující audio a video komunikaci v reálném čase v prostředí internetového prohlížeče se přesune i do firemního segmentu. To společně s posilujícím trendem BYOD[9] bude znamenat komoditizaci řešení pro týmovou spolupráci na dálku.

   Podle údajů amerického úřadu pro statistiky práce (US Bureau of Labor Statistics) bude téměř polovina amerických firem umožňovat nové formy komunikace v rámci týmu, včetně sociálních sítí a spolupráce na dálku. Videokonference, instant messaging[10], blogy a další komunikační nástroje se stanou ve firmách standardem. WebRTC umožní odstranit bariéry a umožní začlenění do týmu i těm, kterým v tom dosud bránil nějaký handicap či jiné překážky. Díky novým technologiím získají zaměstnanci mnohem větší flexibilitu a budou moci pracovat kdykoli a odkudkoli. To dovolí mnohem lépe vyvážit svůj osobní a pracovní život. Nástroje pro vzdálenou spolupráci v týmu tak například usnadní návrat ženám po mateřské dovolené, stejně jako třeba lidem s tělesným postižením, kteří z různých důvodů nemohou docházet do kanceláře. Stejně tak ale umožní všem zaměstnancům rozložit si práci tak, aby jim zbýval čas na koníčky a rodinu.

10. Nároky na bezpečnost internetu věcí dále porostou. Rostoucí počet zařízení připojených k internetu bude znamenat i změnu nároků na bezpečnost. Hranice ICT bude postupně smazána. Bude potřeba vyvinout zcela nové bezpečnostní standardy, které zajistí bezpečné připojení zařízení, se kterými se dosud svět ICT nesetkával. Může jít například o nositelnou elektroniku, ale i chytré elektroměry či senzory, ať již v domácnostech, tak ve městech či průmyslu.

    Hranice počítačových sítí se s nástupem internetu věcí smazávají. K internetu už nejsou připojeny jen počítače či notebooky, ale i nositelná elektronika, senzory a další zařízení. To ale znamená zároveň nárůst počtu potenciálních slabých míst, protože jejich výrobci

---

[8] Cloud computing je na Internetu založený model vývoje a používání počítačových technologií. Lze ho také charakterizovat jako poskytování služeb či programů uložených na serverech na Internetu s tím, že uživatelé k nim mohou přistupovat například pomocí webového prohlížeče nebo klienta dané aplikace a používat je prakticky odkudkoliv. Uživatelé neplatí za vlastní software, ale za jeho užití. Nabídka aplikací se pohybuje od kancelářských aplikací, přes systémy pro distribuované výpočty, až po operační systémy provozované v prohlížečích.

[9] BYOD (angl.. "Bring Your Own Device") je vzrůstajícím trendem, který znamená, že si zaměstnanci nosí svá vlastní "chytrá" zařízení (jako jsou notebooky, smartphony, wi-fi routery apod.) do firemního prostředí. To samozřejmě zvyšuje tlak na informační bezpečnost, kterou BYOD znesnadňuje.

[10] Instant messaging je internetová služba, umožňující svým uživatelům sledovat, kteří jejich přátelé jsou právě připojeni, a dle potřeby jim posílat zprávy, chatovat, přeposílat soubory mezi uživateli a i jinak komunikovat. Hlavní výhodou oproti používání např. e-mailu spočívá v principu odesílání a přijímání zpráv v reálném čase.

nemají dosud s kybernetickou bezpečností téměř žádné zkušenosti. Bude tak nutné připravit zcela nové standardy a změnit pohled na tuto problematiku.

Například chytré elektroměry mohou pomoci dodavatelům elektřiny přizpůsobit rozvodnou síť aktuálním potřebám odběratelů. Zároveň je ale třeba zajistit, aby data odesílaná takovým elektroměrem byla pro další zpracování anonymizována a nemohlo dojít k jejich zneužití.

Dalším příkladem jsou třeba výrobní stroje v průmyslu, které mají na rozdíl od spotřební elektroniky delší životní cyklus a možnosti pro upgrade jejich ICT částí jsou jen velmi omezené. Přesto bude potřeba zajistit, aby byly během svého dlouhého životního cyklu ochráněny před případnými kybernetickými útoky, a zároveň mohly firmy využívat informací z jejich senzorů pro optimalizaci výroby.

11. Fog Computing přesune data blíže k uživateli. Senzory připojené k internetu budou zasílat data do cloudu a zároveň je z něj přijímat. Jak jejich počet poroste, může docházet ke zpožděním při přenosu dat.

    Fenomén Fog Computingu umožní přenést data blíže k místu, kde jsou potřeba. To sníží nároky na kapacitu sítí, jejíž další navyšování by již nemělo smysl. Mezi cloudem a zařízeními tak vznikne prostor pro datová úložiště a ICT infrastrukturu, která budou shromažďovat data blíže uživateli. Nástup cloudových technologií a internetu věcí přinese výrazné zvýšení provozu v datových sítích. Aby nedocházelo k přetěžování některých přenosných tras, umožní Fog Computing vložit inteligenci na rozhraní mezi ICT infrastrukturou či třeba senzory a cloudem. Například přepínač doplněný o aplikaci analyzující spotřebu energie u odběratele může automaticky, aniž by data procházela internetem až do cloudu, přepínat mezi jednotlivými zdroji energie podle aktuální spotřeby a dostupnosti. Může tak například místo centrálního přívodu přepnout na energii dodávanou fotovoltaickými panely a tím pomůže snižovat náklady na energie.

12. Poroste význam analýzy dat v reálném čase. Možnost analýzy dat v reálném čase se stane jednou z nejdůležitějších vlastností nové generace ICT infrastruktury. Analytické nástroje integrované do síťových zařízení umožní zaznamenávat dění v síti, monitorovat její výkon a detektovat případné anomálie. To umožní mnohem efektivnější ochranu proti případným útokům, ale také optimalizaci sítě v reálném čase. Analytické nástroje založené na velkých datech a jejich real-time analýze pak otevírají prostor rozvoji aplikací pro business intelligence, řízení dopravy či přenosových sítí.

    V roce 2050 překročí populace Země hranici 9 miliard lidí. Jen pro pokrytí z toho plynoucí poptávky bude nutné zvýšit produkci potravin o 70 procent. Právě analýza dat v reálném čase může významně přispět ke zvýšení produktivity a zmenšení ztrát. Přesnější předpověď počasí s využitím analýzy dat v reálném čase pomůže například stanovit ideální čas sklizně či hnojení, stejně jako přesněji odhadovat úrodu.

13. Analýza chování uživatelů napomůže odhadu jejich potřeb.

    Zejména v oblasti dopravy a prodeje bude znamenat revoluci schopnost odhadovat přání či záměry uživatelů na základě jejich dosavadního chování a umístění. Tzv. Context-Aware Computing pomůže ICT infrastruktuře připravit ta data, která budou v krátké době potřeba. Podle odhadu expertů je téměř třetina veškerého provozu ve městech způsobena řidiči hledajícími místo k parkování. Pokud budou mít řidiči ve svých chytrých telefonech aplikaci, která jim umožní najít nejbližší aktuálně volné parkovací místo, může doprava ve městech poklesnout až o 40 procent a ruku v ruce s tím klesnou i emise oxidu uhličitého. Stejně tak například data ze senzorů monitorujících okolní prostředí mohou

pomoci dodavatelům energií lépe odhadovat nároky na rozvodnou síť. Chytré termostaty tak například nejenže zapnou či vypnou vytápění, ale zároveň mohou informovat dodavatele o klesající teplotě v nějaké oblasti a tedy o pravděpodobném zvýšení nároků na dodávku elektřiny či plynu pro vytápění.

14. Zjednodušení síťové infrastruktury.

    V roce 2018 bude k internetu připojeno více než 20 miliard zařízení. To si vyžádá zjednodušení síťové infrastruktury a vývoj autonomních sítí, které se budou schopny přizpůsobovat momentálním potřebám uživatelů, aplikací, ale třeba i senzorů. Vývoj aplikací a sítí bude tak do budoucna mnohem úžeji propojen. Dosavadní architektura sítí neodpovídá požadavkům, které na ně bude klást nástupu internetu věcí a Internet of Everything. Propojení lidí, procesů, dat i zařízení do sítě přinese zcela nový typ požadavků na síťovou infrastrukturu a otevře prostor pro zcela nové aplikace. Bez zjednodušení by byla stávající infrastruktura velmi zranitelná. Východiskem jsou Softwarově definované sítě (SDN), které umějí automaticky přizpůsobit architekturu sítě momentálním potřebám uživatelů nebo aplikací. Takovéto autonomní sítě a prvky zjednoduší celou architekturu, a zároveň sníží nároky na čas administrátorů, protože se budou schopné automaticky konfigurovat, spravovat a v případě potřeby i opravit.

Společnost Sophos (2015) zveřejnila zprávu Security Threat Trends 2015, ve které se zaměřila na největší bezpečnostní rizika nadcházejícího roku – viz také článek (CIO, 2015).

1. Menší závažnost exploitů[11] a jejich obtížnější zneužití povede nižšímu počtu hrozeb. Hackeři se po mnoho let zaměřovali především na operační systémy Microsoft Windows. Díky velkému úsilí společnosti Microsoft o snížení závažnosti zneužitelných programátorských chyb je dnes ale vytvoření škodlivého software mnohem obtížnější. Spolu s tím, jak roste složitost využití exploitů, vrací se kyberzločit zpět k technikám sociálního inženýrství. A mnozí z nich se zaměřují i na jiné platformy, než na ty z dílny společnosti Microsoft.
2. Útoky na svět internetu věcí (Internet of Things). Během roku 2014 jsme se setkali s mnoha důkazy toho, že výrobci zařízení z kategorie internetu věcí na bezpečnost moc nemyslí. Vzhledem k tomu, že mnohdy nedodržují ani ty nejzákladnější bezpečnostní standardy, mohou mít útoky na svět internetu věcí opravdu velmi vážné negativní dopady na svět veskrze reálný. Bezpečnostní průmysl tak musí zohlednit i tento druh rizik.
3. Šifrování se stává standardem. Povědomí o důležitosti bezpečnosti se bezesporu zvyšuje. V podstatě ruku v ruce s růstem obav o soukromí, mimo jiné i v důsledku odhalení nekalých špionážních aktivit zpravodajských služeb. Pozitivním dopadem je, že šifrování se konečně stává standardní součástí mnoha systémů a aplikací. Nicméně některým organizacím, ke kterým patří i celá řada právních institucí, se to nelíbí. Odpůrci argumentují především tím, že šifrování má negativní vliv na bezpečí nás všech.
4. Nově se objeví se další zatím skryté chyby v široce využívaném softwaru. Zranitelnosti Heartbleed (openSSL) a Shellshock (bezpečnostní chyba) ukázaly jednu nepříjemnou věc. Existuje softwarový kód, který je všeobecně považován za bezpečný a používán

[11] Exploit je speciální program, data nebo sekvence příkazů, které využívají programátorskou chybu, která způsobí původně nezamýšlenou činnost software a umožňuje tak získat nějaký prospěch. Obvykle se jedná o ovládnutí počítače nebo nežádoucí instalaci software, která dále provádí činnost, o které uživatel počítače neví (např. nějaký druh malware). Běžně používanou ochranou je včasná instalace aktualizací, které vydá tvůrce chybného software.

v celé řadě dnešních systémů. Podstatné je, že o skutečné bezpečnosti tohoto kódu vlastně mnoho nevíme. A že se ani nemůžeme spolehnout na to, že by muselo jít o ojedinělé případy. Události roku 2014 vedly k zájmu počítačových zločinců o systémy a aplikace, které zůstávaly na okraji zájmu. Dnes již víme, že díky falešnému pocitu o jejich skvělém zabezpečení. Firmy by se proto na tuto změnu přístupu počítačového podsvětí měli dobře připravit.

5. Regulační orgány si vynucují stále větší pravomoci včetně širšího přístupu k datům a informacím, a to především v Evropě. Technologie i bezpečnost se velmi rychle vyvíjejí. Bohužel legislativa nezvládá s touto rychlostí držet krok. V následujících obdobích dojde v oblasti práva k celé řadě změn, které jsou prosazovány již po mnoho let a souvisí právě s počítačovou bezpečností. Je přitom velmi pravděpodobné, že tyto změny vyvolají další vášnivé diskuse o nutnosti právní úpravy ochrany dat. A také o rozsahu soudních pravomocí v této oblasti.
6. Růst zájmu útočníků o mobilní platební systémy poroste, ale zatím se nevyrovná tradičním podvodům. Mobilní platební systémy se staly jedním z témat roku 2014 poté, co nepříliš poklidné bezpečnostní vody ještě více rozvířily diskuse o novém platebním systému Apple Pay. Počítačoví zločinci budou v příštích měsících a letech pátrat po chybách i nedostatcích těchto systémů, které jsou ale často velmi dobře zabezpečené. Oprávněně proto můžeme očekávat, že počítačová kriminalita bude v případě platebních systémů ještě hodně dlouhou dobu využívat „klasické“ postupy. Například zneužívání kreditních i debetních karet.
7. Znalostní propast se bude i nadále zvětšovat.

   Spolu s tím, jak jsou technologie stále běžnější součástí našeho života a tvoří jeden ze základů globální ekonomiky, uvědomují si vlády i firmy rostoucí důležitost dovedností souvisejících s počítačovou bezpečností. Jde ovšem o běh na velmi dlouhou trať a některé státy předpokládají, že se stav nezmění nejméně do roku 2030.
8. Služby umožňující útoky i exploit kity přichází na nové platformy včetně mobilních. Několik posledních let počítačové kriminality velmi úzce souviselo s růstem popularity univerzálních útočných produktů a služeb, které výrazně zjednodušují tvorbu škodlivého kódu i útoky. Vzhledem ke stále větší oblibě mobilních platforem (a také zvětšujícímu se objemu dat na mobilních zařízeních), nebude trvat dlouho a začne se objevovat stále více zločineckých balíčků zaměřených právě na tato zařízení. Obdobně se tento trend týká i dalších platforem ze světa internetu věcí.
9. Zabezpečení řídicích a dispečerských systémů bude zaostávat. Průmyslové řídicí systémy zaostávají z pohledu bezpečnosti za běžnými systémy nejméně o jedno desetiletí. Během následujících let se setkáme s celou řadou problémů, které v těchto systémech počítačoví zločinci bez váhání zneužijí. Motivy navíc budou velmi různorodé. Vedle všech dnes běžných důvodů se setkáme například i se státem podporovanými útoky v rámci mezinárodních konfliktů či boje s terorismem. Stručně řečeno jde o oblast, kde je mnoho ohrožených subjektů.
10. Zajímavé vlastnosti rootkitů[12] a botů mohou vést k novým typům útoků. Spolu s tím, jak se vyvíjí informační technologie, dochází i ke změnám hlavních platforem a protokolů,

[12] Rootkit je sada počítačových programů a technologií, pomocí kterých lze maskovat přítomnost zákeřného softwaru v počítači (například přítomnost virů, trojských koní, spyware a podobně). Rootkit je technologie maskující přítomnost zákeřných programů skrýváním adresářů, v nichž jsou instalovány do položek registru Windows, procesů, síťových spojení

které tvoří základy IT světa. Tyto změny na velmi nízké úrovni mohou odhalit „zajímavé“ chyby, které by mohly počítačovým zločincům nabídnout nové možnosti. Velké množství změn v dosavadních bezpečnostních technologiích tak povede nejen k opětovnému zneužití již známých možností, ale také k rizikům spojeným s novými bezpečnostními chybami.

Internet v současnosti čelí riziku, že se rozdělí na dva tábory a to uživatele chráněné pokročilými zabezpečovacími programy a na nevědomé přenašeče, kteří prostřednictvím svých nechráněných počítačů šíří většinu infekcí.

5 Závěr

Otázkou zůstává, jakým směrem se bude v budoucnu ubírat počítačový zločin a s ním související ochrana informačních technologií. Předpokládá se prudké rozšíření Internetu ve firmách, státních institucích, ale též v domácnostech. Zvýší se množství elektronicky přenášených dat a s tím i pravděpodobnost útoků na ně. Mezi odborníky v oboru informačních technologií se čím dál tím častěji hovoří o tzv. profesionalizaci kybernetické kriminality a tím i organizované kybernetické kriminalitě. Lze si například představit i situaci, kdy organizovaný zločin vyzbrojený dokonalými znalostmi dobře placených hackerů začne vybírat něco jako elektronické výpalné. A instituce, které se budou obávat případného útoku a nutných astronomických investic do zabezpečení, které bude stejně dříve nebo později prolomeno, raději zaplatí mafiánům za „ochranu“.

Dalším mimořádně nebezpečným jevem je tzv. lidský faktor. Ze strany pachatelů kybernetické kriminality bude pravděpodobně čím dál tím častěji docházet k podplácení a následnému využití osob s přístupovými právy do systému, tedy zaměstnanců, administrátorů apod. Potvrzuje se zde tedy, že největší riziko hrozí systému nikoli průnikem zvenčí, ale především od lidí, kteří mají přístupová práva.

Poděkování

Tento příspěvek byl vytvořen v rámci řešení Projektu vědeckovýzkumného úkolu č. 4/4 „Informační bezpečnost a kybernetická kriminalita v organizaci“, který byl součástí Integrovaného výzkumného úkolu na léta 2010-2015 „Analýza bezpečnostních rizik společnosti a jejich transfer do teorie bezpečnostních systémů“ realizovaný Fakultou bezpečnostního managementu Policejní akademie České republiky v Praze.

Seznam použitých zdrojů

Business IT. (2014). *IT v roce 2015: Fog Computing a analýza dat v reálném čase*. Retrieved from: http://www.businessit.cz/cz/it-v-roce-2015-fog-computing-a-analyza-dat-v-realnem-case.php

Dolejš, R. (2014). *Co čeká IT v roce 2015*. Retrieved from: http://computerworld.cz/udalosti/co-ceka-it-v-roce-2015-cisco-technology-radar-51616

Caponi, S. (2014). Cybersecurity Trends for 2014. *Corporate Compliance Insights*. Retrieved from: http://www.corporatecomplianceinsights.com/cybersecurity-trends-for-2014/

Cherry Bekaert. (2014). *Cybersecurity Trends for 2014*. Retrieved from: http://www.cbh.com/cybersecurity-trends-for-2014/

a systémových služeb tak, aby přítomnost zákeřného softwaru nebyla běžně dostupnými systémovými prostředky odhalitelná.

Ciccatelli, A. (2013). Top 5 Cybersecurity Trends for 2014. *Inside Counsel*. Retrieved from: http://www.insidecounsel.com/2013/12/27/top-5-cybersecurity-trends-for-2014

CIO. (2015). *10 trendů v počítačové bezpečnosti pro rok 2015*. Retrieved from: http://businessworld.cz/analyzy/10-trendu-v-pocitacove-bezpecnosti-pro-rok-2015-12079-p13186

Přibyl, T. (2015). *Počítačové viry a jejich svět*. Retrieved from: http://docplayer.cz/1872082-I-n-f-o-r-m-a-t-i-k-a-a-v-y-p-o-c-e-t-n-i-t-e-c-h-n-i-k-a-pocitacove-viry.html

Sophos. (2015). *Security Threat Trends 2015*. Retrieved from: https://www.sophos.com/en-us/threat-center/medialibrary/PDFs/other/sophos-trends-and-predictions-2015.pdf

Trestní zákoník. (2009). *Zákon č. 40/2009 Sb. Trestní zákoník*. Retrieved from: www.mvcr.cz/soubor/sb011-09-pdf.aspx