SOUČASNÉ TRENDY V OBLASTI (NE) BEZPEČNOSTI INFORMAČNÍCH SYSTÉMů

CURRENT TRENDS IN (UN) SECURITY OF INFORMATION SYSTEMS

Dagmar BRECHLEROVÁ, Radim KRUPIČKA, Zoltán SZABÓ
dagmar.brechlerova@fbmi.cvut.cz, krupicka@fbmi.cvut.cz, szabo@fbmi.cvut.cz

Abstract

The article summarizes the current situation in the area of risks related to the usage of the IT and stresses those risks that are the most actual today. The most frequent types of attacks are discussed as well as new types such as attacks against clouds. The danger resulting from these attacks is mainly stressed in relation to the population protection, healthcare etc. We also include statistical data. Aim of this article is to point out the bad situation in this area and to give rise to attention needed to devote to this problem.

Key words

DDos attack, botnet, mobile device, social platform.

Dnešní společnost je nesmírně závislá na informačních technologiích (dále IT). Následující text shrnuje současnou situaci v oblasti rizik při užití IT a poukazuje na nejčastější útoky, ke kterým dnes dochází. Je nutno si uvědomit, že na provozu informačních technologií jsou závislé i organizace, které dodávají energie, telekomunikační operátoři, záchranné složky, velká zdravotnická zařízení, laboratoře atd. Výpadek IT technologií z důvodů napadení při krizových situacích (např. při záchranných pracích, při řešení velké havárie apod.) by mohl být fatální. Bohužel situace je stále taková, že útočníci vždy jsou v předstihu před ochranou IS a uživatelé si ani řádu rizik neuvědomují. Navíc situace se spíše zhoršuje. Dalším problémem je, že útoky v oblasti IT jsou v určitých komunitách považovány za témě hrdinské činy, ač se jedná o trestnou činnost. A řádní útočníků vůbec nedojde, že jejich útok (který považují za zábavu) může způsobit tragédii.

V poslední době jsou velmi častým typem útoků tzv. DDoS útoky. Je to distribuovaný DoS útok – Distributed Denial of Service attack a je charakterizován velkým množstvím počítačů, snažících se najednou zahltit cíl útoku. Útok se nejčastěji využívá k zahlcení webových serverů (např. útok na české zpravodajské servery v březnu 2013), případně k oslabení nebo vyřazení sítě. Útok nebývá dlouhodobý, ale bývá konkrétně cílený a často při něm vznikají nemalé ekonomické ztráty. Cílený DDoS útok během krizové situace může způsobit kolaps celého komunikačního systému. Často je tento útok veden bez vědomí majitelů útočících počítačů a jedná se o důsledek napadení a úspěšného infikování těchto systémů. Infikované systémy může být vzdáleně řízeny a jejich služby je si možné zakoupit na černém trhu a směrovat DDoS útok na libovolnou organizaci. Do těchto útoků se zapojovalo v minulých měsících tisíce českých počítačů a jejich majitelé vědomě či nevědomě riskovali často značné postihy. Mimo jiné v České republice je zapojení se do DDoS útoků trestným činem podle § 230 odst. 3 písmeno b) trestního zákoníku [1], což si málokdo uvědomuje.

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 újmu 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.

Velkou měrou se na kybernetických útocích v posledních letech podepsaly také krádeže osobních a firemních dat a jejich následné zneužívání. Podstatně se záporně projevují i sociální sítě a šíření klamných informací a podvodných odkazů skrze ně, tento trend probíhá už několik let.

Velkým rizikem je užití mobilních telefonů a dalších mobilních zařízení, jak bude podrobněji uvedeno v další části.

Znalou část incidentů tvoří také případy ‚legraceň‘ souhrnně označované jako *Lulz*. Mohou mít různou podobu od spíše nevinných případů, jako je zmanipulování hlasování na Internetu, po závažnější typ jako šíření poplašné zprávy přes sociální média, až po velmi závažné, jako je zapojení se do DDoS útoků proti velkým společnostem a odstavení jejich serverů. Problém s těmito útoky často je, že nejdou předvídat, neboť útočníci obvykle nemají zájem o tyto útoky z hlediska jejich možného zpenězení, útoky pošádají často z ‚principuň nebo ideových důvodů.

Během mezinárodního zátahu proti kybernetickým útočníkům v Irsku, Velké Británii a Spojených Státech bylo zatčeno 7 hackerů, z nichž někteří působili ve skupině Lulzsec. Následně jim byla sdělena obvinění z celé řady trestných činů v oblasti IT, například organizace DDoS útoků. [2]

Jak zaznamenává společnost Verizon ve své výroční zprávě za rok 2012 [3], zvýšil se také počet útoků na citlivá uživatelská a průmyslová data, ať už výrobní tajemství, vojenské a jiné dokumenty či osobní data uživatelů. V této oblasti došlo podle Verizonu (pracujícímu pouze s nahlášenými incidenty) v různých zemích svět a k 855 incidentům (případům krádeží dat), při čemž počet kompromitovaných záznamů se blíží k 174 milionům. Ke zpracování podobných dat bývají často přizvány specializované soukromé a státní orgány, jako například Tajná služba Spojených států amerických (USSS – United States Secret Services), australská policie či Irská služba IRISS (Irish Reporting and Information Security Service). Jednotlivé organizace přispívající informacemi do zprávy sice používaly jemně odlišné metody sběru informací, nicméně v zásadě se příliš nelišily.

Za průniky do databází stojí dle některých zdrojů ve většině případů útočníci zvenčí. Zaměstnanců, kteří by útočili zevnitř firemní struktury, jsou jen 4 %, což je zhruba stejně jako v roce 2011 s tím, že ostatní hodnoty (útoky aktivistických skupin – hacktivismus) drasticky vzrostly. V 58 % jsou pak podle výše uvedené zprávy útočníci nějakým způsobem spojeni s různými ideovými skupinami a hnutími. Ovšem jiné zdroje naopak uvádějí, že nejčastější pachatel útoku je vnitřní zaměstnanec.

Průniky do soukromí jsou obvykle prováděny některou z forem hackingu (existují různé výklady tohoto pojmu, zde je tím míněno prolamování do IS různými způsoby). Příkladem může být průnik pomocí malware (škodlivý software, který umožní vniknutí nebo poškození počítačového systému) nebo ovládnutí počítače, mobilního telefonu či v současné době nejčastěji domácích směrovačů pomocí tzv. backdoor (‚zadní vrátkaň schovaná výrobcem v programu umožňující obejít běžnou autentizaci, která za běžných okolností brání uživateli v neoprávněném využívání systému).

Sociální inženýrství zaznamenalo slabý propad, nicméně se stále jedná o efektivní metodu při krádeži dat. Slabý pokles zaznamenalo rovněž zneužití pravomocí při krádeži zevnitř systému a vynášení informací.

Co se týče obětí jednotlivých útoků, přibližně 80 % je náhodně vybráno, protože byly snadným cílem a zároveň disponovaly citlivými informacemi nebo byl skrz ně možný přístup. 96 % útoků bylo poměrně jednoduchých a nevyžadovalo žádné speciální techniky ani nadměrné úsilí, což je poměrně alarmující číslo. Na většinu útoků se přišlo obvykle až po několika týdnech, a to obvykle tak, že poškozený byl kontaktován třetí stranou s tím, že jsou někde k dispozici ukradená data.

*Hacker **p0keu** ze skupiny AntiSec provedl řadu pravděpodobně náhodných útoků, při kterých ukradl a následně zveřejnil řadu osobních a přihlašovacích údajů uživatelů náhodně zvolených serverů. Jedním z nejpravděpodobnějších kritérií byla snadná napadnutelnost těchto serverů.* [4]

Dalším významným průzkumem, prováděným pravidelně je průzkum firmy Symantec – Symantec Internet security threat report [5].

Vychází z poznatků, shromážděných v rozsáhlé síti 69 milionů bezpečnostních senzorů v 157 zemích světa. Zpráva je velmi zajímavá a rozsáhlá a obsahuje řadu i nečekaných závěrů.

Některé trendy podle tohoto průzkumu:

- Malé organizace jsou pro útočníky zajímavé (31 % všech napadených organizací je do 250 zaměstnanců). Ovládnutá počítačová síť je ideální prostředník pro útok na větší instituce.
- Malware funguje jako Big Brother pro získání informací.
- 58% nárůst „mobilního malware".
- Tzv. zranitelnosti nulového dne.
- Hactivistické DDoS útoky jako krycí manévr pro kriminální útoky.

Kybernetická kriminalita v roce 2012 tedy nenesla žádné známky útlumu, naopak množství používaných velmi propracovaných metod útoků je známkou, že je nutné se vývojem a zlepšováním zabezpečení v této oblasti zabývat daleko intenzivněji. Některé typy ne úplně obvyklých útoků v roce 2012 zesílily (tzv. hacktivismus), nicméně známá část kybernetických útočníků stále provádí útoky s vidinou zisku – cílem jsou tedy hlavně bankovní účty, obchodní a platební portály či zneužívání důvěrnosti jednotlivců. Podružné útoky se pak často týkají kradení rozličných informací a zneužívání identity.

Trendy roku 2012/2013 podrobněji

Sociální platformy

Velmi ohroženou oblastí, kde stále přibývají uživatelé a zároveň se i množí útoky, jsou sociální platformy (Facebook, Twitter, atd.). Vzhledem k důvěrnosti velké části uživatelů webových stránek tohoto typu není pro útočníky problém nalézt jejich slabinu a pomocí sofistikovaných metod sociálního inženýrství ji využít k útoku. Často navíc obětí samy pomáhají útočníkovi sdílením informací ostatním tzv. přátelům, přičemž nevědomky šíří falešné informace svým profilem. Pokud se stále šířící vlnu rozšiřujících se obětí nedaří zastavit, šíří se pak skrz sociální weby jako lavina.

Příkladem útoků může být například využití systému přímých zpráv a zkracovačů adresních řádků, např. bit.ly. Uživateli přijde od jeho známého kontaktu (dá se tedy předpokládat, že je to buď známý dotyčného, nebo nějaká osoba, jejíž aktivity uživatel sleduje) zpráva znějící zhruba „koukej, co jsem o tobě našel na této adrese/vidím jsem s tebou video/četl jsem tenhle článek o tobě" apod.". Uživateli ale už často nedojde, že se nejedná o zprávu od jeho známého, ale o zprávu, rozeslanou útočníkem všem kontaktům. Protože je v ní obsažená zkrácená adresa, není patrné, kam bude uživatel přesměrován. Po kliknutí pak může dojít

k ukradení osobních údajů, umožnění přístupu na vlastní profil, odeslání podobné zprávy dalším lidem ze seznamu kontaktů apod.

Společnost Facebook se z podobných případů poučila a ve spolupráci s několika společnostmi (Microsoft, McAfee, TrendMicro, Symantec, Sophos) vytvořila systém, využívající aktualizované databáze podvodných linků a dalších škodlivých elementů, díky kterým je možné hrozby odstraňovat relativně včas. Mezitím jsou paralelně vyvíjeny i další bezpečnostní prvky, které by web s více než miliardou uživatelských účtů mohly lépe ochránit.

Příkladem současného trendu zneužívání důvěřivosti běžných uživatelů sociálních médií může být aplikace Facebook 2013 demo. Ta nabízela fiktivní aplikaci prostřednictvím stránky, tvářící se jako rozhraní oficiální Facebook stránky. Pomocí instrukcí nabádajících k přihlášení prostřednictvím údajů z pravého Facebooku pak docházelo k jejich odcizení. [6]

Mobilní zařízení

Významně se zaměřená projevovat zacílení na nová zařízení a platformy – například „chytré“ telefony stále nejsou zabezpečené natolik, aby dokázaly vzdorovat útokům, přitom se dají považovat za plnohodnotné miniaturní počítače obsahující často velmi citlivá a zneužitelná osobní data. Především populární operační systém Android je v tomto ohledu stále velmi zranitelný a spolu s nepoučeností uživatelů se jedná o pro útočníky potenciálně snadno napadnutelnou oblast. [12]

Operační systém Android je pod útokem: podle společnosti Kaspersky Lab došlo mezi prvním a druhým čtvrtletím roku 2012 k trojnásobnému nárůstu škodlivého software pro tento operační systém. Obvykle se jedná o multifunkční trojany, které jsou jednak schopné odesílat citlivá data (seznamy kontaktů, obsahy zpráv), ale zároveň také v případě potřeby stáhnout do telefonu další škodlivý software. [7]

Trojan (trojský kůň) je typ malwaru, který bez vědomí uživatele je skryt v nainstalované aplikaci.

Jak již bylo naznačeno v textu, mobilní aplikace obecně jsou dnes velmi oblíbeným způsobem, jak bez velké námahy infikovat množství přístrojů. Tento problém se týká především telefonů a dalších zařízení (tabletů), běžících na systému Android od společnosti Google. Uživatelé jiných systémů nejsou natolik ohrožení, nicméně stále mohou být prostředníky a šířit škodlivé aplikace dál.

Část podvodných aplikací funguje na principu napadení přístroje a následného neautorizovaného odesílání prémiových SMS zpráv, které jsou draze placené. Tyto aplikace se mohou tvářit jako užitečné doplňky, hry (často i napodobovat jinou, populární hru) apod., nicméně ve výsledku poškozují uživatele. Vzhledem k tomu, že vytvořit podobnou aplikaci je poměrně jednoduchá záležitost, a na internetu, kde se vše sdílí a většina uživatelů naprosto ignoruje jakékoliv bezpečnostní zásady práce s počítačem (tabletem, chytrým telefonem), dochází k šíření velmi snadno.

Škodlivé aplikace jsou většinou poměrně primitivní, nicméně i zde dochází k postupnému vývoji pokročilejších metod útoku. Příkladem může být modifikovaná verze populární hry Angry Birds, šířící se přes neoficiální servery s Android aplikacemi. Ta již dokáže využít kapacitu procesoru přístroje k jeho zapojení do tzv. botnet sítě (botnet viz dále), podobně jako kdyby napadla normální počítač. Vzhledem k tomu, že mobilní telefony jsou již dostatečně výkonné a bývají připojené do internetu, je podobný útok velmi nebezpečný z hlediska jejich využitelnosti pro celou řadu ilegálních aktivit. Navíc, jak již bylo zmíněno, na rozdíl od počítače jsou mobilní telefony často daleko hůře chráněné proti útoku.

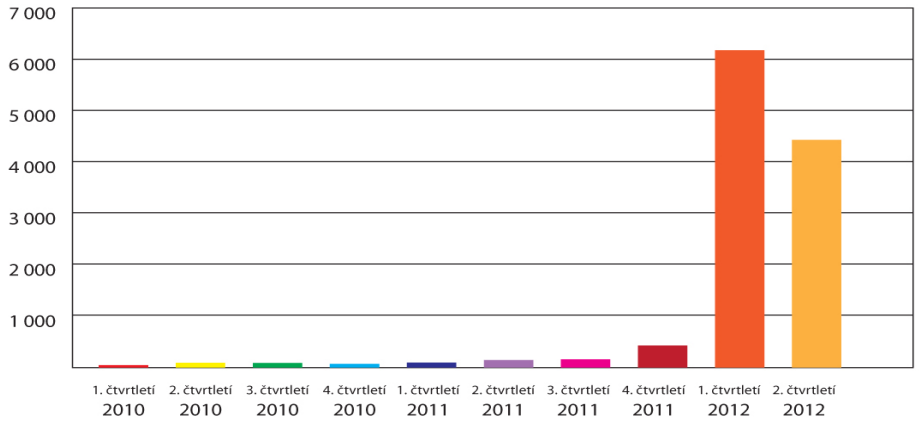
Společnost Check Point podpořila v roce 2013 významný průzkum Vliv mobilních zařízení na informační bezpečnost: Průzkum mezi IT profesionály, který provedla společnost Dimensional research. Bylo dotázáno 790 účastníků z USA, Kanady, Německa, Japonska, USA a GB. Všichni dotázaní pracují v oblasti bezpečnosti IS.

Celý průzkum a jeho výsledky jsou velmi zajímavé a alarmující, celý je možno získat na této adrese http://www.dimensionalresearch.com/company/ nebo je možno od Check pointu získat i české shrnutí.

Jako zásadní shrnutí se uvádí, že:

- Trend BYOD (Bring Your Own Device – používání vlastních zařízení pro pracovní účely) se výrazně zesiluje a ovlivňuje podniky všech velikostí.
- Podnikové informace uložené v mobilních zařízeních představují vyšší hodnotu než zařízení samé.
- Bezpečnostní incidenty související s mobilním zařízením jsou velmi nákladné i v případě malých a středních podniků.

Např. 93 % společností uvádí problémy spojené právě s BYOD. Stejně tak 93 % respondentů uvedlo, že se do jejich podnikové sítě připojují uživatelé z mobilních zařízení. U 79 % došlo v minulém roce k bezpečnostnímu incidentu v souvislosti s mobilním zařízením atd. Je zřejmé, že při budování bezpečnostní politiky a dalších podobných dokumentů je nutné mobilní zařízení zahrnout a považovat je za závažné riziko.



Výskyt nových škodlivých kódů pro mobilní telefony podle čtvrtletí [8]

Cloudy

Vzrůstající je také ohrožení uživatelů při použití cloudových a datastorage služeb. Cloud computing je na Internetu založený model vývoje a používaní počítačových technologií. Lze ho 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. V posledních letech vzrůstá počet společností, které ke svému podnikání využívají v rostoucí míře právě cloud služby, a to především díky jednoduchosti sdílení dat mezi jednotlivými uživateli, absenci médií a paralelnímu zálohování dat v cloudu. Kromě obvyklých rizik, spojených například s veřejnými

služ̌bami zdarma, které mohou představovat nebezpečí pro nahraná data, se na data sdílená v cloudu začali zaměřovat i útočníci.

Vzhledem k tomu, že sdílení dat probíhá pomocí přenosů, je možné pro případného útočníka odchytávat proud nezašifrovaných dat. Je proto nutno dbát na důsledné šifrování dat tak, aby i při případném odposlechu bylo pro útočníka nemožné data rozšifrovat bez znalosti klíče.

Jiným případem útoku může být vydávání se za jednoho z účastníků cloudu, při pojujícího se ke zdroji. K heslu se útočník může dostat celou řadou způsobů, od odchycení hesla, přes použití sociálního inženýrství, až po krádež počítače/paměťového média.

Dalším zabezpečovacím prvkem by tedy měla být autentizace jednotlivých uživatelů daného cloudu, což samozřejmě neeliminuje všechna rizika, nicméně část z nich ano.

V roce 2012 společnost Dropbox, jeden z nejrozšířenějších poskytovatelů cloudových služeb, přiznala, že došlo k odcizení přihlašovacích údajů některých uživatelů. Na tento fakt se přišlo tak, že někteří uživatelé, mající e-mailovou adresu pouze pro Dropbox účet, na ní začali dostávat spam zvenčí. Společnost následně přiznala, že jeden z jejích pracovníků měl sdílené heslo pro několik účtů a po odchycení tohoto hesla došlo ke kompromitaci účtu, který měl vzhledem k obsaženým důvěrným informacím být daleko lépe chráněn. Tato událost poukázala na nutnost mít rozdílné přihlašovací údaje podle úrovně zabezpečení tak, aby k přesnění tomuto případu nemohlo dojít. Společnost Dropbox na tento případ zareagovala nabízením volitelného rozšíření, které umožňuje dvoufázové přihlašování pomocí hesla a dočasného kódu, zasílaného na mobilní telefon. Dále také umožňuje uživatelům sledovat aktivní připojení k jejich účtu. [9]

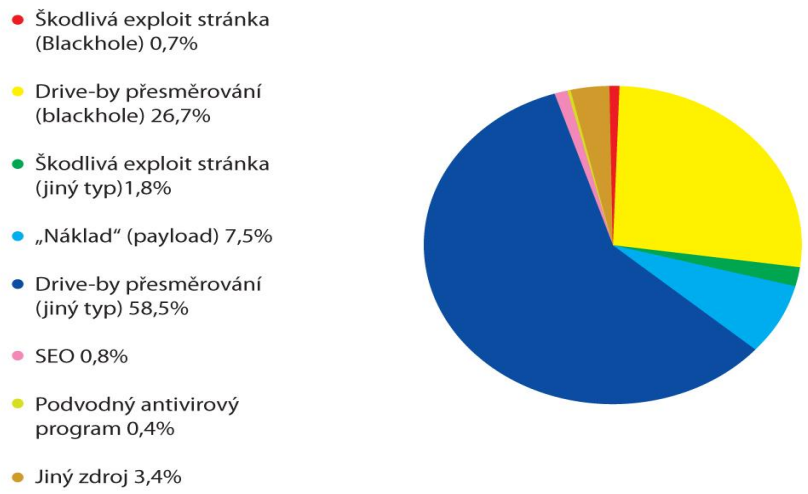
Na druhou stranu datová centra, která implementují cloude, mají vypracovanou bezpečnostní politiku a mohou si dovolit vyšší zabezpečení než menší firmy. Příkladem dobrého zabezpečení uživatelských dat může být společnost Google.

Dalším často využívaným způsobem útoku je napadení programů a prostředí, která jsou využívána pro některé specifické účely. Typickým příkladem může být v poslední době zneužívání chyb prostředí Java Runtime, které využívají některé online aplikace. Situace zašla tak daleko, že útočníci jsou schopni napadnout novou verzi v ten samý den, kdy byla vydána. Americká vláda vydala oficiální prohlášení, ve kterém doporučuje na počítačích prostředí vypnout a zamezit tak jeho zneužití. Vzhledem k tomu, že pokud dojde k objevení bezpečnostní trhliny, stává se z ní pro kybernetické zločince pomocí lukrativní zboží, motivují některé společnosti úhodné hackery a testery, aby trhliny objevovali a dostávali za objevené chyby zaplaceno. [10]

Malware (škodlivý software)

Vývoj škodlivého software prochází známými změnami – místo toho, aby si útočník na černém trhu pořídil (za často vysokou cenu) program, který bude za půl roku zastaralý, se vývojáři podobných programů inspirovali v politice prodejců běžného kancelářského software. Nabízejí za poplatek časově omezené licence (roční, půlroční), které mohou být v závislosti na vývoji nových verzí upgradovány, dají se k nim dokoupit další vylepšení ve formě pluginů (zásuvný modul neboli plugin je software, který nepracuje samostatně, ale jako doplňkový modul jiné aplikace, a rozšiřuje tak její funkčnost), je k nim poskytovaná technická podpora (většinou za další příplatek) atd. Díky tomu je možné i pro nepříliš zkušeného útočníka napáchat značnou škodu. Často má malware na infikovaném počítači i schopnost se aktualizovat a případně změnit svoje zaměření a schopnosti.

V oblasti malware je jednou z nejvýznačnějších hrozeb balíček Blackhole exploit kit. Tento původem ruský malware je schopen odhalovat slabiny v rozličných neaktualizovaných programech – pomocí nalezení slabého místa vytvoří umělou výzvu pro instalaci, kterou si pak program sám automaticky stáhne jako update po navštívení infikované stránky (*drive-by metoda* – malware je stažen během návštěvy), nebo po přesměrování na jinou infikovanou stránku.



Nejčastější hrozbou podle společnosti Sophos bylo v roce 2012 přesměrování na škodlivou stránku a následné stažení škodlivého kódu či podobný typ útoku [11].

Botnety

Botnet je označení pro softwarové agenty nebo pro internetové roboty, kteří fungují autonomně nebo automaticky. V současné době je termín nejvíce spojován s malware, kdy botnet označuje síť počítačů infikovaných speciálním software, který je centrálně řízen. Botnet provádí nežádoucí činnost, jako je rozesílání spamu, DDoS útoky a podobně. Botnety obecně představují jednu z nejvážnějších hrozeb v posledních několika letech. Dříve nebylo zdaleka tak jednoduše ovládat vážný množství počítačů na dálku, ale v posledních několika letech se vzhledem k vývoji škodlivého software a celkové propojenosti daší napadat i stovky počítačů, které pak mohou být ovládnuty na dálku jedním řídícím přístrojem. Následně je možné ovládat je pomocí tzv. zadních vrátek, instalovat potřebné aplikace bez vědomí uživatele a využívat je k různým účelům.

Těmi může být celá řada škodlivých často i trestných činů od šíření spamu přes zapojení přístrojů do cíleného DDoS útoku až například po bruteforce prolamování hesel.

Závěr

Situace v oblasti bezpečnosti IT se nelepší a je nutno toto mít na zřeteli, pokud jsme na uživatelské IT závislí. Neuvážené zavádění IT do oblastí, kde může dojít k jejich napadení, může mít nedozírné následky. Bohužel často díky tlaku firem či dalších i politických tlaků dochází k zavádění neprověřených technologií, ne zcela odladěného softwaru. Málokdo se také zamýšlí nad rizikem lidského faktoru v této oblasti, kdy může dojít díky chybám uživatele k závažným selháním. V budoucnu bude nutné věnovat oblasti bezpečnosti IT vážnější pozornost a také tyto snahy koordinovat. Bohužel riziko napadení IT je vysoké a je s ním nutno počítat, stejně tak jako počítáme s dalšími riziky. A tak bude nutné hledět na trestnou činnost v oblasti IT stejně jako na každou jinou.

Literatura

[1] http://business.center.cz/business/pravo/zakony/trestni-zakonik/cast2h5.aspx [Cit. 2013-11-20]
[2] http://www.bbc.co.uk/news/technology-17270822 [Cit. 2013-11-20]
[3] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf [Cit. 2013-11-20]
[4] http://news.softpedia.com/news/Antisec-Hackers-Begin-Attacking-Websites-at-Random-210308.shtml [Cit. 2013-11-20]
[5] http://www.symantec.com/security_response/publications/threatreport.jsp [Cit. 2013-11-20]
[6] http://www.mobilesecurity.com/articles/332-fraudulent-facebook-2013-demo [Cit. 2013-11-20]
[7] http://www.kaspersky.com/about/news/press/2012/Android_Under_Attack__Malware_Levels_for_Googles_OS_Rise_Threefold_in_Q2_2012 [Cit. 2013-11-20]
[8] McAfee quaterly threat q2/2012 report.
[9] http://businessworld.cz/it-strategie/Dropbox-konecne-priznal-ze-byl-napaden-hackery-Zodpovedni-jsou-pry-lehkovazni-uzivatele-9395 [Cit. 2013-11-20]
[10] http://cdr.cz/clanek/cdr-security-update-java-7-zranitelnost-nulteho-dne-iphone-bezpecnost [Cit. 2013-11-20]
[11] Sophos security threat report 2013. [Cit. 2013-11-20]. Dostupné z: http://www.is4security.com/trends/ security-threat-report.html
[12] http://www.independent.co.uk/life-style/gadgets-and-tech/news/android-devices-attract-79-of-malware-attacks-ios-gets-just-07-8788158.html [Cit. 2013-11-20]

Informace o autorech

RNDr. Dagmar Brechlerová, Ph.D. (1954)

Odborná asistentka Fakulty biomedicínského inženýrství ČVUT v Praze, Katedry biomedicínské informatiky. Zabývá se výukou předmětů z oblasti informatiky, zejména týkajících se bezpečnosti IT, logiky a matematiky, výzkumu. Specializuje se na bezpečnost informačních systémů, vztah IT a práva, bezpečnost IT ve zdravotnictví, problém ochrany osobních údajů, vzdělávání v bezpečnosti, bezpečnostní rysy internetových technologií atd.

Absolventka Matematicko-fyzikální fakulty Univerzity Karlovy v Praze, oboru fyzika (1978), postgraduální doktorské studium na Vysoké škole ekonomické v Praze, Katedře informačního a znalostního inženýrství, práce „XML bezpečnost a její uplatnění v univerzitním informačním prostředí" (2008).

Zastupuje Českou republiku v IFIP (International Federation for Information Processing) v TC11 (bezpečnost a ochrana informačních systémů – národní delegát), členka pracovní skupiny 11.7 IFIP – vztah bezpečnosti a práva. Autorka či spoluautorka kapitol knih u nás i v zahraničí, učebních textů, zhruba 150 příspěvků na konferencích v ČR i v zahraničí, v časopisech apod., v posledních letech zejména v oblasti bezpečnosti IS, právních a etických problémů užívání informačních technologií atd. Členka programových výborů konferencí a seminářů, školitelka grantů.

Mgr. Radim Krupička, Ph.D. (1981)

Tajemník Katedry biomedicínské informatiky na Fakultě biomedicínského inženýrství ČVUT v Praze.

Vystudoval softwarové inženýrství na Matematicko-fyzikální fakultě Univerzity Karlovy v Praze (2007). Specializuje se na zpracování biomedicínských dat a biomedicínský software.

Je řešitelem grantů IGA MZ ČR „Vytvoření systému a software pro strukturované funkční hodnocení pro účely dlouhodobé péče, pro získávání a zpracovávání dat o dlouhodobé péči, její kvalitě a potřebě“ a „Analýza bradykineze a poruch řeči u Parkinsonovy nemoci“. V posledních letech se podílel na vytvoření 3 užitných vzorů (např. Zařízení pro měření bradykineze pohybů prstů horní končetiny) a publikoval výsledky výzkumu na národním a mezinárodním fóru.

Ing. Zoltán Szabó, Ph.D. (1971)

Vedoucí Katedry biomedicínské informatiky Fakulty biomedicínského inženýrství České vysokého učení technického v Praze. Podílí se na výuce předmětů „Zpracování obrazových dat“, „Informační systémy ve zdravotnictví“.

Absolvent Katedry radioelektroniky Vysoké školy elektrotechnické v Koženicích (1994). Doktorandské studium absolvoval na Ústavu biomedicínského inženýrství Vysokého učení technického v Brně, kde obhájil disertační práci s názvem „Contour Coding for Compression of Still Images and Image Sequences“ (2001).

V současnosti je hlavním řešitelem projektu s názvem „Rozvoj oboru Biomedicínská informatika na Fakultě biomedicínského inženýrství v Kladně“ v rámci Operačního programu Vzdělávání pro konkurenceschopnost a dvou grantů IGA MZ ČR „Vytvoření systému a software pro strukturované funkční hodnocení pro účely dlouhodobé péče, pro získávání a zpracovávání dat o dlouhodobé péči, její kvalitě a potřebě“ a „Analýza bradykineze a poruch řeči u Parkinsonovy nemoci“. Je předsedou disciplinární komise Fakulty biomedicínského inženýrství a členem Akademického senátu Fakulty biomedicínského inženýrství.