KAPITOLA OSMÁ

Kriminalita v kyberprostoru

Mgr. Zbyněk Loebl, LL.M.

8.1 Úvod

Na zasedání ICANN jezdívají dva experti na internetovou bezpečnost, oba jsou z USA, oba jsou velmi přátelští a oba pracují v soukromém sektoru. Zajímavé na nich je to, že jsou to jedni z mála lidí na světě, kteří dokážou udržet krok s rozvojem a technologickou úrovní kyberkriminality. Oba radí vládám, firmám, asi i armádám po celém světě, jeden měl mimo jiné také akci na Slovensku. Kde je však policie, prokuratura a další státní orgány, které by měly mít v boji s kriminalitou v kyberprostoru hlavní úlohu? Ve většině zemí světa teprve hledají svou úlohu v tomto boji a ještě ani účinného pokroku nejsou schopni. Výjimky, o nichž se občas dozvídáme v televizi, jako např. o rozkrytí velké mezinárodní sítě webů s dětskou pornografií, spíše potvrzují pravidlo. Důvodů je víc, od nedostatku financí po nedostatečnou kvalifikaci policistů, prokurátorů i soudců. Také je to dáno tím, že internetový systém zatím prostě není na efektivní vyšetřování a postihování závažné kriminality postavený.

Tato kapitola se zabývá příčinami a důvody, proč je stávající stav takový, jaký je, a uvádí, co bychom měli dělat doma v České republice, aby se do budoucna mohla současná situace postupně zlepšovat.

8.2 Typy kriminality v kyberprostoru

Níže jsou uvedené hlavní typy kriminality související s Internetem. Některé jsou vlastní jen Internetu, většina však je obecná, pouze v oblasti Internetu dostává mnohem větší rozměr a škodní potenciál. Většina této kriminální činnosti je velmi výdělečná.

Jaké jsou tedy hlavní typy této virtuální kriminality?

8.2.1 Phishing, pharming

Obě kriminální činnosti nemají český termín. Jde o často spojené techniky krádeží identity na Internetu za účelem vykrádání bankovních kont, kreditních karet aj. Phishing je termín užívaný pro metody získávání osobních údajů od uživatelů Internetu, včetně citlivých údajů. Pharming označuje techniku přesměrování přístupu na určitou webovou stránku na úplně jinou stránku. Např. uživatel online bankovnictví přistupuje na web své bankovní aplikace, ale jedná se přitom o web online zloděje, který tímto způsobem získá informace o heslech a dalších tajných přístupových kódech, s jejichž pomocí potom vykrade bankovní účet příslušného uživatele. Pharming je nebezpečný tím, že ke své detekci vyžaduje speciální technologii, a to i na straně uživatelů. Běžné antivirové programy nebo programy proti tzv. spyware neboli počítačovým štěnicím a trojským koňům jsou proti pharmingu neúčinné.

8.2.2 Spam neboli nevyžádaná obchodní sdělení

Spam je u nás známý a i legislativně výslovně upravený. Velmi nebezpečné jsou spamové útoky, tedy použití spamu jako viru, kdy je informační systém přehlcen obrovským množstvím zasílaných datových zpráv a po určité době kolabuje. Sofistikovaný a dlouhodobý spamový útok přežije jen výjimečně chráněný informační systém pod neustálým dohledem.

8.2.3 Hacking

Hacking je i v ČR známý výraz označující získání neoprávněného přístupu do počítačů a jejich obsahů. Existuje celá řada hackerských technik zaměřených na odstranění té které ochrany informačního systému. Existují dokonce hackerské techniky na zkompromitování systému dvou klíčů, tajného a veřejného. Hackerství je nebezpečné nejen kvůli neoprávněnému přístupu k datům kompromitovaného počítače, ale také proto, že kompromitované počítače jsou využívány k páchání další závažné trestné činnosti, k ukrývání nelegálního obsahu nejhoršího druhu, pro účely phishingu a případně dalších kriminálních praktik.

8.2.4 Dětská pornografie na Internetu

Dětská pornografie na síti Internet je jedním z dalších negativních projevů relativně snadné dostupnosti obsahu zakázaných obrazových nebo audiovizuálních materiálů na celosvětové síti. V tomto ohledu se dá hovořit o dostupnosti jako vlastnosti, která má globální charakter, což s sebou nese riziko přístupnosti informací jakéhokoli obsahu na kterémkoliv místě, bez možnosti skutečně účinnými prostředky limitovat uživatele sítě, kterým se právě objeví *„zakázané ovoce dětské pornografie“* na obrazovce jejich monitoru. Dětskou pornografii šířenou prostřednictvím internetu nelze však pouze paušalizovat na ukládání a distribuci obrazových a audiovizuálních souborů na serverech, které jsou bez dalšího přístupné ostatním uživatelům Internetu. Nebezpečí je daleko většího charakteru a může zejména spočívat v navazování kontaktů sexuálně narušených jedinců s nezletilými osobami. K prvotnímu kontaktu mezi sexuálně narušeným jedincem a nezletilým dítětem může dojít na Internetu na zdánlivě bezpečném místě, o kterém nikdo nepochybuje, že by mohlo sloužit ku prospěchu osob se sexuální poruchou. Typickým příkladem takového místa se stávají sociální sítě umožňující kromě poznávání nových lidí i sdílení obrázků a videí. Dále již není nic jednoduššího než využít anonymity a nepostižitelnosti internetové komunikace k navázání kontaktu, který může mít pro děti v konečném důsledku fatální následky. Je důležité připomenout, že subjektem aktivním při šíření dětské pornografie na Internetu nejsou pouze dospělé osoby, ale jsou běžné i případy, kdy nezletilé dítě bez prvotní a vnější iniciace poskytuje prostřednictvím Internetu své fotky nebo videa se sexuálním podtextem dalším osobám. Dětská pornografie šířená Internetem tak s ohledem na její nebezpečnost pro společnost představuje nepřijatelný patologický jev společnosti, se kterým je nutno bojovat. Snaha projevující se v odporu a úsilí eliminovat dětskou pornografii na Internetu musí být uskutečňována i za účelem snižování pocitu anonymity sexuálně narušených jedinců skrytých ve virtuálním světě.

8.2.5 Obtěžování po Internetu

Obtěžování je pojem, kterým lze obecně označit chování spočívající ve vytrvalém napadání někoho jiného nebo působení na jeho život takovým způsobem, který v této osobě vzbuzuje nepříjemné pocity, ba i dokonce

pocit ohrožení vlastního života. Skrze Internet se posouvá hranice nadefinovaného obtěžování na vyšší úroveň, kdy je umožněno prostřednictvím Internetu zasahovat do života desítek nebo tisíců osob z rozličných důvodů. Uskutečňování obtěžování v prostředí Internetu tak lze označit za tzv. kyberšikanu. Účelem samotného obtěžování na Internetu bývá nejčastěji snaha nepříznivým způsobem ovlivňovat život ostatních osob, často pro pocit sebeuspokojení takového agresora či pro pocit vydobytí si dominantního postavení ve společnosti. Nelze ani opominout fakt, že agresorovo jednání mající charakter obtěžování v prostředí Internetu je uskutečňováno se záměrem *„názorově se zviditelnit“* široké veřejnosti. Jako prostředky k uskutečnění kyberšikany jsou nejčastěji v široké míře využívané chaty s nejrůznějším tematickým zaměřením a současně se vyznačující fluktuací osob s podobnými zájmy. Častým jevem je také obtěžování na Internetu uskutečňované prostřednictvím sociálních sítí, které často disponují vlastními hojně užívanými chaty, a nelze zapomínat ani na běžně používané e-maily. Z výše naznačených nástrojů používaných k uskutečnění kyberšikany vyplývá digitální forma obtěžování, která se vyznačuje širokou anonymitou. Zdánlivě skrytá identita osob uchylujících se k obtěžování jiných po Internetu je velice nebezpečným faktorem, který posiluje v agresorech takového jednání pocit bezpečí a bezúhonnosti.

8.2.6 Obchodování s drogami prostřednictvím Internetu

Dalším z projevů neustále globalizovanějšího světa je i obchodování s drogami prostřednictvím Internetu. Mohla by být položena otázka, z jakého důvodu se přesouvá sjednávání prodeje drog *„z ulice“* do prostředí kyberprostoru. Odpověď na tuto otázku je nasnadě. Budování prodejních kanálů, distribuce a vyhledávání potenciálních zájemců o koupi drogy na Internetu nese pro obě strany nelegálního obchodu řadu výhod, které spočívají zejména v rychlém vyhledání případného zájemce o koupi drogy, bezprostředním kontaktu obou stran obchodu, které jsou fakticky skryty v anonymním prostoru digitálního světa, nebo i v možnosti si následně ověřit, s kým se prodej drog má uskutečnit. Nespornou výhodou obchodu drog na Internetu se stává častá nemožnost identifikovat prodejce či kupce drogy vzhledem k tomu, že vzájemná interakce mezi uvedenými stranami probíhá i za pomoci výpočetní techniky veřejných internetových kaváren,

vysokých škol či jiných veřejných institucí, kde možnost vyloučit z využití Internetu nepovolané osoby je jen minimální.

8.2.7 Trestné porušování práv k nehmotným statkům

Trestným porušováním práv k nehmotným statkům lze rozumět protiprávní činnost spojenou s užíváním moderních informačních prostředků celou řadou jejich uživatelů, kteří jsou vzájemně v bezprostředním informačním styku, propojeni pomocí sítě Internet. Moderní technologie tak mimo jiné umožňují sdílet, kopírovat či rozmnožovat nehmotné statky, jako jsou hudební soubory, filmové tituly či jiné programové vybavení pro výpočetní techniku atd. Praktickým dopadem tak je stav, kdy zejména shora uvedené nehmotné statky, k jejichž užívání mají výhradní autorská práva určité subjekty, jsou zpřístupňovány jiným bez souhlasu těchto oprávněných subjektů. Prostředí Internetu však nevytváří právně nedotknutelnou oblast, kde by bylo možno bez dalšího porušovat práva k nehmotným statkům jejich poskytováním dalším do dispozice pro jejich další užití. Na jedné straně tak dochází k protiprávní činnosti, kdy určité osoby zpřístupňují ostatním prostřednictvím Internetu nehmotné statky, které jsou uloženy ve výpočetní technice na hardwarech takových poskytovatelů. V těchto případech je identifikace subjektů porušujících práva k nehmotným statkům ulehčena. V současné době se protiprávní činnost posouvá i do jiné roviny, kdy určité osoby samy neumožňují stahování vizuálních, audiovizuálních či jiných děl majících povahu nehmotných statků přímo ze svých hardwarových komponentů, ale naopak vytvářejí a usnadňují uskutečňování takového protiprávního jednání. Za protiprávní tak lze považovat i jednání, kdy jsou nehmotné statky zpřístupněny široké veřejnosti v určitém čase a prostoru prostřednictvím hypertextové odkazu (tzv. embedded link) na data uložená u určitého uživatele Internetu. Dalším projevem neoprávněného nakládání s nehmotnými statky je i vytváření softwarů určených k vyhledávání, sdílení a kopírování obsahů datových souborů s nejrůznějším obsahem bez souhlasu oprávněných subjektů. Jako příklad by mohla posloužit mediálně známá kauza se zástupci serveru Pirate Bay.

Typů kriminálních aktivit souvisejících s Internetem je nepřeberné množství. Často se používá termín „cyber warfare“, tedy něco jako kybernetická válka nebo kybernetické válčení. Jde o velmi závažné otázky, destruktivními technikami na Internetu se zabývají nejen zločinci, ale i největší světové

tajné služby a armády. Problém je, že každá další nově objevená technika v armádním prostředí nebo prostředí tajných služeb dříve či později může uniknout a být používána zločinci a teroristy.

8.3 Fast flux

Fast flux představuje účinnou metodu, jak skrýt svou identitu na Internetu a využít toho k páchání i nejvážnější trestné činnosti. Níže uvedený text vychází ze zprávy, kterou připravila pracovní skupina ICANN právě pro fast flux a které se účastnil autor této kapitoly. Plný text zprávy – tzv. GNSO fast Flux Report – naleznete v angličtině na webu ICANN www.icann.org. fast flux je jen jednou z technik používaných zločinci v souvislosti s Internetem.

fast flux je metodou, jak se osoby zapojené do obvykle vážnějších forem počítačové kriminality související s Internetem snaží uniknout odhalení. Jedná se o techniku, kdy se opakovaně a velmi často v krátkých časových intervalech mění záznamy v DNS udávající IP adresu, tedy identifikaci serveru technicky provozujícího příslušnou doménu.

Lze si představit příklad běžné domény – např. „loebl.com“. Tato doména je spojená vždy jen s jednou IP adresou, identifikující server, který tuto doménu propojuje do Internetu a kde je tato doména umístěná. Běžně se IP adresa často nemění. Cílem fast fluxu naopak je, aby se tyto IP záznamy u jedné a té samé domény měnily velmi rychle. Obvykle se pro tyto účely používá naprogramovaný automat skupiny IP adres a velmi krátké hodnoty TTL (short time-to-live), v řádech sekund. Za těmito neustále se měnícími IP adresami, kterých jsou stovky nebo spíše tisíce, je skrytý server s příslušným ilegálním obsahem. Všechny IP adresy na tento server skrytě odkazují. Takovému serveru, na kterém je umístěn škodlivý obsah nebo datové zprávy, se říká „mothership“.

Znamená to, že i při velmi rychlém opakovaném kliknutí na stejnou webovou stránku – např. www.loebl.com – vždy dojde ke spojení s jiným serverem. Všechny servery v rámci takové fast flux sítě používané ke kriminální činnosti jsou přitom napadené, tj. legální provozovatelé těchto serverů vůbec nevědí, že jejich servery jsou takto využívány, a ani nevědí o nelegálním obsahu, který je na nich umisťován. Proto velké procento počítačů zapojených do fastfluxových sítí, tvoří domácí počítače, často nedostatečně nebo zcela nechráněné proti napadení.

Navíc fast flux sítě si samozřejmě vybírají počítače s rychlým připojením k Internetu a používají nejmodernější internetové monitorovací techniky, které umožní vyřadit z takové sítě ty servery, které nejsou aktivní, a nahradit je jinými. Stejně tak se pro fast flux využívají i doménová jména, která neodpovídají tzv. rizikovým faktorům používaným systémy detekce.

Fast flux se používá pro skrytí nejzávažnějších typů kriminality na Internetu, včetně phishingu, náborových webů pro hackery nebo sítí s dětskou pornografií. Nicméně, a to je pro boj s fast fluxem dalším problematickým faktorem, tato technika má rovněž několik legitimních způsobů využití. Je např. využívána v rámci rozsáhlých firemních serverových sítí pro optimalizaci využití dostupných kapacit a k co nejrychlejší aktualizaci obsahu na nich a dále hráči na Internetu, ovšem nikoliv na kompromitovaných serverech, aj.

Dalším využitím fast fluxu je, že umožňuje obejít techniky využívané vládami některých států za účelem znemožnění přístupu svým občanům na některé webové stránky a k jejich službám (tzv. black-holing).

Z výše uvedeného vyplývá, že fast flux je účinnou metodou, jak zabránit policejním složkám po celém světě identifikovat a zadržet pachatele nejzávažnější trestné činnosti na Internetu. Výsledkem byla ještě před několika lety velmi vážná situace, kdy nejlepší a nejrozsáhlejší policejní síly na světě v podstatě nevěděly, kdo stojí za fast flux sítěmi, kdo jsou jejich protivníci. Autor této kapitoly se účastnil před asi pěti lety konference, na které se vyšetřovatelé FTC (Ministerstva obchodu USA), FBI a Scotland Yardu vážně dohadovali, kdo jsou osoby za těmito sítěmi, zda je jich 50 nebo víc, z jakých zemí pocházejí atd. Celé to tehdy opravdu věrně připomínalo filmy o Fantomasovi. Bohužel v praxi je fast flux odpovědný za velmi závažné zločiny a umožňuje zločincům unikat spravedlnosti.

Jak proti nelegálnímu fast fluxu bojovat? Studium fast fluxu vede experty k závěru, že snažit se detekovat zdroj – tzv. *mothership* – nebo atakovat jednotlivé kompromitované počítače je neúčinné, stojí to spousty peněz a času a výsledky nejsou nijak vynikající. Proto i policejní síly, které si v průběhu řady let vybudovaly rychlé a systematické metody zásahů proti počítačům s nelegálním obsahem, jako je např. holandská policie, jsou proti fast fluxu relativně bezmocné.

Jak bylo uvedeno výše, provozovatelé fast flux sítí využívají pro své útoky nejčastěji domácí počítače připojené k broadbandovým sítím, kterých je po světě obrovské množství, jejich kompromitace je příliš jednoduchá a úsilí potřebné k ukončení přístupu těchto kompromitovaných počítačů k Internetu

je enormní. Navíc i při rostoucí ochotě poskytovatelů připojení k Internetu (tzv. ISP firem) vzájemně spolupracovat a spolupracovat i s policejními složkami je současně celá řada jiných ISP firem, které staví svůj obchodní model právě na službách pro ty klienty, kteří by u jiných ISP neprošli.

Proto se stále více mluví o tom, že řešení je třeba hledat na úrovni správy DNS – tedy v podstatě nastavit taková pravidla, která by omezila možnost využívat prvky, které z fast fluxu dělají tak přitažlivou metodu pro zločince na webu. To je ovšem velice citlivé, protože taková pravidla nutně omezí i legální využití fast fluxu, navíc vyžadují aktivní zapojení ICANN. ICANN, který byl ustaven, jak je uvedeno ve druhé kapitole této knihy, jako kvazisoukromá společnost globálního charakteru, jejímž posláním je samospráva DNS systému, by nyní měl pomáhat různým národním policejním orgánům? Měl by ICANN nutit správce a registrátory, aby změnili svoje současné aktivity směrem k aktivnějšímu vyhledávání fast fluxu a počítačové kriminality obecně, což v podstatě vede k tomu, že jim ubývají zákazníci? Nicméně přesně tímto směrem vývoj směřuje a je to tak jenom správně, lepší řešení zatím nikdo na světě nevymyslel.

Správci domén a registrátoři mohou pomoci účinně bojovat s fast fluxem tím, že budou monitorovat DNS záznamy a hlásit podezření na fast flux příslušným policejním orgánům (fast flux lze zjistit z jeho jasných projevů – viz výše), a dále mohou změnit svou činnost tak, aby provozovatelům fast fluxu co nejvíc ztížili jejich činnost, např.:

a) požadováním prokázání identity osob žádajících o změnu DNS záznamů;
b) znemožněním automatizovaných změn DNS záznamů;
c) požadavkem na minimální dobu trvání TTL pro účely změn záznamů DNS (pro fast flux jsou typické hodnoty kolem 300 sekund, doporučenou praxí je 30 minut);
d) omezením počtu serverů, které mohou být uváděny pro jednu doménu nebo
e) omezením počtu změn DNS záznamů u jedné domény v průběhu dané doby.

Nyní jde o to, jak nastavit výše uvedená opatření tak, aby nepoškozovala subjekty, které fast flux techniky používají legálně, a také získat v rámci internetové komunity konsenzus, že tato opatření by ICANN a jeho orgány měly prosadit a všeobecně zavést. Tento proces může trvat delší dobu. V mezidobí jsme svědky toho, že víc a víc firem se dobrovolně rozhoduje používat „best practice“ zahrnující výše uvedená opatření.

8.4 Jak s kriminalitou na Internetu bojovat v České republice

Boj s internetovým zločinem je velmi obtížný kdekoliv na světě, a v malých zemích s omezenými finančními zdroji zejména. Asi nejdůležitější pro veřejnou správu a politiky je znát reálnou situaci, která zdaleka není růžová, ale naopak je velice alarmující. Je třeba si uvědomit, že o většině závažné internetové kriminality probíhající v České republice s největší pravděpodobností vůbec nic nevíme a že jde o stav, který již asi trvá několik let a bude ještě delší dobu velmi pravděpodobně trvat.

Veřejná správa by se měla spojit se sektorovými asociacemi a začít postupně budovat ve spolupráci se soukromým sektorem systémy best practice, podobné těm, které jsem popsal výše u části týkající se fast fluxu. Zatím taková spolupráce existuje jen v několika málo nejvyspělejších zemích světa. Ve Velké Británii v listopadu 2010 např. vládní kabinet oznámil, že ve spolupráci se správcem národní domény .uk, sdružením Nominet, vytvoří rychlé a účinné alternativní online soudiště, které bude schopné rychle rozhodovat o suspendaci webových stránek v případě trestného porušování soukromí, obtěžování po Internetu aj. Jde o jeden z prvních takových systémů na světě, ale podle mého se právě takovýmto směrem bude ubírat příští vývoj. Velká Británie určitě uvítá spolupráci s dalšími zeměmi, protože bez globálního pohledu její systém nebude účinný.

To je další důležitý bod – pro úspěšný boj s kriminalitou na Internetu by se česká policie měla co nejaktivněji zapojit do mezinárodních diskusí a mezinárodní spolupráce. Věřím, že naše policie již v těchto strukturách zapojená je. Nicméně ještě nikdy jsem např. na zasedáních ICANN, kde je téma internetové bezpečnosti a boje s kriminalitou ve virtuálním světě Internetu stále důležitější, neviděl zástupce české policie. Naopak tam pravidelně jezdí agenti FBI či Scotland Yardu.

Konečně je třeba v rámci policie postupně budovat tým expertů, kteří budou mít špičkovou expertizu v tomto úzkém, ale důležitém oboru kriminalistiky a budou také nadšení a zapálení pro věc. Pokud by se toto podařilo a globální správa Internetu se dále vyvíjela směrem k bezpečnějšímu Internetu, potom bychom se mohli cítit o něco bezpečněji.