Cybercrime- Kybernetický zločin.

Insp. P. Caruana (1)

(1) Cybercrime Unit, Police Corps of the Republic Malta

First published in/Původně publikováno v:
il-Pulizija / The Police, July 2005, Vol 12, No.: 2,
vydává „ il-Pulizija“, C.M.R.U., Police Headquarters, Floriana CMR 02, Malta

Preface, Introductory Remarks and Translation/Úvodní slovo a překlad do češtiny
Petr P. (2,3,4), Kalová H. (2,3,4 5), Dolista J. (3,4).

2) Pracoviště klinické farmakologie, GŘ Nemocnice České Budějovice a.s., B. Němcové 54, 370 87 České Budějovice, vedoucí lékař Doc. MUDr Petr Petr, PhD
3) Vysoká škola Evropských a Regionálních studií o.p.s., Žižkova 6, 370 01 České Budějovice, rektor Prof. Dr. Josef Dolista, ThD,PhD
4) Katedra veřejného a sociálního zdravotnictví , Zdravotně sociální fakulta Jihočeské university, Staroměstská 16, 370 04 České Budějovice vedoucí katedry Doc. MUDr Vladimír Vurm, C.Sc.
5) Nadační fond EMA- European Medical Agency, České Budějovice President nadačního fondu Mgr. Hana Kalová

Souhrn:
Autor předkládá definici a vymezení pojmů cybercrime , a computer-related crime a podrobně diskutuje úlohu policie při prevenci a represi tohoto druhu trestné činnosti.

Klíčová slova:
Cybercrime, kybernetický zločin, computer related crime, zločin v souvislosti s počítači, policie.

Summary:
The author presents the definitions of cybercrime and computer-related crime. The meticulous discussion of the role of the Police corps in prevention and represion of those crimes is presented.

Key words:
Cybercrime,computer related crime, Police Corps.

Úvodní slovo k českému vydání.
V květnu 2005 uplynul právě jeden, první, rok od vstupu České republiky do Evropské unie. Prakticky ve stejné době jako my se plnoprávným členem EU stala i Malta. Přes zeměpisnou odlehlost a rozdílnost našich států, - vnitrozemská Česká republika a ostrovní Malta, co by zdánlivě mohlo být odlišnějšího, - nacházíme tolik podobností jak v našich úkolech tak v cílech, že se neubráníme pocitu sounáležitosti . Ten je silně umocněn i málo známými historicko-kulturními vazbami mezi Maltou a Českou republikou , na kterých se podílel zejména řád rytířů sv. Jana – Johanitů, Maltézských rytířů.
Bezprostředně po návratu z Malty předkládáme českému čtenáři odborný článek na thema nejsoučasnější a dá se říci žhavé, cybercrime – kybernetický zločin. Autor , pan policejní inspektor P. Caruana, je příslušníkem Policie Maltské republiky, a jak doufáme, naším perspektivním zahraničním spolupracovníkem. **Jím zpracovaná thematika má obrovský a**

zásadní význam jak pro přístup k organisovanému zločinu obecně, tak k boji proti drogám (drug enforcement) zvláště.

Je důležité připomenout hned na začátku, že pro označení zločinného použití počítačových technologií existuje mnoho termínů. Čtenářům velmi pomůže, pokud tyto termíny na úvod zopakujeme. Termíny „ computer crime- komputerový zločin“ , „ high-tech crime – zločin s použitím špičkových technologií“, „ IT (rozuměj Information Technologies , pozn. Překladatelů) crime – IT zločin“, a „ cybercrime- kybernetický zločin“ jsou používány promiscue, jsou různě zaměňovány a mezi sebou propleteny. Existence více termínů vede či může vést k nedorozumění a zmatku. Podle Oxford Reference Online je „ cybercrime“ definován jako trestný čin/zločin spáchaný po Internetu. Webopedia definuje cybercrime jako „……jakýkoliv kriminální čin, týkající se počítačů a sítí “. Navíc, obecně je do pojmu „ cybercrime“ zahrnován a jakýkoliv „ tradiční“ trestný čin/zločin, pokud byl proveden po Internetu. Praktické příklady toho, co se má a může jako cybercrime označovat podává manuál OSN „ United Nations Manual on Prevention and Control of Computer-Related Crime“. Podle tohoto manuálu se do pojmu cybercrime zahrnuje zejména : podvod, padělání, sabotáž computerů, neautorisovaný přístup ke computerovým programům a neautorisované kopírování computerových programů , jako nejčastější příklady.

Cybercrime a jeho vyšetřování.

Použití computerů a dalších zařízení (dále technologie) zločincem a význam zajistitelných dat pro policejního vyšetřovatele můžeme seřadit následujícím způsobem:

technologie je cílem zločinného útoku

toto je tradičně považováno za „ opravdový computerový “ zločin, patří sem hackeři, dále útok mající za následek odepření služby a také rozšiřování virů.

technologie je pomocným prostředkem k provedení trestného činu/ zločinu

tento stav nastane, pokud jsou computery a/nebo jiná související zařízení použity k provedení tradičních trestných činů, například k výrobě padělaných dokumentů, k odeslání výhružky smrtí, k odeslání vyděračských požadavků, nebo k vytvoření a distribuci ilegálního materiálu, jako kupř. dětské pornografie.

technologie jako svědek trestného činu/zločinu

k tomu dochází, když průkaznost nějakého faktu obsažená v zařízeních informační technologie může sloužit jako podpůrný průkaz pro jev, se kterým nesouvisí s tímto faktem přímo, kupř. k potvrzení nebo popření alibi podezřelého, nebo tvrzení svědka.

technologie jako nástroj komunikace

zločinci užívají technologie ke vzájemné komunikaci, aby snížili pravděpodobnost odhalení, například tím, že používají šifrování

technologie jako skladovací medium

je to úmyslné či neúmyslné uchovávání informací na technologiích/zařízeních zmíněných v kterémkoliv z předchozích odstavců, typicky jde o data obsažená v počítačových systémech obětí, pachatelů a podezřelých.

Vyšetřování ve spojení s cybercrime-kybernetickým zločinem- má společné základní principy průkaznosti , které se vztahují na celou oblast počítačů a dalších špičkových technologií.Ať už je medium uchovávající informace jakékoliv, vyšetřovatelé takovýchto trestných činů/zločinů sdílejí týtéž zásady. Sdružení velících policejních důstojníků (Associacion of Chief Police Officers) formulovalo v roce 2001 tyto zásady následujícícm způsobem (1):

1. žádná akce podniknutá orgány činnými v trestním řízení nesmí vést ke změně dat uchovávaných v počítači či na jakémkoliv mediu, které by mohly být spolehlivě použity během soudního řízení.
2. ve výjimečných případech, kdy je nezbytné přistoupit přímo k originálním datům uloženým v computeru nebo na nějakém mediu, musí tak učinit osoba kompetentní (míněno technicky kompetentní) a musí být jednoznačně patrno, že tato aktivita byla relevantní, jak proběhla a jaké jsou její důsledky a dopady.

3. Je nezbytné vytvořit a uchovávat podrobný záznam všech procedur(ve formě podkladů pro audit) , kterým byla data uložená v computerisované elektronické formě vystavena. Nezávislá třetí strana musí být schopna sledovat tento proces, a dojít ke stejnému výsledku.

4. osoba mající zodpovědnost za případ (pověřený vyšetřovatel- case officer) má osobní zodpovědnost za dodržení zákonnosti a těchto principů, během vyšetřování.

Zásady, tak jak jsou zde vytčeny Sdružením velících policejních důstojníků, zdůrazňují, že vlastně neexistují rozdíly mezi tradičním vyšetřováním a vyšetřováním kybernetického zločinu. Vyšetřování může, již pro samu podstatu věci, zahrnovat odlišné techniky nezbytné k prozkoumání technologií , ale základní principy zůstávají tytéž. Hlavní požadavek kladený na vyšetřovatele a současně hlavní břemeno na něj kladené je nezbytnost současně nashromáždit důkazy, a současně pečovat o neporušenost důkazů a o zajištění dostatečné průkaznosti důkazů před soudem. Toto je zřejmě ten největší rozdíl mezi vyšetřovatelem a správcem sítí/systémů či technikem. Zatímco ti později jmenovaní se snaží vyřešit problém způsobený útokem kybernetického zločinu , vyšetřovatel se snaží rekonstruovat místo/ scénu trestného činu a rekonstruovat modus operandi. Navíc, zatímco jakákoliv akce a aktivita vyšetřovatele musí být před soudem dokumentovatelná a vysvětlitelná, není správce sítí/systémů či technik tímto povinován. Naneštěstí mnoho případů bylo ztraceno v důsledku intervence osob neškolených, což vedlo k nepoužitelnosti shromážděných důkazů pro soudní účely.
Shromažďování důkazů při vyšetřování kybernetických trestných činů/zločinů je obtížné zejména také proto, že tyto případy neberou ohled na národní hranice ani na národní zvyklosti.
Útoky kybernetického zločinu jsou prováděny přes Internet což je celosvětově rozšířená síť, která propojuje miliony computerů, a to od malých domácích notebooků a stolních počítačů až po průmyslové počítače. Koncept místa činu, jak jej používá klasická kriminologie, se posouvá z fysikální do virtuální úrovně. Osoby používající Internet mohou komunikovat s dalšími uživateli bez ohledu na čas a prostor. Uživatel Internetu navíc má prospěch z určité anonymity, a možnosti zůstat skryt. Tento scénář je používán osobami či organisacemi s nelegitimními záměry. Zdá se že tento fakt, totiž taktopojaté místo činu, je to hlavní, co odlišuje vyšetřování „ kybernetického trestného činu/zločinu“ od tradičního vyšetřování trestné činnosti.

Sběr dat.

Jako určitá předehra k jakémukoliv útoku kybernetického trestného činu/zločinu musí nastat zajištění přístupu na Internet pro jednotlivce či organisaci, - budoucího pachatele. Přístup k Internetu lze docílit pouze prostřednictvím nějakého poskytovatele internetových služeb- tzv. ISP- Internet Services Provider. Vlastní přístup k Internetu pak probíhá buďto skrze otevřený účet o některého komerčního ISP (2), nebo je pachatel sám vlastníkem nebo provozovatelem ISP. ISP má schopnost uchovávat u sebe data, která mohou být při vyšetřování kybernetického trestného činu/zločinu považována za velmi důležitá. Takováto informace může zahrnovat údaje o uživateli, typ internetové komunikace která byla poskytnuta, a místo kde byla služba nainstalována (3). Naneštěstí je tato informace nepoužitelná, pokud nejsou k disposici současně data o přenosu, tzv. traffic data. Data/údaje o přenosu, tedy traffic data zahrnují všechnu informaci nashromážděnou u ISP, která se vztahuje ke dni, času a typu spojení, k trvání spojení , zahájení a ukončení každé komunikace, a kategorie informace, ke které byl během této doby zjednán přístup. Kvality informací uchovávaných jednotlivými ISP se liší od jednoho poskytovatele k druhému. Údaje o přenosu/ traffic data se obecně v teorii vyšetřování považují za ekvivalent otisků prstů v klasickém vyšetřovacím schematu ohledání a zajištění místa činu. Naneštěstí tyto informace nejsou (povinně) uchovávány všemi ISP. Nedostatečné sladění (harmonisace) legislativy vede k tomu, že orgány činné v trestním řízení nemohou zaručit stejnou úroveň pro všechna vyšetřování. Ve většině případů jsou tyto orgány vydány „ na milost a nemilost“ jednotlivým ISP, pokud se týče toho jaká data jsou vůbec uchována a tedy k disposici, a jaká data budou vyšetřovateli předána. Data o přenosu/traffic data jsou pro vyšetřování kybernetického zločinu naprosto vitální.Obecně řečeno, datat od ISP většinou umožní orgánům činným v trstním řízení vyšetřování započít.

Závěr.

V dnešní době hrají počítače důležitou roli téměř při každém spáchaném trestném činu/zločinu.To však neznamená že každý takovýto čin je automaticky i „ computerovým zločinem“. Znamená to však, že orgány činné v trestním řízení musejí být mnohem více „ počítačově gramotné“ už jen proto, aby vůbec udržely krok s kriminálními živly. Komputerová soudní věda, (Computer forensic) je proces zahrnující získání, prošetření a uchování elektronických dat získaných z různých typů ukládacích medií, a to způsobem vhodným pro následnou presentaci během soudního jednání. Zahrnuje v sobě dovednosti, techniky a speciální programové vybavení-software, vyvinuté pro následnou presentaci složek (files), a fragmentů složek files fragments), založených ve známých formátech pod rozličnými operačními systémy.

Zatím neexistuje jednoduchá jednotná metodologie pro provádění computerového soudního vyšetřování a analysy. Přesto je computerová soudní věda- Computer forensic- vědou exaktní. Je obtížná a detailně pečlivá. Pro omyl zde není žádný prostor (5). Jakýkoliv omyl vede totiž k tomu, že průkazní materiál se stane nepoužitelným pro soudní jednání.

Poznámky a odkazy:

1) ACPO (2002), Good Practice Guide to Computer Based Evidence. Associacion of Chief Police Officers (UK)

2) For the purpose of this article a commercial ISP is taken to include access to Cyber Kiosks and and cafés. Pro účely totoho článku se pod pojem komerční ISP zahrnují i Cybekiosky a počítačové- Internetové kavárny

.

3) Toto se týká zejména širokopásmových spojení, jako jsou ADSL a kabelová připojení.

4) Po tragediích z 11. září a po teroristických útocích v Madridu se jednotlivé národní legislativní sbory snaží uvbést v život zákony, které by zavazovaly ISP uchovávat přenosová data. Příkladem tohotoprocesu je CyberCrimeConvention(Budapest, 2001) a připravovaná směrnice EU - Proposed Draft Framework Decision regarding the Retention of Traffic Data, která se v současnosti široce diskutuje.

5) Vaca R. John (2002), Computer Forensics-Computer Crime Scene Investigation. CharlesRiver Media (USA).

Adresa pro korespondenci:

Mgr. Hana Kalová
Pracoviště klinické farmakologie
Nemocnice České Budějovice a.s.
B. Němcové 54
370 87 České Budějovice

e-mail address: kalova@nemcb.cz