Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra statistiky

Teze diplomové práce

Počítačová kriminalita

Bc. Vítězslav Chochola

Počítačová kriminalita

Souhrn

Práce se zabývá počítačovou kriminalitou v České republice. Hlavním cílem je nalezení souvislosti mezi jejím nárůstem a chováním uživatelů Internetu.

Tvoří ji základní přehled těch nejčastějších oblastí kriminality, seznamuje se stručnou historií technologií obsahující první projevy související kriminality. Následuje hlavní část, která je analýzou chování uživatelů, zpracované na základě empirického výzkumu.

Ten se zaměřil na používání běžně dostupných bezpečnostních prostředků a znalost některých důležitých prvků internetové komunikace. U souvisejících otázek zjišťuje závislosti zjištěných výsledků. Empirická část dále sleduje dosavadní průběh počtu případů počítačové kriminality v České republice a na základě něj za použití statistické metody odhaduje budoucí vývoj.

Zjištění z empirické části je dále sumarizováno v závěrečné části a na základě nalezení slabých míst české uživatelské základny jsou navrhována opatření, která mohou úspěšnost pachatelů počítačové kriminality zmírnit.

Průběžně je práce doprovázena případy z kazuistiky, jejichž účelem je přiblížit závažnost a reálné dopady podceňování bezpečnosti používání Internetu.

Klíčová slova: informační a komunikační technologie, počítačová kriminalita, Internet, zabezpečení dat, bezpečné chování, bezpečnostní software, přenos dat, vývoj kriminality, kazuistika, pravidla bezpečného chování

Empirický dotazníkový průzkum, který tvoří základní prvek práce, zahrnuje odpovědi na 18 otázek od 152 respondentů. Otázky byly sestaveny na základě řešené problematiky v oblasti bezpečnosti chování běžných uživatelů Internetu. Byly kladeny především ve spojitosti s prostředky, jejichž užívání lze v současné době pokládat za běžné nebo je jejich existence většině běžných uživatelů Internetu známá. Jsou to prostředky běžně používané jak k připojení k Internetu, tak k samotnému užívání.

Nad rámec tématu byla položena otázka na kurzy a školení v oblasti bezpečnosti, aby bylo možné potvrdit či vyvrátit domněnku o nedostatečném systému vzdělávání v této oblasti.

Výsledky byly zpracovány v tabulkovém procesoru, odpovědi byly procentuálně vyhodnoceny a pro potřeby nalezení vícenásobné shody souvisejících ukazatelů byla použita odpovídající funkce, vracející počet záznamů vyhovujících více kritériím současně. Z těch byly dále vytvořeny kontingenční tabulky a vypočítány síly závislosti mezi jednotlivými aspekty chování. Ostatní odpovědi jsou popsány základními popisnými charakteristikami ve formě grafického vyjádření absolutních a relativních četností a jsou doprovázeny komentáři.

Pro potřeby zmapování vývoje počítačové kriminality byla použita data o počtu řešených případů v oblasti informačních technologií ze zdrojů Policie České republiky a Vojenské policie. Z těchto dat byl pomocí statistické metody časových řad vytvořen přehledný grafický trend. Metoda spočívala v nalezení vhodné funkce, která byla následně použita pro odhad budoucího vývoje pro roky 2015 – 2017.

Kapitola „Přehled řešené problematiky“ čtenáře seznamuje s nutnou terminologií této práce, včetně definic počítačové kriminality. Ty jsou pojaty jak z pohledu obecné formulace a členění, tak i z pohledu aplikace do legislativy. Legislativní pohled v sobě zahrnuje i nutnost reakce na vývoj kriminality a mezinárodní spolupráci, na jejímž základě byla legislativa upravena pro současné potřeby. V kapitole dále následuje popis těch nejčastějších projevů počítačové kriminality z praktického hlediska, doprovázený možnostmi obrany proti nim. Mezi ty nejdůležitější patří phishing, porušování autorského práva, viry a škodlivé kódy atd. V dalším pokračování kapitoly jsou popsány některé zásadní milníky v historickém vývoji technologií, doprovázené popisem prvních projevů počítačové kriminality. Zde jsou již popsány první případy z kazuistiky.

Vlastní empirická část je rozdělena do několika oblastí. Tou první je zabezpečení dat. Zde jsou rozebírány otázky z průzkumu, které se zabývaly problematikou používání hesel, blokování přístupu k datům či zálohování dat. Na tuto oblast, stejně jako některé následující, je nahlíženo i z pohledu stále se rozšiřujícího využívání „chytrých“ mobilních telefonů. Jako výchozí bod slouží hypotéza, že uživatelé zabezpečují počítače a chytré telefony rozdílně, a to i přesto, že se mezi těmito přístroji technicky i po uživatelské stránce rozdíl stírá. Prostřednictvím kontingenční tabulky je zjišťováno, zda existuje závislost mezi typem telefonu a způsobem zabezpečení jeho dat a hledá se tak potvrzení či vyvrácení této hypotézy. Další podkapitola se věnuje sociálním sítím. Na ně je nahlíženo jakožto na častý prostředek kybernetických útoků všeho druhu. Mezi tyto útoky patří používání falešných identit za účelem páchání další, mnohem závažnější, počítačové kriminality např. zneužívání dětí, dále phishing, šíření virů nebo škodlivých kódů. Následuje pozornost věnovaná antivirovým programům a komplexním zabezpečovacím softwarům a jejich používání v počítačích a mobilních telefonech. Po zmapování oblasti zabezpečení dat v koncových zařízeních následuje téma přenosu dat, které zkoumá používání bezdrátových sítí Wi-Fi a protokolu HTTPS. Prostřednictvím kontingenční tabulky byla hledána závislost mezi znalostí HTTPS a schopností jej zohledňovat na jedné straně a využívání internetového bankovnictví a placení kartou on-line na straně druhé. I téma bezpečných datových přenosů bylo doprovázeno ilustrujícími příklady z kazuistiky.

Empirickou část uzavírá podkapitola „Policejní statistiky“. Ta využívá získaná data ze znaleckých pracovišť státní správy k vytvoření grafu za účelem volby vhodného modelu trendu, ze kterého bylo možné co nejkvalitněji odhadnout budoucí vývoj. Po verifikaci zvolené lineární funkce pomocí indexu determinace a střední absolutní procentuální chyby (MAPE) byl vypočten odhad počtu vyřízených dožádání do příštích let.

Práci uzavírá kapitola „Zhodnocení výsledků a doporučení“.

Z empirické části vyplynulo, že zabezpečení počítačů lze pokládat za relativně dostačující. Nejen přístupová hesla, ale i antivirové programy se staly běžnou součástí používání počítačů a i počet uživatelů s komplexním řešením bezpečnosti činí téměř třetinu. Bude-li se počet používaných komplexních řešení zvyšovat, lze pokládat výsledky za uspokojivé. V tématu přenosu dat byly výsledky rozporuplné. Na jedné straně uživatelé kvalitně zabezpečují své domácí sítě Wi-Fi, na druhé straně v hojné míře využívají volné sítě. To z bezpečnostního hlediska příliš doporučit nelze. Velké nedostatky byly nalezeny

v používání šifrovaného internetového protokolu HTTPS a to především v souvislosti s používání bankovních aplikací či platbami kartou on-line.

Jak bylo uvedeno výše, respondenti jsou si dobře vědomi potřeby zabezpečení počítačů. Jinak je tomu však u chytrých mobilních telefonů, které využívá 71 % dotazovaných. To, co by v případě osobního počítače uživatelé považovali za bezpečnostní riskování, nevnímají při užívání mobilního telefonu jako hrozbu. Na základě zjištění empirického výzkumu tedy bylo možné zkonstatovat, že je stále mylně chápán rozdíl mezi nutností zabezpečení počítačů a mobilních telefonů. Zatímco u počítačů je základní ochrana samozřejmostí, jsou běžně chráněny přístupovými kódy a antivirovými programy, v případě mobilních telefonů tomu tak není. Důraz na jejich zabezpečení by měl být kladem z několika důvodů. Jejich funkcionality se od počítačů neliší a naproti tomu jsou mnohem více vystaveny riziku ztráty nebo krádeže. Navíc z jejich mobility vyplývá několik dalších zneužitelných funkcionalit. K instalaci škodlivých kódů jsou telefony stejně náchylné jako počítače, ale díky absenci bezpečnostních softwarů jsou mnohem snáze napadnutelné. To může v kombinaci například s bankovní aplikací způsobit značné újmy.

Z toho vyplývá jednoznačné doporučení věnovat se zabezpečení mobilního telefonu minimálně na stejné úrovni, nebo dokonce na vyšší, než je tomu u osobních počítačů. Výrobci bezpečnostních softwarů nabízejí mnohá kvalitní řešení, která jsou navíc s ohledem na jejich menší rozšíření zatím zpravidla zdarma.

Dalším důležitým závěrem je nutnost investic a vzdělávání v oblasti zabezpečení. Výsledky průzkumu ukázaly tuto oblast jako velmi slabou. Na základě dalších otázek tohoto průzkumu lze konkrétně ve vzdělávání doporučit důraz na zabezpečení chytrých mobilních telefonů, odhalování nastražených phishingových zpráv ze všech zdrojů a používání bezpečnostních prvků při používání internetového bankovnictví a plateb kartou on-line.

Z výše uvedených důvodů kapitolu uzavírá formulace několika základních pravidel, jejichž dodržování může značně přispět k nižšímu riziku napadení počítačovým útokem. Také díky těmto pravidlům je uskutečňován záměr práce – zmírnit nárůst počítačové kriminality v České republice.

Vybrané bibliografické citace:

CEJPEK, Jiří. *Informace, komunikace a myšlení.* 2. vyd. Praha: Karolinum, 2005. ISBN 80-246-1037-X.

HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech.* 1. vyd. Praha: Triton, 2012. ISBN 978-80-7387-545-9.

KOLOUCH, Jan, VOLEVECKÝ, Petr. *Trestněprávní ochrana před kybernetickou kriminalitou.* 1. vyd. Praha: PAČR, 2013. ISBN 978-80-7251-402-1.

MATĚJKA, Michal. *Počítačová kriminalita.* 1. vyd. Praha: Computer Press, 2002. ISBN 80-7226-419-2.

MUSIL, Josef. *Elektronická média v informační společnosti.* 1. vyd. Praha: Votobia, 2003. ISBN 80-7220-157-3.

NAUMANN, Friedrich. *Dějiny informatiky – Od abaku k internetu.* 1. vyd. Praha: Nakladatelství Academia, 2009. ISBN 978-80-200-1730-7. Přeložila Michaela Voltrová.

PETROWSKI, Thorsten. *Bezpečí na Internetu pro všechny*. 1. vyd. Liberec: Dialog, 2014. ISBN 978-80-7424-066-9. Přeložil Tomáš Kurka.

POŽÁR, Josef, KALAMÁR, Štěpán, POKORNÝ, Vladimír. *Základy teorie informační bezpečnosti.* 1. vyd. Praha: PAČR, 2007. ISBN 978-80-7251-250-8.

PROKEŠ, Josef. *Člověk a počítač aneb svítání digitální kultury.* 1. vyd. Tišnov: Sursum, 2000. ISBN 80-85799-82-0.

SMEJKAL, Vladimír. *Internet a §§§.* 1. vyd. Praha: Grada Publishing, 2001. ISBN 80-247-0058-1.

SVATOŠOVÁ, Libuše, KÁBA, Bohumil. *Statistické metody II.* 1. vyd, 1. dotisk. Praha: ČZU PEF, 2008. ISBN 978-80-213-1736-9.