Internetová kriminalita

Nesolidní lidi najdete i v prostředí jedniček a nul

MARTIN CHLEBOUN

Od samotných počátků lidské civilizace využívají pachatelé protispolečenských či protiprávních činů nové a nové prostředky, které jim poskytuje daná doba. Nejinak je tomu dnes, kdy internet a informační technologie poskytují velké množství moderních prostředků pro nelegální aktivity nebo se samy stávají předmětem útoku, nikoli jen jeho prostředkem. Internetová kriminalita, ještě nedávno nový pojem, v kriminalistice pomalu zdomácněl.

Odjakživa také platí, že pachatelé nelegálních činů mají před těmi, kdo je vyšetřují, náskok – nejsou totiž svázáni žádnou hierarchií, administrativními postupy nebo nedostatkem potřebného technického vybavení. V oblasti internetové kriminality to platí dvojnásob. Ti, kdo chtějí internet využít jako prostředek páchání trestného činu, mají v ruce nepřeberné množství možností.

Terminologie

Na internetu se můžeme setkat zpravidla se čtyřmi okruhy zločinů:

1. zločiny narušující soukromí (nezákonný sběr údajů a jejich šíření),
2. nelegální obsah (pornografie, vyzývání k násilí, rasismus apod.),
3. ekonomické zločiny (napadení systémů, podvody, šíření virů atd.),
4. porušování duševního vlastnictví (zejména v souvislosti s distribucí nelegálního softwaru a audio- či videosouborů).

Současná praxe internetové kriminality v ČR je poměrně rozvinutá, ať už se týká kriminálních činů, v nichž hraje internet hlavní a jedinou roli, nebo rozsáhlejších deliktů, ve kterých je internet součástí komplexnější trestné činnosti. V největší míře se jedná o mravnostní trestné činy, tedy zločiny související se zveřejňováním nelegálního obsahu, projevy extremismu, útoky na data, finanční podvody, výhrůžky a pomluvy a porušování autorského práva.

Zločiny slovem a obrazem

Mravnostní a verbální kriminalita, neboli nelegální obsah zveřejňovaný na internetu, je logickým důsledkem prakticky neomezených možností této sítě. Zatímco ostatní typy médií umožňují naplnění svobody slova jen velmi obtížně (většinou je to dáno ekonomickými omezeními – ne každý si může zřídit vlastní televizní stanici), internet byl ke komunikační otevřenosti přímo stvořen a dává prostor každému, aby se vyjádřil bez nutnosti masivních investic. Kromě velmi diskutované dětské pornografie představuje velké riziko zveřejňování návodů k násilné trestné činnosti (např. na výrobu výbušnin) a verbální kriminalita (projevy extremismu). Do této oblasti spadají výhrůžky, které anonymita internetu umožňuje, a také vydírání. Zatím k nejznámějšímu případu verbální kriminality došlo v ČR loni, kdy anonym adresoval státu výhrůžku, že pokud nedostane 840 000 Kč, zaútočí bombou v Praze a v Brně. Za tři dny tentýž člověk zvýšil svůj požadavek na 50 milionů, záhy byl však dopaden.

Ekonomické zločiny

Mediálně atraktivními činy bývají útoky na data, a tak se o nich dozvídáme často, přestože pravděpodobně nebudou mezi ostatními zastoupeny tak výrazně – taková kriminalita vyžaduje přece jenom vyšší znalost technologií než například zveřejňování nežádoucího obsahu. Zajímavé jsou zejména proto, že se cílem útoků stávají velké a renomované společnosti a jde při nich nejen o jejich důvěryhodnost, ale také o velké peníze, stejně jako tomu bylo v případě pachatele, který nejprve prostřednictvím internetu získal data velké společnosti, aby jí je vzápětí stejným způsobem nabídl s výhrůžkou, že jinak je poskytne třetí osobě. Velké starosti dělá kriminalistům využívání informačních technologií k praní špinavých peněz a dalším formám finanční kriminality. Internet umožňuje provést během okamžiku velké množství transakcí, které dokonale zamlží původ peněz, jež je potřeba skrýt před zraky vyšetřovatelů. Technicky velmi vyspělé skupiny organizovaného zločinu tak mohou značně snížit riziko svého odhalení. O peníze jde ale také v případě drobnějších finančních podvodů, které se na internetu vyskytují poměrně často. Někdy může jít o nabídku kradeného zboží, jindy o snahu vylákat z důvěřivého adresáta e-mailu peníze na nejrůznější účely (už nějakou dobu jsou aktuálním tématem internetu důvěrné dopisy bývalých členů vlád afrických zemí, kteří slibují provizi za pomoc při převodu ukrytých peněz).

Hacking

Zatímco někdy je narušení dat motivováno ekonomickým zájmem, jindy jde o „hru“ s cílem exhibovat se, byť i takový útok a neoprávněné pozměnění dat může pro vlastníka znamenat velkou finanční újmu. V této věci u nás proslula zejména hackerská skupina CzERT, které se podařilo pozměnit internetové stránky Ministerstva zdravotnictví, KSČM, Union banky či Seznamu.cz.

Mezi tyto činy zahrňme také snahu (rovněž ne ojedinělou) nejrůznějších lidí o získání osobních údajů prostřednictvím veřejně přístupných internetových služeb. Čas od času dostanou uživatelé freemailů nebo jiných služeb vyžadujících registraci e-mail z adresy, která má záměrně vyvolat pocit, že dopis byl odeslán poskytovatelem služby. Odesílatel požaduje od uživatele zaslání přístupových údajů, většinou pod záminkou vývoje služby či přidání dalších funkcí. Ač se zkušenějším uživatelům internetu může zdát tato věc úsměvná, pisatelům se daří uvedená data v mnoha případech získat.

Proti autorům

Freehostingové služby, neveřejné sítě či počítače jednotlivců se v rámci internetu stávají úložišti softwaru nebo dalších datových souborů, které jsou prostřednictvím internetu šířeny nelegálně. Ať už nabízejí správci těchto prostorů software, MP3 nahrávky nebo videosoubory za úplatu nebo zcela zdarma, páchají trestný čin, protože porušují autorský zákon. Ve věci distribuce a používání nelegálního softwaru je u nás aktivní zejména Business Software Aliance, na nezákonné sdílení a zveřejňování hudebních nahrávek aktivně dohlíží vedle policie např. Mezinárodní federace fonografického průmyslu.

Statistiky

Přestože se v případě internetové kriminality jedná o oblast rozsáhlou, podrobnější statistiky jednotlivých typů trestných činů spadajících do této oblasti naše policie zatím nevede. Možná bude vstup do EU znamenat zrovnoprávnění internetové kriminality s ostatními formami trestné činnosti jak z hlediska oddělené práce s konkrétními daty, tak kvalitnějšího vybavení a lepšího personálního pokrytí nelegálních aktivit souvisejících s internetem. Policie sice nechce sdělit počet lidí, kteří mají internetovou kriminalitu na starosti, ani popsat jejich vybavení, závěry nedávno zpracované analýzy nicméně dávají tušit, že za mnohem lépe vybavenými pachateli zatím zaostává. 4 0357/FEL ❑