Vydírání po síti

Pokud po sobě zanecháte stopy, můžete se stát obětí nátlaku, vydírání či obtěžování

VOJTĚCH BEDNÁŘ

Moderní technologie a internet zvláště sice slouží dobrým účelům, avšak mohou být také snadno zneužity, například jako prostředek vydírání svých uživatelů. Mohou být jak médiem, tak i kompromitujícím faktorem. Názory na tento problém se sice liší, nicméně objektivně existuje.

Pohled první: dej sem peníze!

Prakticky každý, kdo pracuje s internetem má ve své elektronické identitě hned několik různých způsobů, kterými může být kontaktován. E-mailová schránka, ICQ nebo jiný Instant Messanger, přezdívka na chatu, to vše jsou unikátní nebo takřka unikátní znaky, podle nichž můžeme najít konkrétního člověka a komunikovat s ním. Stejně tak mohou však všechny tyto znaky být i zcela anonymní a odtržené od konkrétní osoby. Právě obou těchto vlastností se dá velmi snadno využít, respektive zneužít.

Jestliže v minulosti (a ve filmech) vyděrači používali k vyhrožování svým obětem poštu a telefon, v současné době ke stejnému účelu poslouží chat, e-mail a další vymoženosti internetu. Prakticky všechny tyto prostředky lze pořídit zcela anonymně, anebo se zfalšovanými údaji. Uživatelům tak může být snadno vyhrožováno, mohou po nich být požadovány například peníze, přičemž může být obtížné zjistit, odkud přesně útok přichází.

Pohled druhý: vím o tobě všechno!

Tak jako může být internet komunikačním médiem, může být i samotným zdrojem vydírání. Prakticky žádný systém ochrany elektronických dat, který byl zatím představen, není úplně dokonalý. Dokumenty, fotografie nebo obrazové záznamy, to všechno se snadno může v nepravých rukou stát nástrojem možného zkompromitování uživatele. V některých případech dokonce není nutné kopírovat důležité a tedy i zabezpečené informace, stačí z počítače nebohé oběti, například úředníka nebo manažera, dostat historii prohlédnutých internetových stránek a podívat se, zda neobsahuje klíčová slova nebo soubory v cache, odpovídající třeba dětské pornografii.

Ještě lepší je v této oblasti zneužívání inzerce, zejména seznamovací. Stačí, když si náš útočník založí anonymní schránku a podá si na ni inzerát typu „krásná a velmi žádostivá blondýnka hledá milence". Samozřejmě že nabídky se jen pohrnou, a bude-li některou z nich ženatý muž, obzvláště pokud se pachateli podaří o něm zjistit co nejvíce informací, může za své mlčení dostat dobře zaplaceno, nebo skončit v místech s mřížemi, avšak bez internetu.

Zcela specifickým způsobem je vydírání zneužitím virtuální identity. Je vskutku velmi jednoduché odeslat e-mail z cizí schránky a pod cizím jménem, není k tomu třeba, vyjma samotné adresy a jména, znát absolutně nic ani mít žádné speciální hackerské dovednosti. Některým lidem může velmi ublížit, je-li jejich schránky takto zneužito k „nekorektní" komunikaci, a protože je to jednoduché, tak se to dost často i děje. Obrana proti takovému typu útoku je analogická jako v případě ukradených firemních dokladů nebo razítka – potenciální příjemce podvržené pošty včas varovat.

Sladce jednoduchá výtržnost

Vydírání s pomocí elektronických komunikačních prostředků je stejným trestným činem jako jakékoli jiné. Právě anonymita, respektive její vidina však z nich tvoří prostředek mnohem lákavější, mnohem zajímavější a mnohem jednodušší. Mnoho výhružných e-mailů, které mohou končit ve vaší schránce, je ve skutečnosti pouze vtipem kolegy – recesisty, kamaráda, rodinného příslušníka nebo prostě někoho, kdo k vaší identitě přišel náhodně a teď mu dělá velikou legraci bavit se na váš účet.

Problém je v tom, že i taková zábava může snadno jít za hranice zákona, a pokud by byla prošetřována policií, může být kvalifikována jako jeho porušení, na médiu totiž nezáleží. Mnoho uživatelů internetu žije stále ještě se zakořeněným klišé, poplatným konci devadesátých let minulého století. A sice, že síť je naprosto anonymním prostředím, ve kterém není možné nikoho vystopovat. To skutečně není pravda.

Například uživatel anonymního e-mailu při jeho registraci sice zadal naprosto smyšlené údaje, a tedy si myslí, že je v bezpečí, ve skutečnosti však při jeho zadávání sedí u naprosto konkrétního počítače s unikátní IP adresou, případně za unikátním proxy serverem. Může jít o počítač v internetové kavárně nebo v jiném veřejném prostoru, avšak náš uživatel ho používá v určitou hodinu, respektive v určitém časovém období. Analýzou tohoto časového úseku na daném počítači se lze dopracovat k druhotným znakům, které jej identifikují naopak velmi dobře. Bezpečně se zamaskovat dokáže ve virtuálním prostředí pouze odborník na bezpečnost, a těch se kriminality tohoto typu moc neúčastní.

▲ **Informace o anonymizérech se dozvíte na stránkách i Žurnálu na www.rozhlas.cz/izurnal /porapoc/_zprava/85555.**

▲ **Bezpečnosti a anonymitě na internetu se věnuje knížka od Marka Střihavky z vydavatelství Computer Press Praha.**

Co mám dělat?

Sednul jsem si k počítači a vybíral e-mail. Když jsem zjistil, že mi někdo píše, že mi rozbije pusu, myslel jsem si, je to jen legrace. Druhý den mi ale přišla zpráva, ve které mi psal kde jsem včera byl, co jsem tam dělal a že když mu nezaplatím, tak mě zabije.

Asi takto vypadá příběh oběti prvního ze dvou pohledů na vydírání po síti, tedy tam, kde je síť využita jako spojovací médium. Pokud se vám stane něco podobného a s určitou pravděpodobností víte, že nejde o vtip, je dobré se ihned obrátit na policii. V některých místech je možné, že policisté mohou podobný problém, stejně jako další nešvary typu domácího násilí, bagatelizovat, ale to by vás nemělo v žádném případě odradit.

Nějaký trouba mi napsal, že jestli mu nedám deset tisíc, ukáže mému šéfovi fotky, které jsem si prohlížel před týdnem v práci.

Toto je klasická ukázka druhého typu vydírání, relativně méně nebezpečného. V okamžiku, kdy k němu dojde, se optimální řešení – kromě pomoci policie, jež by mohla mít stejný efekt jako splnění útočníkových hrozeb – hledá špatně, mnohem efektivnější je však prevence. Především je třeba si uvědomit, že existují dva způsoby přístupu k potenciálně citlivým informacím. První z nich počítá s naprostým utajením takové informace. Druhý naopak s jejím úplným zveřejněním, což je ekvivalentní stavu, kdy žádné „citlivé" informace nemáme, respektive mít nechceme.

Některé informace, které se mohou potenciálně hodit k nátlaku na jejich původce, vznikají – jako například už zmíněná historie prohlédnutých stránek – zcela spontánně a automaticky, majitel o nich dost možná až do okamžiku, než jsou zneužity, neví. Přesto je dobré uvědomit si všechna podobná rizika. Na pracovišti, a v případě veřejně angažovaných osob také kdekoliv jinde, není příliš dobrým nápadem prohlížet si pornografické servery, nebo místa s jiným, podobně citlivým obsahem. Počítač nebo počítačová síť, kterou používáte, by měly být vždy maximálně chráněny proti průnikům zvenčí. I když před útokem skutečného profesionála vás pravděpodobně nezachrání vůbec nic, mnoho potenciálních útočníků zažene i obyčejný osobní firewall, vypnuté nebo omezené funkce sdílení souborů a tiskáren, záplatovaný operační systém s bezpečnostní politikou nastavenou tak, aby nebyl okny vesmíru otevřenými dokořán. Mezi bezpečnostní rizika, která mohou být zneužita ve váš neprospěch, patří také, i když se o tom neví, využívání ilegálních kopií softwaru (v extrémním případě také legální kopie s aplikovaným crackem), stejně tak jako vlastnictví či nabízení většího množství ilegálních multimediálních souborů. Oblíbeným cílem skutečných, byť virtualizovaných zločinců jsou taktéž mnozí „vypalovači", často studenti, kteří si přivydělávají vypalováním CD jako brigádou. Už se vyskytlo několik případů, kdy bylo prostřednictvím e-mailu právě takovým osobám vyhrožováno. Jako nástroje vydírání posloužily snímky obsahu jejich disků, obě dříve popsané koncepce se tedy setkaly v jediném, pro oběť dvojnásobně nepříjemném celku.

Budoucnost hrozivá i bezpečnější

Internet, ačkoliv se tak zdá být, není zcela bezpečným anonymním komunikačním médiem. Takjak se vyvíjejí stále sofistikovanější postupy, umožňující najít i maskující se osobu nebo stroj, vyvíjí se i nástroje tohoto maskování, nikdy však k absolutní dokonalosti. Když vám někdo zavolá na pevnou telefonní linku, už dávno jeho identifikace netrvá za pomoci speciálních nástrojů celé desítky sekund, během nichž je třeba „pachatele" udržet na lince, nýbrž zlomek okamžiku. Internetové (de)anonymizování je v podobném stavu, jako analogové a digitální telefonní linky. Břídila lze objevit během chvilky, profesionála velmi stěží.

Tak jak dochází k rozšiřování elektronické komunikace, očekává se i nárůst míry jejího zneužívání. To je logické a nedá se proti tomu dost dobře nic dělat. Zákony nicméně platí ve světě jedniček a nul stejně tak, jako v tom reálném, a to je rozhodně pozitivum. 3 0746/FEL ❑