Václav Jirovský

Kdo má informace, má moc

TEXT: PETR MELNIČUK FOTO: MARTIN SVOZÍLEK

NEDÁVNÉ ÚTOKY HACKERŮ NA VLIVNÉ ČESKÉ FIRMY POTVRZUJÍ, ŽE OCHRANA SÍTÍ U NÁS JE NEDOSTATEČNÁ. POČÍTAČOVÁ KRIMINALITA VYNÁŠÍ ORGANIZOVANÉMU ZLOČINU ASTRONOMICKÉ ČÁSTKY. ÚNIKY DAT MOHOU MÍT NEDOZÍRNÉ NÁSLEDKY. A KAUZA WIKILEAKS MŮŽE BÝT PROVOKACÍ TAJNÝCH SLUŽEB. TO VŠE ŘÍKÁ PŘEDNÍ ODBORNÍK NA KYBERNETICKOU BEZPEČNOST VÁCLAV JIROVSKÝ.

Než jsem se s Václavem Jirovským potkal, chtěl jsem vidět, co dokáže šikovný hacker. „Jste prý zvědavý, jak si umí velké firmy chránit počítačové servery a databáze?“ řekl tiše na uvítanou před Národním technickým muzeem v Praze na Letné. Kývl jsem a čekal, co se bude dít. Mladík ve věku středoškoláka vybalil notebook a sedl si s ním na schody. Stačilo mu pár minut, aby se postupně proháčkoval na server významné české banky. Byl tak šikovný, že se dostal do služební i soukromé e-mailové pošty nejvyššího šéfa bankovního domu. Ani on, ani já jsme si v ní ale nechtěli číst. Mladý muž mi ještě ukázal soubory strategických záznamů a rozhodnutí nadnárodní firmy, která působí v Česku. Dostal se k nim za pouhých deset minut. „Stačí?“ zeptal se. Neměl jsem co dodat. Mladý hacker se spokojeně usmál, pak se rychle sbalil a zmizel. S tímhle zážitkem a mnoha otázkami jsem šel další den za Václavem Jirovským.

Jak je tohle možné?
Jednoduše – čím dál tím složitější počítačové systémy zákonitě mají „díry“. Těch se ročně objevuje kolem devíti až dvanácti tisíc. Když ty díry umíte najít, můžete vstoupit do systémů, aniž byste musel znát klasickou přihlašovací cestu, třeba jako když jdete do své elektronické pošty.

Jak to, že firmám nevadí, že někdo může nahlížet do jejich kuchyně?
Určitě vadí, jenže velmi záleží na tom, jakou bezpečnostní politiku mají, bez ohledu na to, zda jsou malé, nebo velké. Když se vedení společnosti rozhodne, že zápisy a strategická rozhodnutí z porad se budou ukládat v šifrované formě, která bude přístupná jen exekutivě firmy, tak si zvědavý hacker s největší pravděpodobností nic nepřečte.

Proč to netvrdíte se stoprocentní jistotou?
Protože i v tomto systému může být díra, ovšem dostat se přes ni bude složitější. Asi vás překvapím, ale devadesát procent všech úspěšných útoků je možné vést proto, že lidé, kteří odpovídají za počítačové sítě vědomě či nevědomě někomu, promiňte mi ten výraz, vykecají podstatu jejich ochrany. Jen zbývajících deset procent úspěšných napadení připadá na dovednost hackerů.

Z toho, co teď říkáte, mám tak trochu husí kůži. Jak jsou u nás chráněny důležité databáze například ministerstev obrany, vnitra, financí?
V době před třemi či čtyřmi roky, kdy se rozjížděly takzvané elektronické schránky, byla jejich ochrana na velmi špatné úrovni.

A dnes?
Na tuto otázku nejlépe odpovídají nedávné úspěšné útoky hackerů na servery českých bank, médií i mobilních operátorů. Těžko se proti nim brání, ochrana není jednoduchá. Zajímavé na útocích je jejich zaměření na servery patřící vždy stejnému „segmentu“ trhu. Banky, zpravodajské servery, operátoři – někdo tyto struktury v Česku dobře zná. Ale téměř všude na světě se podceňuje význam kybernetické bezpečnosti přesně do doby, než dojde k napadení. Důvodem může být i nedostatek skutečných IT odborníků. V posledních letech došlo u nás k devastaci odbornosti, mimo jiné i proto, že ji není nutno nikde prokazovat. Do velkého byznysu ochrany dat jsou tak často zapojeny i ty firmy, které o bezpečnosti nic nevědí. A to je docela tristní.

Často zdůrazňujete, že mnohem víc než hackerů se obáváte tzv. agregátů, tedy třeba obchodních řetězců, bank, pojišťoven či sociálních sítí, které o nás shromažďují nejrůznější data. Na prvním místě „nebezpečnosti“ uvádíte mobilní operátory. Proč?
Protože o nás vědí úplně všechno. Uvedu vám příklad ze sousedního Německa. Tam se nedávno jeden politik Strany zelených rozhodl soudit se společností Deutsche Telecom o data, která o něm coby zákazníkovi ukládala do svých databází.

> **Práce nepoučeného člověka s internetem? To je, jako kdyby se procházel po minovém poli.**

Když proces vyhrál, poskytl veškeré informace jednomu magazínu, který z nich – a také z dalších veřejně dostupných dat – složil půl roku jeho života. Minutu po minutě. Kde kdy byl, co dělal, kde se zastavil, jak dlouho tam jednal, kde nakupoval, kterou restauraci navštívil, jak dlouho mu trvalo vypití kávy, v které škole byl a co tam přednášel, kam chodil k lékaři. Poslanec Bundestagu chtěl, aby se veřejnost dověděla, jak je sledován nejen on, ale i další miliony občanů. V Česku situace není jiná.

Jak by tato data mohla být zneužita?
Nejhorší je podle mne možnost změny údajů. Stačí drobná úprava a život sledovaného člověka se z gruntu obrátí. Představte si, že někdo „neviditelně" vyjme z telekomunikačních databází váš zaznamenaný pohyb na služební cestě v Jičíně a změní ho na pobyt v Jindřichově Hradci. Na tom není na první pohled nic strašného. Ovšem jen do té doby, než místní policie začne vyšetřovat vraždu vašeho známého, s kterým jste neměl nejlepší vztahy. Budete mít dost problémů s vysvětlováním, že jste v inkriminovanou dobu v Hradci nebyl. Podobné příklady nejsou ojedinělé.

V knize Rozbité okno americký spisovatel Jeffery Deaver tvrdí, že klíč k penězům a moci drží právě ti, kteří disponují největším počtem informací o našich kreditech, zdraví nebo nákupních zvyklostech. Už jsou známé i případy zneužití těchto dat?
Bezpochyby existují, ale nikdo s nimi nepůjde veřejně na trh. Osobně se obávám hlavně zneužití dat soukromou osobou. Vezměte si například telefonní odposlechy. Činnost policie je přísně vymezená zákonem, ale soukromé bezpečnostní agentury si dělají, co chtějí. Vloupou se do bytu, nainstalují štěnice, odposlouchávají telefony a je jim fuk, zda je to zákonné, nebo ne. Mimochodem, dnešní chytré telefony jsou prvotřídní špioni, kteří o nás podávají zprávy, aniž bychom to chtěli. Ty se střádají na nějakém serveru a jeho majitel je na tom lépe než americká Národní bezpečnostní agentura. Má totiž v jedné ucelené databázi obrovský přehled například o lidech ze sociálních sítí, mobilních telefonů i přístupových bodů sítí wi-fi. A někomu se ty informace mohou hodit…

Co říkáte aféře WikiLeaks, která nelegálně zveřejňuje utajované vládní a korporátní dokumenty? Je získání těchto materiálů krádež, nebo selhání dnes už obviněného vojína americké armády?
Víte určitě, že kauza WikiLeaks je nelegální činnost? Nemůže to být třeba akce zpravodajské služby? Možná celá WikiLeaks má za úkol změnit nazírání lidí na nějaký politický problém, změnit veřejné mínění. Může to být třeba politický mocenský útok vůči nějaké vlivné skupině, kterou někdo chce zdiskreditovat. Připomenu krátce americký film Vrtěti psem z roku 1997: Ve Spojených státech vrcholí předvolební kampaň a stávající prezident má výborné vyhlídky na znovuzvolení, jenže čtrnáct dnů před volbami se v médiích objeví informace o jeho sexuálním styku s mladistvou.

Václav Jirovský (* 1947)

- Vystudoval Elektrotechnickou fakultu ČVUT v Praze.
- V letech 1975 a 1986 pracoval v Oblastním výpočetním centru vysokých škol.
- V roce 1987 byl pod jeho vedením dokončen pilotní projekt řízení hromadné dopravy pro hlavní město Prahu.
- Ten samý rok přešel na Matematicko-fyzikální fakultu UK, kde působil do roku 2007. V letech 1991 až 1998 pracoval jako ředitel útvaru výzkumu a vývoje firmy Advanced Computer Applications v USA, pak se zase vrátil na Matfyz.
- Nyní je proděkanem a současně i vedoucím Ústavu bezpečnostních technologií a inženýrství na Fakultě dopravní ČVUT, kde se věnuje otázkám počítačové kriminality a protiprávního jednání na sítích.

Okamžitě se sejdou prezidentovi nejbližší spolupracovníci, aby se dohodli, co s tím udělají. Dobrou pověst prezidenta má vytvořit – jako ostatně pokaždé – expert na politickou propagandu. Jak se mu to daří s pomocí manipulace masmédií a veřejného mínění, o tom film přesně je. Stejné to může být podle mého soudu i u WikiLeaks. Samozřejmě, že se to nedá prokázat, ale charakter této akce splňuje všechny náležitosti zpravodajské operace a tato hypotéza není nepravděpodobná. Čemu dnes věřit ve virtuálním světě, ale i v médiích, to je jeden velký otazník.

Vraťme se k obyčejným uživatelům internetu. Na začátku tohoto roku dosáhl v Česku jejich počet čtyř milionů. Jak vysoké procento z nich si uvědomuje, že jejich počítače a práce na nich se dá zneužít?
To nedokážu odhadnout, ale jistě mezi nimi nejsou samí experti. Naopak. Na jaké úrovni vědomostí se pohybujeme, nejlépe dokládá phishing. Úspěšnost podvodných e-mailů s nejrůznějším obsahem, často překládaných automaticky z cizího jazyka do češtiny, které vylákají z lidí heslo nebo číslo kreditní karty, je pět procent. Převedeme-li toto procento na celou populaci, pak tu máme půl milionu internetově negramotných. Jediná cesta, jak se vyhnout nejrůznějším nástrahám, a na tom se shodují všichni experti, je ale právě zvyšování počítačové gramotnosti v tom nejširším smyslu slova.

Neopatrnost lidí, na kterých parazituje kyberkriminalita, přináší i ekonomické škody. Troufnete si je odhadnout?
Před dvěma lety představovaly ztráty jen u obchodníků v USA 3,4 bilionu dolarů. Když vztáhneme tuto hodnotu na celý svět a obory využívající síťových technologií, dostaneme se k částce v řádu trilionů dolarů. Jsou to neuvěřitelné sumy. Krade se především z účtů lidí, firem i bank. Ovšem nejnebezpečnější je zcizení identity. Třeba jen ve Spojených státech dochází ročně ke čtyřem milionům případů krádeží PIN, hesel, osobních údajů. Zloději pak za okradeného uzavírají leasingové smlouvy, hypoteční úvěry, kupují auta a domy. Miliardové sumy vynáší mafiím i skimovací zařízení montovaná do bankomatů, kterým se finanční ústavy po celém světě jen velmi obtížně brání.

Na co by si tedy měli dávat pozor běžní uživatelé internetu?
První věc je naučit se chovat ve virtuálním prostoru. Znát toho, s kým mluvím nebo si píšu. Dávat si pozor na to, abych nereagoval na některé nesmyslné věci, které mi přicházejí do počítače nebo chytrého telefonu. Například už zmíněné phishingové e-maily. A pak si dávat také pozor na to, v jakém stavu je můj počítač. Tvrzení, že musím mít hlavně antivirový software, nestačí. Mimo něj je totiž důležitý i personální firewall. Lidé by měli uvažovat také nad tím, kdy kliknou na tlačítko ANO a k čemu vlastně dávají souhlas. Věřte, že nepřeháním, když řeknu, že práce nepoučeného člověka s internetem je doslova chůzí v minovém poli. v