3 SVĚTOVÁ KYBERNETICKÁ

TŘETÍ SVĚTOVÁ VÁLKA STRAŠÍ LIDSTVO OD OKAMŽIKU, KDY SKONČILA TA DRUHÁ. BĚHEM LET SE PŘEDSTAVY O JEJÍM PRŮBĚHU NEUSTÁLE MĚNILY. STŘET VÝCHODU SE ZÁPADEM VYSTŘÍDAL BOJ ZÁPADU S ISLÁMEM. NEDÁVNO SE OBJEVILA DALŠÍ VARIANTA: VÁLKA ODEHRÁVAJÍCÍ SE V ELEKTRONICKÝCH SYSTÉMECH, V SÍTÍCH A NA INTERNETU. A K TOMU SI JEŠTĚ PŘIČTĚTE KYBERTERORISMUS. STANE SE KLÁVESA ENTER NOVOU ZBRANÍ HROMADNÉHO NIČENÍ?

AUTOR: PAVEL KUČERA
FOTO: JAN MALÝ JR.

Jednadvacáté století přineslo řadu vymožeností. Válku lze nově rozpoutat nejen na zemi, ve vzduchu, na moři a ve vesmíru, ale také prostřednictvím drátů. Těch drátů, jaké vedou u vás doma z počítače k internetové přípojce. A pokud se domníváte, že se jedná o lepší vyhlídku, než kdyby začaly padat bomby, nemáme pro vás dobré zprávy. Rozsáhlý kybernetický konflikt by mohl být stejně ničivý a dramatický jako konvenční válka a téměř jistě by v něm umírali lidé.

TRPASLÍCI VERSUS OBŘI

Kybernetické útoky i obrana proti nim jsou už několik let předmětem plánování vojenských kampaní většiny vyspělých zemí. Týdeník The Economist dokonce před časem kyberprostor nazval pátou kolonou všech moderních válek. Výhodou či nevýhodou (záleží na tom, zda konflikt chcete rozpoutat, nebo se před ním bránit) takové války je, že může být vedena, aniž by ji někdo oficiálně vyhlásil. „Žádný stát doposud nevyhlásil jinému státu válku a následně neprovedl otevřený útok v kyberprostoru. Z tohoto pohledu tedy žádný kybernetický vojenský útok není potvrzen," tvrdí Jiří Štábl z tiskového oddělení Ministerstva obrany ČR. „Je však zřejmé, že řada států je schopna takovýto útok vést a disponuje odborníky v této oblasti. Ve virtuálním a anonymním prostředí internetu je však dokazování původu útoku obtížné až nemožné," dodává.

Oficiálně tedy kybernetické války neexistují. Existují však důkazy o útocích, jež byly tak sofistikované a na takové technologické úrovni (o nutnosti velkorysého financování nemluvě), že je prakticky vyloučeno, aby za nimi stál jednotlivec či soukromá organizace. Mediálně známá je např. aféra, při níž byly centrifugy jaderného zařízení v íránském Búšehru napadeny virem Stuxnet. To mělo mít podle odborníků za následek zdržení výroby jaderné bomby, z níž je Ahmadínežádův režim dlouhodobě podezříván. Celý proces napadení byl přitom obrovsky složitý. Počítače centrifug kupříkladu vůbec nejsou připojeny k internetu. Virus se tedy nejprve musel dostat do notebooků búšehrských inženýrů, zde zahnízdit a při jejich připojení do interní sítě elektrárny se přesunul na své místo a aktivoval se. V souvislosti s tímto útokem se mluví zejména o Izraeli, snad ve spolupráci s Američany, kteří měli možnost zasáhnout Írán na citlivém místě. A přitom tajně (původce viru se nepodařilo prokázat) a bez nutnosti vyvolat méně pohodlnou konvenční válku.

Bohaté zkušenosti s útoky prostřednictvím počítačů má i Rusko. V polovině srpna 2008 se rozhořel konflikt mezi Ruskem a Gruzií, který byl doprovázen rozsáhlou ofenzivou ze strany ruských hackerů. Zda s oficiálním požehnáním státu či bez něj, je předmětem dohadů. Hackeři napadli stránky gruzínského prezidenta i parlamentní weby a země byla nucena po nějakou dobu používat jako svou oficiální informační stránku blog na Blogger.com. Sílu ruských počítačů v posledních letech pocítilo i Estonsko, u nějž hackeři v reakci na návrh zákona, který staví komunistické a nacistické symboly na stejnou úroveň, na týden vyřadili z provozu vládní a poté bankovní systémy. A totéž potkalo i Litvu. Kybernetické zuby ukázala i Severní Korea, jejíž obyvatelstvo sice strádá hlady, ale podle odborníků země disponuje asi tisícovkou špičkových hackerů. Těm se před dvěma lety podařilo zasáhnout počítače svého jižního souseda i Spojených států. Kybernetická válka není běžnou válkou, kde větší armáda automaticky poráží tu menší. Dnes může trpaslík zranit i obra.

TAJEMNÝ CIRC

Přestože u nás k žádnému významnému kybernetickému útoku zatím nedošlo, česká vláda tohle nebezpečí nebere na lehkou váhu. Koncem února tiskem proběhla zpráva, že se připravuje zákon, jehož prostřednictvím hodlá Česko lépe čelit kybernetickým útokům na klíčové podniky a instituce. Dokonce bude možno vyhlásit kybernetický stav nebezpečí, kdy by byla na premiérův přímý pokyn celá země preventivně odstřižena od internetu. Tento plán vzniká pod dohledem Národního bezpečnostního

úřadu a o jeho zařazení do zákona se uvažuje od roku 2015.

Nad kybernetickou bezpečností naší republiky bdí také CIRC (Cyber Incident Response Capability, něco jako „způsobilost odezvy na kybernetickou událost"). Tento vojenský útvar sídlí v Brně, ale jedná se o „režimové pracoviště", takže vstup sem mají pouze osoby uvedené vnitřní směrnicí. Jak pracoviště funguje? „CIRC je specializovaný prvek Armády ČR a jeho úkolem je odhalovat a řešit kybernetickou zranitelnost, hrozby a útoky na komunikační a informační systémy resortu obrany," odpověděl na můj dotaz Jiří Štábl z Ministerstva obrany ČR. „Zúčastňuje se cvičení zaměřených na kybernetickou bezpečnost v NATO." Vzhledem k tomu, že jde o věci podléhající vojenskému a možná i státnímu tajemství, jejichž vyzrazení by mohlo přispět k přímému ohrožení státu, mě strohost odpovědi ani nepřekvapuje. Jsem rád, že si s otázkou kybernetické bezpečnosti naší vlasti láme hlavu někdo fundovaný, a vydávám se raději na obhlídku elektrárny.

BUDIŽ TMA

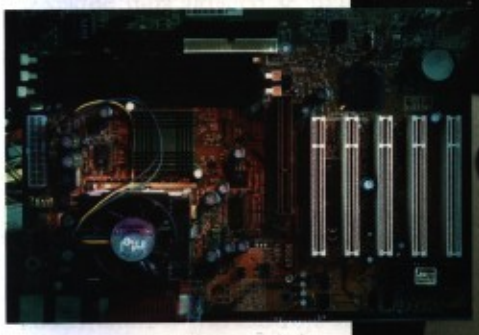
Viděli jste Smrtonosnou past 4.0? Pokud ano, máte díky tomu poměrně dobrou představu, co je to kybernetický terorismus. V tomto akčním filmu bojuje Bruce Willis coby John McClane s hackery, kteří se snaží ochromit celé Spojené státy tím, že vyřadí z provozu dopravní uzly, elektronická média, telekomunikace i internet a stejnou cestou se chystají zastavit i dodávky elektřiny a plynu. Výsledkem má být osobní msta, ale především panika a chaos. Je to reálné i mimo Hollywood? „Toto nebezpečí nejenže existuje, ale taky velmi rychle roste," říká mi ve své kanceláři ing. Jiří Sedlák, vedoucí odboru Bezpečnost ICT a systém řízení společnosti ČEZ. Zajímá mě, zda někdo, kdo sedí na druhé straně zeměkoule, je schopen, pokud se k tomu odhodlá, vypnout elektřinu třeba v celé naší zemi a vrátit nás tak o sto let zpátky. „Nejde ale jenom o rozpětí kybernetických útoků, které mohou přijít, ale i o spektrum zbraní, které k němu mohou být použity. Problémem je, že subjekty, které jsou kybernetickým útokem ohroženy, nemají zdaleka takové prostředky, jakými disponují útočníci," vysvětluje Jiří Sedlák.

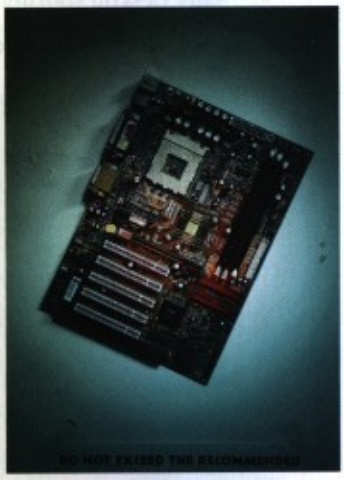
Zranitelnost našeho systému zvyšuje i fakt, že nikdo dopředu nemůže stanovit, jaké budou cíle potenciálního útočníka. Bude si tím chtít jen dokázat svou ajťáckou šikovnost? Bude z toho mít finanční profit? Nebo bude usilovat o politický převrat? Proto je prakticky nemožné připravit se na všechny alternativy. „Pokud by například u energetické sítě k takovému útoku a následnému plošnému výpadku došlo, je už celkem jedno, zda by trval v řádu minut či hodin. Jeho důsledky by každopádně pro stát i národní hospodářství byly devastující," říká Jiří Sedlák a tváří se při tom smrtelně vážně. Při představě ohňů hořících po několik dní na Václavském náměstí, všeobecného chaosu a rabování při rozsáhlém black-outu pouze naprázdno polknu. Ještěže mám peníze bezpečně uložené v bance. Nebo nemám?

VESMÍRNÉ OPICE

Existuje názor, že bude-li někdo chtít konkrétnímu státu provést něco hodně ošklivého, může mu násilně vnutit svou představu o rovnostářství tím, že vynuluje údaje o bankovních účtech jeho obyvatel. Přesně o to v románu Klub rváčů usilovaly Vesmírné opice, tajná podzemní armáda pod vedením Tylera Durdena, která si vytkla za cíl smazat všechny údaje o úsporách, úvěrech i hypotékách a veškeré záznamy o vlastnictví pozemků a nemovitostí. Výsledkem měl být návrat společnosti do bodu nula, kdy každý vlastní jen to, co má právě u sebe, a všichni začneme pěkně od začátku.

Může k tomu dojít? „Nemůže," uklidňuje mě Mgr. David Lorenc, ředitel úseku Přímé bankovnictví České spořitelny. „Všechny velké instituce, ať už banky, mobilní operátoři nebo katastry nemovitostí a další, mají tyto informace hned v několika různých počítačích. A především existují zálohy na dalších médiích. Magnetické pásky, harddisky, cokoliv. A ty rozhodně





Hacker je někdo kreativní, kdo je schopný u konkrétní technologie vidět její možnosti i způsob, jak je využít. Je to člověk, který vidí dveře i tam, kde ostatní vidí zeď.

nesmažete tak, že k tomu dáte někomu, kdo sedí u počítače, pokyn. Musel byste je fyzicky vytáhnout z archivu, vložit do zařízení a smazat. Čistě teoreticky by se mohlo stát, že ty pásky někdo přejede magnetem, ale to už je kombinace s fyzickým útokem. Z počítače odněkud z Asie se tohle skutečně udělat nedá." V reálu to tedy vypadá tak, že pokud někdo podobný útok na vaši banku naplánoval, může vám dočasně znemožnit, abyste se dostali ke svým penězům. Na stav vašeho konta by to nemělo mít vliv. Pokud tedy výpadek nebude dlouhodobý a způsobené ekonomické škody tak rozsáhlé, že mezitím vaše úspory pozbudou svoji hodnotu. Kybernetické útoky na české banky vůbec nejsou ojedinělé. Nicméně cílem není destabilizace ekonomiky a v první fázi ani luxování kont jejich klientů. Většinou jde o krádež informací o klientech a jejich následný prodej. Jak pravil Gordon Gekko ve filmu Wall Street, „informace jsou to nejcennější zboží, co znám". Hovoříme o mediálně dobře známých termínech phishing a pharming, jimž byla právě Česká spořitelna vystavena ve velkém v roce 2008. Tehdy statisíce klientů i neklientů tohoto bankovního domu obdržely podvodné e-maily, jimiž se útočník podepsaný Českou spořitelnou pokoušel vymámit údaje, na jejichž základě by se mohl dostat k citlivým informacím, např. kolik peněz mají na účtu, kolik a komu platí nebo jaké produkty mají s bankou uzavřené. Podobné praktiky vedle hackingu úzce souvisí i s další zábavnou disciplínou nazývanou sociálním inženýrstvím. A sociálním inženýrem se může stát každý, i když ukončil vzdělání pátou třídou základní školy a jeho IT znalosti končí u otírání prachu z displeje počítače. Stačí být drzý, přesvědčivý a vlastnit třeba mobilní telefon, jehož prostřednictvím se budete vydávat za pracovníka banky a někdo hodně důvěřivý vám svěří svůj PIN. Bravurně to zvládl například Heath Ledger ve filmu Candy.

MEZI NÁMI HACKERY

Hackery si asi většina z nás představuje jako neviditelnou záškodnickou sílu ohrožující náš systém a řád. Termín hacker (hack v angličtině znamená rozsekat na kousky) však může označovat v podstatě jakéhokoliv kutila či modeláře, který se rád svým hračkám koukne do vnitřností. A je jedno, zda se jedná o software, hardware či železniční modely. Za líheň počítačového hackingu jsou považovány kampusy amerických univerzit v první polovině 70. let. Vzhledem k tomu, že internet tehdy prakticky neexistoval, je však zřejmé, že cílem první hackerů nebylo „někam se nabourat" nebo „něco shodit", spíše zjistit, jak věci fungují.

„Z našeho pohledu je hacker někdo kreativní, kdo je schopný u konkrétní technologie vidět její možnosti i způsob, jak je využít. Je to člověk, který vidí dveře i tam, kde ostatní vidí zeď," říká mi hacker s přezdívkou Růža, člen volného sdružení pražských hackerů, zastřešeného neziskovkou brmlab, sídlícího v budově bývalých Elektrických podniků na Vltavské. Během návštěvy nabývám dojmu, že jsem se ocitl v seriálu Ajťáci. Dvě místnosti pozvolna zaplňují sympatičtí nerdi (ženu jsem tu nezaznamenal žádnou), z nichž většina klove do notebooků před sebou (klidně i do dvou současně), jiní něco pájí, montují nebo měří na zařízení, jejichž funkci si netroufám odhadnout. A všude kolem se povalují počítače, dráty, klávesnice, moduly a další součástky, z nichž by nejspíš bylo možné postavit družici. Všichni se tváří velmi přátelsky, a tak jediné, co naší schůzce dodává konspirační nádech, jsou jejich přezdívky. Pod skutečným jménem nejsou členové brmlabu ochotni mluvit na diktafon (byť je redakce zná). Důležitá poznámka: dnes tolik frekventovaný znak hnutí Anonymous jsem nikde nezaregistroval.

Počítačoví hackeři se mezi sebou navzájem rozdělují do několika kategorií. Především na „ty hodné" a „ty zlé", tedy white hats a black hats (bílé a černé klobouky). Označení vychází z černobílých westernů, kde kladný hrdina většinou nosil bílou pokrývku hlavy a záporňák černou. „Někteří hackeři se zabývají hledáním bezpečnostních chyb v softwaru a hardwaru," vysvětluje mi další z pražských hackerů s přezdívkou Kermit. „Hlavní rozdíl

je ten, že white hats, když chybu objeví, ji publikují, případně se podílejí i na její opravě. No a black hats ji zneužijí ke svému prospěchu. Ale jsou i tací, co to hrají na obě strany podle situace." Když se přítomných hackerů zeptám, jestli mezi sebou mají i nějaké black hats, nebo jsou všichni rození klaďasové, namísto odpovědi se dočkám mlčení a pobavených úsměvů.

CUCÁCI ZDROJOVÉHO KÓDU

„Existuje řada lidí, co se nazývají hackery, ale ve skutečnosti o fungování počítačů nebo jejich zabezpečení nic nevědí," říká Kermit. „Stačí jim využívat něco, co vytvořil někdo jiný. Dneska je internet plný nástrojů, které si někdo vyrobí, aby mohl demonstrovat nějakou chybu v zabezpečení a tím na ni upozornit. Třeba ani nemá v úmyslu ji zneužívat. Pak je ale sorta lidí, kterým se říká script kiddies (cosi jako cucáci zdrojového kódu), kteří si tyto nástroje stáhnou, tupě je používají a třeba tím shazují servery. Přitom vůbec nevědí, na jakém principu tyto nástroje fungují," dodává Kermit. I hackerské útoky (myšleno ty amatérské, nikoliv armádní) se řadí do mnoha kategorií, a to podle obtížnosti a rozsahu. Dnes je nejrozšířenější „shazování stránek", tedy DDoS (Distributed Denial of Service), jež v uplynulých týdnech zaznamenala i řada českých institucí, například Ochranný svaz autorský. Zjednodušeně řečeno, stránku shodíte tím, že se na ni zkusíte podívat z mnoha (v řádech desítek či stovek tisíc) počítačů najednou, čímž ji svými požadavky zahltíte. Je pochopitelné, že tolik počítačů nikdo nemá a tato funkce se dá nasimulovat softwarově. A nejvíc je těchto útoků právě proto, že jsou z podstaty velmi jednoduché a člověk nemusí mít žádné extrémní IT znalosti. „Řada lidí se schovává za jméno Anonymous. To jsou často ti, kteří tomu ani moc nerozumějí. Říkají, že webserver shodili, což není pravda. On běží dál, jenom nestíhá odpovídat," pokračuje Kermit. „Ale třeba nedávné pozměnění webové stránky ODS, to už je trochu komplikovanější. Ti, co to spáchali, museli najít nějakou bezpečnostní skulinu, nahrát tam, co potřebovali, a ještě po sobě museli smazat stopy. To už byl trochu sofistikovanější útok. A lidí, co tohle svedou, je výrazně méně."

Co tedy můžeme od Anonymous slibující co chvíli, že vypne Facebook, Google či rovnou celý internet očekávat do budoucna? Naprosto cokoliv. Růža to vysvětluje na příkladu. „Ta síla a neštěstí Anonymous je v tom, že je prostě anonymní. To není žádná centralizovaná skupina, je to spíš myšlenka. A může za ni být kdokoliv. Já tady vyhodím zástrčku od serveru, něco tím vypnu, vyhlásím, že jsem Anonymous. A nikdo proti tomu nemůže nic namítnout, protože to bude pravda."

Jak se žilo bez počítačů, není tak těžké zjistit. Převážná část obyvatel planety si to pamatuje. Ano, bez nich se žilo docela dobře. Ale mají i řadu výhod. Přesto často vyhrožujeme, že profil na Facebooku smažeme, notebook prohodíme zavřeným oknem a začneme zase chodit do lesa nebo na pivo. Vzpomeňte si na to, až budete na slevových serverech pátrat po nejlevnějším víkendovém lyžování v Alpách nebo kursech vaření. Počítače prostě ovládly naše životy a tato závislost přináší řadu rizik. Největším nebezpečím pro civilizaci není počítač sám, ale člověk za jeho klávesnicí. A podle všeho to tak ještě dlouho zůstane.