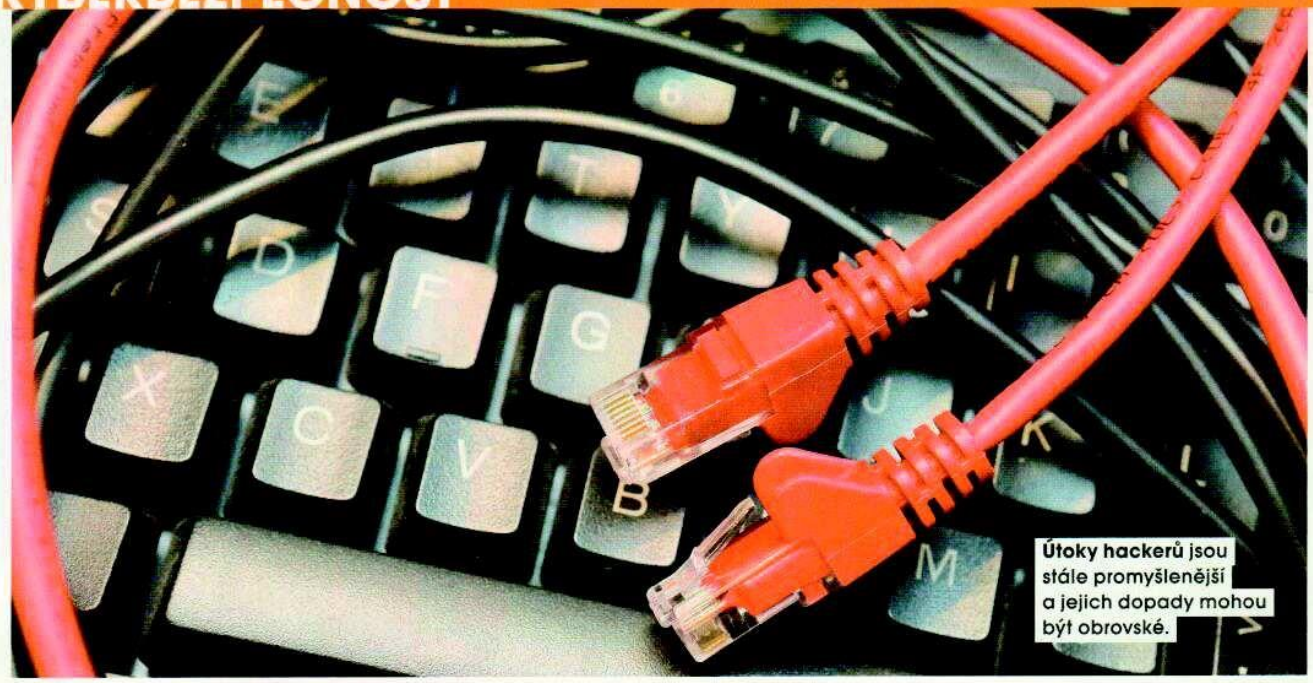

Útoky hackerů jsou stále promyšlenější a jejich dopady mohou být obrovské.

Česká zbraň na hackery

KRÁDEŽE CITLIVÝCH DAT, PENĚZ, OCHROMENÍ ELEKTRÁRNY NEBO LETIŠTĚ. TO VŠECHNO DOKÁŽOU ŠPIČKOVÍ HACKEŘI. NA SVĚTĚ KAŽDÝ DEN DOCHÁZÍ KE STOVKÁM TISÍC RŮZNĚ NEBEZPEČNÝCH KYBERNETICKÝCH ÚTOKŮ. UNIKÁTNÍ ZAŘÍZENÍ V ČESKU UČÍ, JAK SE JIM UBRÁNIT.

Stres narůstá. K prolomení ochrany počítačů řídících dodávky elektřiny pro většinu republiky chybí kousek. Jakákoli chyba může mít fatální následky. A právě na ni tým hackerů čeká. „Že v Čechách žádná taková událost ještě nenastala, je spíše náhoda. A je jen otázka času, kdy k tomu dojde," říká Milan Balážik, manažer výcvikové arény CyberGym Europe, zatímco vstupujeme do speciálního zařízení kousek od Prahy.

Tým zkušených IT specialistů, bezpečnostních odborníků i expertů na psychologii a mezilidskou komunikaci tady cvičí takzvané obránce - lidi, kteří mají na starost ochranu klíčových počítačových systémů v soukromých i veřejných organizacích. Například bankách, vládních institucích nebo velkých průmyslových podnicích. „Když třeba začne hořet elektrárna, vypadne proud nebo se stane něco podobného, je už pozdě. Takovým případům se snažíme předejít. Vyškolit obránce tak, aby se nic podobného nestalo," popisuje Balážik.

SUPERMAN NESTAČÍ

Nezbytnost pohotových obránců počítačových systémů stoupá s naší závislostí na výpočetní technice. Svět jedniček a nul dnes řídí téměř vše - od ledničky přes nemocniční přístroje až po naváděcí systémy letadel. „Zároveň se významně posouvají typy útoků. Od amatérů k týmům zkušených hackerů, kteří pracují pro konkurenci, ale třeba i pro vlády nebo státní služby," vysvětluje Balážik.

Zatímco dříve stačili na ohlídání kybernetické bezpečnosti organizací jedinci, dnes by to nezvládl ani Superman. „Útok je většinou veden na několik různých technologií najednou. Musíte mít tým zkušených obránců, kteří skvěle ovládají konkrétní problematiku a zároveň mezi sebou dokážou komunikovat," říká Rostislav Jirkal, předseda představenstva CyberGym Europe.

Vstupujeme do místnosti modrého týmu. Na první pohled vypadá jako běžná počítačová učebna. Na několika monitorech blikají číselné kódy, jinak je tu naprostý klid. Při tréninku zde bývá rušněji. Právě tady se učí klientské týmy, tedy obránci. S různou razancí a intenzitou na ně útočí červený tým hackerů. Kybernetické útoky neprobíhají podle univerzálního scénáře, naopak. Příprava tréninku trvá několik týdnů a celý proces je šitý na míru požadavkům konkrétní organizace. Instruktoři vlastně nasimulují pracovní prostředí obránců, kteří zde vykonávají svou každodenní práci. Netuší, kdy a jak k útoku hackerů dojde. Vše pečlivě sleduje takzvaný bílý tým tvořený IT odborníky - koordinuje útoky hackerů a zároveň modrému týmu radí, jak jim čelit.

„Naši hackeři jsou hodní. Jde o lidi, kteří se dokonale naučili určité postupy a techniky a používají je v pozitivním smyslu," vysvětluje Jirkal. Největší bonus vidí v tom, že si lidé zažijí konkrétní

situaci kyberútoku, poznají, jak se pod návalem stresu chovají, a vylepší své dovednosti. „Často se setkáváme s tím, že k nám přijde tým s nějak rozdělenými rolemi. Jakmile ale začne působit stres, lidé se mění. Trénink potom ukáže nejenom jejich teoretické znalosti, ale také konkrétní schopnosti v praxi," dodává Balážik.

SMART NENÍ SAFE

Průběh kyberútoku musí být co nejvěrohodnější. Proto je součástí tréninkové arény třeba model elektrárny či zařízení simulující distribuci plynu nebo vody. Všechna tato zařízení patří mezi cíle hackerů. Podobně jako systémy e-bankovnictví nebo třeba vládní počítače s tajnými informacemi. „Každá instituce provozující velkou informační strukturu dnes denně čelí tisícovkám kybernetických útoků," odhaluje Jirkal. Většina z nich je prý vedena automatizovanými nástroji, třeba programy pokoušejícími se najít bezpečnostní skulinky.

Pouze pět procent všech útoků mají na svědomí týmy profesionálních hackerů, jsou ale extrémně nebezpečné. Nejzáludnější bývají situace, kdy útočníkům pomáhá osoba infiltrovaná přímo do napadené organizace, takzvaný insider. „I s tím počítáme a obránce učíme nejenom zastavit útok, ale rovněž insidera odhalit. To už je v podstatě detektivní práce," usmívá se Jirkal, zatímco procházíme okolo nenápadných dveří. „Jediné místo, kam se nepodíváme. Tady sedí naši hackeři," vysvětluje Balážik.

Podobných zařízení pro trénink kyberobránců je prý na světě okolo pěti. Aréna, v níž jsme, slouží pro výcvik specialistů z celé Evropy. „Současná společnost je kyberneticky závislá. Všechno tedy potřebuje patřičnou úroveň obrany," říká Jirkal a poukazuje na koncept smart cities – chytrých měst využívajících digitální, informační a komunikační technologie. „Smart city nemusí vždy znamenat safe, tedy bezpečné city," glosuje. Stačí třeba promyšlený útok na systém řídící semafory a město je ochromeno. „Nechci ani domýšlet, kolik lidí by takový kolaps stál život – třeba jen v Praze," nastiňuje Jirkal.

LÁKADLO PRO HACKERY

Hackeři se neustále zlepšují. Proto také narůstá zájem o odborníky na kyberbezpečnost i kvalitní absolventy takto zaměřených studijních programů. S tréninkovou arénou začal v Česku jako první z tuzemských vysokých škol spolupracovat CEVRO Institut. Studenti MBA programu management a kybernetická bezpečnost zde absolvují výcvik v rámci studia.

„Nejčastějšími problémy, které s obránci řešíme, je nepřiměřenost jejich reakcí nebo jejich úplná nepřítomnost. To všechno lze ale během výcviku naučit a vylepšit," říká Jirkal. Ostatně i instruktoři CyberGymu musejí být stále minimálně o krok napřed. Čas od času totiž jejich připravenost prověří skuteční hackeři. „Samozřejmě jsme jim trochu trnem v oku a útoky na nás zkoušejí. Nemají to ale snadné, zatím jsme se ubránili."

Hackeři v akci

Kauza CIA
V březnu zveřejnil server WikiLeaks informace o technikách hackerů CIA. Obsahuje popis jejich útoků na takzvané chytré televize, aby díky nim mohli sledovat domácnost diváků, na chytré telefony nebo systémy Android a Windows.

Napadený Zaorálek
České ministerstvo zahraničí je prý terčem hackerů dlouhodobě, letos v lednu se jim však podařilo proniknout do e-mailových schránek desítek zaměstnanců včetně ministra Lubomíra Zaorálka.

Okradené Yahoo!
Přes miliardu e-mailových adres, telefonních čísel a dalších dat ukradli hackeři technologické firmě Yahoo!. Útok z roku 2013 přiznala společnost až loni.

Ukrajinský blackout
Přes sedm set tisíc obyvatel bez elektřiny, zmatek, chaos. Rozsáhlý výpadek proudu, který postihl v prosinci 2015 Ukrajinu, byl prý rovněž dílem hackerů.

Ochromená ocelárna
Příkladem napadení průmyslového podniku je útok na ocelárnu v Německu z roku 2014. Hackeři tehdy získali kontrolu nad jednou z vysokých pecí a znemožnili její vypnutí.

Český týden
Začátkem března 2013 měli čeští experti na kyberbezpečnost napilno. Během jediného týdne se hackerům při celkem primitivním DDoS útoku podařilo zahltit tuzemské zpravodajské servery, nejnavštěvovanější domácí vyhledávač, weby bank a mobilních operátorů.

„Když začne hořet elektrárna nebo vypadne proud, je už pozdě," varuje Milan Balážik.

Současná společnost je podle Rostislava Jirkala kyberneticky závislá. A technologie tak potřebují patřičnou ochranu.

Foto: Jakub Stadler a iStockPhoto