Česká zbraň na hackery

Na světě dochází každý den ke stovkám tisíc různě nebezpečných kybernetických útoků. Špičkoví hackeři mohou ukrást citlivá data či peníze, ochromit elektrárnu nebo letiště. Unikátní zařízení v Česku učí, jak se takovým napadením ubránit.

Fatální následky by mohlo mít třeba prolomení počítačů řídících energetickou síť Česka. „Že u nás 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 ležícího několik kilometrů od Prahy.

Foto: iStockphoto.com

▲ **HACKEŘI** stále více těží z kybernetické závislosti současné společnosti. Jejich útoky jsou přitom čím dál propracovanější.

Tým zkušených IT specialistů, bezpečnostních odborníků i expertů na psychologii a mezilidskou komunikaci tady cvičí takzvané obránce, lidi, kteří mají na starosti ochranu klíčových počítačových systémů v soukromých i veřejných organizacích. Například v bankách, vládních institucích nebo velkých průmyslových podnicích. „Když začne třeba 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," upřesňuje Balážik.

Superman nestačí

Nezbytnost pohotových obránců počítačových systémů stoupá se závislostí společnosti na výpočetní technice. Svět jedniček a nul dnes řídí téměř všechno od ledničky přes nemocniční přístroje až třeba po naváděcí systémy letadel. „Zároveň se významně posouvají typy útoků. Od hackerů amatérů k týmům zkušených hackerů, kteří pracují pro konkurenci, ale třeba i pro vlády, státní služby," vysvětluje Balážik. Zatímco dříve v některých případech postačili k ohlídání kybernetické bezpečnosti organizací jedinci, dnes už jsou takoví Supermani passé. „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 vykonávají svou každodenní práci. Netuší, kdy a jak k útoku hackerů dojde. Vše pečlivě sleduje takzvaný bílý tým tvořený IT odborníky. Ten koordinuje útoky hackerů a zároveň modrému týmu pomáhá a 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 je podle něho v tom, že lidé zažijí konkrétní situaci kybernetického útoku, 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.

Nebezpeční špioni

Průběh kyberútoku musí být co nejvěrohodnější. Proto je součástí tréninkové arény také model elektrárny či zařízení simulující distribuci plynu, vody či vodní páry. Všechna tato zařízení patří mezi cíle hackerů podobně jako speciální technologie pro řízení průmyslové výroby, systémy elektronického bankovnictví nebo třeba vládní počítače s tajnými informacemi.

„Každá instituce provozující velkou informační strukturu denně čelí tisícovkám kybernetických útoků," říká Jirkal. Většina z nich je prý vedena

automatizovanými nástroji, třeba programy pokoušejícími se najít bezpečnostní skulinky. Jen okolo pěti procent všech útoků mají na svědomí týmy profesionálních hackerů. Takové ataky jsou ale extrémně nebezpečné. Nejzáludnější jsou situace, kdy útočníkům pomáhá osoba infiltrovaná přímo do napadené organizace. „I s tím počítáme a obránce učíme nejen zastavit útok, ale rovněž takového 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.

Aréna, v níž právě jsme, slouží pro výcvik specialistů z celé Evropy. „Současná společnost je kyberneticky závislá. Všechno tedy potřebuje patřičnou úroveň obrany," nastiňuje Jirkal.

O krok napřed

Hackeři se neustále zlepšují. Proto také narůstá zájem o odborníky na kybernetickou bezpečnost i kvalitní absolventy takto zaměřených studijních programů. S tréninkovou arénou v Česku začal 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 i skuteční hackeři. „Samozřejmě jsme jim trochu trnem v oku a útoky na nás zkoušejí. Nemají to ale snadné, zatím jsme se ubránili."

Lukáš Seidl

Kybernetické útoky

- **NAPADENÝ ZAORÁLEK** – na české ministerstvo zahraničí prý útočí hackeři 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 citlivých osobních dat ukradli hackeři technologické firmě Yahoo!. O útoku, k němuž došlo v roce 2013, informovala společnost loni.
- **UKRAJINSKÝ BLACKOUT** – přes sedm set tisíc obyvatel bez elektřiny, zmatek, chaos. Rozsáhlý výpadek elektrického proudu, který postihl v prosinci 2015 Ukrajinu, byl prý rovněž dílem hackerů. Spekuluje se, že za útokem stálo Rusko.
- **OCHROMENÁ OCELÁRNA** – klasickým příkladem napadení průmyslového podniku je útok na ocelárnu v Německu v roce 2014. Hackeři tehdy získali kontrolu nad jednou z vysokých pecí a znemožnili její vypnutí.
- **ČESKÝ TÝDEN** – začátkem března 2013 měli čeští experti na kybernetickou bezpečnost napilno. Během jediného týdne se hackerům při celkem primitivním DDoS útoku podařilo zahltit tuzemské zpravodajské servery, nejnavštěvovanější domácí vyhledávač, weby bank a internetové stránky mobilních operátorů.