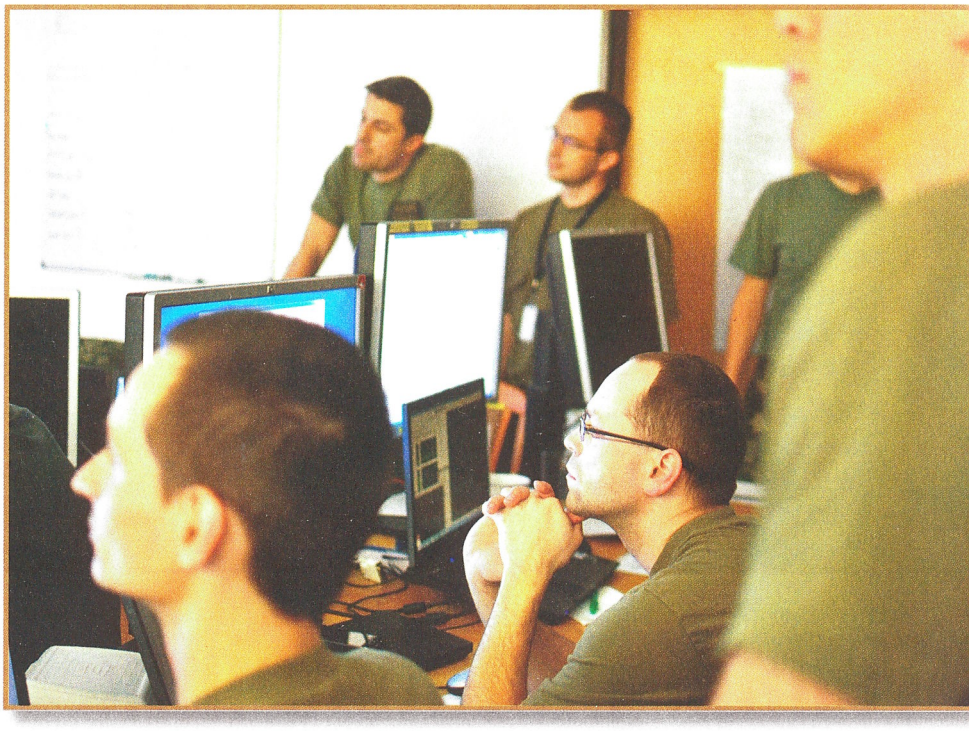
Špeciálne jednotky kybernetického priestoru

/ kpt. Peter GARAJ

Projektor premieta na stenu graf. Pod ním sú v mriežke umiestnené zelené polia. V miestnosti vládne pokoj, všetky hlavy sú sklonené. V rohu miestnosti je na obrazovke trojrozmerný obraz, v ktorom sa mihajú malé lenivé bloky.



Bojové polia boli vždy definované dobou a jej výdobytkami. Prvé „vojny" boli vybojované holými rukami. Potom prišiel niekto s myšlienkou, že kameň v ruke je efektívnejší a môže rozhodnúť o výsledku boja. Neskôr prišli palice, praky, luky a kopije. Potom sa vymysleli meče a brnenia. Ďalším nápadom boli kone. Vznikla jazda. Z lodí vznikli ponorky. Prišli lietadlá a bojové vrtuľníky. Z jazdy vznikli motorizované jednotky, z lietadiel vesmírne stanice. Ďalšie vojnové pole, ktoré ešte niektorí stratégovia neuznávajú, je to digitálne. Nepomôžu na ňom ani rýchle nohy, ani veľké svaly, výkonné motory či hrubý pancier. Pomôže len inteligencia, skúsenosti a prehľad. A je potrebný „nový druh vojaka".

Tak ako existujú civilní a vojenskí lekári, letci, pyrotechnici, policajti, ekonómovia alebo kuchári, tak by sme sa mali zamyslieť aj nad tým, či nie je najvyšší čas začať budovať skupinu, ktorá bude chrániť ozbrojené sily pred kybernetickou hrozbou. „Spojovacie vojsko" už dávno nie je len o spojení, a časy, keď jedinou spojovacou technikou bol poľný telefón, sú dávno preč. Konkurenčné výbery, ktoré u nás fungujú už niekoľko rokov, fungujú aj mimo nášho rezortu, a tak väčšina (či už začínajúcich, alebo tých zabehnutých) odborníkov z nášho rezortu odchádza, prípadne je prepustená. Strácame tak nielen draho vyškolených odborníkov, ale aj naše interné know-how, ktoré sa už nedá nahradiť ani kúpiť. O tom, že žiadny takýto odborník z civilu nad prácou v našom rezorte ani len neuvažuje, netreba hovoriť. O stave našej elity dosť napovedá aj fakt, že na cvičenie sa zvolávali ľudia z celého Slovenska, z rôznych pozícií typu servisný technik, pričom sa počas cvičenia museli zabezpečovať aj akcie typu čestná čata na pohreb...

A tak celá naša kybernetická elita je zložená z pár dobrovoľníkov, ktorí nočné služby, nulové ohodnotenia, priemerné pracovné podmienky a pretrvávajúce nepochopenie zo strany velenia ešte stále nevymenili za vysoký plat, neskutočné benefity, pracovnú pohodu a pokojný rodinný život v súkromnej IT firme.

Tento príbeh je o nich...

Na trojrozmernom obraze sa začne chaoticky pohybovať veľké množstvo blokov a všetky smerujú do jedného miesta. Graf na stene začne prudko stúpať, „niečo sa blíži". Hlavy sa začnú dvíhať a sledujú meniaci sa graf a ďalšie obrazovky. V tichu počuť slová: „šopa je dole."

Spoločnosť Blue 8 je spoločnosť poskytujúca pripojenie a iné internetové služby. Jej IT oddelenie má však momentálne len desať záložných zamestnancov, pretože hlavný tím bude prednášať na konferencii v Afrike o tom, ako spolu s Interpolom vypátrali a zatkli niekoľko internetových aktivistov. Žiaľ, ako to už chodí, títo aktivisti neboli sami a ich priatelia vyhlásili spoločnosti Blue 8 odplatu. Takú kybernetickú.

Cvičenie Locked Shields 2012 bol nápad Centra výnimočnosti pre spoločnú kybernetickú ochranu (ďalej len CCDCOE) sídliaceho v Estónsku. Celý projekt bol pripravovaný niekoľko mesiacov a jeho úlohou bolo pripraviť prostredie, v ktorom by sa dal pozorovať kybernetický útok a aj to, ako sa mu čo najlepšie brániť, ako sa navzájom o ňom informovať a ako si pomáhať.

Celý projekt bol postavený na jednoduchých princípoch. Jedna zlá skupina napádala deväť identických dobrých skupín. Dobré skupiny si navzájom pomáhali a chránili svoje systémy a spoločne jeden veľký, oddelený systém. Celé sa to bodovalo a kto mal na konci najviac bodov, ten vyhral. Jednoduché.

Plusové body boli za to, že veci fungovali, že sa hlásili bezpečnostné incidenty, že sa spolupracovalo s médiami. Mínusové body za to, že veci nefungovali, že sa nevykonávali príkazy „šéfa podniku", prípadne zákazníkov. Mínusové body boli za „hacknutie", či už išlo o defacement (defacement je vizuálna zmena webového sídla obete či už vložením textu, obrázka, alebo niečoho iného, čo viditeľne ukazuje, že daný web bol napadnutý a prelomený), krádeže (krádeže väčšinou zahŕňajú informácie o klientoch, ich kreditných kartách, telefónnych číslach a adresách, prípadne ich prístupové údaje), znefunkčnenie alebo vírusové napadnutie.

Aby si mohol čitateľ urobiť obraz o skórovaní a dôležitosti jednotlivých prvkov cvičenia, povedzme si, že za dostupnosť napríklad webovej stránky bolo približne 10 bodov za hodinu. Defacement bol ohodnotený - 1 200 bodmi. Za nahlásenie bežného incidentu bolo tiež 10 bodov. Za nahlásenie incidentu aj s jeho vyriešením bolo 200 bodov. Za odhalenie špeciálnych útokov bolo 300 bodov.

Čo sa vlastne „strážilo"? Firma Blue 8 mala jednu webovú stránku, jednu osobitnú webovú stránku na hlásenie problémov, online predajňu, webovú poštu, server pre doménový hosting (taký server slúži na vytváranie nových webových sídiel spolu s osobitnou poštou a používateľmi, náš server obsahoval 5 takých kompletných sídiel). K tomu bola interná zóna, kde bolo 5 klientskych pracovných staníc, interná pošta, doménový server a autorizačný server. K tomu si treba prirátať ešte firewally, switch, router, radius server, ipsec a niekoľko ďalších zariadení a serverov.

Každý systém mal v sebe ukrytých niekoľko veľkých (a veľa malých) dier, chýb a zadných dvierok. V kombinácii s nedostatkom personálu celé cvičenie sľubovalo dynamický priebeh. Aby však tento scenár nebol priveľmi zložitý z pohľadu cvičiacich, každý tím mal asi tri dni na zoznámenie s infraštruktúrou. Tieto tri dni boli nato, aby sme si prešli systém, zoznámili sa s topológiou a našli všetky bezpečnostné problémy. Mohli sme si skúsiť aj ich opravy, ako aj rekonfiguráciu systémov ako takých. Po troch dňoch sa však všetko vrátilo do stavu, v akom to bolo na začiatku. Počas troch dní sme v plnom nasadení dokázali opraviť odhadom 80 percent bezpečnostných anomálií a zadných dvierok (v angličtine backdoor). Takisto sme sa počas týchto dní zoznámili s nasadenými aplikáciami. Napríklad aplikačný