

balík na doménový hosting bol veľký približne 400 MB a tri dni hľadať v takom množstve informácií nejaké chyby a backdoory je rovako účinné ako hasiť lesný požiar vedrami.

Počas prípravného týždňa sme teda pochopili, že plán „oprav a obraňuj“ možno nebude ideálnym riešením vzhľadom na čas a možnosti. No rozhodli sme sa, že budeme pracovať čo najrýchlejšie a budeme sa usilovať nepustiť útočníkov do našej siete.

### Kybernetický útočník

Červený tím (oficiálne označenie kybernetických útočníkov je red team) pozostával zo štyridsiatich [az na konci cvičenia sme sa dozvedeli, že ich bolo 40 a nie 30] externe naverbovaných pentesterov (pentester je človek živiaci sa odhalovaním zraniteľnosti v oblasti IT praktickými metódami), bezpečnostných analytikov a ďalších ľudí, ktorí majú poznatky z tejto oblasti. CCDCOE týchto ľudí zverbovalo a na vlastné náklady dopravilo do Tallinu, poskytlo ubytovanie a všetko potrebné. Červení boli rozdelení do šiestich skupín, pričom každá bola zameraná na inú oblasť. Nevieme, aké to boli oblasti, no predpokladáme, že to boli oblasti ako aplikačná bezpečnosť, webové zraniteľnosti, systémová bezpečnosť, sociálne útoky a útoky na sieťovú vrstvu. Červený tím mal tú výhodu, že podľa neho sa odvial celý dej cvičenia. Použila sa taktika White Box Approach, čo znamená, že červený tím vedel presne a do detailov, na čo útočí, ako je siet poprepájaná a čo sa na ktorom serveri nachádza. A ak červený tím nemal dostatočný úspech, dostał pomoc v podobe informácií o tom, kde by mala byť siet zraniteľnejšia, kde sa nachádzajú niejaké ďalšie skryté zraniteľnosti. Treba uznáť, že červený tím bol naozaj dobrý a do 10 minút od prvého útoku mali všetky tímy „defacnúté“ webové stránky. Hovorilo sa, že len dva tímy boli v obrane svojej stránky lepšie a ich prelomenie trvalo o päť minút dlhšie.

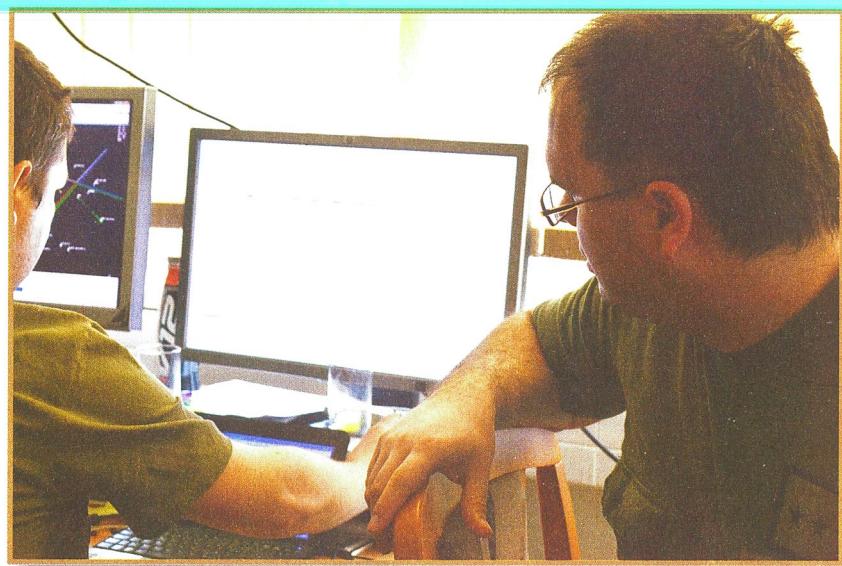
Okrem červeného tímu a nás modrých boli na cvičení prítomní aj zelení [v originálni Green Team], ktorí sa starali o to, aby technika a vlastne všetko fungovalo tak, ako malo, bieli [v originále White Team], ktorí sa starali o riadenie celého cvičenia a zároveň o simulovanie klientov na pracovných staniciach, žltí [v origináli Yellow Team], ktorí vyberali úlohy a starali sa o analýzu a dokumentovali celý priebeh cvičenia a legal tím [v origináli Legal Team], ktorý trénoval komunikáciu v otázkach právneho charakteru, ktoré počas cvičenia nastali.

Celé cvičenie bolo koordinované z Estónska, ktoré je v inom časovom pásme, a tak si nás tím musel poradiť aj s tým, že prvý týždeň sme mali posun dve hodiny a po víkendovej prechode Slovenska na letný čas bol posun už len hodinový.

*Graf na stene stagnuje, zelené pole scervená. Všetci sa pozerajú do monitorov, miňajúce sa ruky plnia riadky príkazmi. Pokojná atmosféra je preč. Ticho prerušujú výrazy neznámej terminológie: „Bloknite nieko tú ípēčku na fajervole, je to eskveel indžekt, krádhu nám čísla kreditných kariet.“*

Samotné cvičenie bolo pre nestranného pozorovateľa zdánlive nudné: celý nás tím bol sústredený v jednej miestnosti ZaSKIS-u (Základňa Stacionárnych Komunikačných Informačných Systémov) a okrem množstva techniky a občasných výkrovov prekvapenia a zlosti sa zdánlive nič nedialo. Nás tím však počas dvoch dní odrazil asi 100 útokov, vytvoril pár obranných nástrojov pre ďalšie tímy, niektoré služby celé preinštaloval, niektoré presunul. Zároveň bránil svojich interných klientov pred vírusmi a iným škodlivým softvériom z internetu. Cvičenie nemalo prestávky, takže počas dňa sa z miestnosti vychádzalo len zriedkavo, pretože každý člen tímu bol trvale potrebný a počas celého cvičenia neboli čas na oddych. Stále bolo čo riešiť, stále bolo nad čím premýšľať, stále bolo čo brániť. Pri takomto výtažení nie je prekvapením, že členovia tímu boli po každom dni unavení rovnako ako pri náročnom celodenneom polnom cvičení.

Tažko sa hodnoti výsledok. Na jednej strane bolo počas prvého dňa viditeľné, že červený tím mal prevahu a využíval najdené chyby v serveroch rýchlo, efektívne a perzis-



tentne. Napríklad jeden napadnutý server menil heslo pre administrátora každú minútu na prázdnne, pričom odhaliť a zastaviť to bolo celkom náročné. Na sklonku prvého dňa bola väčšina serverov v dezoliatnom stave a niektoré s nich museli byť obnovené zo záloh (ďalej minulosové body). Taktika, ktorú sme si vytýčili, potrebovala na konci prvého dňa drobné zmeny, ale inak sme postupovali podľa jasného a jednoduchého plánu: oprav a ochraňuj. Druhý deň už táto taktika začala prinášať svoje výhody a červený tím mal omnoho menej úspešných akcií.

Celé cvičenie bolo dôležité najmä pre skúsenosti, ktoré inak nemôžeme získať. Testovací priekopnik do rezortnej siete je vec nereálna a nechcená. Pri cvičení však môžeme „škodcov“ nechať preniknúť do siete a sledovať, ako sa ich vplyv v sieti rozrástá, čo im spôsobuje problémy, a naopak, čo im pomáha. Už teraz sú zozbierané tzv. Lesson Learned (z anglického: naučené lekcie), kde participanti na cvičení riešia, čo sa naučili, čo im spôsobovalo tažkosť a čo, naopak, bol dobrý nápad uvedený do praxe. Kedže momentálne nemáme vybudované žiadne ucelené postupy na riešenie podobných incidentov, toto cvičenie by mohlo byť základným kameňom pre budúci CERT (Computer Emergency Response Team) Ozbrojených síl Slovenskej republiky.

Takže ak si to celé zhrieme: na pôde ZaSKIS-u sa stretli naši najlepší, týždeň sa pripravovali na toto rozsiahle a komplexné cvičenie, dva dni nevychádzali z miestnosti (prestávka na obed neprichádzala do úvahy) a každý deň minimálne sedem hodín bez prestávky bojovali s kyber-

netickou hrozobou. Popri tom riešili spoluprácu s ostatnými tímmi, riešili spoluprácu s nadnárodným strediskom CERT (Computer Emergency Response Team), radili sa s právnikmi, aké môžu podniknúť kroky a či sú správne po legislatívnej stránke, dávali tlačové vyhlásenia a odpovedali na telefonáty novinárov, riešili nespokojných zákazníkov, ako aj uzatvárali a plnili nové kontrakty a vysvetlovali fiktívnu šéfovi Blue B, prečo mu nejde pošta. To, že sme skončili na druhom mieste, odzrkadluje dobrú timovú prácu, nadpriemerné vedomosti o problematike, no najmä dlhorčnú a nezistnú obetavosť všetkých zúčastnených. Reprezentovali nás ZaSKIS, ale aj ozbrojené sily ako celok a Slovensko ako krajinu, ktorá v oblasti informačnej bezpečnosti rozhodne nezaostáva za svetovou špičkou. A za to im patrí naša vďaka a úcta.

*Trojrozmerný obraz sa upokojí, graf na stene poklesne. Červené pole ostáva červené. „Prečo nejde šopa? Ako ju rozhasili? Ja tam dám mod sekurity.“ Jeden člen tímu začne klepať do klávesnice, ďalší dvaja mu asistujú zo svojich pracovísk. „Ide ďalší útok“, hľasi analyticki sledujúci trojrozmernú mapu siete a zainteresovaní sa opäť pustia do svojich klávesnic...*

