V čem spočívají kybernetická cvičení?

Několik kybernetických cvičení se stalo součástí každoročního plánu především pro národní, vládní anebo armádní týmy. Každé cvičení má však jinou cílovou skupinu, odlišné cíle a je jiným způsobem koncipované.

ZUZANA DURAČINSKÁ

Národní tým CSIRT.CZ se účastní pravidelně různých kybernetických cvičení. Nejvíce pozornosti však soustředí na cvičení Cyber Europe pořádané jednou za dva roky Evropskou agenturou pro síťovou a informační bezpečnost (ENISA), a to hned ze dvou důvodů.

Je to totiž zaprvé jediné cvičení určené pro veřejnou i soukromou sféru a jeho cílem je posílení spolupráce mezi nimi. A za druhé, CSIRT.CZ je jeho koordinátorem za Českou republiku.

Jak vlastně vypadají taková cvičení? Pojďme si jejich průběh nastínit díky letošnímu Cyber Europe 2016.

Přípravy a koordinace

ENISA letos pořádala již čtvrtý běh tohoto mezinárodního cvičení, které je určeno pro všechny členské státy Evropské unie a krajiny EFTA a jeho hlavní část trvá zpravidla dva dny.

V uplynulých letech se na plánování scénáře a úkolů do značné míry podíleli také zástupci jednotlivých států. S narůstáním komplexnosti cvičení a počtu hráčů se však celé přípravy ujala samotná ENISA.

Jejím cílem bylo připravit cvičení, které splní následující:

1. Musí být dostatečně univerzální, aby bylo vhodné pro všechny státy (bez ohledu na jejich velikost, právní úpravu, uspořádání oficiálních CSIRT týmů apod.);
2. Musí být zajímavé jak pro bezpečnostní týmy řízené státem, tak pro CSIRT týmy internetových providerů a různých soukromých společností;
3. Jeho scénář musí být připraven vždy tak, že při řešení úkolů je v určitém momentu nutná spolupráce mezi týmy na národní úrovni, tj. mezi hrajícími týmy v jednom státu a pak později taky mezi jed-

Průběh cvičení Cyber Europe v centrále cvičení.

notlivými státy navzájem. Například každý stát získá analýzou malwaru určitou část klíče potřebného pro jeho deaktivaci.

4. Všechny jeho úkoly musejí být propojené jedním scénářem. Například může jít o hromadné útoky na zásobárny pitné vody, které začnou sociálním inženýrstvím na zaměstnance, jsou doprovázeny DDoS útoky, část zařízení je napadena malwarem, je nutná analýza logů ze serveru dané zásobárny nebo analýza malwaru.

5. Úkoly musejí být rozplánované tak, aby všichni hráči byli naplno zaneprázdněni během dvou dnů, úkoly je bavily a zároveň jim dávaly smysl jak po technické, tak po logické stránce věci.

Skloubit všechny tyto věci a zajistit, aby všichni obdrželi během cvičení úkoly ve správném čase, je skutečně náročné jak operačně, tak technicky. Letošního ročníku se účastnilo přes 300 různých organizací od provozovatelů cloudových řešení po ministerstva, přičemž během dvou dní bylo zasláno přes 4 000 podnětů k řešení.

Ty na sebe musejí navazovat, a je proto nutné, aby byly zasílány v přesně stanoveném logickém pořadí. Aby se ENISA dokázala předem domluvit se všemi hráči, je v každém státě určen jeden koordinátor, který hráče na cvičení připraví.

Zároveň pokud se během cvičení stane, že se náhodou některý z hráčů na úkolu zdrží, může mu koordinátor, který často plní také úlohu moderátora, trochu napomoct. Vzhledem k tomu, že hlavní část cvičení trvá jenom dva dny, všechno musí jít hladce a tomu předchází měsíce příprav. Takto tedy vnímají celý běh cvičení jeho plánovači a koordinátoři.

Úloha hráčů

Hráč má před cvičením jenom pár jednoduchých úkolů, které by měly zajistit, aby vše v daný den probíhalo hladce. Konkrétně ve cvičení Cyber Europe si musí ověřit, zda má správný přístup do systému, pročíst si pravidla, zajistit, že e-mailový server neblokuje příchozí podněty, a zorganizovat si kolem sebe dobrý tým.

Aby mělo cvičení dopad na všechny typy organizací, jsou definovány různé druhy týmů, například CSIRT tým, tým poskytovatele cloudových služeb nebo tým poskytovatele internetového připojení. Každý si předem vybere, za koho bude „hrát“, a podle toho mu jsou pak zasílány úkoly na řešení.

Většinou cvičení začíná sérií novinových článků, aby byl hráč uveden do aktuální situace. Může jít například o schválení sporné legislativy nebo podepsání spojenectví s fiktivním státem. Vzhledem k tomu, že jde o evropské cvičení, vždy je to situace, která nějakým způsobem ovlivňuje všechny státy.

To ale na začátku cvičení nemusí být úplně zřejmé a jen postupně se hráči dozvídají více z úkolů, na kterých pracují. Úlohy, které hráči řeší, jsou hlavně technické a operační. Například zatímco se jeden tým věnuje analýze malwaru, poskytovatel internetu řeší analýzu provozu, zaměstnancům CSIRT týmu se přes úspěšné sociální inženýrství dostal do sítě malware a musejí zjistit z poskytnutých logů, kam všude se dostal.

Za každým hráčem (např. ISP) by měli být minimálně dva lidé, kteří si rozdělí dílčí úkony. Pokud jeden pracuje na technické analýze, druhý sepisuje report, který již od něho vyžaduje „ředitel“ jejich společnosti, dále musejí připravovat odpovědi na otázky od „novinářů“, protože do tisku unikly informace o útoku na jejich společnost, k tomu všemu potom komunikují s ostatními hráči.

Na hráče je také cíleně vyvíjen nátlak, aby se situace co nejvíce přiblížila realitě, při níž je na společnosti veden útok. Nepsaným heslem cvičení je „Nebojujte se scénářem“. Hráči se musejí od vlastní práce trochu odpoutat a skutečně se vžít do role fiktivní organizace, za kterou hrají.

K čemu je to dobré?

Hlavním smyslem kybernetického cvičení je lépe poznat ostatní partnery v oblasti kybernetické bezpečnosti a vyzkoušet si řešení nových a neobvyklých úkolů. Organizaci, která se do cvičení zapojí, to stojí čas dvou až tří lidí na dva a půl dne i s přípravou. Je ale jasné, že jde o velice dobrou investici, která týmy naučí výborně spolupracovat. ■

Autorka pracuje jako bezpečnostní analytička sdružení CZ.NIC, které provozuje Národní bezpečnostní tým CSIRT.CZ.