Jak probíhá kybernetické cvičení?

Zuzana Duračinská

Kybernetické cvičení je poměrně nový fenomén, které se v ICT bezpečnosti stále výrazněji profiluje. Cílem takového cvičení je poskytnout týmům a bezpečnostním specialistům prostor pro zlepšení schopností a natrénování reakcí v reálných situacích, které mohou během více či méně sofistikovaného útoku nastat.

Organizace a příprava takového cvičení, které nemají vžité ani hráči ani plánovací týmy, je o mnoho náročnější než se může zdát. Proto se o to už počtvrté postarala Evropská agentura pro síťovou a informační bezpečnost (ENISA). Jak už její název napovídá, jde o evropskou agenturu, která na vládní, národní, akademické i soukromé úrovni koordinuje část bezpečnostních aktivit. Úlohou ENISA bylo v roce 2014 naplánovat cvičení, které prověří schopnost reakce a technickou i strategickou připravenost jednotlivých týmů. Cvičení s příznačným názvem Cyber Europe 2014 je tak zatím nejrozsáhlejším a nejkomplexnějším kybernetickým cvičením, které se kdy v Evropě odehrálo.

Důležité jsou zkušenosti

Je nutné poznamenat, že nic podobného by se nemohlo naplánovat bez předešlých zkušeností, které hráči a hlavní plánovači (ENISA) nabyli za poslední roky. Při prvních ročnících se identifikovaly problémy s hledáním kontaktů v případě útoku, neaktuálními kontakty či neschopností iniciovat šifrovanou komunikaci. Po odstranění těchto a dalších problémů identifikovaných cvičením se celá bezpečnostní komunita posunula dál a dnes můžeme říct, že letošní trojfázové cvičení má úspěšně za sebou první, technickou fázi. Nutno poznamenat, že úspěšnou také pro Českou republiku, jejíž týmy vedly ve finálním hodnocení poměrně složitých technických úloh.

Každý tým měl 48 hodin na to, aby správně vyřešil co nejvíce úloh. A protože se jednalo o technickou část, jednalo se například o analýzu malwaru, forenzní analýzu, identifikaci botnetu, analýzu síťového provozu skrze IPv6 a podobně. Každý tým si mohl ve stanoveném čase vybrat, které úlohy bude řešit, přičemž jim v tom pomáhal i indikátor náročnosti. Po „převzetí“ úlohy v systému speciálně navrženém pro potřeby kybernetického cvičení se hráčům vygeneroval soubor otázek, jejichž správné zodpovězení sloužilo jako indikátor správnosti řešení. Otázky, za jejichž zodpovězení byly týmy hodnoceny, si můžete představit jako základní informace, které při řešení incidentu obvykle potřebujete vědět. V případě malwaru v pracovní stanici by to byl například způsob, jak se škodlivý kód do stanice dostal, kde se uložil, kam se připojuje, jaké informace odesílá a podobně.

I v bezpečnosti lze soutěžit

Dosažený počet bodů mohl tým porovnat s ostatními evropskými týmy, které se rozhodly zveřejnit svůj výsledek. Zájem získat co nejvyšší počet bodů sloužil jako motivace a vnesl do této fáze cvičení prvek zdravé soutěživosti. Nejenže se tak české týmy mohly porovnávat mezi sebou, ale mohly soutěžit i se zbytkem Evropy, protože ve stejném čase cvičilo přibližně 800 bezpečnostních expertů. Počet bodů je však jen orientačním ukazatelem úspěšnosti, protože každý tým si mohl dovolit uvolnit jen určitý počet hráčů.

Složení týmů bylo v České republice skutečně pestré a mělo zástupce z veřejného, soukromého i akademického prostředí. Týmy o minimálně dvou lidech se podařilo poskládat samotnému koordinátorovi cvičení, národního týmu CSIRT.CZ, sdružení CESNET, peeringovému uzlu NIX.CZ, společnosti Active24, vládnímu CERTu, akademickému CSIRT-MU, Policejní akademii České republiky v Praze a společnosti Unicorn. Nejen, že se týmy navzájem poznaly, ale mohly si také na samostatném společném setkání vyměnit zkušenosti se správným řešením úkolů a použitými nástroji. Vytvořený komunikační kanál také pomohl vzájemné komunikaci, přičemž společná chatovací místnost se ujala jako nejlepší způsob rychlé komunikace při řešení akutních záležitostí. Pro české bezpečnostní týmy tak byla technická část cvičení Cyber Europe 2014 nejen možností vyzkoušet si technické výzvy, ale i příležitostí pro prohloubení vztahů či seznámení se s ostatními bezpečnostními analytiky.

Další část cvičení proběhne v říjnu 2014

Koncem října čeká týmy další, operační část. Ta bude zaměřena na procvičení reakcí na incidenty, komunikaci s jinými týmy a médii či postupy při eskalaci incidentu. V této fázi cvičení, která naváže na scénář z technické části, si mohou procvičit krizový management především více manažersky orientovaní členové týmů. V poslední strategické fázi už půjde o cvičení na nejvyšší rozhodovací úrovni. Všechny tři fáze jsou propojeny jedním scénářem, který je namodelovaný na kybernetickou bezpečnostní krizi napříč Evropou.

Bezpečnostní hrozby se dnes objevují stále častěji a právě cvičení pomáhají týmům připravit se na konkrétní úlohy. Často se stává, že si lidé myslí, že danou situaci by v případě potřeby dokázali vyřešit, ale všechny cvičení zatím odhalily i mnoho slabých stránek a nedostatků, které by se mohly objevit v případě krize. A to už by mohlo být pozdě. ■

CSIRT.CZ
powered by CZ.NIC

Autorka je bezpečnostní analytičkou sdružení CZ.NIC, které provozuje Národní bezpečnostní tým CSIRT.CZ.