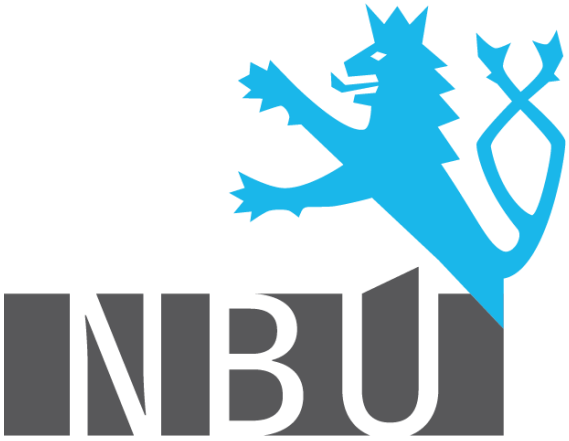
NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

Národní centrum kybernetické bezpečnosti



CYBER CZECH 2014

Zpráva o národním cvičení v oblasti kybernetické bezpečnosti

Dne 6. října 2014 uspořádal Národní bezpečnostní úřad (dále NBÚ) prostřednictvím Národního centra kybernetické bezpečnosti (dále NCKB) první národní cvičení v oblasti kybernetické bezpečnosti **CYBER CZECH 2014**. Jednalo se o „netechnické“ cvičení, které proběhlo formou skupinové diskuze neboli table-topu. Primárním cílem cvičení bylo procvičit schopnosti spolupráce při zvládání kybernetických bezpečnostních incidentů a zároveň ověřit komunikační kanály, které se při řešení používají.

Celodenní národní cvičení probíhalo v prostorách NBÚ. Zúčastnili se ho zástupci ministerstev s výjimkou Ministerstva zemědělství, zdravotnictví, místního rozvoje a kultury. Dále byli přítomni zástupci z České národní banky, Českého telekomunikačního úřadu, Úřadu pro ochranu osobních údajů NBÚ. Skupina cvičících byla složena z bezpečnostních ředitelů a zaměstnanců odpovědných za bezpečnost informačních technologií, tzn. manažerů bezpečnosti informačních technologií či manažerů informačních technologií. Cvičící byli rozděleni do čtyř čtyřčlenných týmů, v rámci kterých společně řešili zadané úkoly. Následně své návrhy řešení představili ostatním cvičícím i porotcům.

Skupinu cvičících doplňovala dvanáctičlenná odborná porota složená ze zástupce národního bezpečnostního týmu CSIRT.CZ, akademického týmu Masarykovy univerzity CSIRT-MU, poskytovatele internetových služeb ACTIVE 24, nejvyššího státního zastupitelství, Policejního prezidia, Vojenského zpravodajství, Úřadu pro zahraniční styky a informace, Bezpečnostní informační služby, odborníka na právo informačních a komunikačních technologií, tiskového mluvčího NBÚ a odborníka z Odboru právního a legislativního z NBÚ. Úkolem poroty bylo hodnotit a doplňovat návrhy a odpovědi cvičících.

Hostem národního cvičení byl policejní prezident brig. gen. Mgr. Bc. Tomáš Tuhý.

Cvičení bylo implementováno do prostředí fiktivního Ministerstva kybernetických záležitostí České republiky. Všichni cvičící zastávali roli bezpečnostního ředitele, jež je nejvyšší osobou zodpovědnou za bezpečnost informační sítě zmíněného ministerstva. V rámci simulovaných scénářů se museli bezpečnostní ředitelé potýkat s dvěma hrozbami – DDoS útokem a phishingovou zprávou.

V prvním scénáři šlo o procvičení reakce bezpečnostního ředitele na probíhající DDoS útoky. Ty způsobovaly několikahodinové výpadky na webových stránkách ministerstva. Vzhledem k finančním ztrátám i k možné ztrátě důvěry ze strany občanů byly útoky označené jako vážné. Úkolem cvičících bylo analyzovat tyto útoky a následně rozhodnout, jak je vyřešit a koho případně kontaktovat. Postupem času se intenzita útoků stupňovala. Navíc se objevily spekulace, že útok na klíčový orgán státní správy byl jen zastíracím manévrem možné ztráty dat. Ohroženy byly citlivé údaje týkající se výčtu subjektů kritické informační infrastruktury a významných informačních systémů, jež obsahovaly technické parametry a stupeň kritičnosti pro stát.

Později se výpadky začaly objevovat nejen na koncových sítích, ale také na straně poskytovatelů internetových služeb. Součástí scénáře bylo také představení projektu Fénix (bezpečná VLAN), který si dává za cíl umožnit v případě DDoS útoku dostupnost internetových služeb v rámci subjektů zapojených do této aktivity.

Obsahem druhého scénáře byl probíhající phishingový útok doručený zaměstnancům fiktivního Ministerstva kybernetických záležitostí České republiky. Závažnost e-mailu spočívala v tom, že vypadal jako by jej odeslalo personální oddělení daného ministerstva. E-mail obsahoval informace o ukládání části výplaty na důchodové pojištění s velmi výhodnou státní podporou. Jeho součástí byl odkaz na stránku, která věrně imitovala stránky interní sítě ministerstva. Na tuto zprávu zareagovalo několik desítek zaměstnanců, kteří na phishingové stránce vyplnili své přihlašovací údaje do interního systému. Brzy bylo zřejmé, že útok byl cílený a několik desítek uživatelských účtů, včetně jednoho s privilegovaným oprávněním, bylo kompromitováno. Na základě toho se museli cvičící rozhodnout, zda situaci zvládnou sami nebo zda budou někoho informovat. Součástí scénáře byl také malware využívající zero-day zranitelnost. Ten pachatelům zajistil přístup k citlivým osobním údajům některých i vysoce postavených zaměstnanců.

Cvičení CYBER CZECH 2014 bylo samotnými cvičícími i odbornou porotou hodnoceno kladně. Všichni zúčastnění se aktivně zapojovali do plnění úkolů i následných odborných diskuzí. Všechny zadané úkoly se podařilo splnit. Každému z účastníků cvičení byl odeslán dotazník a na jeho základě bylo možné určit silné i slabé stránky.

Za silné stránky cvičení lze považovat přítomnost velkého množství erudovaných odborníků, s kterými vedli cvičící obsáhlé diskuze. Další silnou stránkou je reálnost zvolených scénářů, struktura a záběr řešených úkolů, podnětné brainstormingové prostředí, příjemná a přátelská atmosféra, bezprostřednost reakcí odborné poroty a načasování cvičení s ohledem na zavedení nového zákona č. 181/2014 Sb., o kybernetické bezpečnosti. V neposlední řadě lze jako výhodu zmínit navazování kontaktů a prohloubení důvěry ze strany cvičících, odborné poroty i NCKB.

Slabou stránkou cvičení bylo nedodržení časového harmonogramu, únava a nesoustředěnost některých cvičících. S ohledem na časovou a pracovní vytíženost některých účastníků je doporučováno plánovat společná setkání a informovat o nich s větším předstihem. Jako další doporučení do příštích let je nastavení užších mantinelů scénářů a zaměření na již řešené incidenty.

Ze strany cvičících byla vznesena prosba o sepsání obecně platných bezpečnostních doporučení, která jsou součástí Vyhodnocení národního cvičení. Někteří cvičící nás prostřednictvím dotazníků, které jim byly zaslány elektronickou formou po skončení cvičení, informovali o tom, že poznatky ze cvičení reflektovali do svých již zavedených

bezpečnostních politik a že by se také rádi zúčastnili dalšího ročníku. Díky tomu se potvrdila úspěšnost a užitečnost národního cvičení. Do přípravy příštího ročníku promítneme poznatky a zkušenosti z toho letošního tak, aby se zvýšila jeho profesionální úroveň a bylo dosaženo ještě lepších výsledků.