



Tisková zpráva

16. 1. 2020

Nemocnice Na Homolce, Roentgenova 2, 150 30 Praha 5
<http://www.homolka.cz>

Homolka hostila celorepublikový workshop k ochraně zdravotnických zařízení před kybernetickými útoky

Do Nemocnice Na Homolce se dnes sjelo více než 250 zástupců zdravotnických zařízení z celé České republiky na workshop věnovaný poučení z kybernetického útoku na benešovskou nemocnici, který ve spolupráci s Ministerstvem zdravotnictví, Nemocnicí Rudolfa a Stefanie Benešov a Spolkem pro ochranu osobních údajů uspořádali IT odborníci z Nemocnice Na Homolce. Účast na akci přijali i zástupci Národního úřadu pro kybernetickou a informační bezpečnost, Úřadu pro ochranu osobních údajů a sekce kyberkriminality Národní centrály proti organizovanému zločinu Policie ČR.

„Kyberútoky nelze bohužel v budoucnu plně vyloučit, a proto je nutné dělat maximum, abychom případné hrozby maximálně eliminovali. Věřím, že díky dnešnímu workshopu pro nemocnice dojde k dalšímu rozvoji povědomí o kybernetické bezpečnosti, rizicích a vhodných strategiích, jak předcházet incidentům podobným tomu v benešovské nemocnici,“ uvedl ministr Adam Vojtěch.

Incident v benešovské nemocnici potvrdil, že postupný a stále intenzivnější průnik informačních technologií do oblasti zdravotnictví staví poskytovatele zdravotních služeb do role velice atraktivního cíle kyberútku a že Česká republika nezůstane stranou tohoto globálního trendu. Ochota a schopnost včasného sdílení zkušeností, poučení se z možných chyb a potvrzení si správné praxe je proto důležitým předpokladem pro posílení obranyschopnosti vůči kybernetickým hrozbám, a to nejen v sektoru zdravotnictví.

„Věřím, že nejen pověřenci pro ochranu osobních údajů, manažeři kybernetické bezpečnosti, vedoucí IT oddělení ale i zástupci managementu zdravotnických zařízení z celé ČR získali na workshopu důležité a praktické zkušenosti a hlavně poučení z benešovského kyberútku,“ uvedl iniciátor akce Dušan Chvojka, náměstek pro informační technologie Nemocnice Na Homolce.

Podle Adama Kučínského, ředitele odboru regulace NÚKIB, mezi nejčastější nedostatky patří kromě technických nedostatků (jako je slabá segmentace sítě, neošetřené zranitelnosti, neaktuální software, vystavování služeb do internetu bez reálného důvodu) také manažerská pochybení, například nedodržování pravidel minimálního přístupu k systému či ovlivňování bezpečnosti provozem či managementem, nedostatečné nebo žádné proškolení uživatelů, jak se chovat v prostředí internetu, a nedostatečný monitoring toho, co se v síti děje. Jako nejčastější cesty útočníků v těchto případech

byly označeny phishingový (podvržený) e-mail, veřejně dostupné služby z internetu, neautorizovaný přístup umožněný technickými nedostatky (např. nezabezpečenou wifi) a osobní zařízení připojovaná do sítě, která nejsou pod kontrolou organizace (mobily, notebooky).

Poučení z kyberútoku na benešovskou nemocnici, které zaznělo na workshopu: Dostatečně silná ochrana před kybernetickými útoky vyžaduje know-how, finanční prostředky a jednotnou koncepci architektury pro boj proti možným kybernetickým útokům. Je potřeba zřídit systém včasného varování všech nemocnic a nastavit spolupráci s NUKIB i dalšími institucemi zabývající se kybernetickou ochranou. Musí být nastaven systém jednotného vzdělávání pracovníků ve zdravotnictví v oblasti kybernetické hygieny a zavedena důsledná ochrana koncových uživatelů ICT, administrátorů s privilegovanými účty a všech medicínských zařízení. Je třeba zajistit kontinuální několikaúrovňové zálohování a nastavit promyšlené segmentování sítě.

Kontakt na tiskovou mluvčí Nemocnice Na Homolce:

Mgr. Martina Dostálová

tel.: +420 257 273 056

mobil: +420 724 083 906

e-mail: martina.dostalova@homolka.cz