Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č. j.: 1009/2018-NÚKIB-E/210

Brno 11. května 2018

Počet listů: 1

Přílohy: nejsou

Odpověď k žádosti o poskytnutí informací podle zákona č. 106/1999 Sb.

Vážený pane,

k Vaší žádosti o poskytnutí informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů Vám tímto podáváme odpovědi na Vaše dotazy přeformulované níže.

1. K otázce, jakým způsobem Česká republika řeší problémy kybernetické průmyslové špionáže a zda je součástí strategie s konkrétními opatřeními, sdělujeme následující.

Česká republika řeší problém kybernetické průmyslové špionáže komplexně, spolu s dalšími zásadními kybernetickými hrozbami, které mohou narušovat či ohrožovat systémy, sítě nebo služby mající podstatný význam pro fungování státu nebo informační společnosti – viz povinné orgány či osoby podle ustanovení § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů ve vztahu ke KII, VIS, PZS, PDS. Povinné orgány/osoby musí s ohledem na znění ZKB a případně dalších přiléhavých právních předpisů zavádět a vykonávat řadu bezpečnostních opatření směřujících k zajištění své kybernetické bezpečnosti (a to nejen ve vztahu k hrozbě kybernetické průmyslové špionáže). Jinými slovy řečeno, povinné orgány či osoby jsou sami individuálně zodpovědné za bezpečnost svých systémů, přičemž Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) jim k tomu poskytuje pomoc a metodickou podporu, avšak zároveň u těchto subjektů provádí audity, resp. kontrolu souladu zavedených opatření s právními předpisy dotýkajícími se kybernetické bezpečnosti. Jde zejména o provádění analýzy a řízení rizik, bezpečnostní politiku, organizační bezpečnost, stanovení bezpečnostních požadavků pro dodavatele, bezpečnost lidských zdrojů a podobně. Pokud tedy tyto subjekty zodpovědně dodržují předmětná ustanovení dotýkající se kybernetické bezpečnosti, riziko kybernetické průmyslové špionáže by mělo být minimalizováno.

2. K dotazu, s jakými zeměmi Česká republika sdílí informace o kybernetických hrozbách, v jaké intenzitě a jací jsou největší partneři České republiky v předmětné oblasti, uvádíme následující.

V rámci kybernetické bezpečnosti má Česká republika celkem tři významné strategické partnery, se kterými navázala užší formu spolupráce a intenzivnější sdílení informací – jsou jimi Spojené státy americké, Korejská republika a Izrael. NÚKIB a jeho pracoviště vládní CERT – GovCERT.CZ (jakožto řádný člen globální CERT/CSIRT komunity) pak sdílí či může sdílet informace o kybernetických hrozbách dle potřeby a nutnosti s téměř všemi státy světa.

Podrobnější údaje týkající se mezinárodní spolupráce České republiky při sdílení informací o kybernetických hrozbách, lze dohledat ve zprávě o stavu kybernetické bezpečnosti České republiky za rok 2016 zpracované Národním bezpečnostním úřadem (dále jen „NBÚ“), Národním centrem kybernetické bezpečnosti (dále jen „NCKB“) – viz https://nukib.cz/download/Zpravy-KB-vCR/Zpr%C3%A1va-stavu-KB-2016.pdf.

3. K otázce, kde má Česká republika vyslané zástupce pro kybernetickou bezpečnost v zahraničních a mezinárodních institucích a jak se zapojuje do aktivit talinského Centra excelence, lze uvést následující.

Česká republika má v současné době vyslány dva cyber attaché – ve Washingtonu a v Bruselu (při EU a NATO). V druhé polovině letošního roku by mělo dojít k opětovnému dosazení třetího cyber attaché v Tel Avivu (v současné době je tato pozice neobsazena). Další stálý pracovník (právní poradce) je při Cooperative Cyber Defence Centre of Excellence (dále jen „CCDCoE“) v Tallinnu, kam byl vyslán ještě v rámci NBÚ a kde jako tzv. voluntary national contribution publikuje analýzy, podílí se na přípravě kybernetických cvičení a organizaci konferencí pořádaných CCDCoE.

V CCDCoE je Česká republika aktivní již čtvrtým rokem, kde se podílí na činnosti zaměřené především na výzkumnou a vědeckou činnost v oblasti kybernetické bezpečnosti a obrany, je zároveň členem řídícího výboru (Steering Committee) CCDCoE. Samotní pracovníci NÚKIB se účastní řady školení a kybernetických cvičení, které CCDCoE organizuje (v této souvislosti je možno zmínit, že cvičení Locked Shield při CCDCoE tým NÚKIB v loňském roce vyhrál, letos pak byl na třetím místě).

Podrobnější údaje týkající se účasti zástupců České republiky pro kybernetickou bezpečnost v zahraničních a mezinárodních institucích, potažmo v CCDCoE, je možné nalézt ve zprávě o stavu kybernetické bezpečnosti České republiky za rok 2016 zpracované NBÚ, NCKB – viz https://nukib.cz/download/Zpravy-KB-vCR/Zpr%C3%A1va-stavu-KB-2016.pdf.

S pozdravem

Mgr. Pavel Král
ředitel odboru právního