Zástupci NÚKIB sdíleli zkušenosti s bojem proti ransomware na summitu Bílého domu ve Washingtonu

4.10.2024 - | Národní úřad pro kybernetickou a informační bezpečnost

V rámci Summitu zástupci na vysoké úrovni celkem 68 států a organizací, vč. např. Interpolu, diskutovali o nárůstu ransomwarových útoků proti strategickým institucím a subjektům, o posílení sdílení informací nebo o aktivním narušování činnosti ransomwarových skupin. Summit byl zároveň příležitostí pro diskusi o dalších strategických tématech jako například využívání umělé inteligence v boji s kybernetickými hrozbami, posilování odolnosti a bezpečnosti dodavatelského řetězce v oblasti energetiky nebo budování kapacit kybernetické bezpečnosti jako součásti kybernetické diplomacie.

Během čtyřdenního summitu, který organizoval Bílý dům, zástupci NÚKIB upozornili na nárůst sofistikovanosti ransomwarových útoků proti strategickým institucím a subjektům v ČR, což potvrzuje i již dříve zveřejněná Zpráva o stavu kybernetické bezpečnosti ČR za rok 2023. Zároveň představili dosavadní spolupráci v rámci mezirezortní pracovní skupiny pro boj s ransomware, kterou NÚKIB spolu s Národní centrálou proti terorismu, extremismu a kybernetické kriminalitě (NCTEKK) Police ČR založil v lednu 2024.

Během uplynulého roku se ČR, zejména prostřednictvím NÚKIB, zapojila do řady projektů a aktivit v rámci tzv. International Counter Ransomware Task Force, kterou vede Austrálie. Zástupci NÚKIB se rovněž účastnili mezinárodního table-top cvičení proti ransomware, které organizoval Singapur ve spolupráci s Velkou Británií v červnu 2024.

„Úzká spolupráce se zahraničními partnery je klíčová pro úspěšné čelení ransomware, což se potvrdilo v letošním roce, kdy jsme díky varování ze strany našich amerických partnerů byli schopni ochránit před ransomwarovým útokem jeden ze subjektů v ČR. Díky včasnému sdílení informací a operativní spolupráci s naším CERT jsme mohli potenciální oběť informovat dříve, než k němu mohlo dojít,“ sdělil náměstek ředitele NÚKIB Pavel Štěpáník, který se v rámci summitu setkal i s řadou dalších zahraničních partnerů a navštívil Centrum kybernetické bezpečnosti Ministerstva obrany USA a centrálu vesmírné agentury NASA.

Letošní summit opět potvrdil, že ransomware zůstává jednou z klíčových hrozeb pro národní bezpečnost, kterým čelí státy napříč kontinenty. Podobně jako v přechozích letech, bylo na Summitu přijato obecné společné prohlášení a zároveň prohlášení vyzývající k odpovědnému chování států v kyberprostoru a využívání všech dostupných nástrojů a prostředků v boji proti ransomware. K oběma prohlášením se připojila i ČR.

V minulém roce bylo na Summitu přijato společné prohlášení proti placení výkupného. Neplatit výkupné NÚKIB doporučuje opakovaně, mj. i ve vydaném doporučení k ransomware, jež bylo aktualizováno v první polovině roku 2023.

Ransomware je druh škodlivého kódu (malware), který zašifrováním zabrání uživateli v přístupu k datům. Ve většině případů poté útočník vyžaduje zaplacení určité částky za jejich obnovení (dešifrování). Motivací pro použití této praktiky je tedy zejména finanční zisk, nicméně existují i případy, kdy útočník data jednoduše zničí a žádné výkupné (angl. ransom) nepožaduje. Čím dál

častější je i hrozba jejich zveřejněním, zejména pak při napadení firem, které uchovávají a zpracovávají data obsahující citlivé informace o zákaznících.

https://nukib.gov.cz/cs/infoservis/aktuality/2171-zastupci-nukib-sdileli-zkusenosti-s-bojem-proti-ransomware-na-summitu-bileho-domu-ve-washingtonu