Vláda schválila Zprávu o stavu kybernetické bezpečnosti ČR za rok 2023

17.7.2024 - | Národní úřad pro kybernetickou a informační bezpečnost

Ze Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2023 vyplývá, že v roce 2023 meziročně narostl celkový počet kybernetických incidentů evidovaných NÚKIB o 80 %. Zatímco v roce 2022 bylo evidováno 146 incidentů, v minulém roce to bylo 262. Za tímto nárůstem stojí opakované vlny DDoS útoků vedených především ruskojazyčnými hacktivistickými skupinami. Nejčastějším původcem těchto útoků byla ruskojazyčná skupina, jejíž kampaně proti českým cílům probíhaly v návaznosti na dění či výroky spojené s konfliktem na Ukrajině i na další významné události. Česká republika zároveň patřila mezi státy Evropy tímto aktérem nejzasaženější.

Z pohledu závažnosti evidovaných incidentů v roce 2023 bylo naopak možné sledovat pozitivní vývoj. Počet méně významných incidentů byl oproti roku 2022 trojnásobně vyšší, počet významných incidentů byl o třetinu nižší. Nejčastější typy útoků představovaly v uplynulém roce různé druhy phishingu, scanning, vishing a podvodné e-maily či útoky na dostupnost (převážně formou DDoS útoků). Phishing dominuje statistikám dlouhodobě, využívání této techniky se však proti předchozím rokům stupňuje. Mimo to pokračovaly i ransomwarové útoky, které jsou již dlouhodobým trendem. V roce 2023 NÚKIB poprvé zaznamenal typ ransomwarového útoku, který využíval přístup „extortion-only“, což znamená, že data oběti nebyla útočníkem zašifrována, nýbrž exfiltrována, načež útočník vydíral oběť jejich zveřejněním. *„Platba výkupného útočníkům nezaručí vyřešení incidentu ani obnovení dat, ale podporuje útočníky v další škodlivé činnosti,“* konstatoval ředitel NÚKIB Lukáš Kintr. Na konci roku 2023 se Česká republika připojila k mezinárodnímu prohlášení Counter Ransomware Initiative, čímž se zavázala k neplacení výkupného.

V roce 2023 pokračovaly přípravy návrhu nového zákona o kybernetické bezpečnosti, který je důležitým krokem pro zachování bezpečnosti kyberprostoru České republiky. Nový zákon reaguje na dynamický vývoj v bezpečnostním prostředí a reflektuje praktické zkušenosti z téměř desetileté práce s aktuálně platným zákonem o kybernetické bezpečnosti. Jeho součástí je nová evropská kyberbezpečnostní směrnice NIS 2, kterou má Česká republika jako stát Evropské unie povinnost propsat do svého právního řádu. Návrh obsahuje i dosud chybějící mechanismus prověřování bezpečnosti dodavatelského řetězce u nejkritičtější infrastruktury České republiky.

Zprávu o stavu kybernetické bezpečnosti České republiky za rok 2023 naleznete zde.

[1] NÚKIB na začátku roku 2024 rozeslal dotazník se 63 otázkami, a to jak subjektům regulovaným dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti, ZKB), ve znění pozdějších předpisů, tak i řadě dalších klíčových institucí a organizací, které zákonem o kybernetické bezpečnosti regulovány nejsou. Otázky se týkaly širokého záběru témat, například kybernetických útoků, nákladů na kybernetickou bezpečnost, personálních kapacit v oblasti kybernetické bezpečnosti, uživatelů, technologií i zavedených procesů. Dotazník vyplnilo celkem 423 subjektů, z toho 339 regulovaných a 84 neregulovaných. Ze získaných dat NÚKIB čerpal informace pro potřeby Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2023 (dále také jen „Zpráva“). Veškeré údaje z dotazníků jsou anonymizovány.

https://nukib.gov.cz/cs/infoservis/aktuality/2139-vlada-schvalila-zpravu-o-stavu-kyberneticke-bezpecnosti-cr-za-rok-2023