Upozorňujeme na zvýšené riziko ransomwarových útoků

20.6.2023 - | Národní úřad pro kybernetickou a informační bezpečnost

Jedním z častých vektorů útoku, skrze který útočníci získávají přístup do sítí obětí, je zneužívání zranitelností. O některých z nich již NÚKIB v minulosti informoval (upozornění naleznete na našich webových stránkách). S ohledem na současné ransomwarové hrozby jsme identifikovali sadu zranitelností, jejichž opravu považujeme za klíčovou:

Úspěšný průnik do systémů využívající zmíněné zranitelnosti jako vektor útoku může mít za následek krádež dat ze systémů oběti, jejich zašifrování a následné vydírání jak za účelem dešifrování dat, tak jejich zveřejněním ze strany útočníka. Doporučujeme ověřit, zda zranitelné aplikace nevyužíváte a pokud ano, aktualizovat je na nejnovější verzi. Výše uvedený výčet aktuálně zneužívaných zranitelností není konečný, a proto doporučujeme průběžně aktualizovat operační systémy, programy a aplikace a udržovat je na nejaktuálnější verzi.

Zároveň doporučujeme věnovat pozornost také dalším často užívaným vektorům útoku, jako je phishing, kompromitace účtů (doménových/lokálních/VPN), nezabezpečených služeb otevřených do internetu (např. RDP, FTP, SMB…) či kompromitace skrze poskytovatele služeb.

Vedle opravení kritických zranitelností a posílení infrastruktury též doporučujeme nastavení detekčních pravidel na základě dostupných indikátorů kompromitace (IoCs). Subjekty a orgány povinné dle zák. č. 181/2014 Sb., zákon o kybernetické bezpečnosti, mohou využívat sady IoCs sdílené ze strany NÚKIB prostřednictvím platformy Neweb.

Kromě výše uvedeného doporučujeme dodržovat základní bezpečnostní opatření k zabezpečení sítě před ransomwarem:

Detailní přehled jednotlivých opatření a doporučení naleznete v našem nově aktualizovaném dokumentu RANSOMWARE: DOPORUČENÍ PRO MITIGACI, PREVENCI A REAKCI.

https://www.nukib.cz/cs/infoservis/aktuality/1972-upozornujeme-na-zvysene-riziko-ransomwarovych-utoku