NÚKIB aktualizoval Minimální požadavky pro kryptografické algoritmy

5.2.2025 - | Národní úřad pro kybernetickou a informační bezpečnost

Aktualizovaná verze dokumentu zahrnuje několik důležitých úprav. Jednou z nich je vyřazení dosluhujících kryptografických algoritmů, které již nesplňují bezpečnostní požadavky. Dále jsme aktualizovali algoritmy na základě finálního znění postkvantových kryptografických standardů, které vydal americký NIST v srpnu 2024 - přibyly přesné názvy či parametry. Další úpravou je přidání dvou módů pro ochranu integrity (KMAC a GMAC) a zároveň byly upraveny parametry u algoritmů pro ukládání hesel. Tyto změny zajistí, že Minimální standardy pro kryptografické algoritmy zůstanou aktuální a budou i nadále poskytovat spolehlivé pokyny pro zajištění kybernetické bezpečnosti.

Současně s Minimálními požadavky na kryptografické algoritmy došlo k aktualizaci přílohy Kvantová hrozba a kvantově odolná kryptografie. Kvantové počítače mohou ve svých výkonech výrazně překonat současné klasické počítače. Jejich schopnosti slibují průlom v mnoha vědeckých odvětvích, nicméně zároveň představují hrozbu pro většinu současných metod šifrování. Škodliví aktéři mohou zneužít kvantových počítačů, které budou schopné útoků, jež překonají současné šifrování (tzv. kryptograficky relevantní kvantové počítače) s cílem odcizení dat, či demonstrativních útoků s cílem podlomit důvěru v určité organizace a služby (např. vládní orgány, internetové bankovnictví atd.). Neustále probíhá vývoj nových šifrovacích standardů, které kvantovým počítačům odolají. Klíčová bude jejich efektivní a včasná implementace, potažmo schopnost rychle přijímat případné aktualizace.

Aktuální dokumenty naleznete zde:
https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

https://nukib.gov.cz/cs/infoservis/aktuality/2219-nukib-aktualizoval-minimalni-pozadavky-pro-kryptograficke-algoritmy