Členské státy EU varují před kvantovou hrozbou a vyzývají k přechodu k postkvantové kryptografii

17.1.2025 - | Národní úřad pro kybernetickou a informační bezpečnost

Společné prohlášení poukazuje na nebezpečí kvantové hrozby a apeluje na entity z veřejné správy, kritické infrastruktury, poskytovatelů IT i soukromého sektoru, aby přechod k PQC stanovili jako svou prioritu. NÚKIB se ztotožňuje se závěry dokumentu a zároveň podporuje přípravné kroky, které dokument uvádí. Ty mimo jiné spočívají v provedení analýzy dopadů kvantové hrozby a v přípravě implementačního plánu pro přechod k PQC, zaměřeného zejména na oblast rizik. Zmíněna je i obecná podpora výzkumu PQC a standardizace v této oblasti.

Společné prohlášení upozorňuje na kvantovou hrozbu v souvislosti se strategií „store now, decrypt later“. Tento přístup využívají útočníci ke shromažďování zašifrovaných dat. Jakmile budou mít k dispozici kryptograficky relevantní kvantové počítače, mohou nashromážděná data dešifrovat. Pro zajištění ochrany důvěrnosti informací, zejména v případech nejcitlivějšího využití, se doporučuje co nejdříve přejít na PQC, ideálně nejpozději do roku 2030. Dokument vedle toho upozorňuje i na riziko, které plyne z časové náročnosti přechodu k PQC, zvláště pokud jde o komplexnější systémy. Příkladem takového systému je infrastruktura veřejných klíčů (PKI), která slouží k distribuci a správě veřejných klíčů a digitálních certifikátů. Neproběhne-li u těchto systémů přechod k PQC včas, bude ohrožena jak důvěrnost, tak především autenticita v nich obsažených dat. Vzhledem k jejich složitosti však přechod k PQC bude trvat delší dobu – a právě proto se doporučuje začít s ním co nejdřív.

Závěrem společné prohlášení zmiňuje vznik pracovní skupiny v rámci Skupiny pro spolupráci v oblasti bezpečnosti sítí a informací, jejímž úkolem je připravit implementační plán pro přechod k PQC v návaznosti na doporučení Evropské komise. Do těchto prací je vedle Francie, Německa, Nizozemska a dalších členských států EU zapojena též Česká republika.

NÚKIB v rámci svých aktivit dlouhodobě usiluje o zvýšení odolnosti vůči hrozbě, kterou pro bezpečnou komunikaci představují kvantové počítače. Nedávno vyjádřil podporu dokumentu „Position paper on Quantum Key Distribution“. Minulý rok NÚKIB zavedl kvantově odolnou (postkvantovou) kryptografii pro zajištění bezpečné komunikace mezi webovým prohlížečem a webovou aplikací Portál NÚKIB. Dříve zase připravil podpůrné materiály, které objasňují povahu kvantové hrozby a kroky, které bude v následujících letech nutné učinit, aby se jí předešlo.

https://nukib.gov.cz/cs/infoservis/aktuality/2208-clenske-staty-eu-varuji-pred-kvantovou-hrozbou-a-vyzyvaji-k-prechodu-k-postkvantove-kryptografii