Portál NÚKIB nově podporuje kvantově odolnou kryptografii

27.8.2024 - | Národní úřad pro kybernetickou a informační bezpečnost

Kvantová hrozba znamená existenci kryptoanalyticky relevantního kvantového počítače, který bude možné použít k dešifrování komunikace zašifrované pomocí současných asymetrických kryptografických algoritmů. NÚKIB odhaduje, že první kryptoanalyticky relevantní kvantové počítače mohou být k dispozici až v horizontu 5-15 let, přesto je potřeba se na příchod těchto počítačů připravovat již nyní.

Důvodem zavedení postkvantové kryptografie je strategie zpětného prolomení (anglicky nazývaná „Harvest now, decrypt later“), kdy útočník může již v současné době zaznamenávat šifrovanou komunikaci a dešifrovat ji až následně s příchodem kryptoanalyticky relevantního kvantového počítače.

Kvůli této strategii a taktéž z důvodu testování v reálném provozu a propagaci kvantově odolné kryptografie NÚKIB na svém nedávno spuštěném Portálu NÚKIB (Portál) zavedl podporu pro hybridní algoritmus pro ustanovení klíčů s označením X25519Kyber768 – ten využívá jak klasický algoritmus X25519, tak kvantově odolný algoritmus Kyber768.

Oba typy algoritmů se kombinují, protože existuje riziko možného prolomení postkvantových algoritmů pomocí současných počítačů. Zatím totiž neexistují dostatečné záruky, že odpovídající matematické problémy, na jejichž praktické neřešitelnosti je založena bezpečnost příslušných postkvantových algoritmů, jsou opravdu prakticky neřešitelné. I kdyby tak došlo k prolomení Kyber768 klasickým počítačem, algoritmus bude díky X25519 stále odolný proti prolomení klasickým počítačem. A i kdyby došlo k prolomení X25519 kvantovým počítačem, díky Kyber768 by měl zůstat proti kvantovým počítačům odolný.

Komunikace uživatelů Portálu NÚKIB, kteří k aplikaci přistupují pomocí některého z podporovaných prohlížečů, je tak již nyní zabezpečena proti hrozbě kvantového počítače. Zjednodušeně řečeno: komunikace by měla zůstat v bezpečí i v případě, že potenciální útočník kryptograficky relevantní kvantový počítač v současné době již má nebo jej v budoucnu získá.

V souvislosti s hrozbou prolomení současných kryptografických systémů NÚKIB již minulý rok připravil podpůrné materiály pro ochranu před hrozbou, kterou představují kvantové počítače.

https://nukib.gov.cz/cs/infoservis/aktuality/2156-portal-nukib-nove-podporuje-kvantove-odolnou-kryptografii