Libor Štourač

Je interní auditor a manažer v oblastech řízení kvality, životního prostředí a bezpečnosti informací ve společnosti ITS akciová společnost. Má za sebou více než 25 let zkušeností v oblasti IT, mimo jiné působí i jako lektor spolupracující s ČIIA na vybraných kurzech, primárně z oblasti kybernetické bezpečnosti a auditu IT. Podílel se na mnoha projektech pro významné zákazníky, jak v oblasti firemní klientely, bankovnictví, tak státní správy, včetně externích bezpečnostních auditů a konzultací.

Než vyprší čas: proč vědět o kvantových hrozbách jako interní auditor

Šifrování je dnes základním kamenem informační bezpečnosti. Chrání data při přenosu, uchovávání i zpracování a zajišťuje důvěrnost, integritu a autenticitu informací. Jako interní auditoři se setkáváte nepřímo s šifrováním v mnoha kontrolních oblastech – od správy přístupů, zálohování po ochranu osobních údajů, přenos dat atd., v rámci kybernetické bezpečnosti. S nástupem kvantových počítačů se však mění i samotné základy kryptografie. Technologie, které dnes považujeme za bezpečné, mohou být během několika let prolomeny.

V posledních letech se kvantové počítače posunuly z laboratoří teoretické fyziky do oblasti praktických experimentálních zařízení. Ačkoliv dnes nemají výkon na masové dešifrování, jejich vývoj je natolik rychlý, že již dnes představují strategickou hrozbu pro stávající kryptografické systémy.

Většina v současnosti používaných kryptografických metod (RSA, ECC apod.) – vychází z matematicky obtížně řešitelných úloh, které jsou pro klasické počítače prakticky neřešitelné. Kvantový počítač dokáže tyto problémy řešit velmi rychle.

Jaká jsou rizika pro organizace?

- Útoky typu „Harvest now, decrypt later“ – útočníci dnes shromažďují šifrovaná data a dešifrují je v budoucnu, až budou dostupné kvantové výpočetní prostředky.
- Riziko prolomení dat, která mají dlouhou životnost, např. finanční záznamy, zdravotní záznamy, citlivé smlouvy či komunikace.

Pro auditory je klíčové chápat, že klasické zabezpečení certifikátů, dat, záloh a archivů, VPN či e-mailové komunikace může být v horizontu několika let neúčinné, pokud organizace nezačne implementovat quantum-safe kryptografii. Pokud organizace vyhodnotí,

že vlastní data, která mají dlouhou životnost, představují při dešifrování bezpečnostní riziko, není čas příliš otálet a je nutné připravit organizaci na tzv. post-quantum (quantum-safe) šifrování. Quantum-safe kryptografie zahrnuje algoritmy navržené tak, aby odolaly útokům jak klasických, tak kvantových počítačů.

„Kvantové počítače přinesou revoluci v oblasti výpočetní techniky i kybernetické bezpečnosti.“

Přechod na PQC (Post-Quantum Cryptography) je dlouhodobý proces, který vyžaduje identifikaci rizika, strategické plánování a sledování technologického vývoje. Kde začít? Příprava na quantum-safe kryptografii zahrnuje:

- Inventarizaci všech kryptografických prvků používaných v organizaci (např. certifikáty, klíče, protokoly, knihovny.
- Posouzení rizik – které systémy jsou nejvíce ohroženy a mají dlouhou životnost dat.
- Crypto-agility – schopnost organizace rychle přejít na nové algoritmy bez zásadního narušení provozu.
- Plán migrace na nové algoritmy doporučené organizacemi jako NIST (např. Kyber, Dilithium).
- Hybridní řešení – kombinace klasických a post-quantum algoritmů, aby byla bezpečnost zachována během přechodu.
- Průběžné testování kompatibility nových řešení s existující infrastrukturou.
- Monitoring a reporting implementace pro vedení organizace.

Naše společnost se problematice postkvantové kryptografie (PQC) dlouhodobě věnuje, a proto víme, že přechod na tzv. quantum-safe řešení – tedy taková, která zůstanou bezpečná i po nástupu kvantových počítačů – není otázkou dnů, týdnů, ani měsíců. Důvod je jednoduchý: jen zmapování všech kryptografických prvků je časově hodně náročné, a řada technologií a softwarových řešení zatím není na PQC připravena a stále využívá klasické kryptografické algoritmy. Znamená to hledat nová řešení, jednat s dodavateli současných systémů o přechodu na PQC, zmapovat související systémy a komponenty, aby i po změně šifrování byly systémy plně funkční. Kryptografie je navíc hluboce integrována do většiny IT prostředí – od síťové komunikace přes infrastrukturu až po operační systémy a informační aplikace.

Ačkoli se v současnosti hodně diskutuje o novém kybernetickém zákonu, směrnici NIS2 či o rizicích a přínosech umělé inteligence, postkvantová kryptografie je dalším klíčovým tématem, kterému by se měly organizace aktivně věnovat, pokud chtějí zůstat bezpečné i v budoucnosti.

Interní auditor by se měl tedy ptát nejen „Jsme dnes zabezpečeni?“, ale také „Máme plán, jak zůstaneme zabezpečeni i po nástupu kvantových počítačů?“

„Technologie, které dnes považujeme za bezpečné, mohou být během několika let prolomeny.“

Kvantové počítače přinesou revoluci v oblasti výpočetní techniky i kybernetické bezpečnosti. I když masové využívání kvantových počítačů není zatím realitou, organizace by měly začít plánovat přechod na postkvantovou kryptografii. Interní auditoři hrají v tomto procesu klíčovou roli: jejich úkolem je upozornit a také společně s vrcholovým vedením zajistit, aby organizace byla připravena nejen na dnešní hrozby, ale i na ty budoucí, které přinese kvantová éra.

ITS se podílí na mnoha aktivitách v oblasti osvěty okolo Quantum safe – mimo jiné je technologickým partnerem projektu Quantum Innovation Center Czech Republic, jehož konsorciální členové jsou přední české vysoké technické školy a Akademie věd. Platforma tak pomáhá tak vychovávat budoucí odborníky na post-kvantovou kryptografii již nyní.

Quantum Innovation Center
THE CZECH REPUBLIC

CEO společnosti ITS Ing. Lumír Srch přednáší o kvantových hrozbách na posledním workshopu ČIIA v Přerově interním auditorům z veřejné správy.

Co jsou kvantové počítače

Kvantové počítače vznikly jako odpověď na limity klasických výpočetních technologií a jako snaha využít jedinečné jevy kvantové fyziky k řešení úloh, které běžné počítače nezvládnou. Pokusím se to stručně objasnit. Klasické počítače pracují s bity, které mají hodnotu 0 nebo 1. Kvantové počítače používají tzv. qubity, které díky jevu superpozice mohou být současně 0 i 1. Další klíčovou vlastností je *entanglement* – provázání qubitů, které umožňuje kvantovým počítačům provádět masivní paralelní výpočty. Existuje několik technologií, které výrobci používají pro realizaci qubitů. Například IBM, Google a Rigetti Computing využívají supervodivé obvody; Atom Computing používá neutrální atomy; IonQ a Honeywell iontové pasti (ion trap); Microsoft vyvíjí topologické qubity a Xanadu pracuje s fotonovými qubity. Každá z těchto technologií má své výhody i nevýhody, a zatím není jasné, která se prosadí, případně zda se udrží všechny. První komerční kvantový počítač s 20 qubity IBM Q System One byl představen v lednu 2019. Nyní se pohybujeme na úplně jiné úrovni výkonu: IBM Condor s 1121 qubity a Atom Computing s 1180 qubity patří k nejvýkonnějším kvantovým počítačům světa. Některé země, i když se aktivně věnují vývoji kvantových počítačů, nezveřejňují podrobnosti o výkonech svých zařízení. Výkon kvantových počítačů se neprojevuje přímo jako rychlost klasického procesoru, ale schopností zpracovávat exponenciálně rostoucí počet stavů díky qubitům – zatímco 1 qubit může být ve 2 stavech (0 a 1), 3 qubity současně reprezentují 8 stavů a 50 qubitů už více než bilion stavů najednou, což klasický počítač nedokáže. Díky těmto vlastnostem mohou kvantové počítače řešit některé matematické problémy mnohonásobně rychleji než klasické stroje. To zahrnuje například faktorizaci velkých čísel nebo hledání diskrétních logaritmů, což jsou základy algoritmů používaných v běžné kryptografii. Organizace NIST (National Institute of Standards and Technology, Americký národní institut pro standardy a technologie) vybral první standardizované postkvantové algoritmy (např. CRYSTALS-Kyber pro šifrování a výměnu klíčů, CRYSTALS-Dilithium, FALCON, SPHINCS+ pro podpisy). ■