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.

Kvantové počítače: konec bezpečnosti tak, jak ji známe

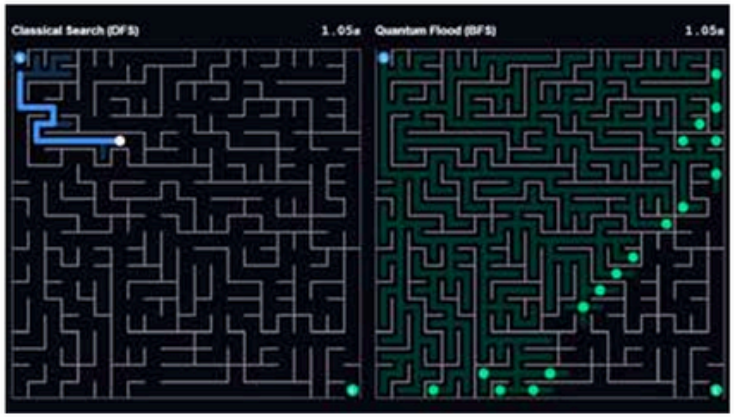
Na nedávném workshopu veřejné správy v Hradci Králové zaznělo na více místech v rámci přednášek o kybernetické bezpečnosti i téma kvantových hrozeb. Proč se toto téma dostává v posledních měsících tolik do popředí?

Kvantové počítače už dávno nejsou jen věcí laboratoří nebo scénářů ze sci-fi filmů. V posledních letech došlo k obrovskému technologickému posunu. Díky zrychlenému vývoji a rostoucímu výpočetnímu výkonu pro specifické operace, pro které jsou kvantové počítače vhodné, jsou aktuálnějším tématem než kdy jindy. Dnes do nich ve velkém proudí investice vlád, armád i technologických gigantů. A právě tak, jak se rozjela horečka umělé inteligence, startuje další zásadní závod: tentokrát kvantový. Analytici tomu říkají *nový vesmírný závod* – jen se tentokrát hraje o kontrolu nad informačním světem.

Kde mohou mít kvantové počítače zásadní dopad a jsou podstatné ze strategického pohledu? Kybernetické bezpečnost, armáda, špionáž, vývoj umělé inteligence, globální ekonomika, to je jen malý výčet.

Proč jsou tak jiné?

Nejprve je potřeba pochopit, že kvantové počítání má blíže k fyzice než klasické elektrotechnice. Klasické počítače spoléhají na bity – nuly a jedničky. Kvantové počítače pracují s tzv. qubity, které díky kvantové fyzice zvládnou najednou reprezentovat celou škálu „stavů" – to znamená vše mezi nulou a jedničkou. Výsledkem jsou rychlosti výpočtů, které klasické superpočítače nechávají za sebou, zejména u specifických úloh.



IBM, Google i Microsoft dávají najevo, že doba, kdy kvantové počítače překonají klasické v praktických úlohách („quantum advantage“), je na dohled. Již nyní kvantové počítače počítají určité komplexní simulace a výpočty až tisíckrát rychleji než ty nejsilnější klasické superpočítače.

„Běžný uživatel možná vnímá kvantové počítače jako technologickou kuriozitu, ale pro odborníky na kyberbezpečnost znamenají existenční problém.“

První využití už existují: modelují molekuly a materiály, optimalizují dopravní a logistické systémy, pomáhají tvořit efektivnější jízdní řády. Do budoucna nám mohou významně pomoci v oblastech, jako je vývoj léků a medicíny, vývojem nových materiálů, vesmírným výzkumem, finančním modelování, s vyhodnocováním velkého objemu dat, optimalizací ekonomiky apod.

Největší bezpečnostní hrozba za poslední dekády

S technologií přichází o otázka největší bezpečnostní hrozby za poslední dekády – prolomení šifrování. Běžný uživatel možná vnímá kvantové počítače jako technologickou kuriozitu, ale pro odborníky na kyberbezpečnost znamenají existenční problém.

Na šifrování stojí bankovnictví, e-maily, e-shopy, komunikace přes VPN, státní systémy i kryptoměny. Aktuálně používané metody, hlavně RSA a ECC, jsou pro klasické počítače bezpečné, ale kvantový počítač, vyzbrojený Shorovým algoritmem, je může prolomit výrazně rychleji. Google letos otevřeně varoval: první reálný kvantový útok přijde klidně už kolem roku 2029.

Harvest now, decrypt later

Objevila se nová strategie útoku: *Harvest now, decrypt later.* Jde o přístup, kdy útočníci už nyní dokážou zašifrovaná data ukrást – zdravotní, výzkumná, data finančních transakcí, vojenskou a diplomatickou výměnu informací, a mnoho dalších. Jakmile budou mít kvantový počítač s dostatečným výkonem, zpětně tato historická data budou schopni rozšifrovat. Proto začal závod s časem: přechod k nové generaci šifrování nesnese odkladu.

„Kvantové počítače už dávno nejsou jen věcí laboratoří nebo scénářů ze sci-fi filmů.“

PQC – Post-Quantum Cryptography

Mezinárodní reakce je jasná. Americký NIST už několik let vede úsilí o standardizaci kryptografie odolné proti kvantovým útokům. Již jsou schválené první standardy: ML-KEM (Kyber), ML-DSA (Dilithium), SLH-DSA (SPHINCS+) a HQC. Jedná se o tzv. Post-Quantum Cryptography (PQC), které se stává novou normou šifrování.

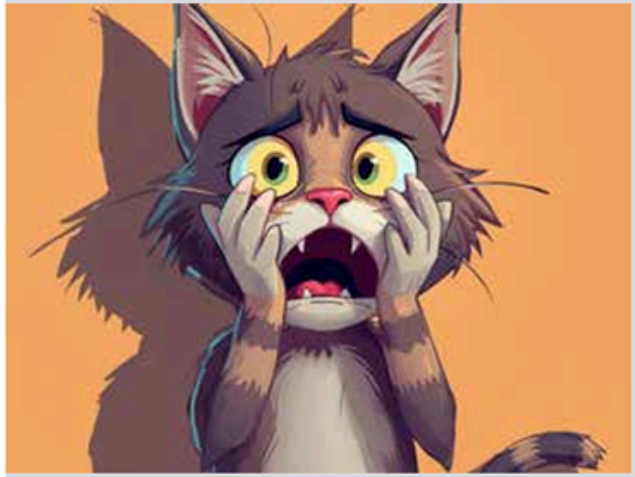
Technologické firmy nespí. Meta (Facebook, Instagram, LinkedIn…) popsala zkušenosti s migrací na PQC a zdůraznila nutnost okamžitě začít mapovat staré kryptografické systémy. Google zavedl hybridní post-quantum TLS do Chromu, Cloudflare otestoval kvantově odolné zabezpečení pro VPN, Signal chrání komunikaci PQC už od loňska a celosvětové finanční instituce připravují masivní přechod. Ale není to žádný rychlý update. IT infrastruktura je

ZNÁTE SCHRÖDINGEROVU KOČKU?

Schrödingerova kočka je slavný myšlenkový experiment rakouského fyzika Erwina Schrödingera z roku 1935, který měl ilustrovat zvláštní chování kvantových systémů. Představte si uzavřenou krabici, ve které je kočka spolu se zařízením napojeným na radioaktivní atom. Pokud se atom rozpadne, spustí mechanismus, který kočku usmrtí. Pokud se nerozpadne, kočka zůstane naživu.

V klasické fyzice by kočka byla buď živá, nebo mrtvá – nic mezi tím. Kvantová fyzika ale říká, že dokud se na systém nepodíváme, může být atom současně „rozpadlý i nerozpadlý“. Z toho vyplývá, že i kočka je v určitém smyslu zároveň živá i mrtvá – existuje ve stavu tzv. superpozice. Teprve akt pozorování (otevření krabice) rozhodne, v jakém stavu se skutečně nachází.

Tento experiment má ukázat, jak odlišně se kvantový svět chová oproti našemu běžnému vnímání reality. Princip superpozice a nejistoty je přitom základem moderních kvantových technologií – ale také potenciálních „kvantových hrozeb“, například v oblasti šifrování. Kvantové počítače totiž mohou pracovat s více stavy současně, což jim dává obrovskou výpočetní sílu, ale zároveň narušuje dosavadní představy o bezpečnosti dat.



ITS JAKO SPOLEHLIVÝ PARTNER

Společnost ITS je ryze českou firmou, která se pohybuje v informačních technologiích, kybernetické bezpečnosti a vývoji softwaru již řadu let. Mimo jiné jako dlouholetý partner IBM participuje na projektu Quantum Innovation Center Czech Republic, jež je součástí sítě dalších padesáti kvantových center po celém světě. ITS se intenzivně věnuje edukaci a osvětě v této oblasti, primárně však působí především jako partner v procesu přechodu na post-kvantové technologie pro řadu organizací a institucí. Je rovněž dlouholetým partnerem ČIIA a vzdělávání v oblasti auditu kybernetické bezpečnosti a IT. Více na www.its.cz

Libor Štourač vedl jednu pracovní skupinu na workshopu ČIIA v Hradci Králové.

„Role interního auditora je v tuto chvíli minimálně otevřít konverzaci na toto téma, pokud se tak dosud nestalo.“

spletitá: servery, certifikáty, IoT zařízení, průmyslové systémy, cloud i např. mobilní aplikace a celá vývojová vrstva, v neposlední řadě dodavatelský řetězec. Každý prvek využívá kryptografii jinak. Výměna algoritmů není jednoduchý upgrade softwaru, ale roky trvající transformace. Na hradeckém workshopu jsme zmiňovali mimo jiné i lokální regulátory – Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) doporučuje přechod na post-kvantově odolné algoritmy do roku 2027.

Kdy nastane Q-Day a role auditu

Role interního auditora, který má přehled o chodu celé organizace, strategickém plánování a řízení rizik, je v tuto chvíli minimálně otevřít konverzaci na toto téma, pokud se tak dosud nestalo. Proces přechodu na tzv. Quantum safe je otázkou i několika let, a proto není čas otálet.

Nikdo dnes nezná přesné datum, kdy kvantové počítače opravdu prolomí současné šifrování. Jisté je ale jedno: bezpečnost, jak ji dnes známe, čeká nejhlubší změna v historii. Teď už nejde o to, jestli to přijde. Otázka zní: kolik času na přechod nám ještě zbývá? ■