

KONIEC TAJOMSTIEV NA INTERNETE? PRICHÁDZA NEVIDITEĽNÁ REVOLÚCIA, KTORÁ OCHRÁNI NAŠE PENIAZE AJ SÚKROMIE

Keď dnes platíme kartou cez internet, prihlasujeme sa do internet bankingu, posielame správu v chatovacej aplikácii alebo komunikujeme so štátom, spoliehame sa na šifrovanie. Je to niečo ako neviditeľný trezor digitálneho sveta. Bežný človek ho nevidí, no bez neho by nefungovala dôvera v banky, e-shopy, zdravotníctvo ani súkromnú komunikáciu. S nástupom kvantových počítačov sa však začína nová kapitola kybernetickej bezpečnosti.

Bratislava, 7.7.2026

Neznamená to, že zajtra prestane fungovať internet alebo že sa ľuďom zrazu vymažú účty. Riziko je nenápadnejšie. Údaje, ktoré sú zachytené dnes, môžu mať hodnotu aj o desať rokov. Ak ich útočník uloží a v budúcnosti získa technológiu na ich prelomenie, môže sa k nim vrátiť neskôr. Postkvantové šifrovanie znie technicky, no v skutočnosti ide o veľmi praktickú vec: ako zabezpečiť, aby naše platby, zdravotné údaje, heslá a súkromné správy zostali chránené aj v budúcnosti. Jej cieľom je pripraviť banky, firmy, štátne inštitúcie, technologické platformy aj výrobcov zariadení na budúcnosť, v ktorej dnešné šifry nemusia stačiť.

„Postkvantové šifrovanie znie ako téma pre vedcov, ale v skutočnosti sa týka každého, kto má bankový účet, zdravotnú kartu, smartfón alebo súkromné správy. Nejde o paniku. Ide o to, aby ochrana, na ktorú sa dnes spoliehame, fungovala aj v budúcnosti,“ hovorí Mária Krahulecová, spoluzakladateľka konferencie venujúcej sa kybernetickej bezpečnosti Qubit Conference[®].

Čo robia naše smartfóny zle?

Samotné smartfóny nerobia nič zle. Problém nie je v telefóne ako takom. Problém je v tom, že celý digitálny svet okolo nás používa bezpečnostné riešenia navrhnuté pre dnešné počítače. Keď otvoríme bankovú aplikáciu alebo odošleme správu, nejde iba o náš mobil. Do hry vstupujú aj servery banky, cloudové služby, certifikáty, aplikácie a množstvo technológií, ktoré bežný používateľ nikdy nevidí.

WEB

www.qubitconference.com

EMAIL

info@qubitconference.com

OFFICE

Qubit Conference[®]
Martinčekova 17
821 01 Bratislava

Preto nejde o jednorazové preprogramovanie telefónu, ale o postupnú modernizáciu celého digitálneho sveta. Pre používateľov sa väčšina zmien pravdepodobne udeje na pozadí, podobne ako dnes prebiehajú aktualizácie systému alebo aplikácií. Ľudia si preto pravdepodobne nebudú musieť hromadne kupovať nové telefóny. Rizikom však môžu byť veľmi staré zariadenia a systémy, ktoré už nedostávajú bezpečnostné aktualizácie.

Útok sa môže začať dnes, aj keď škoda príde až o roky

Jedným z najväčších rizík je scenár známy ako store now, decrypt later, teda zachytiť dnes, prečítať neskôr. Útočník nemusí vedieť údaje rozlúštiť okamžite. Stačí, že ich uloží. Ak budú mať hodnotu aj o desať rokov, môžu sa stať problémom v budúcnosti. Týka sa to najmä dát s dlhou životnosťou: zdravotných záznamov, finančných údajov, právnych dokumentov, interných firemných správ, štátnych registrov, výskumu alebo obchodných tajomstiev. Inými slovami, nie všetky dáta strácajú hodnotu po pár dňoch. Niektoré môžu byť citlivé celý život. „Kryptografická migrácia sa nezačína v deň, keď je hrozba na titulných stranách. Vtedy už môže byť neskoro. Incident, ktorý uvidíme v roku 2034, sa môže začať tým, že sa v roku 2026 neurobí nič,“ upozorňuje Nicol Danková, odborníčka na kybernetickú bezpečnosť a autorka prezentácie *Post-Quantum Is Not Postponable*. Presný dátum, kedy budú kvantové počítače schopné plošne prelomiť dnes používané kryptografické mechanizmy, nepoznáme. Práve preto sa na túto zmenu treba pripravovať vopred. V bezpečnosti totiž nestačí reagovať až vtedy, keď problém nastane.

Čo by sa stalo s bankami?

Prelomenie dnešného šifrovania by neznamenal, že ľuďom zo dňa na deň zmiznú peniaze z účtov. Väčším rizikom je strata dôvery v digitálne bankovníctvo. „Bežný používateľ by mal používať podporované zariadenia a aplikácie, pravidelne ich aktualizovať a neodkladať bezpečnostné aktualizácie. Hlavná zodpovednosť však leží na bankách, firmách, štáte a technologických dodávateľoch, ktorí musia už dnes mapovať používanú kryptografiu a pripravovať systémy na prechod na nové štandardy,“ vysvetľuje Mária Krahulecová. Banková aplikácia musí vedieť dokázať, že sa pripájate naozaj k svojej banke, že údaje po ceste nikto nečíta a že transakciu nemožno spätne spochybniť alebo zmeniť. Ak by sa tieto mechanizmy oslabili, banky by museli rýchlo meniť certifikáty, protokoly, aplikácie a bezpečnostné mechanizmy. Najväčším problémom by bol chaos pri neskorej migrácii. Ak organizácia nevie, kde všade má svoje digitálne zámky a kľúče, nevie ich ani rýchlo vymeniť.

WEB

www.qubitconference.com

EMAIL

info@qubitconference.com

OFFICE

Qubit Conference®
Martinčekova 17
821 01 Bratislava

Dva zámky namiesto jedného

Postkvantové šifrovanie možno vysvetliť jednoducho. Ide o nový typ zámku pre digitálne údaje. Dnešné zámky sú stále silné voči bežným počítačom. Problém je, že budúce kvantové počítače môžu mať úplne iný spôsob, ako sa k nim dostať. Preto sa v prechodnom období často hovorí o hybridnom prístupe. Znamená to, že sa používajú dva zámky naraz. Dnešný silný zámok a nový zámok navrhnutý aj proti budúcim kvantovým útokom. „Pre lepšie pochopenie to vieme prirovnať k vzorkám krvi v archíve. Dnes z nich možno nevieme získať všetky informácie, pretože nemáme vhodnú technológiu. Ak si ich však niekto odloží a o desať rokov bude mať pokročilejšie nástroje, z rovnakých vzoriek môže získať informácie, ktoré dnes získať nevie. Pri dátach je to podobné. Útočník ich nemusí vedieť prečítať dnes. Stačí, že ich zachytí a odloží si ich na neskôr. Postkvantové šifrovanie je preto spôsob, ako chrániť aj údaje, ktoré musia zostať tajné dlhé roky,“ vysvetľuje Mária Krahulecová.

Sú slovenské firmy a štát pripravené?

Nedá sa férovo povedať, že slovenské firmy a štátne inštitúcie sú ako celok pripravené alebo nepripravené. Dôležité je, či si vedia odpovedať na veľmi praktické otázky.

Vedia organizácie, kde používajú šifrovanie?

Vedia, aké certifikáty, algoritmy, protokoly a kľúče majú v systémoch?

Vedia, kto je za ne zodpovedný?

A vedia, čo používajú ich dodávatelia?

Prvý krok nie je nákup novej technológie. Prvý krok je urobiť si poriadok vo vlastných systémoch. Organizácia musí vedieť, čo má, kde to má, čo tým chráni a ako dlho musia tieto dáta zostať dôverné. Druhým krokom je prioritizácia. Inak sa pristupuje k bežnému internému systému a inak k zdravotníctvu, bankovníctvu, štátnym registrom alebo infraštruktúre, ktorá má fungovať ešte mnoho rokov. Tretím krokom je crypto agility – schopnosť meniť kryptografiu rýchlo, riadene a bez chaosu. Jednoducho povedané, organizácia má byť schopná vymeniť digitálne zámky skôr, než sa stanú slabým miestom. „Cieľom nie je vymeniť jednu šifru za druhú a tváriť sa, že máme hotovo. Cieľom je schopnosť meniť kryptografiu podľa potreby. Organizácie sa musia dostať do stavu, keď vedia robiť bezpečnostné zmeny v minútach, nie v mesiacoch,“ hovorí Jan Dušátka, odborník na agilnú kryptografiu.

WEB

www.qubitconference.com

EMAIL

info@qubitconference.com

OFFICE

Qubit Conference®
Martinčekova 17
821 01 Bratislava

Neviditeľná zmena, ktorá sa dotkne každého

Pre bežného človeka bude postkvantové šifrovanie pravdepodobne neviditeľné. A práve to je cieľ. Tak ako dnes väčšina ľudí nemusí vedieť, ako presne funguje šifrovanie v bankovej aplikácii, ani v budúcnosti nebude musieť riešiť technické detaily. Rozdiel je v tom, že firmy, banky, štát a technologickí dodávatelia musia začať včas. Ak majú niektoré údaje zostať tajné desať alebo dvadsať rokov, nestačí ich začať chrániť až o desať alebo dvadsať rokov. „Postkvantové šifrovanie je neviditeľná infraštruktúra dôvery. Ak sa urobí dobre, ľudia si možno nič nevšimnú. A to bude najlepší výsledok,“ konštatuje M. Krahulecová.

Qubit Conference® prináša odborníkov na kybernetickú bezpečnosť, technologické inovácie a digitálnu odolnosť. Téma postkvantového šifrovania, ktorá rezonovala aj na medzinárodnej konferencii Qubit Conference® v máji v Prahe, ukazuje, že budúcnosť bezpečnosti sa nezačína v laboratóriách, ale v rozhodnutiach, ktoré organizácie robia už dnes.

WEBwww.qubitconference.com**EMAIL**info@qubitconference.com**OFFICE**

Qubit Conference®
Martinčekova 17
821 01 Bratislava