Experti varujú, že svet sa nachádza „len pár rokov“ od kvantovej apokalypsy

- CZ24 News | 23. ledna 2023

Vo veľmi blízkej budúcnosti by podľa čínskych vedcov mohol pokrok v kvantovej výpočtovej technike viesť ku „kvantovej apokalypse“, ktorá prelomí všetky šifry od online bankovníctva až po „bezpečné“ vládne platformy plné štátnych tajomstiev.

Akademická štúdia na túto tému varuje, že súčasné šifrovanie, ktoré uchováva všetky naše údaje „v bezpečí“, sa rýchlo stane zraniteľným a možno sa úplne zrúti v dôsledku toho, že kvantové počítače budú príliš „inteligentné“ pre súčasný spôsob fungovania internetu.

Výskumníci z *Chicagskej univerzity* tvrdia, že pracujú na nenapadnuteľnom kvantovom internete budúcnosti – Web 3.0, ako ho mnohí nazývajú – ale bude to fungovať?

Ako dnes funguje šifrovanie a ako to ovplyvnia kvantové počítače

Počítače dnes používajú na ochranu informácií systém nazývaný šifrovanie verejným kľúčom. Textové správy sa napríklad prenášajú na telefóny, ktoré obsahujú dva kľúče: jeden je verejný a druhý súkromný.

Zariadenie, ktoré nadväzuje kontakt, používa na šifrovanie správy verejný kľúč, zatiaľ čo súkromný kľúč príjemcu ju otvára. To zaisťuje, že nikto iný mimo týchto dvoch zariadení nemôže zachytiť a odšifrovať správu.

Podľa Tima Callana, vedúceho oddelenia pre kybernetickú bezpečnosť v spoločnosti Sectigo, by kvantové počítače, ktoré sa v súčasnosti vyvíjajú, mohli jedného dňa „spôsobiť, že šifrovanie, ktoré teraz používame, už nebude vyhovovať svojmu účelu“.

(Súvisiace: Pamätáte si, keď blázniví liberáli kritizovali časopis Nature za zverejnenie štúdie o „nadradenosti“ kvantových počítačov, pričom tvrdili, že slovo nadradenosť vyvoláva rasistické predstavy?)

Budú všetky tajomstvá nakoniec nezašifrované a sprístupnené všetkým prostredníctvom kvantových počítačov?

Pri dnešných počítačoch to nie je problém. Prelomenie spomínaných kľúčových kódov by trvalo asi 300 biliónov rokov. Ale keďže kvantový počítač bude onedlho debutovať, existujúce šifrovacie technológie sa môžu čoskoro stať zastaranými.

Možno je vám známa súčasná binárna kombinácia núl a jednotiek, ktoré tvoria elektronické a optické impulzy. Takto sa vytvárajú, ukladajú a prenášajú údaje na existujúcich počítačoch.

Kvantové výpočty na druhej strane namiesto elektrónov používajú fotóny alebo svetelné častice, ktoré je možné nastaviť na nulu, jednotku alebo obe zároveň – jednotku aj nulu. Navyše, rýchlosť

fotónu je 136-krát vyššia ako rýchlosť elektrónu.

Táto pridaná flexibilita zahrnutia nuly aj jednotky do toho istého fotónu by umožnila kvantovým počítačom rýchlo kódovať a prelomiť všetky možné riešenia šifrovania, čím by sa odstránila počítačová a online bezpečnosť, ako ju už dlho poznáme.

„Vývoj kvantových počítačov vytvára významnú hrozbu pre bezpečnosť dát,“ varuje Callan.

„Ich obrovský výpočtový výkon je schopný prelomiť šifrovanie veľkou rýchlosťou, takže dôležité dáta sa stanú zraniteľné – od údajov o bankových účtoch cez lekárske záznamy až po štátne tajomstvá.“

Tento scenár je taký alarmujúci, že ho odborníci nazývajú „kvantová apokalypsa“.

Callan pokračoval a vysvetlil, že kvantové výpočty budú tiež miliónkrát rýchlejšie ako „klasické počítače“ vďaka použitiu jednotiek, núl alebo jednotiek a núl súčasne – čo je technológia známa ako „qubits“.

Keď sa to stane, bude to deň Q – slovná hračka výrazu „deň D“ – v ktorom nastane to, že sa všetky svetové tajomstvá stanú zraniteľné. Týka sa to najmä vlád, ktoré skrývajú najrôznejšie veci, o ktorých nechcú, aby sa široká verejnosť dozvedela.

Kvantové útoky nie sú vecou budúcnosti, dejú sa už dnes

Bidenov režim v USA je jednou z takýchto vlád, ktorá sa obáva kvantových počítačov, keďže bola minulý rok napadnutá kvantovým útokom.

Spoločnosti ako IBM a Google horúčkovito pracujú na vytvorení pokročilejších kvantových počítačov, hoci ich masové rozšírenie je ešte niekoľko rokov vzdialené – podľa čínskych expertov možno 8 až 20 rokov.

„Nedávne tvrdenie, že výskumníci prelomili šifrovanie, nás vyzýva, aby sme sa zamysleli, či kvantová apokalypsa už náhodou nenastala,“ hovorí Callan.

„V súčasnosti však tento „prelom“ zostáva len teoretický.“

AUTOR: Ethan Huff

ZDROJ

Spracoval: Badatel.net