Experti varují, že svět se nachází „jen pár let“ od kvantové apokalypsy

infokuryr.cz/n/2023/01/23/experti-varuji-ze-svet-se-nachazi-jen-par-let-od-kvantove-apokalypsy

kuryr 23. ledna 2023

Ve velmi blízké budoucnosti by podle čínských vědců mohl pokrok v kvantové výpočetní technice vést ke „kvantové apokalypsě“, která prolomí všechny šifry od online bankovnictví až po „bezpečné“ vládní platformy plné státních tajemství.

Akademická studie na toto téma varuje, že současné šifrování, které uchovává všechny naše údaje „v bezpečí“, se rychle stane zranitelným a možná se zcela zhroutí v důsledku toho, že kvantové počítače budou příliš „inteligentní“ pro současný způsob fungování internetu.

Výzkumníci z *Chicagské univerzity* tvrdí, že pracují na nenapadnutelném kvantovém internetu budoucnosti – Web 3.0, jak jej mnozí nazývají – ale bude to fungovat?

Jak dnes funguje šifrování a jak to ovlivní kvantové počítače

Počítače dnes používají k ochraně informací systém nazývaný šifrování veřejným klíčem. Textové zprávy se například přenášejí na telefony, které obsahují dva klíče: jeden je veřejný a druhý soukromý.

Zařízení, které navazuje kontakt, používá k šifrování zprávy veřejný klíč, zatímco soukromý klíč příjemce ji otevírá. To zajišťuje, že nikdo jiný mimo tyto dva zařízení nemůže zachytit a odšifrovat zprávu.

Podle Tima Callana, vedoucího oddělení pro kybernetickou bezpečnost ve společnosti Sectigo, by kvantové počítače, které se v současnosti vyvíjejí, mohly jednoho dne „způsobit, že šifrování, které nyní používáme, už nebude vyhovovat svému účelu“.

(Související: Pamatujete si, když bláznivíliberálové kritizovali časopis Nature za zveřejnění studie o „nadřazenosti“ kvantových počítačů, přičemž tvrdili, že slovo nadřazenost vyvolává rasistické představy?)

Budou všechna tajemství nakonec nezašifrována a zpřístupněna všem prostřednictvím kvantových počítačů?

U dnešních počítačů to není problém. Prolomení zmíněných klíčových kódů by trvalo asi 300 bilionů let. Ale protože kvantový počítač bude zanedlouho debutovat, stávající šifrovací technologie se mohou brzy stát zastaralými.

Možná je vám známa současná binární kombinace nul a jednotek, které tvoří elektronické a optické impulsy. Takto se vytvářejí, ukládají a přenášejí data na stávajících počítačích.

Kvantové výpočty na druhé straně namísto elektronů používají fotony nebo světelné částice, které lze nastavit na nulu, jednotku nebo obě zároveň – jednotku i nulu. Navíc, rychlost fotonu je 136krát vyšší než rychlost elektronu.

Tato přidaná flexibilita zahrnutí nuly i jednotky do téhož fotonu by umožnila kvantovým počítačům rychle kódovat a prolomit všechna možná řešení šifrování, čímž by se odstranila počítačová a online bezpečnost, jak ji již známe.

„Vývoj kvantových počítačů vytváří významnou hrozbu pro bezpečnost dat,“ varuje Callan.

„Jejich obrovský výpočetní výkon je schopen prolomit šifrování velkou rychlostí, takže důležitá data se stanou zranitelná – od údajů o bankovních účtech přes lékařské záznamy až po státní tajemství.“

Tento scénář je tak alarmující, že jej odborníci nazývají „kvantová apokalypsa“.

Callan pokračoval a vysvětlil, že kvantové výpočty budou také milionkrát rychlejší než „klasické počítače“ díky použití jednotek, nul nebo jednotek a nul současně – což je technologie známá jako „qubits“.

Když se to stane, bude to den Q – slovní hříčka výrazu „den D“ – ve kterém nastane to, že se všechna světová tajemství stanou zranitelná. Týká se to zejména vlád, které skrývají nejrůznější věci, o kterých nechtějí, aby se široká veřejnost dozvěděla.

Kvantové útoky nejsou věcí budoucnosti, dějí se již dnes

Bidenův režim v USA je jednou z takových vlád, která se obává kvantových počítačů, jelikož byla loni napadena kvantovým útokem.

Společnosti jako IBM a Google horečně pracují na vytvoření pokročilejších kvantových počítačů, ačkoli jejich masové rozšíření je ještě několik let vzdáleno – podle čínských expertů možná 8 až 20 let.

„Nedávné tvrzení, že výzkumníci prolomili šifrování, nás vyzývá, abychom se zamysleli, zda kvantová apokalypsa už náhodou nenastala,“ říká Callan.

„V současnosti však tento „přelom“ zůstává jen teoretický.“

Více článků, jako je tento, naleznete na stránce Collapse.news .

Autor: Ethan Huff, Zdroj: naturalnews.com

Sdílet:

Continue Reading

Previous Ivan Štubňa: Zvítězí v prezidentských volbách v ČR generál Pávek Čaputa?