Više od polovice najposjećenijih internetskih stranica na svijetu već je spremno za eru kvantnih računala, no Europa pritom znatno zaostaje za Amerikom, pokazalo je istraživanje objavljeno svega tri mjeseca prije isteka roka u kojem svaka država članica EU-a mora pripremiti plan za obranu svojih ključnih digitalnih mreža.
Kvantna računala su iznimno moćni strojevi koji, umjesto klasičnih bitova (0 ili 1), koriste kvantne kubite kako bi obrađivali podatke i rješavali složene zadatke u isto vrijeme, što im omogućuje da u nekoliko sekundi razbiju šifre za koje bi današnjim računalima trebale tisuće godina.

Navedeno istraživanje je provela američka tvrtka F5, jedan od vodećih svjetskih proizvođača mrežne sigurnosne opreme.

Analizirajući milijun najposjećenijih internetskih stranica, F5 je utvrdio da njih 54 posto podržava takozvanu postkvantnu kibernetičku sigurnost.

Međutim, zasluga za taj rezultat ne pripada samim organizacijama, već pružatelju mrežnih usluga Cloudflareu, koji je ovu zaštitu automatski uključio svim svojim korisnicima.

Bez stranica koje prolaze kroz njegovu mrežu, globalni udio zaštićenih stranica drastično pada na svega 22 posto.

Europsko zaostajanje zorno prikazuju i brojke: dok je u SAD-u osigurano 62 posto korporativnih stranica, u Francuskoj je to 39, a u Njemačkoj tek 36 posto.

Stručnjaci razlog vide u tome što se Europa radije oslanja na vlastite, lokalne poslužitelje umjesto na globalne cloud platforme. Najveći rizik pritom snose čuvari najosjetljivijih podataka – državni aparat i telekomi – čija zaštita iznosi skromnih 35 posto.

Prema europskom planu iz lipnja prošle godine, države moraju do 31. prosinca izraditi nacionalne planove, popisati što i gdje šifriraju te pokrenuti probne projekte.

Najvažniji sustavi, poput energetike, vode, zdravstva, prometa i financija, trebali bi biti zaštićeni najkasnije do kraja 2030., a ostatak do 2035., koliko god je to moguće.

Europa na prekretnici

Plan je zasad preporuka, a ne zakon, pa kazne za kašnjenje ne postoje. O prijedlogu se još pregovara u Europskom parlamentu i Vijeću EU-a, a nakon usvajanja države bi imale godinu dana da ga prenesu u svoje zakone.

Tema se tiče svakoga tko koristi mobitel, internetsko bankarstvo ili e-usluge. Zaštita koja čuva naše lozinke, novac, zdravstvene podatke i privatne poruke u velikoj je mjeri ista koju bi kvantna računala mogla razbiti. Ako se prijelaz ne obavi na vrijeme, ne prijeti samo državama i bankama nego svakome.

Politički pritisak raste. Potpredsjednica Europske komisije Henna Virkkunen rekla je kad je plan objavljen da je nova zaštita "ključna za visoku razinu kibernetičke sigurnosti".

Phoca PDF

Ravnatelj francuske agencije ANSSI Vincent Strubel najavio je da će od 2027. Francuska ocjenjivati samo sigurnosne proizvode s novom zaštitom, a od 2030. neće preporučivati kupnju proizvoda bez nje.

Podaci tvrtke F5 nisu jedini znak europskog zaostajanja. Procjena ENISA-e, europske agencije za kibernetičku sigurnost, na više od 1350 organizacija u 27 država pokazala je da je većina nespremna, a dio operatera u važnim sektorima uopće ne planira ulagati.

Njemačka agencija BSI skratila je procjenu opasnosti s 20 na 10 godina. Stefan-Lukas Gazdag, stručnjak za sigurnost u njemačkoj tvrtki Genua, rekao je prošlog ljeta da bi prvi napadi kvantnim računalima mogli biti mogući već krajem desetljeća.

Kvantni strojevi otključavaju prošlost

Gotovo cjelokupna internetska zaštita – od prepoznatljivog lokota u pregledniku do digitalnih potpisa – temelji se na složenim matematičkim zadacima koje današnja računala ne mogu riješiti u razumnom roku.

Međutim, dovoljno snažno kvantno računalo te bi prepreke svladalo s lakoćom. Zato postkvantna kriptografija donosi nove, napredne „brave“ koje besprijekorno rade na običnim računalima, a ostaju neprobojne čak i za kvantna računala.

Takav stroj danas ne postoji, ali opasnost je stvarna već sada. Napadači već danas mogu presretati i pohranjivati šifrirane podatke kako bi ih dešifrirali čim im kvantna tehnologija postane dostupna.

Olivier Daloy, stručnjak za sigurnost u tvrtki Zscaler, slikovito opisuje ovaj rizik: „Netko danas pošalje liječniku nalaz ili banci osjetljive podatke, i sve je pravilno šifrirano. Napadač to presretne i pohrani – trenutno ne može pročitati ništa, ali strpljivo čeka".

"Ako se prijelaz na novu zaštitu ne obavi na vrijeme, te bi podatke mogao otvoriti za deset ili petnaest godina. Zdravstveni nalaz, privatna poruka ili digitalni identitet i tada će biti itekako osjetljivi i podložni zloupotrebi, no stara ih zaštita više neće čuvati“, rekao je.

Radna skupina G7 za kibernetičku sigurnost i američka agencija CISA objavile su 3. rujna zajednički poziv da se s prijelazom krene odmah. Pišu da prijetnja više nije problem daleke budućnosti i da se tiče svih sektora.

Problem koji nadilazi krađu tajni

No, postoji i druga, jednako ozbiljna opasnost koja nadilazi samo krađu tajni.

Digitalni potpisi i certifikati služe kao digitalna osobna iskaznica – oni nam jamče s kim doista komuniciramo i potvrđuju da iza neke poruke ili softvera stoji legitimna banka, država ili proizvođač telefona.

Kada bi napadači uspjeli krivotvoriti te potpise, mogli bi bez problema preuzeti tuđi identitet,

Phoca PDF

podmetati zlonamjerna ažuriranja aplikacija ili krivotvoriti pravne ugovore.

Radna skupina G7 stoga izričito upozorava da bi napadači u tom scenariju mogli kompromitirati ključnu opremu, manipulirati podacima i potpuno urušiti digitalno povjerenje.

Upravo je na ovom polju napredak najsporiji. Prema podacima tvrtke F5, certifikata s novom zaštitom na javnom internetu danas praktički nema jer se regulatorna i tehnička pravila za njihovu primjenu još uvijek dovršavaju.

Za običnog građanina to donosi rizik od potpunog sloma povjerenja u ono što danas smatramo bezuvjetno sigurnim: internetsko bankarstvo, e-poštu i digitalne ugovore.

Google je u ožujku objavio da svoj prijelaz planira završiti do 2029., jer su kvantni strojevi napredovali brže od očekivanja, a Cloudflare je ubrzo postavio isti rok.

Razlog za uzbunu leži u matematici. Googleov znanstvenik Craig Gidney dokazao je da bi za razbijanje najraširenije svjetske šifre, RSA-2048, bio dovoljan kvantni stroj čak 20 puta manji (s manje od milijun bučnih kubita) nego što se dosad procjenjivalo.

Čak je i profesor Scott Aaronson sa Sveučilišta Teksas u Austinu, jedan od najvećih skeptika i kritičara prenapuhanih kvantnih obećanja, priznao da mu najugledniji stručnjaci za hardver sada potvrđuju kako bi stroj sposoban za takve napade mogao postati stvarnost oko 2029. godine.

Poznati kriptograf Filippo Valsorda zaključuje kako se predviđanja uvijek mogu pokazati pogrešnima, ali jednako tako mogu ubrzo postati i bolno točna – a to je rizik koji moderna digitalna infrastruktura više ne smije ignorirati.

Mogu li institucije stići na vrijeme?

Koliko je situacija alarmantna, najbolje pokazuje potez iz Washingtona. Američki predsjednik Donald Trump potpisao je dvije ključne uredbe. Prva pokreće ambiciozni nacionalni projekt s ciljem izgradnje kvantnog računala za znanstvena istraživanja već do 2028. godine.

Druga uredba postavlja rigorozne rokove za obranu: savezne agencije i sve privatne tvrtke koje rade za državu moraju svoje najosjetljivije sustave prebaciti na postkvantnu zaštitu do kraja 2030. godine, a nove digitalne potpise implementirati najkasnije do kraja 2031. Time je raniji rok iznenada skraćen za čak četiri godine.

Stručnjaci Cloudflarea, Sharon Goldberg i Vincent Voci, ocjenjuju da nametanje 2031. godine kao krajnjeg roka zorno pokazuje kako vlada u Washingtonu čvrsto vjeruje da bi opasni kvantni stroj mogao postati stvarnost upravo tada.

Nije riječ samo o bankama. Stručna skupina G7 za financije postavila je 2035. kao rok za dovršetak, a za najkritičnije sustave razdoblje od 2030. do 2032. Europski plan nabraja i vodu, energetiku, zdravstvo, promet i telekomunikacije.

To je u ovom opsegu teško dovršiti na vrijeme bez automatizacije. Građani sami ne mogu

Phoca PDF

zamijeniti šifre u bankama i bolnicama. Ali ovise o tome hoće li to napraviti institucije kojima povjeravaju podatke.

Zato je za Europu ključna provjera 31. prosinca, kad će se vidjeti koliko je država stvarno predalo plan. (H)

Phoca PDF