

SR / LEARNING SERIES

Uvod u postkvantnu bezbednost

Šta organizacije mogu odgovorno da urade danas

SCIENCE · TECHNOLOGY · TALENT · FUTURE

Nezavisna edukativna publikacija. Za istraživačke, inženjerske i bezbednosne odluke pojmove treba proveriti prema primarnim stručnim izvorima.

1. Rizik

Dovoljno sposoban kvantni računar sa korekcijom grešaka mogao bi Shorovim algoritmom da ugrozi RSA i kriptografiju eliptičkih krivih.

Tačan rok je neizvestan. Migracija je ipak važna jer danas prikupljeni šifrovani podaci mogu ostati osetljivi godinama.

KLJUČNI POJMOVI

Shorov algoritam • RSA • ECC • prikupi sada, dešifruj kasnije

2. Kriptografski inventar

Utvrdite gde se kriptografija javnog ključa koristi u aplikacijama, uređajima, sertifikatima, identitetima, lancu dobavljača i kod partnera.

Zabeležite algoritme, dužine ključeva, vlasnike sistema, vek podataka i ograničenja nadogradnje.

KLJUČNI POJMOVI

sredstva • algoritmi • vlasnici • vek podataka

3. Kriptoagilnost i migracija

Projektujte sisteme tako da se algoritmi i ključevi mogu menjati bez potpune rekonstrukcije proizvoda. Testirajte standardizovane postkvantne algoritme u kontrolisanim uslovima.

Ne izmišljajte sopstvenu kriptografiju. Planirajte interoperabilnost, performanse, sertifikate, hardversku podršku i ponašanje pri grešci.

KLJUČNI POJMOVI

kriptoagilnost • standardi • testiranje • interoperabilnost

4. Početni plan za 90 dana

Nedelje 1-3: odredite odgovornost i obuhvat. Nedelje 4-7: popišite kritične sisteme i dugovečne podatke. Nedelje 8-10: procenite rizike i zavisnosti. Nedelje 11-13: definišite pilot migracije.

KLJUČNI POJMOVI

odgovornost • inventar • prioriteti • pilot

Predlog za vežbu

Koristite interaktivne module na quantumserbia.com da proverite ideje iz vodiča. Pre svake simulacije zapišite predviđanje, zatim uporedite rezultat i objasnite razliku.