4 passaggi chiave per prepararsi alla crittografia post-quantistica

Si prevede che i progressi del calcolo quantistico renderanno gli standard di crittografia non sicuri già nel 2029.[1] Ciò significa che la crittografia resistente alla decrittografia basata sul calcolo quantistico diventerà presto una necessità per ogni azienda. Per affrontare questa minaccia incombente e gli attacchi "harvest now, decrypt later" che costituiscono già un rischio effettivo, Red Hat mette a disposizione quattro passaggi essenziali che permetteranno alla tua organizzazioni di prepararsi alla crittografia post-quantistica.

1 Valuta i dati sensibili della tua organizzazione e i protocolli crittografici esistenti

La fase preliminare alla preparazione per la crittografia post-quantistica prevede la valutazione delle vulnerabilità attuali dei dati aziendali.

La strategia più efficace per questo passaggio è disporre di un team interfunzionale (inclusi membri dei team operativi, legali e di conformità, IT e di ogni altro reparto interessato) che, con ruoli e competenze diverse, identifichi e tenga traccia di tutti i percorsi di accesso ai dati. Sulla base di questi risultati, i team possono iniziare a distinguere quali dati sono considerati sensibili nell'immediato, nel prossimo o nel lontano futuro.

Successivamente, è fondamentale fare un inventario dei protocolli crittografici attualmente in uso e valutare quali hanno più urgente bisogno di essere aggiornati, quali possono essere modificati e quali devono rimanere invariati a causa di limitazioni hardware o software.

2 Identifica le risorse a cui dare priorità

Con una chiara analisi dei dati sensibili aziendali, i team possono procedere a stabilire le priorità delle risorse da tutelare.

Non è pratico, men che meno realistico, affrontare contemporaneamente la sicurezza di tutte le varie risorse. Questo è il motivo per cui è essenziale adottare un approccio pragmatico alla pianificazione, attingendo alle informazioni acquisite dal lavoro preliminare già svolto dai team. In questo modo, è possibile valutare attentamente quali risorse e sistemi dovrebbero essere una priorità da affrontare fin da subito e quali possono essere gestiti in un secondo momento.

1 Horvath, Mark. "Inizia subito la transizione alla crittografia post-quantistica". Gartner, 30 settembre 2024

3 Inizia a testare nuovi algoritmi quantistici nel tuo ambiente

La maggior parte degli enti di conformità consiglia alle organizzazioni di avviare la migrazione ai nuovi algoritmi e protocolli crittografici post-quantistici il prima possibile; inclusi i primi standard finalizzati, pubblicati ad agosto 2024 dal National Institute of Standards and Technology (NIST).[2]

Per ottenere una migrazione efficace, è necessario che i team testino gli algoritmi e gestiscano da subito i problemi che potrebbero ostacolarla. Se l'azienda soddisfa pienamente i requisiti di conformità obbligatori, sarà in grado di mitigare i rischi legati agli attacchi "harvest now, decrypt later".

Per supportare la tua organizzazione nella fase di test dei nuovi algoritmi resistenti al calcolo quantistico, valuta la possibilità di adottare o eseguire l'upgrade a Red Hat® Enterprise Linux® 10. Questo sistema operativo include la prima versione di algoritmi resistenti al calcolo quantistico, tra cui OpenSSL, ML-KEM (FIPS 203) e ML-DSA (FIPS 204), che offrono scambio di chiavi, crittografia e firma con ulteriori funzionalità pianificate per le versioni future.

4 Avvia la transizione su larga scala e passa alla fase di produzione

Sebbene sia l'ultima fase di questo processo di transizione, l'implementazione di nuovi algoritmi resistenti ai calcoli quantistici è quella più complessa.

Per ottenere efficacia, la tua organizzazione deve affrontare questo passaggio in maniera graduale e costante, con l'obiettivo di sfruttare vantaggi a lungo termine.

L'aggiornamento di ogni algoritmo crittografico nell'ambiente non avviene immediatamente, ma le informazioni acquisite e le priorità identificate nei passaggi preliminari consentiranno alla tua organizzazione di raggiungere un successo sostenibile.

Quando si apportano le modifiche ai protocolli crittografici e si incorporano algoritmi resistenti al calcolo quantistico nella produzione, occorre prestare particolare attenzione alle interdipendenze identificate durante la fase di test per mitigare le conseguenze impreviste o i downtime.

Inizia subito a prepararti alla crittografia post-quantistica

Consulta questa pagina per scoprire come Red Hat Enterprise Linux 10 integra algoritmi resistenti al calcolo quantistico che aiutano la tua azienda a prepararsi alle sfide della crittografia post-quantistica.

---

2 "NIST Releases First 3 Finalized Post-Quantum Encryption Standards." National Institute of Standards and Technology, 13 agosto 2024.

ITALIA
it.redhat.com
italy@redhat.com

EUROPA, MEDIO ORIENTE, E AFRICA (EMEA)
00800 7334 2835
it.redhat.com
europe@redhat.com

facebook.com/RedHatItaly
twitter.com/RedHatItaly
linkedin.com/company/red-hat

it.redhat.com