Quatro etapas para você se preparar para a criptografia pós-quântica

Projeções indicam que, a partir de 2029, os avanços da computação quântica poderão comprometer a segurança dos padrões atuais de criptografia.[1] Por isso, em breve, todas as empresas precisarão usar criptografia resistente a ataques quânticos. Para lidar com a ameaça iminente e com os ataques do tipo "coletar agora, descriptografar depois", que já ocorrem hoje, sua organização deve considerar estas quatro etapas essenciais para se preparar para a criptografia pós-quântica.

1 Avalie os dados confidenciais da sua organização e os protocolos criptográficos existentes

A primeira etapa para se preparar para a criptografia pós-quântica é avaliar a vulnerabilidade dos dados que sua organização precisa proteger.

A melhor maneira de fazer isso é reunir uma equipe multifacetada, como representantes de operações de negócios, jurídico e de conformidade, TI e outros departamentos relevantes, para identificar e rastrear todos os caminhos de acesso a esses dados. Com essas informações, suas equipes podem classificar os dados confidenciais atuais e os que poderão ser em um futuro próximo ou distante, entre outras considerações.

Em seguida, é importante fazer um inventário dos protocolos criptográficos que sua organização tem em vigor e avaliar quais precisam de atualização mais urgente, quais podem ser modificados e quais devem permanecer os mesmos devido a limitações de hardware ou software.

2 Identifique quais recursos precisam ser priorizados

Agora que suas equipes têm uma compreensão clara dos dados confidenciais, você já pode começar a priorizar quais recursos precisam ser protegidos com mais urgência.

Garantir a segurança total de todos os ativos simultaneamente não é uma meta prática nem realista. É por isso que é crucial adotar uma abordagem pragmática de planejamento, aproveitando os insights obtidos no trabalho preliminar realizado por suas equipes e, assim, definir com cuidado quais ativos e sistemas devem ser priorizados imediatamente e quais podem ser tratados em uma etapa posterior.

1 Horvath, Mark. "Begin Transitioning to Post-Quantum Cryptography Now." Gartner, 30 de setembro de 2024

3 Comece a testar novos algoritmos com resistência quântica no seu ambiente

A maioria das entidades de conformidade já recomenda que as organizações comecem a migrar o quanto antes para novos algoritmos e protocolos criptográficos pós-quânticos, incluindo os primeiros padrões publicados em agosto de 2024 pelo National Institute of Standards and Technology (NIST).[2]

Quanto mais cedo suas equipes começarem a testar algoritmos e resolver problemas que possam impedir uma transição bem-sucedida, mais preparada sua organização estará para atender aos requisitos de conformidade que em breve serão obrigatórios, além de reduzir os riscos de "coletar agora, descriptografar depois".

Para começar a ajudar sua organização a testar novos algoritmos com resistência quântica, adote ou faça o upgrade para o Red Hat® Enterprise Linux® 10. Esse sistema operacional inclui o primeiro conjunto de algoritmos com resistência quântica, como OpenSSL, ML-KEM (FIPS 203) e ML-DSA (FIPS 204), que oferecem troca de chaves, criptografia e assinatura. Mais funcionalidades serão adicionadas em lançamentos futuros.

4 Inicie sua transição de forma escalável e comece a migrar para a produção

Embora seja a etapa final, a implementação de novos algoritmos com resistência quântica é a fase mais extensa e complexa de todo o processo.

Em vez de um sprint em busca de resultados imediatos, sua organização deve encarar essa etapa como um esforço contínuo, focado em benefícios de longo prazo.

A atualização de todos os algoritmos criptográficos no seu ambiente não acontecerá imediatamente, mas os insights obtidos e as prioridades definidas nas fases iniciais ajudarão a preparar sua organização para um sucesso duradouro.

Ao começar a aplicar mudanças nos protocolos criptográficos e integrar algoritmos com resistência quântica em produção, é fundamental estar atento às interdependências identificadas na fase de testes, para evitar consequências inesperadas ou tempo de inatividade.

Comece a se preparar para a criptografia pós-quântica.

Explore esta página para mais informações sobre como o Red Hat Enterprise Linux 10 incorpora algoritmos com resistência quântica que podem ajudar sua organização a se preparar para a era da criptografia pós-quântica.

---

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

Sobre a Red Hat

A Red Hat ajuda os clientes a definirem padrões entre diferentes ambientes e a desenvolver aplicações nativas em nuvem, além de integrar, automatizar, proteger e gerenciar ambientes complexos com serviços de consultoria, treinamento e suporte premiados.

facebook.com/redhatinc
@redhatbr
linkedin.com/company/red-hat-brasil

AMÉRICA LATINA
+54 11 4329 7300
latammktg@redhat.com

BRASIL
+55 11 3629 6000
marketing-br@redhat.com

br.redhat.com