DELL Technologies

Criptografia pós-quântica

Começar

Introdução

A computação quântica está impulsionando uma reformulação fundamental da tecnologia, criando oportunidades incríveis e novos desafios. Embora esse futuro seja empolgante, ele representa uma ameaça significativa aos sistemas criptográficos que protegem nosso mundo digital.

Por que a computação quântica está em ascensão?

Os computadores convencionais, sejam eles notebooks, smartphones ou servidores, processam informações usando bits, que existem em um estado de zero ou um. Esse modelo binário impulsionou décadas de progresso, mas limita a forma como as informações podem ser representadas e manipuladas. Os computadores quânticos usam qubits, que podem existir em vários estados simultaneamente por meio de princípios como superposição e emaranhamento. Isso permite que as máquinas quânticas explorem um grande número de soluções possíveis em paralelo, proporcionando uma vantagem computacional para classes específicas de problemas.

O que é criptografia pós-quântica?

A criptografia pós-quântica (PQC) refere-se a uma nova geração de algoritmos projetados para proteger sistemas digitais contra ataques clássicos e quânticos. Ao contrário da distribuição de chaves quânticas, que requer hardware especializado, o PQC foi projetado para ser executado na infraestrutura clássica atual — servidores, endpoints, redes — tornando-o a maneira mais prática e escalável de se preparar para a era quântica.

Quais são os riscos imediatos que as organizações enfrentam com a computação quântica?

As consequências vão muito além do risco teórico. As organizações que não conseguem se preparar enfrentam a exposição de propriedade intelectual confidencial, interrupção de sistemas financeiros, violações de dados de saúde e ameaças à segurança nacional.

A ameaça "Coletar agora, descriptografar depois" aumenta a urgência: os adversários só precisam capturar dados criptografados hoje e esperar pelos meios para descriptografá-los. Quando os computadores quânticos criptograficamente relevantes chegarem, o dano já será irreversível.

"Harvest Now, Decrypt Later" ou "Coletar agora, descriptografar depois", também conhecido como "Record Now, Decrypt Later" (Gravar agora, descriptografar depois), é o ato de adversários coletarem e armazenarem dados criptografados hoje com a intenção de descriptografá-los no futuro assim que os computadores quânticos criptograficamente relevantes estiverem disponíveis.

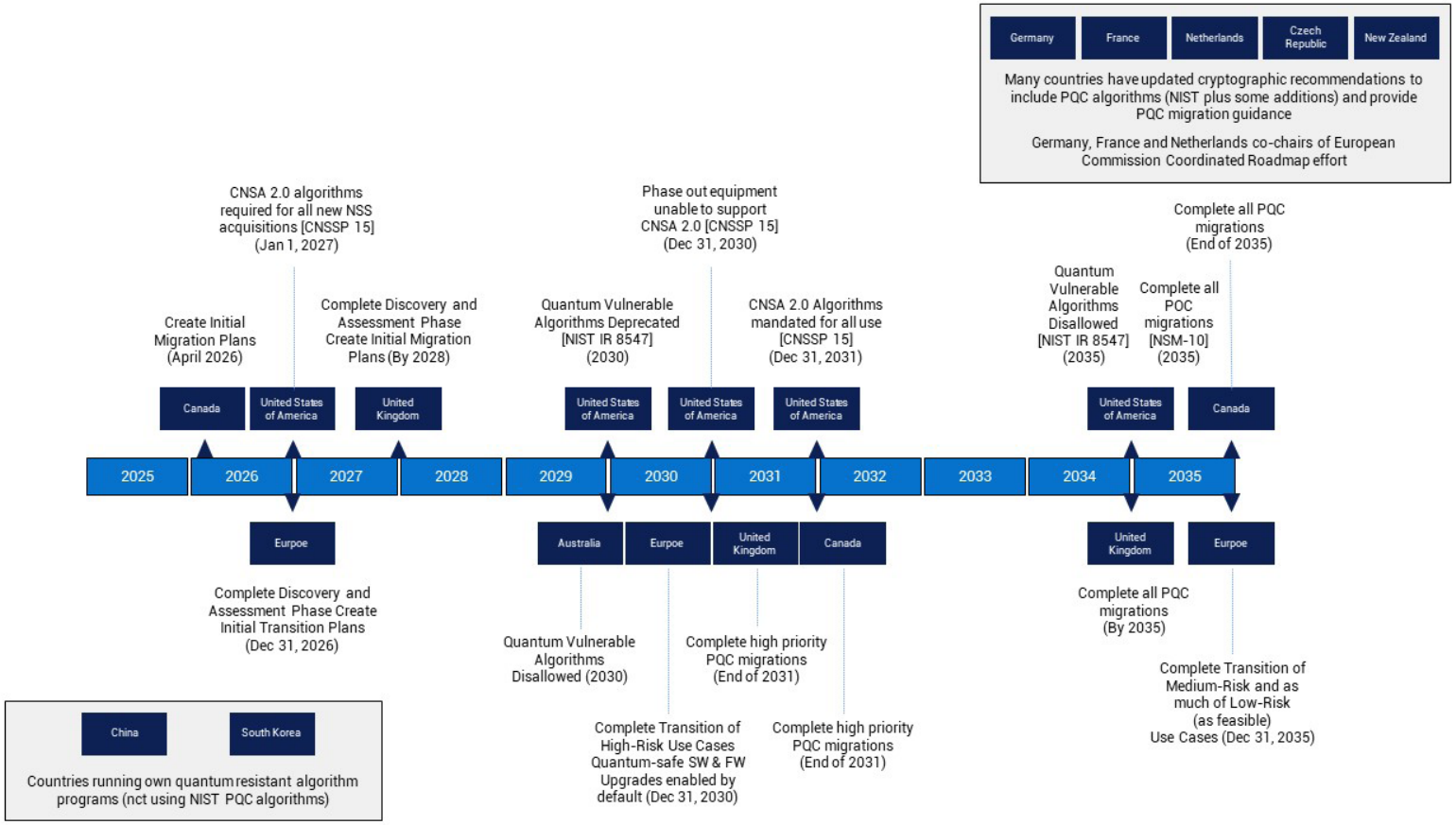
Como as organizações devem se preparar para a transição para o PQC?

A jornada para um futuro seguro em termos quânticos é uma maratona, não uma corrida de velocidade, e uma jornada em constante evolução. Uma abordagem proativa, em camadas e faseada ajudará sua organização a gerenciar riscos, alinhar recursos e construir uma postura de segurança resiliente a longo prazo. A Dell fornece as tecnologias e orientações de que você precisa em todas as etapas. A seguir, estão os principais passos para orientar sua organização na criação de um plano de transição para o PQC.

Cronograma de transição do PQC

Ao reconhecer a urgência da ameaça, os governos e órgãos de padronização fizeram do PQC uma prioridade global. Ao perceber a importância de adotar algoritmos criptográficos resistentes à computação quântica, o governo federal dos EUA começou a emitir requisitos de PQC para agências federais. Entre eles, estão o Memorando de segurança nacional 10 (NSM-10), o Conjunto de algoritmos de segurança nacional comercial (CNSA 2.0), o Memorando 23-02 do Escritório de gestão e orçamento (OMB M-2302) e o Relatório interagências 8547 do Instituto nacional de padrões e tecnologia (NIST IR 8547), entre outros.

Outras organizações em todo o mundo também definiram diretrizes para a transição de PQC. Essas datas não são arbitrárias — elas refletem os prazos de entrega necessários para reprojetar, validar e implementar criptografia em ecossistemas complexos de TI. As empresas devem vê-los como mais do que mandatos governamentais; eles são indicadores práticos da mudança global em direção à resiliência quântica. Abaixo estão alguns dos diferentes mandatos de países.



Inventário e auditoria de ameaças criptográficas

A primeira prioridade é compreender o seu panorama criptográfico atual. Esta etapa fundamental orienta toda a sua estratégia de migração.

Boa higiene da segurança

O primeiro passo para se preparar para o futuro quântico é reforçar as defesas já existentes. As organizações devem utilizar práticas recomendadas sólidas de higiene de segurança, como impor o acesso com privilégios mínimos, implementar a autenticação baseada em vários fatores e manter o gerenciamento rigoroso de patches. Também há duas outras considerações. Pode ser importante desativar a criptografia mais fraca para que novos sistemas com criptografia mais forte possam interoperar com sistemas legados. Para sistemas mais recentes, também é importante aumentar o nível mínimo de segurança — AES-256 para criptografia simétrica e SHA-384 ou superior para resumos — a fim de combater as margens reduzidas introduzidas pelo algoritmo de Grover. Essas medidas não apenas reduzem o risco de hoje, mas também minimizam o acúmulo de dívida criptográfica que, de outra forma, complicaria a migração de amanhã.

Inventário e auditoria de ativos criptográficos

A base de qualquer plano de migração é a visibilidade. As organizações devem realizar um inventário criptográfico abrangente, identificando onde e como a criptografia de chave pública é usada em aplicativos, dispositivos e fluxos de trabalho. Isso inclui certificados TLS, VPNs, sistemas de e-mail, mecanismos de assinatura de código, dados do cliente, dados arquivados e muito mais. Uma vez identificados, os ativos devem ser priorizados com base na importância, na sensibilidade e na vida útil dos negócios. Dados de longa duração, como prontuários médicos ou arquivos confidenciais, devem ser tratados com a máxima urgência, pois são os mais vulneráveis à ameaça de "Coletar agora, descriptografar depois".

Piloto e experimento com a PQC

Com um inventário claro, é possível começar a testar tecnologias prontas para PQC e validar seu desempenho e integração.

Assim que o cenário criptográfico for compreendido, as organizações devem começar a testar soluções de PQC em ambientes controlados. Ao testar essas soluções em laboratórios, as equipes de TI podem validar o desempenho, a interoperabilidade e a capacidade de gerenciamento antes da implementação em larga escala. Criando agilidade criptográfica - a capacidade de alternar algoritmos criptográficos sem reformular sistemas inteiros, é fundamental para a resiliência a longo prazo e a facilidade de migração.

Adote uma abordagem de interoperabilidade

À medida que os padrões PQC amadurecem, você pode começar a planejar o lançamento da produção. Uma abordagem híbrida fornece uma ponte para um ambiente totalmente seguro em termos quânticos.

À medida que os padrões amadurecem, um modelo híbrido fornece uma ponte para o futuro. Muitos fornecedores já estão oferecendo suporte a cipher suites híbridos que combinam algoritmos clássicos e resistentes à computação quântica em uma única implementação. Essa abordagem dupla proporciona continuidade de proteção, mesmo que um algoritmo seja comprometido posteriormente. As empresas devem começar a adotar estratégias híbridas agora, alinhando seus cronogramas internos com marcos e roteiros do produto de seu fornecedor de infraestrutura. Isso garante que, à medida que os algoritmos resistentes à computação quântica atingem a padronização, as organizações possam escalar a adoção sem interrupções.

Execute a migração completa e a validação contínua

O objetivo final é uma empresa totalmente integrada, continuamente validada e com segurança quântica.

Execute a migração completa e a validação contínua

O objetivo final é uma transição completa para PQC em toda a empresa. Isso não será um evento isolado, mas um processo contínuo de validação e adaptação. As organizações devem executar planos detalhados de migração, incorporando a PQC em todas as camadas de sua pilha de TI, enquanto testam continuamente novos padrões e implementações. Ao usar uma abordagem híbrida de computadores quântico-clássicos, os clientes podem simular cenários de ataque, validar a integridade criptográfica e garantir que seus sistemas permaneçam resilientes contra ameaças em evolução.

Colaboração e compartilhamento de conhecimento

Nenhuma organização deve enfrentar esse desafio sozinha.

Os consórcios do setor, pesquisadores acadêmicos e agências governamentais estão reunindo conhecimento para acelerar a transição para PQC. A participação em grupos de padronização, grupos de trabalho e programas piloto permite que as empresas se mantenham alinhadas com as melhores práticas e os requisitos emergentes. O envolvimento ativo da Dell em iniciativas como o projeto PQC do NCCoE da NIST garante que nossos clientes se beneficiem diretamente dessa experiência coletiva.

Conclusão

A era quântica não é mais uma possibilidade distante; é uma realidade iminente que exige uma ação inovadora hoje. Preparar-se para essa mudança tecnológica é um imperativo estratégico para proteger seu ativo mais valioso: seus dados. Como destacamos, uma abordagem em fases, que vai do inventário e auditoria à migração completa, é o caminho mais claro para um futuro seguro contra a computação quântica.

A mudança para PQC será uma das mudanças de infraestrutura mais significativas em décadas. Essa transição afeta quase todos os aspectos de TI, desde servidores e armazenamento até endpoints, plataformas de nuvem e protocolos de rede. O sucesso requer previsão, planejamento e execução disciplinada. Na Dell Technologies, vemos que o caminho a seguir é uma jornada em fases: que equilibra melhorias imediatas de segurança com a prontidão em longo prazo para a adoção da PQC.

A Dell está preparada para ajudar você com sua estratégia de implementação de PQC. Recomendamos um plano de migração por fases e descrevemos um conjunto de atividades para ajudar você a criar estratégias, planejar, executar e monitorar sua transição para PQC.