DELL Technologies

Cryptographie post-quantique

Démarrer

Introduction

L'informatique quantique entraîne une refonte fondamentale de la technologie, créant à la fois d'incroyables opportunités et de nouveaux défis. Cette nouvelle évolution passionnante introduit néanmoins une menace importante pour les systèmes cryptographiques qui protègent notre monde numérique.

Pourquoi l'informatique quantique est-elle en plein essor ?

Les ordinateurs classiques, qu'il s'agisse d'ordinateurs portables, de smartphones ou de serveurs, traitent les informations sous forme de bits (0 et 1). Ce modèle binaire a alimenté des décennies de progrès, mais il limite la façon dont l'information peut être représentée et manipulée. Les ordinateurs quantiques utilisent des qubits, qui peuvent exister dans plusieurs états simultanément grâce à des principes tels que la superposition et l'enchevêtrement. Cela permet aux machines quantiques d'explorer un grand nombre de solutions possibles en parallèle, offrant ainsi un avantage de calcul pour des classes spécifiques de problèmes.

Qu'est-ce que la cryptographie post-quantique ?

La cryptographie post-quantique (PQC) désigne une nouvelle génération d'algorithmes conçus pour sécuriser les systèmes numériques contre les attaques classiques et quantiques. À la différence de la distribution de clés quantiques (qui nécessite du matériel spécialisé), la PQC est conçue pour fonctionner sur l'infrastructure classique actuelle (serveurs, terminaux, réseaux), ce qui en fait le moyen le plus pratique et évolutif de se préparer à l'ère quantique.

Quels risques immédiats les entreprises encourent-elles face à l'informatique quantique ?

Les conséquences vont bien au-delà du risque théorique. Les entreprises incapables de se préparer sont exposées à des problèmes de propriété intellectuelle sensibles, à des perturbations des systèmes financiers, à des violations des données de santé et à des menaces pour la sécurité nationale.

La stratégie « Récolter maintenant, déchiffrer plus tard » aggrave l'urgence : les adversaires capturent les données chiffrées dès aujourd'hui, puis attendent simplement les moyens de les déchiffrer. Dès que les ordinateurs quantiques cryptographiquement pertinents arriveront sur le marché, les dégâts seront déjà irréversibles.

« **Récolter maintenant, déchiffrer plus tard** » (Harvest Now, Decrypt Later, ou HNDL) désigne l'action par laquelle les acteurs malveillants collectent et stockent, dès aujourd'hui, des données chiffrées dans le but de les déchiffrer plus tard, lorsque les ordinateurs quantiques cryptographiquement pertinents seront disponibles.

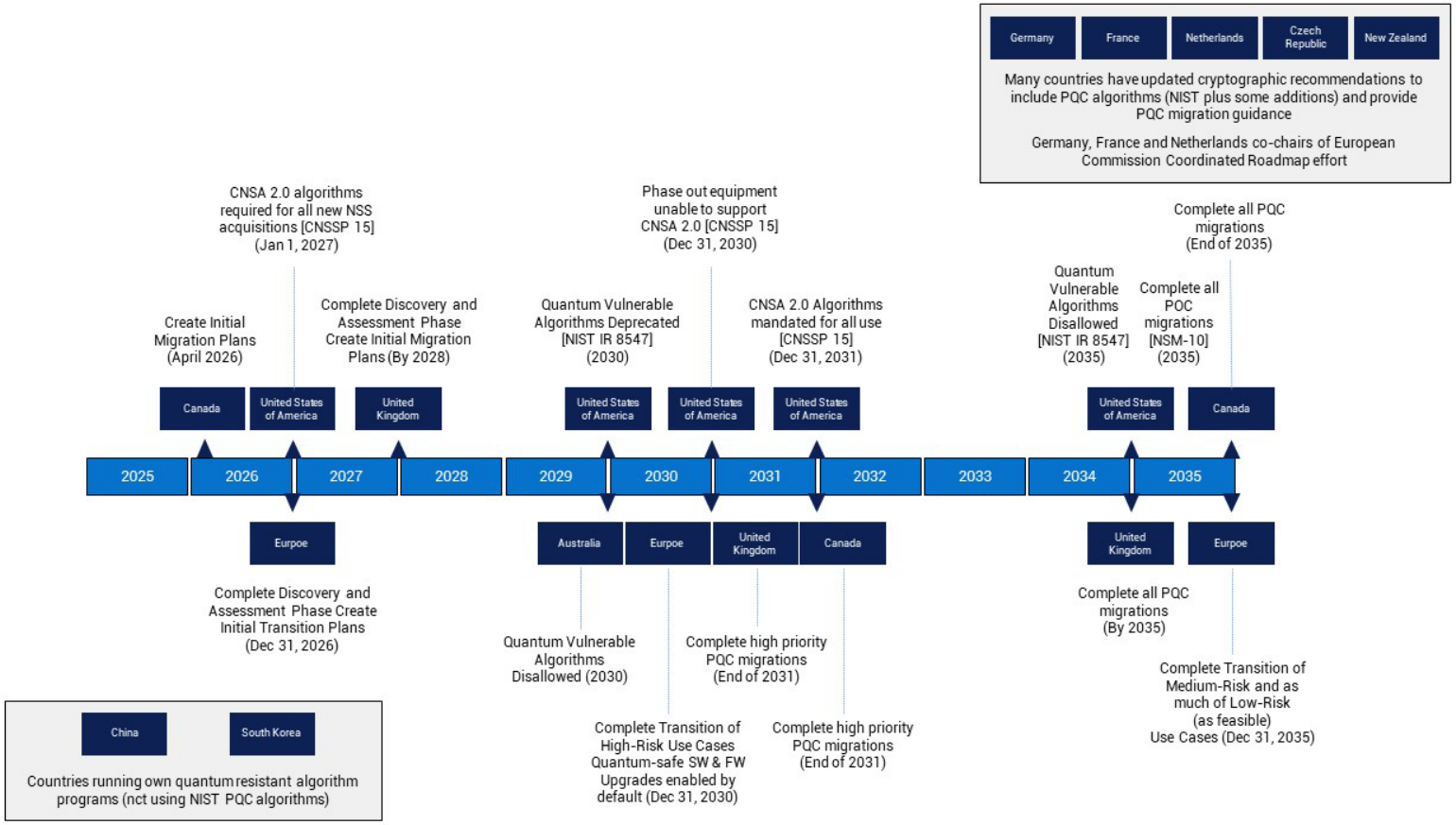
De quelle façon les entreprises doivent-elles se préparer à la transition vers la cryptographie post-quantique (PQC) ?

Loin d'être un sprint, le parcours vers un avenir sûr quantique est une aventure évolutive sur le long terme. Une approche proactive, multiniveaux et par étapes aidera votre entreprise à gérer les risques, à aligner les ressources et à établir une posture de sécurité résiliente dans la durée. Dell fournit les technologies et les conseils nécessaires pour vous aider à chaque étape. Voici les étapes clés qui vous aideront à guider votre entreprise dans la création d'un plan de transition vers la PQC.

Calendrier de transition vers la PQC

Conscients de l'imminence de la menace, les gouvernements et les organismes de normalisation ont fait de la PQC une priorité mondiale. Compte tenu de l'importance de l'adoption d'algorithmes de chiffrement résistants aux menaces quantiques, le gouvernement fédéral américain a commencé à émettre des exigences PQC auprès des agences fédérales. Ces exigences comprennent, entre autres, la directive NSM-10 (National Security Memorandum 10), la suite CNSA 2.0 (Commercial National Security Algorithm Suite 2.0), l'OMB M-2302 (Office of Management and Budget Memorandum 23-02) et le rapport NIST IR 8547 (National Institute of Standards and Technology Interagency Report 8547).

D'autres organisations dans le monde ont également établi des directives pour la transition vers la PQC. Ces dates ne sont pas arbitraires, mais reflètent les délais requis pour reconcevoir, valider et déployer la cryptographie dans des écosystèmes IT complexes. Les entreprises doivent les considérer non pas comme de simples mandats gouvernementaux, mais comme des indicateurs pratiques de la transition mondiale vers la résilience quantique. Vous trouverez ci-dessous quelques exemples de mandats nationaux.



Inventaires et audits face aux menaces cryptographiques

La priorité absolue consiste à comprendre votre environnement cryptographique actuel. Cette étape fondamentale définit l'ensemble de votre stratégie de migration.

Bonne hygiène de sécurité

La première étape de la préparation de l'avenir quantique consiste à renforcer les défenses déjà en place. Les entreprises doivent appliquer de strictes pratiques d'excellence en matière d'hygiène de sécurité, telles que l'application d'un accès du moindre privilège, la mise en œuvre d'une authentification multifacteur et la gestion rigoureuse des correctifs. Deux autres considérations sont également essentielles. Il peut être important de désactiver la cryptographie plus faible afin que les nouveaux systèmes dotés d'une cryptographie plus élevée puissent interagir avec les systèmes existants. Il est également important, pour les systèmes plus récents, de renforcer la sécurité minimale (AES-256 pour la cryptographie symétrique, SHA-384 ou supérieure pour les condensés, ou « digests ») afin de contrer les marges réduites introduites par l'algorithme de Grover. Ces mesures réduisent non seulement les risques actuels, mais aussi le retard de dette cryptographique qui viendrait compliquer la migration future.

Inventaire et audit des actifs cryptographiques

La visibilité est la pierre angulaire de tout plan de migration. Les entreprises doivent effectuer un inventaire cryptographique complet, en identifiant où et comment la cryptographie à clé publique est utilisée dans les applications, les périphériques et les workflows. Cela inclut les certificats TLS, les VPN, les systèmes de messagerie électronique, les mécanismes de signature de code, les données archivées, etc. Une fois identifiés, les actifs doivent être hiérarchisés selon leur importance stratégique, leur sensibilité et leur durée de vie. Les données à long terme (telles que les dossiers médicaux ou les archives classifiées) doivent être traitées en priorité, car elles sont les plus vulnérables à la menace « Récolter maintenant, déchiffrer plus tard ».

Piloter et expérimenter avec la PQC

À l'aide d'un inventaire clair, vous pouvez commencer des expériences pratiques avec des technologies compatibles avec la PQC pour valider les performances et l'intégration.

Une fois le paysage cryptographique pleinement compris, les entreprises doivent commencer à tester les solutions de PQC dans des environnements contrôlés. En pilotant ces solutions dans des laboratoires, les équipes IT peuvent valider leurs performances, leur interopérabilité et leur facilité de gestion avant un déploiement à grande échelle. Développer cette agilité cryptographique (c'est-à-dire la possibilité de changer d'algorithmes cryptographiques sans remanier des systèmes entiers) est essentiel pour la résilience à long terme et la facilité de migration.

Adopter une approche d’interopérabilité

À mesure que les normes de la PQC gagnent en maturité, vous pouvez commencer à planifier les déploiements en production.
Une approche hybride offre une transition vers un environnement entièrement sécurisé.

À mesure que les normes évoluent, un modèle hybride ouvre la voie vers l’avenir. De nombreux fournisseurs prennent déjà en charge des suites de chiffrement hybrides qui combinent des algorithmes classiques et résistants aux quanta en une seule implémentation. Cette double approche assure la continuité de la protection même si un algorithme est compromis par la suite. Dès maintenant, les entreprises doivent commencer à adopter des stratégies hybrides, tout en alignant leur calendrier interne sur les feuilles de route et les étapes de leur fournisseur d’infrastructure. À mesure que les algorithmes quantiquement sûrs sont standardisés, les entreprises peuvent ainsi faire évoluer leur adoption sans interruption.

Exécuter une migration complète et une validation continue

L'objectif ultime est une entreprise entièrement intégrée et validée en permanence, capable de résister aux attaques quantiques.

Exécuter une migration complète et la validation continue

L'objectif ultime est une transition complète vers la PQC dans l'ensemble de l'entreprise. Il ne s'agira pas d'un événement ponctuel mais d'un processus continu de validation et d'adaptation. Les entreprises doivent mettre en œuvre des plans de migration détaillés, en intégrant la PQC dans chaque couche de leur infrastructure IT, tout en testant continuellement les nouvelles normes et mises en œuvre. À l'aide d'une approche hybride combinant ordinateurs classiques et quantiques, les clients peuvent simuler des scénarios d'attaque, valider l'intégrité cryptographique et s'assurer que leurs systèmes restent résistants aux menaces en constante évolution.

Collaboration et partage des connaissances

Aucune entreprise ne doit relever ce défi seule.

Des consortiums industriels, des chercheurs universitaires et des organismes gouvernementaux mutualisent leurs connaissances pour accélérer la transition vers la PQC. La participation à des groupes de normalisation, des groupes de travail et des programmes pilotes permet aux entreprises de rester alignées sur les meilleures pratiques et les exigences émergentes. L'implication active de Dell dans des initiatives telles que le projet PQC du NIST NCCoE garantit que nos clients bénéficient directement de cette expertise collective.

Conclusion

L'ère quantique n'est plus une possibilité lointaine mais une réalité imminente, qui exige dès aujourd'hui une action tournée vers l'avenir. Face à ce changement technologique, une bonne préparation est un impératif stratégique pour protéger vos ressources les plus précieuses : vos données. Comme nous l'avons mentionné plus haut, une approche progressive (inventaire et audit, puis migration complète) représente la voie la plus claire vers un avenir sûr.

La transition vers la PQC représentera l'un des changements d'infrastructure majeurs depuis plusieurs décennies. Cette transition affecte presque tous les aspects de l'IT, des serveurs et du stockage aux terminaux, en passant par les plates-formes Cloud et les protocoles réseau. La réussite exige prévoyance, planification et exécution rigoureuse. Chez Dell Technologies, la voie à suivre prend la forme d'une transition progressive, qui assure l'équilibre entre des améliorations immédiates de la sécurité et une préparation à long terme pour l'adoption de la PQC.

Dell est prêt à vous aider à déployer votre stratégie d'implémentation de la PQC. Outre notre plan de migration progressive, nous avons défini un ensemble d'activités pour vous aider à élaborer des stratégies, planifier, exécuter et surveiller votre migration vers la PQC.