



Comment préparer votre organisation à la sécurité post-quantique ? Un guide pratique étape par étape

02 juillet 2026, 09:00

Farhad Aghili

Ludwig De Loch

De l'inventaire à la feuille de route : 5 étapes vers une organisation prête pour l'ère quantique

Dans un [précédent article](#), nous avons expliqué pourquoi les organisations doivent déjà se préparer à la sécurité post-quantique. L'arrivée d'ordinateurs quantiques cryptographiquement pertinents reste incertaine. En revanche, la préparation de cette transition peut prendre plusieurs années. Une migration complète n'est pas encore nécessaire aujourd'hui. Vous pouvez toutefois déjà prendre des mesures concrètes pour limiter les risques futurs. En identifiant où la cryptographie est utilisée et comment vos systèmes peuvent évoluer, vous rendrez la transition vers la sécurité post-quantique beaucoup plus maîtrisable.

Étape 1 : dressez l'inventaire de votre cryptographie

Une migration réussie commence par une bonne visibilité. De nombreuses organisations ne savent pas précisément où la cryptographie est utilisée ni quels systèmes reposent sur des algorithmes vulnérables. Commencez donc par identifier les domaines où la cryptographie intervient, par exemple dans :

- Les produits
- Les systèmes
- Les protocoles de communication
- Les dépendances logicielles
- Les certificats et les infrastructures PKI
- Les composants embarqués

Cet inventaire constitue la base de toutes les étapes suivantes.



Étape 2 : identifiez les systèmes critiques à longue durée de vie

Tous les systèmes ne nécessitent pas le même niveau de priorité. Commencez par ceux qui resteront opérationnels pendant de nombreuses années ou qui sont difficiles à modifier. Il peut s'agir, par exemple, de systèmes qui :

- Resteront en service pendant de nombreuses années
- Sont difficiles à mettre à jour à distance
- Présentent un coût de remplacement élevé
- Sont essentiels à vos activités

Plus un système reste en service longtemps, plus il est important d'anticiper dès aujourd'hui les futures migrations cryptographiques.

Étape 3 : évaluez la crypto-agilité de vos systèmes

La crypto-agilité est une caractéristique essentielle des systèmes conçus pour durer. Elle désigne la capacité à remplacer des algorithmes cryptographiques sans devoir repenser l'ensemble du système. Vérifiez notamment :

- Quels mécanismes cryptographiques peuvent être remplacés facilement
- Quels composants dépendent fortement d'algorithmes spécifiques
- Dans quelle mesure l'architecture actuelle est modulaire

Plus votre architecture est flexible, plus les futures migrations seront simples à réaliser.

Étape 4 : cartographiez les dépendances

La cryptographie ne se limite pas à vos propres logiciels. Elle est souvent intégrée à des composants et à des services externes. Il est donc essentiel d'avoir une vue d'ensemble de toutes les dépendances. Examinez notamment :

- Les fournisseurs
- Les logiciels tiers
- Les plateformes cloud
- Les écosystèmes industriels

Ces dépendances détermineront en grande partie la complexité de votre future migration.

Étape 5 : élaborer une feuille de route de migration

La transition vers l'ère post-quantique n'est pas un projet ponctuel. C'est un processus de longue durée qui demande de définir des priorités, d'assurer une gouvernance adaptée et de prendre des décisions par étapes. Une feuille de route vous aide à hiérarchiser les actions, à gérer les risques et à répartir les investissements. Vous pouvez ainsi préparer la migration progressivement, sans perturber vos activités.



Développez ensemble des compétences pratiques

La cryptographie post-quantique reste un domaine de recherche très actif. Dans le même temps, de nombreuses organisations recherchent des recommandations concrètes, adaptées aux environnements industriels réels. Les principales questions portent sur :

- Les stratégies de migration
- L'impact sur les intégrations
- La crypto-agilité
- Les contraintes des systèmes embarqués et des environnements OT
- La gestion du cycle de vie
- La faisabilité opérationnelle

Les organisations ont également besoin de méthodes concrètes pour cartographier leurs dépendances cryptographiques, évaluer les différentes options de migration et mesurer leur impact dans des environnements opérationnels réels. Pour accompagner cette transition, Sirris étudie comment des méthodologies pratiques, des activités de validation et une expertise appliquée peuvent aider les entreprises belges à préparer leur migration vers les technologies post-quantiques dans des contextes industriels réalistes.

L'objectif n'est pas d'imposer des technologies ou des fournisseurs spécifiques. Il s'agit d'aider les organisations à comprendre les enjeux, à évaluer leur niveau de préparation et à identifier les étapes les plus pertinentes. À mesure que les systèmes résistants aux attaques quantiques deviennent une réalité, l'apprentissage collectif et l'expérimentation pratique joueront un rôle essentiel pour accompagner l'industrie dans cette transition.

Commencez à vous préparer dès aujourd'hui

Vous souhaitez mieux comprendre les conséquences de la transition post-quantique pour vos produits, vos systèmes ou votre infrastructure numérique ? Vous voulez savoir quelles mesures concrètes prendre dès aujourd'hui ? Sirris accompagne les entreprises dans l'évaluation des risques, l'exploration des trajectoires de migration et le développement de compétences pratiques pour renforcer durablement leur cyberrésilience.

[Contactez-nous](#)

Cet article fait partie d'une série de deux articles consacrés à la sécurité post-quantique.

Partie 1 : [La sécurité post-quantique commence par la migration, pas par les ordinateurs quantiques](#)

Partie 2 : Comment préparer votre organisation à la sécurité post-quantique ? Un guide pratique étape par étape ?

Auteurs



Farhad Aghili



Ludwig De Locht