



La sécurité post-quantique commence par la migration, pas par l'informatique quantique.

02 juillet 2026, 10:00

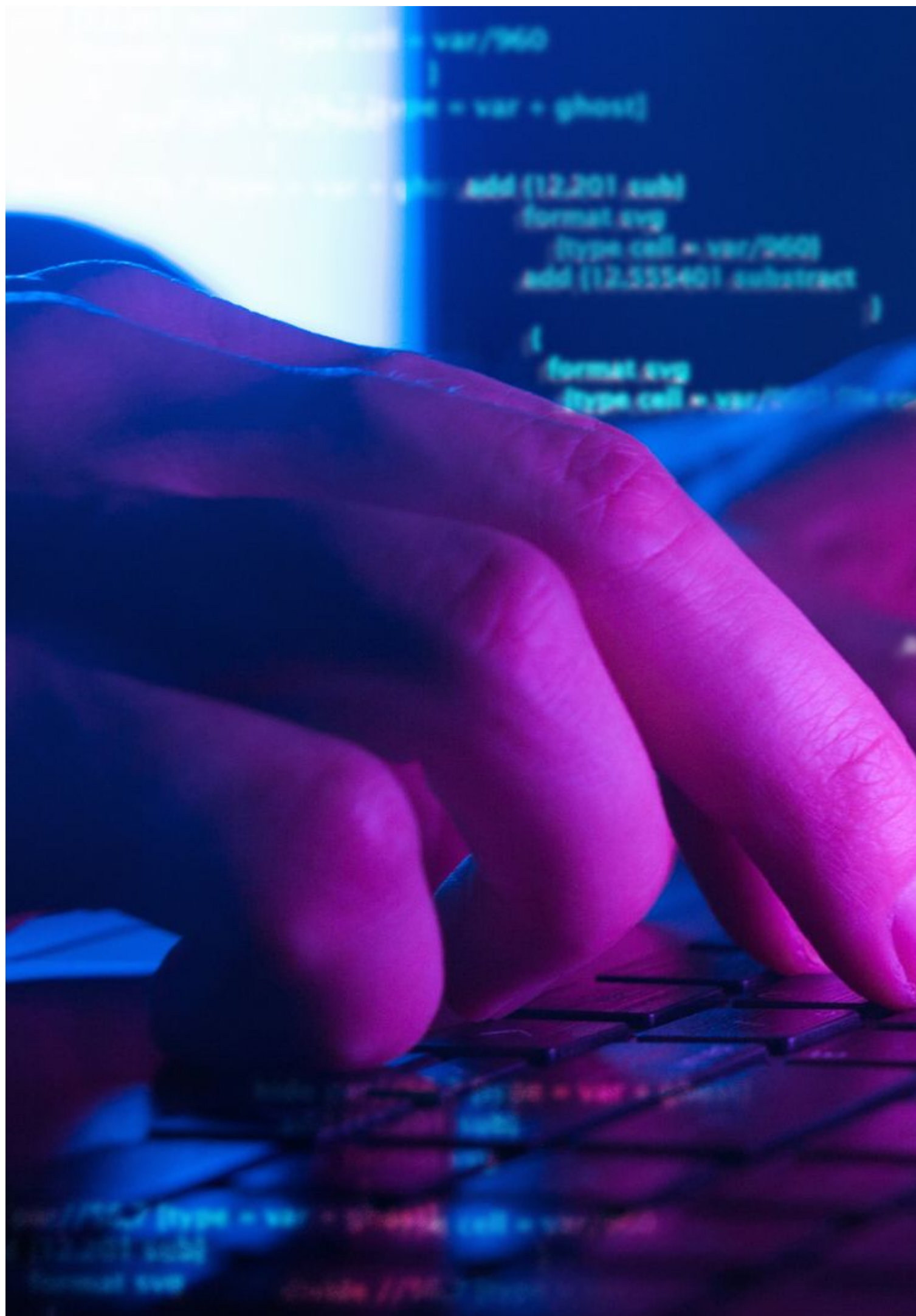
Farhad Aghili

Ludwig De Loch

Pourquoi vous devez vous préparer bien avant le « Q-day »

Beaucoup d'organisations considèrent encore la sécurité post-quantique comme un sujet pour demain. Les ordinateurs quantiques cryptographiquement pertinents (Cryptographically Relevant Quantum Computers ou CRQC), capables de casser la cryptographie à clé publique actuelle, n'existent pas encore à l'échelle industrielle. Personne ne sait non plus quand le « Q-day » arrivera. Pourtant, la vraie question n'est pas de savoir quand ces ordinateurs apparaîtront. Elle est de savoir comment vous pouvez préparer une transition qui prendra plusieurs années.

Les produits connectés, les systèmes industriels et les plateformes numériques restent souvent en service pendant des décennies. Avec le Cyber Resilience Act (CRA) et NIS2, la sécurité devient aussi une responsabilité sur tout le cycle de vie. La sécurité post-quantique devient donc un défi de migration, d'architecture et d'organisation. Et ce défi commence dès aujourd'hui.



Pourquoi la sécurité post-quantique compte déjà

Presque toutes les organisations utilisent aujourd'hui la cryptographie à clé publique, comme RSA et ECC. Elle protège les applications logicielles, les produits connectés, les systèmes industriels, les environnements cloud, les protocoles de communication, les identités et les infrastructures de certificats. Les ordinateurs quantiques menacent une partie de cette base. Dès que des CRQC assez puissants seront disponibles, ils devraient casser de nombreux mécanismes à clé publique utilisés aujourd'hui. Le calendrier exact reste incertain. Mais cette incertitude ne justifie pas d'attendre. La transition n'est plus un simple scénario théorique. Les premières normes de cryptographie post-quantique ont déjà été publiées.

Le scénario « harvest now, decrypt later » mérite une attention particulière. Des données sensibles et chiffrées peuvent déjà être collectées aujourd'hui. Elles pourraient ensuite être déchiffrées plus tard, lorsque la technologie quantique aura progressé. Pour les organisations qui traitent des données confidentielles à long terme, le risque de divulgation future existe donc déjà.

Un autre défi tient à la longue durée de vie des systèmes numériques. De nombreux produits et infrastructures développés ou déployés aujourd'hui seront encore actifs lorsque les menaces quantiques deviendront réelles. Cela concerne les machines industrielles, les produits connectés, les objets IoT, les environnements OT, les systèmes embarqués et les plateformes logicielles à longue durée de vie. Plus un système reste en service, moins vous avez de temps pour organiser une migration fluide.



La migration est le vrai défi

Les discussions sur la sécurité post-quantique se concentrent souvent sur les nouveaux algorithmes et les nouvelles normes cryptographiques. En réalité, la technologie ne représente qu'une partie du défi. Le vrai enjeu consiste à comprendre où la cryptographie est utilisée, à quel point elle est intégrée dans vos systèmes et comment vous pouvez les faire évoluer sans perturber vos activités. De nombreuses organisations se posent déjà des questions très concrètes:

- Où la cryptographie est-elle utilisée dans nos systèmes?
- Quels composants dépendent de mécanismes vulnérables?
- Quels mécanismes devront peut-être être remplacés demain?
- Quels fournisseurs introduisent des dépendances cryptographiques?
- Les systèmes peuvent-ils être mis à jour à distance?
- Quels sont les risques opérationnels de la migration?
- Quel sera l'impact sur les performances ou l'interopérabilité?

Ces questions dépassent la seule cryptographie. Elles touchent à l'architecture des systèmes, à la gestion du cycle de vie logiciel et à l'ingénierie système. Le premier défi consiste donc à savoir précisément où la cryptographie est utilisée. Elle est souvent intégrée plus profondément que vous ne le pensez. Vous pouvez la retrouver dans les piles de communication, les middlewares, les infrastructures PKI, les modules matériels de sécurité, les firmwares, les logiciels tiers et les services cloud. Une migration se résume donc rarement au remplacement d'un algorithme. Elle demande une planification, une priorisation et une exécution progressive.

Chaque secteur rencontre ses propres défis

Produits connectés, machines et systèmes embarqués

Pour les organisations qui développent des produits connectés, des machines industrielles ou des solutions IoT, les limites liées au cycle de vie représentent souvent le plus grand défi. Beaucoup de ces systèmes:

- Restent en service pendant de nombreuses années
- Disposent de ressources de calcul limitées
- Sont difficiles à mettre à jour
- Dépendent de capacités matérielles fixes
- Impliquent plusieurs fournisseurs et protocoles

Dans ces environnements, la préparation à l'ère post-quantique dépend de plusieurs facteurs: la capacité de mise à jour, la crypto-agilité, les architectures modulaires et une conception pensée pour tout le cycle de vie. L'objectif ne consiste pas seulement à sécuriser les systèmes aujourd'hui. Vous devez aussi veiller à ce qu'ils puissent évoluer en toute sécurité au fil du temps. Cela devient encore plus important avec le Cyber Resilience Act. Ce règlement renforce les responsabilités tout au long du cycle de vie des produits numériques.

Fournisseurs SaaS et plateformes numériques

Les fournisseurs SaaS disposent souvent d'une plus grande flexibilité pour mettre leurs systèmes à jour. Pourtant, ils doivent eux aussi relever plusieurs défis. Les principaux points d'attention sont:

- La confidentialité à long terme des données clients
- Les dépendances cryptographiques dans les environnements cloud
- La gestion des identités et des certificats
- Les intégrations avec des services externes
- Les exigences de conformité et de confiance

Pour les organisations actives dans la santé, la finance, l'énergie ou les infrastructures critiques, ces sujets gagnent en importance. La préparation à l'ère post-quantique devient peu à peu un élément des stratégies plus larges de résilience et de confiance.

Entreprises manufacturières et exploitants industriels

Les entreprises industrielles ne développent pas toujours elles-mêmes les technologies sous-jacentes. Elles dépendent toutefois fortement des infrastructures numériques et des environnements de production connectés. Elles doivent donc composer avec des systèmes hérités, des cycles de remplacement très longs, des dépendances vis-à-vis des fournisseurs et une visibilité limitée sur les technologies intégrées qui soutiennent leurs opérations.

De nombreux environnements industriels n'ont jamais été conçus pour offrir une crypto-agilité ou faciliter une future migration cryptographique. À mesure que la connectivité augmente, il devient essentiel de savoir où la cryptographie est utilisée. Il est tout aussi important de comprendre dans quelle mesure vos activités en dépendent.



Vous ne devez pas remplacer toute votre cryptographie dès aujourd'hui. En revanche, c'est le bon moment pour identifier où elle est utilisée et à quoi pourrait ressembler une future migration. Lorsque la sécurité post-quantique deviendra indispensable, la préparation fera toute la différence.

Par où commencer concrètement ? Dans le prochain article, nous présenterons les étapes que vous pouvez déjà suivre pour préparer votre organisation à la migration vers la sécurité post-quantique.

[Lire l'article suivant](#)

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