

Préparation d'Echoworx à la cryptographie post-quantique

Echoworx reconnaît les risques émergents en matière de cybersécurité associés aux avancées de l'informatique quantique et prépare activement sa plateforme pour la transition vers la cryptographie post-quantique (CPQ). Grâce à une évaluation complète de notre architecture cryptographique, nous avons établi une feuille de route alignée sur les normes industrielles et les meilleures pratiques pour l'adoption de technologies cryptographiques résistantes au quantum.

Notre objectif est d'assurer la protection à long terme des communications des clients tout en maintenant la sécurité, la fiabilité et l'interopérabilité que les organisations attendent de la plateforme Echoworx.

Posture de sécurité actuelle

Echoworx emploie des contrôles cryptographiques conformes aux normes industrielles pour protéger les communications des clients et les informations sensibles. Nous avons évalué les principaux chemins de communication cryptographiques à travers notre plateforme, notamment :

- Les flux de livraison de messages sécurisés
- Les services de confiance basés sur des certificats
- L'infrastructure de gestion des clés
- Les services cryptographiques de support

Cette évaluation nous a permis d'identifier les domaines qui nécessiteront en définitive une migration vers la cryptographie résistante au quantum, à mesure que les normes mûrissent et que le support de l'écosystème devient largement disponible.

Notre stratégie post-quantique

L'approche d'Echoworx en matière de cryptographie post-quantique repose sur quatre principes clés :

Agilité cryptographique

Notre plateforme est conçue pour soutenir l'évolution des normes cryptographiques, permettant l'adoption de nouveaux algorithmes et de nouvelles technologies de sécurité avec un minimum de perturbations pour les clients et les intégrations.

Cryptographie hybride

Echoworx prévoit d'adopter des approches cryptographiques hybrides qui combinent la cryptographie classique établie avec des algorithmes post-quantiques. Cette approche offre une sécurité solide tout en maintenant la compatibilité avec les technologies existantes et les écosystèmes industriels.

Alignement sur les normes

Notre feuille de route s'aligne sur les normes industrielles émergentes, notamment les normes de cryptographie post-quantique publiées par le National Institute of Standards and Technology (NIST) des États-Unis, ainsi que sur les développements connexes au sein des organismes de normalisation de la sécurité d'Internet et de la messagerie.

Préparation de l'écosystème

Nous introduisons des capacités post-quantiques en alignement avec la maturité de l'écosystème technologique plus large, notamment les plateformes cloud, les autorités de certification, les clients de messagerie, les navigateurs et les bibliothèques cryptographiques. Cette approche garantit l'interopérabilité et minimise les risques pendant la transition.

Domaines d'intérêt

La cryptographie post-quantique traite principalement les vulnérabilités de la cryptographie à clé publique (par exemple RSA et ECC), couramment utilisée pour l'échange de clés, les signatures numériques et les services de confiance basés sur des certificats. Ce sont les domaines dans lesquels un ordinateur quantique suffisamment puissant pourrait potentiellement affaiblir les protections cryptographiques actuelles.

Notre feuille de route post-quantique inclut l'adoption de capacités résistantes au quantum à travers les technologies de sécurité clés utilisées au sein de la plateforme, notamment :

- Les communications protégées par TLS
- La messagerie sécurisée basée sur PGP
- Les services de certificats et de confiance S/MIME

Ces capacités seront introduites selon une approche progressive qui donne la priorité à la sécurité des clients, à la compatibilité et à la stabilité opérationnelle.

Les messages PDF protégés par mot de passe reposent sur le chiffrement AES pour protéger le contenu des documents et ne constituent donc pas un axe prioritaire de notre feuille de route post-quantique.

Les messages portail utilisent à la fois AES (chiffrement symétrique) et S/MIME. Bien que le contenu des messages soit finalement protégé par le chiffrement AES, le flux de traitement global des messages portail intègre le chiffrement basé sur S/MIME et les services de gestion des clés de support dans le cadre de l'architecture de traitement et de stockage des messages. Par conséquent, des éléments du flux de traitement des messages portail sont inclus dans notre évaluation plus large de la préparation post-quantique et notre feuille de route.

Ce que cela signifie pour les clients

Les clients n'ont aucune action à entreprendre pour le moment.

Echoworx continue de surveiller les développements en matière de cryptographie post-quantique et se prépare activement à l'adoption de technologies résistantes au quantum, à mesure que les normes industrielles et les écosystèmes de support mûrissent. Notre objectif est de fournir une transition transparente qui renforce la sécurité à long terme sans perturber les flux de travail, les intégrations ou les expériences utilisateur existants des clients.