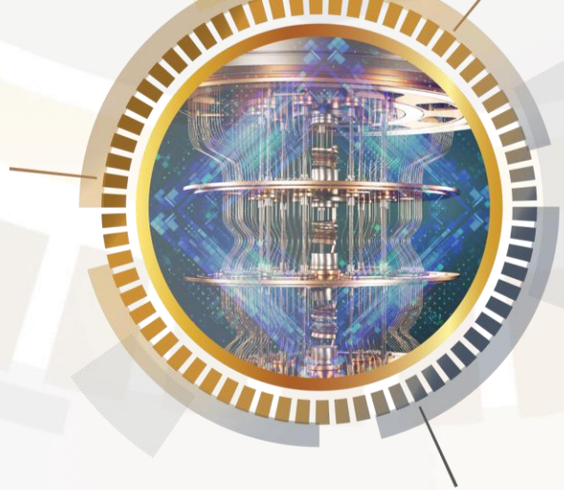
Deloitte.

Perspectives et Actions

Transition Cyber Post-Quantique : la résilience dans l'ère quantique



Les technologies quantiques ont le potentiel d'accélérer l'atteinte des objectifs de votre entreprise. Par exemple, elles permettront des simulations avancées et l'utilisation de capacités de détection et d'analyses approfondies. Cependant, elles comportent également des risques majeurs, dont la possibilité pour des attaquants d'exploiter la grande puissance des futurs ordinateurs quantiques pour déchiffrer vos données les plus sensibles.

Une certitude demeure : le meilleur moment pour se préparer, c'est aujourd'hui. Nos experts sont là pour vous guider à chaque étape, de la qualification et compréhension des risques, à la préparation de votre transition et l'accompagnement dans l'entrée dans l'ère quantique, en toute confiance.

5 choses à savoir

1. **Les ordinateurs quantiques menacent la sécurité de vos données.** Aujourd'hui, les données sont protégées principalement grâce au chiffrement et des milliers d'années sont nécessaires à les déchiffrer avec la puissance de calcul actuelle. Mais il a été démontré que quelques secondes suffiront aux ordinateurs quantiques.
2. **La menace existe déjà.** On ne sait pas exactement quand des ordinateurs quantiques suffisamment puissants seront disponibles. Cependant des attaques visant à s'approprier vos données les plus sensibles ont déjà lieu. Les données volées seront déchiffrées avec des ordinateurs quantiques le moment venu.
3. **Se préparer va prendre beaucoup de temps.** Les précédentes mises à niveau cryptographiques majeures ont pris au moins une décennie, telles que la migration du standard 3DES au standard AES. S'y prendre trop tard vous fait courir le risque d'un niveau de chiffrement devenu obsolète.
4. **Le Législateur va agir.** Il exigera des chiffrements résistants aux attaques quantiques une fois que les nouveaux standards algorithmiques nécessaires seront finalisés. Aux Etats-Unis, les agences fédérales ont déjà été sommées de se préparer à migrer leurs mécanismes de chiffrement.
5. **Agir en premier peut constituer un avantage concurrentiel.** Démarrer votre transition vers la sécurité post-quantique peut être un atout d'image auprès des clients soucieux que leurs données sensibles soient entre de bonnes mains. Il peut également renforcer votre leadership dans le domaine, avec des concurrents qui suivront.

5 actions à entreprendre

1. **Formez vos équipes et sensibilisez-les** aux risques cyber posés par les ordinateurs quantiques et aux raisons d'agir dès maintenant. Cette sensibilisation doit s'adresser à toute votre organisation, avec une sollicitation particulière des échelons de Direction pour leur soutien et les budgets nécessaires à la transition.
2. **Faites l'inventaire de vos données à risque.** Identifiez les données sensibles à long terme dans votre entreprise, puis évaluez si elles sont protégées par des outils et standards cryptographiques qui deviendront obsolètes avec l'émergence d'ordinateurs quantiques suffisamment puissants.
3. **Examinez vos mécanismes de gouvernance et répertoriez les lacunes** affectant votre capacité à modifier vos algorithmes cryptographiques, telles que les politiques et responsabilités associées. Elles seront essentielles quand il s'agira de déployer les nouveaux algorithmes post-quantiques.
4. **Réalisez un pilote pour tester le déploiement des algorithmes post-quantiques.** Cela vous donnera un aperçu des défis à venir lors d'un déploiement à grande échelle, comme les problématiques imprévues, les dépendances, etc. mais aussi les facteurs-clés de succès.
5. **Contactez notre équipe d'experts** pour faire un premier pas vers la résilience. Une évaluation des risques quantiques peut vous aider à comprendre vos risques et vous fournir une approche pragmatique pour aller de l'avant.

En savoir plus

Transition Cyber Post-Quantique | Deloitte

Vos contacts

Imade Elbaraka
Leader Cyber France et Afrique Francophone
Associé
ielbaraka@deloitte.fr

Tamim Khoder
Leader Cyber Technologies Emergentes
Directeur
tkhoder@deloitte.fr

Yoann Viaouët
Deputy Leader Cyber Technologies Emergentes
Senior Manager
yviaouet@deloitte.fr

Auteurs

Colin Soutar
Leader mondial Cyber Post-Quantique
Managing Director
csoutar@deloitte.com

Itan Barmes
Leader programme Cyber Post-Quantique
Specialist Leader
ibarmes@deloitte.nl