Quantum readiness is a migration programme

Quantum security and cryptographic transition — technical reading

Le risque quantique est souvent présenté comme une compétition entre machines nouvelles et chiffrement ancien. Pour un décideur, le problème immédiat est ailleurs : la cryptographie est dispersée dans des systèmes qu’aucune équipe ne connaît totalement. Certificats, accès distants, équipements embarqués, mises à jour, signatures, identités et archives suivent des cycles de remplacement très différents.

Le premier livrable utile n’est pas la promesse d’un avantage quantique, mais une carte des dépendances cryptographiques reliée à la criticité des services et à la durée de confidentialité des données. Une archive devant rester protégée vingt ans mérite un examen différent d’une session de quelques minutes. Un équipement non actualisable crée déjà un risque d’achat.

Le programme classe les dépendances selon protocoles, algorithmes, gestion des clés, propriétaires, contraintes matérielles et engagements des fournisseurs. Viennent ensuite les essais de solutions hybrides ou post-quantiques sur un périmètre maîtrisé : compatibilité, performance, tailles des certificats, latence, reprise, interopérabilité et retour arrière.

La propriété décisive est l’agilité cryptographique : pouvoir remplacer un algorithme ou un prestataire sans reconstruire tout le service. Les nouveaux marchés doivent donc exiger des inventaires lisibles, des composants actualisables, des durées de support et des plans de migration démontrables.

La préparation quantique est une discipline d’ingénierie et d’achat bien avant de devenir un projet de matériel spécialisé. Elle aboutit à un portefeuille de migration ordonné et vérifiable.