Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS

Office fédéral de la cybersécurité (OFCS)
Analyse et prévention

15 novembre 2024

Évaluation par l'OFCS

Cryptographie post-quantique et mesures à envisager

L'OFCS veut pouvoir faire face au développement des superordinateurs quantiques, ainsi qu'aux répercussions possibles sur les procédés et algorithmes cryptographiques déjà utilisés. Il a ainsi publié des Considérations technologiques sur l'ordinateur quantique et la cryptographie post-quantique (CPQ). La situation et la nécessité d'agir qui en découle peuvent être résumées comme suit:

- Les ordinateurs quantiques représentent un danger pour la sécurité de certains procédés et algorithmes cryptographiques[1]. Toutefois, les spécialistes ne s'accordent pas sur la possibilité de construire un ordinateur quantique super puissant, ni sur le moment où cette technologie pourrait arriver à maturité.
- En attendant, la CPQ a permis de développer des procédés et des algorithmes capables de résister aux ordinateurs quantiques. Les normes de cryptographie telles que standardisées par le National Institute of Standards and Technology (NIST) aux États-Unis ont bien des chances de s'imposer au niveau international.
- Dès que ces nouveaux algorithmes seront disponibles, il sera judicieux d'anticiper les problèmes en envisageant et en planifiant à moyen terme une migration[2] des algorithmes existants vers des algorithmes CPQ pour accroître la protection contre les risques.
- Alors que les fabricants et les fournisseurs peuvent concevoir et réaliser eux-mêmes cette planification pour leurs produits informatiques, les organisations sont dépendantes de ces mêmes fabricants et fournisseurs et doivent convenir avec eux d'un plan de migration pour chaque produit.
- Les organisations qui ne peuvent planifier elles-mêmes la migration ont la possibilité de recourir à des partenaires externes ayant l'expertise nécessaire. Elles veilleront à choisir un partenaire qui connaît bien leurs activités et leur infrastructure informatique.

[1] Il s'agit surtout de procédés et d'algorithmes cryptographiques issus de la cryptographie asymétrique (ou cryptographie à clé publique).

[2] L'idéal pour effectuer une telle migration est de recourir à une approche hybride en combinant des algorithmes classiques et des algorithmes CPQ, qui se complètent mutuellement.