Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS
Analyse und Prävention

15. November 2024

Einschätzung BACS

Handlungsbedarf im Zusammenhang mit Post-Quanten-Kryptografie (PQK)

Vor dem Hintergrund der laufenden Bemühungen zum Bau von hinreichend grossen Quantencomputern und den möglichen Auswirkungen auf heute im Einsatz stehende kryptografische Verfahren und Algorithmen hat das BACS eine Technologiebetrachtung über Quantencomputer und Post-Quanten-Kryptografie (PQK) verfasst. Die Situation und der sich daraus ergebende Handlungsbedarf lässt sich folgendermassen zusammenfassen:

- Quantencomputer stellen für die Sicherheit von bestimmten kryptografischen Verfahren und Algorithmen eine Gefahr dar.[1] Allerdings ist sich die Fachwelt nicht einig, ob und ab wann hinreichend grosse Quantencomputer effektiv gebaut werden können.
- In der Zwischenzeit werden Quantencomputer-resistente Verfahren und Algorithmen als Post-Quanten-Kryptografie (PQK) entwickelt und vom U.S. amerikanischen National Institute of Standards and Technology (NIST) standardisiert. Die sich abzeichnenden Standards werden mit hoher Wahrscheinlichkeit auf internationaler Ebene übernommen.
- Sobald diese Algorithmen als Alternativen zur Verfügung stehen, ist es sinnvoll, eine Migration[2] von bestehenden auf PQK-Algorithmen anzudenken und mittelfristig zu planen, um von stärkeren Algorithmen und einem Umsetzen sowohl aus Risikosicht als auch aus proaktiver Sicht profitieren zu können.
- Während die Hersteller und Lieferanten diese Planung für ihre IT-Produkte selbständig angehen und durchführen können, sind Organisationen auf sie angewiesen und müssen produktspezifische Migrationspläne mit ihnen abgleichen.
- Kann eine Organisation eine solche Migrationsplanung nicht «in-house» durchführen, stehen externe Partner mit entsprechendem Fachwissen zur Verfügung. Allerdings sollte dann bei der Auswahl eines Partners darauf geachtet werden, dass dieser sowohl das Geschäft der Organisation als auch deren IT-Infrastruktur gut kennt.

[1] Betroffen sind insbesondere kryptografische Verfahren und Algorithmen aus dem Bereich der asymmetrischen (Public Key) Kryptografie.

[2] Für die Migration bieten sich hybride Betriebsmodi an, im Rahmen derer klassische und PQC-Algorithmen kombiniert und komplementär eingesetzt werden.