Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence, Civil Protection and Sport DDPS

National Cyber Security Centre NCSC
Analysis and Prevention

15 November 2024

NCSC assessment

Action required in relation to post-quantum cryptography (PQC)

In light of ongoing efforts to build sufficiently large quantum computers and the impact this may have on current cryptographic procedures and algorithms, the NCSC has produced a technology brief on quantum computers and post-quantum cryptography (PQC). The situation and the action required can be summarised as follows:

- Quantum computers pose a threat to the security of certain cryptographic procedures and algorithms.[1] However, there is no consensus among experts as to whether and when it will actually be possible to build sufficiently large quantum computers.
- In the meantime, quantum computer-resistant procedures and algorithms are being developed as PQC and standardised by the National Institute of Standards and Technology (NIST) in the US. The emerging standards are very likely to be adopted at international level.
- Once these algorithms are available as alternatives, it is advisable to consider migrating[2] from existing algorithms to PQC variants in the medium term. This will harness the benefits of stronger algorithms, while also enabling a risk-aware, proactive approach to implementation.
- While manufacturers and suppliers can initiate and carry out planning for their IT products independently, organisations are dependent on these vendors and must coordinate product-specific migration plans with them.
- If an organisation cannot plan its migration in-house, external partners with the relevant expertise are available. However, when selecting a partner, care should be taken to ensure that they are familiar with the organisation's business and IT infrastructure.

[1] Cryptographic procedures and algorithms relating to asymmetric (public key) cryptography are particularly affected.

[2] Hybrid operating models, in which classic and PQC algorithms are combined and used in tandem, are ideal for migration.