Securing Tomorrow, Today: Transitie naar Post-Quantumcryptografie

Een gezamenlijk statement van partners uit 18 EU lidstaten:

Secure Information Technology Center Austria, Centre for Cybersecurity Belgium, National Cyber and Information Security Agency Czech Republic, Centre for Cyber Security Denmark, Information System Authority Estonia, Finnish transport and Communication Agency, French National Agency for the Security of Information Systems, Federal Office for Information Security Germany, National Cyber Security Authority Hellenic Republic, National Cyber Security Centre Ireland, National Cybersecurity Agency Italy, Ministry of Defense Latvia, National Cyber Security Centre Ministry of Defense Lithuania, High Commission for National Protection Luxemburg, Netherlands National Communication Security Agency, Ministry of Interior and Kingdom Relations Netherlands and National Cyber Security Centre Ministry of Security and Justice Netherlands; Research and Academic Research Center Poland, Government Information Security Office Slovenia, National Cryptologic Center Spain

Bundesamt für Sicherheit in der Informationstechnik

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

A-SIT
Secure Information Technology Center - Austria
Zentrum für sichere Informationstechnologie - Austria

CENTRE FOR CYBERSECURITY BELGIUM

National Cyber and Information Security Agency

CENTRE FOR CYBER SECURITY

REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

TRAFICOM
Finnish Transport and Communications Agency

National Cyber Security Authority
HELLENIC REPUBLIC

NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT

Ministry of Defence
Republic of Latvia

NATIONAL CYBER SECURITY CENTRE

MINISTRY OF NATIONAL DEFENCE
REPUBLIC OF LITHUANIA

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

National Cyber Security Centre
Ministry of Security and Justice

NASK

REPUBLIC OF SLOVENIA
GOVERNMENT INFORMATION SECURITY OFFICE
URSIV

CCN
centro criptológico nacional

Dit document is een Nederlandse vertaling vanuit het oorspronkelijke Engelse document

Securing Tomorrow, Today: Transitie naar Post-Quantumcryptografie

Asymmetrische cryptografie is essentieel voor de veiligheid van een breed scala aan diensten met een directe impact op ons dagelijks leven. Voorbeelden hiervan zijn het overmaken van geld van een bankrekening, het ondertekenen van een digitaal contract, het gebruiken van slimme apparaten voor in huis, en het gebruiken van communicatiediensten zoals berichtenapps. Als de huidige asymmetrische protocollen gekraakt kunnen worden, zouden de gevolgen voor onze openbare digitale infrastructuur verwoestend zijn. Deze dreiging voor cryptografie wordt gevormd door de ontwikkeling van een grootschalige fouttolerante quantumcomputer, die door het algoritme van Shor traditionele asymmetrische cryptografische protocollen gebaseerd op bijvoorbeeld RSA of elliptische kromme-cryptografie (ECC) kan kraken. Hoewel dergelijke cryptografisch relevante quantumcomputers (CRQC) momenteel niet beschikbaar zijn, gaat de ontwikkeling erg snel [1].
Hierom is het **noodzakelijk dat voorbereiding op de quantumdreiging een essentieel onderdeel wordt van risicobeheer op het gebied van cyberveiligheid**. In een poging om het risico te kwantificeren heeft Quantum Threat Timeline in 2023 [2] een enquête gehouden onder 37 internationale toonaangevende specialisten uit de academische wereld en het bedrijfsleven. 17 van hen denken dat de kans dat een CRQC binnen 10 jaar wordt ontwikkeld, hoger is dan 5%. Bovendien schatten 10 van de ondervraagden in dat die waarschijnlijkheid 50% of hoger is.

Meerdere goed bestudeerde alternatieven van post-quantumcryptografie (PQC) voor op dit moment gebruikte kwetsbare cryptografie, zijn al gestandaardiseerd of klaar om gestandaardiseerd te worden[1], en klaar voor gebruik in productie. Voor verdere diepgaande aanbevelingen en details verwijzen we naar [3,4,5,6,7,8]. Deze alternatieven zijn echter relatief nieuw en de ervaringen met de toepassingen en cryptoanalyse worden nog verder ontwikkeld. Daarom raden we u sterk aan om **PQC in hybride oplossingen te gebruiken** voor de meeste use-cases, bijvoorbeeld door een ingezet cryptografisch protocol zo met PQC te combineren dat de combinatie veilig blijft, zelfs als een van de onderdelen gekraakt wordt.

De twee grootste bedreigingscenario's zijn:

- **het *store-now-decrypt-later*-scenario**, waarbij aanvallers versleutelde data opslaan om deze te ontcijferen wanneer een CRQC beschikbaar wordt. Dit vormt een dreiging als de vertrouwelijkheid van data voor langere tijd gewaarborgd moet worden, bijvoorbeeld gevoelige persoonsgegevens of bedrijfsgeheimen;

- **lange migratieperiodes**, bijvoorbeeld voor complexe systemen zoals asymmetrische infrastructuur (*public key infrastructure*, PKI) of apparaten met een lange gebruiksduur. Zelfs als een systeem niet getroffen wordt door voortdurende aanvallen, zoals in het eerste scenario, ontstaat er nog steeds het risico dat de overgang naar quantumveilige cryptografie niet op tijd voltooid kan worden. Dit brengt de vertrouwelijkheid en authenticiteit van alle communicatie in gevaar.

We verzoeken het openbaar bestuur, leveranciers van vitale infrastructuren, IT leveranciers, en het gehele bedrijfsleven met klem om **een topprioriteit te maken van de transitie naar post-quantumcryptografie**. Om bovengenoemde redenen zouden alle organisaties en overheden **nu**

[1] Protocollen voor PQC-handtekeningalgoritmen voor een specifiek doeleinde zijn al een tijd beschikbaar, waardoor post-quantum firmware en software updates mogelijk zijn. Het NIST heeft nieuwe protocollen voor post-quantum sleuteluitwisseling en handtekeningalgoritmen gepubliceerd op 13 augustus 2024. Aanvullende PQC-protocollen van het NIST en andere SDO's, in het bijzonder ISO, en RFC's van het IETF worden binnenkort verwacht.

moeten beginnen met de transitie door te werken aan de volgende stappen (voor verdere details verwijzen we naar [5] en [6]).

- Voer een analyse voor de quantum-dreiging uit die bestaat uit een inventarisatie van de onderdelen die beschermd moeten worden en de applicaties die gebruikmaken van cryptografie;
- Ontwikkel een risicogerichte routekaart voor de uitvoering van de transitie, met inachtneming van de gevoeligheid en de beschermingstermijn van de informatie, evenals de noodzaak om *store-now-decrypt-later*-aanvallen tegen te gaan en systemen met een lange levensduur te beschermen tegen de quantum-dreiging ruim voordat de dreiging verwezenlijkt wordt. De overgang zou ook rekening moeten houden met crypto-agility, zodat een bestendigere overgang naar PQC kan plaatsvinden;
- Plan de migratie, inclusief een prioritering, waar alle noodzakelijke bedrijfsprocessen en de begroting van de migratie in worden meegenomen;
- Bevorder de voortzetting van uitgebreid onderzoek naar Post-Quantumcryptografie en standaardisatiepogingen.

Het is belangrijk dat systemen die gevoelige data bevatten, beschermd worden tegen CRQC's. Bij de verbetering van de bescherming van de gevoeligste use-cases, moeten we ons niet laten tegenhouden door onzekerheden over de ontwikkeling van de quantumcomputer =. Om een acceptabel niveau van paraatheid te bewerkstelligen, raden wij aan om deze use-cases zo snel mogelijk, maar uiterlijk eind 2030, te beschermen tegen *store-now-decrypt-later*-aanvallen. We raden ook aan om in dez periode gedetailleerde transitieplannen voor asymmetrische infrastructuursystemen te ontwikkelen.

We zetten ons in om samen onze IT-systemen te beschermen tegen de quantum-dreiging voor cryptografie, en om alle sectoren te steunen bij het ontwikkelen van hun transitieplannen om de wereldwijde maatschappelijke weerbaarheid tegen geüpdatete cryptografie te versterken.

Hiervoor is een Werkstroom voor PQC, met Frankrijk, Duitsland en Nederland als medevoorzitters, opgezet als onderdeel van de NIS Cooperation Group. Deze werkstroom volgt uit een aanbeveling [9] van de Europese Commissie. **We raden alle EU lidstaten aan actief betrokken te zijn in deze werkstroom** om een routekaart op te stellen voor de transitie naar post-quantumcryptografie om de quantum-weerbaarheid van de digitale infrastructuur van de Europese Unie veilig te stellen.

Referentielijst:

[1]: BSI, The status of quantum computer development, beschikbaar op https://bsi.bund.de/dok/study_status_quantum_computer
[2]: Global Risk Institute, Quantum Threat Timeline 2023 (2023), beschikbaar op https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/
[3]: ANSSI, ANSSI views on the Post-Quantum Cryptography transition (2022), beschikbaar op https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography-transition
[4]: ANSSI, Follow up position paper on Post-Quantum Cryptography (2023), beschikbaar op https://cyber.gouv.fr/en/publications/follow-position-paper-post-quantum-cryptography
[5]: BSI, Quantum safe cryptography - fundamentals, current developments and recommendations (2021), beschikbaar op https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html
[6]: AIVD, CWI, and TNO, The PQC Migration Handbook (2023), beschikbaar op https://www.tno.nl/en/newsroom/2023/04-0/pqc-migration-handbook/
[7]: ANSSI, AIVD, BSI, Swedish Armed Forces, Position Paper on Quantum Key Distribution, beschikbaar op https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html

[8]: ACN, Crittografia Post-Quantum e Quantistica. Preparazione alla Minaccia Quantistica (2024), beschikbaar op https://www.acn.gov.it/portale/documents/20119/85999/ACN_Crittografia_Quantum_Safe.pdf/d7eb595c-ee7f-848b-6c14-abf64cafb310?t=1721310015826

[9] : European Commission, Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography, beschikbaar op https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography