VOLG ONS:

Volgend bericht Inzet van spyware in Nederland

Vorig bericht De zoektocht naar regeneratieve intelligentie

UITGELICHT

Hoe SoftwareOne bedrijven helpt Microsoft Copilot optimaal te benutten

Microsoft introduceerde op 1 november 2023 Microsoft 365 Copilot, een nieuwe reeks op generatieve AI gebaseerde hulpmiddelen voor alle Microsoft ...

1 2 3 4

Standaard voor encryptie moet omhoog

DOOR KIM LOOHUIS · 23/10/2023

Op dit moment zijn kwantumcomputers nog niet krachtig genoeg om de huidige encryptie te breken, maar verwacht wordt dat dit niet al te lang meer gaat duren. Daarom moeten bedrijven nu al aan de slag met de nieuwe cryptografiestandaarden die volgend jaar verschijnen. Niet alleen omdat migratie een langdurig proces is, maar ook omdat versleutelde informatie nu al kan worden onderschept en bewaard om op een later moment, wanneer kwantumcomputers sterk genoeg zijn, te ontcijferen.

Cryptografie vormt een essentieel onderdeel van de informatiebeveiliging van organisaties en is onmisbaar om diefstal van gevoelige data te voorkomen, te verifiëren of ontvangen data correct zijn en om ongeautoriseerde toegang tot systemen te voorkomen. Met de opkomst van kwantumcomputers zijn de huidige cryptografische standaarden niet meer toereikend.

"Hoewel kwantumcomputers momenteel nog niet sterk genoeg zijn om onze huidige cryptografiesystemen te breken, is de kans reëel dat er in de toekomst wel een moment komt dat ze dat kunnen", zegt Marc Stevens, senior onderzoeker bij de Cryptology onderzoeksgroep bij het Centrum Wiskunde & Informatica (CWI). "Daarom is het noodzakelijk dat bedrijven zich daar nu al op voorbereiden."

Handboek

Om Nederlandse bedrijven hierbij te helpen, ontwikkelde de AIVD samen met TNO en het CWI het handboek 'Post Quantum Cryptografie'. Het is bedoeld voor organisaties die werken met belangrijke informatie die versleuteld wordt, zoals privacygevoelige gegevens of bedrijfsgeheimen. Organisaties kunnen met het handboek risico's identificeren en krijgen concrete stappen om te werken aan een migratiestrategie. "Er is niet één strategie voor alle organisaties", zegt Stevens, "aangezien niet elke organisatie dezelfde belangen en ICT-structuur heeft." Als follow-up op het handboek, werkt een Nederlands consortium van cryptografiebedrijven en kennisinstellingen momenteel aan een keuzetool om organisaties te helpen kiezen uit de verschillende kwantumveilige cryptografie-systemen. "Dat is nog in een beginstadium, dus er is nog niets publiekelijk beschikbaar."

Drie belangrijke redenen

Er zijn drie belangrijke redenen voor bedrijven om zich nu al te oriënteren op kwantumveilige cryptografie, zegt Stevens. "Ook nu de huidige kwantumcomputers nog niet sterk genoeg zijn om traditionele cryptografie te breken, kan versleutelde informatie wel al opgeslagen en bewaard worden voor wanneer kwantumcomputers wél sterk genoeg zijn." Dat wordt 'store now, decrypt later' genoemd.

Daarnaast lopen systemen met een lange levensduur risico. Het is namelijk bijzonder lastig, zo niet onmogelijk, om de systemen en kritieke infrastructuren die nu worden ontwikkeld en geïmplementeerd op een later moment naar kwantumveilige cryptografie te migreren. Dat komt doordat de nieuwe cryptografiestandaarden krachtige hardware nodig hebben en het wellicht op een later moment niet zo eenvoudig is om bestaande hardware van dit soort systemen te vervangen. Stevens: "Denk bijvoorbeeld aan auto's, of bruggen en sluizen."

De laatste reden waarom het belangrijk is voor organisaties om zich nu al te oriënteren op de nieuwe standaarden is dat migratie een langdurig proces is. "We hebben gezien dat de overstap van de vorige standaarden naar de huidige gemiddeld meer dan vijf jaar in beslag nam, dus we gaan ervanuit dat de migratie naar kwantumveilige cryptografie ook minimaal zo lang in beslag zal nemen. Ondertussen kan informatie verzameld worden volgens het store-now-decrypt-later principe en lopen organisaties dus feitelijk al risico."

Bottom-up aanpak

Homepage | Nieuws | Achter het nieuws | Columns / Blogs | Uitgelicht | Kalender | Bedrijfsnieuws | Whitepapers | **Nieuwsbrief**

PQC-migratiehandboek hebben aangeboden aan staatssecretaris Alexandra van Huffelen, lijkt er in Nederland nog niet echt sprake van een politieke beweging om migratie te bewerkstelligen.

"Hoewel je dat zorgwekkend kunt noemen, zien we in Nederland meer een bottom-up aanpak", ziet Stevens. "Zo hebben we het handboek voorgelegd aan een klankbordgroep waarin verschillende technische mensen uit diverse ministeries zaten. Zij hebben intern al een migratie in gang gezet, omdat ze hun eigen systemen graag zo snel mogelijk kwantumveilig willen maken. Daarnaast zie ik verschillende ad-hoc samenwerkingen in ons land. Er is dus wel degelijk beweging op dit vlak."

Cryptografische wendbaarheid

In het handboek worden drie stappen benoemd die organisaties helpen bij de migratie naar kwantumveilige communicatie: diagnose, planning en uitvoering. Stevens benadrukt dat iedere organisatie hiermee aan de slag moet, ook kleinere bedrijven. "Begin in ieder geval met een inventarisatie. Laat je niet verrassen door wat je binnen je organisatie hebt en gebruikt op het moment dat het daadwerkelijk gaat spelen, maar zorg dat je nu al weet waar je risico's liggen en wat je kunt doen."

De CWI-onderzoeker is een groot voorstander van cryptografische agility. "We zien nu vaak dat cryptografie en encryptie heel diep in systemen zijn ingebouwd. Dat is een van de redenen dat migratie zo lang gaat duren, omdat je voor ieder systeem moet bekijken wat er staat en hoe je dat kunt overzetten naar de nieuwe standaard. Je wordt een stuk wendbaarder wanneer je de nieuwe cryptografische implementatie op een centrale plek neerzet waartoe je systemen met generieke calls toegang hebben."

Zeker nu er door het Amerikaanse National Institute of Standards and Technology (NIST) een nieuwe competitie is uitgeschreven voor kwantumveilige digitale handtekeningen. "Dit kan over enkele jaren leiden tot extra standaarden boven op de huidige gekozen normen die in 2024 moeten uitkomen", zegt Stevens. "Een centraal systeem maakt het eenvoudiger om over te stappen op nieuwe standaarden of die toe te voegen. Het centraliseren van cryptografie binnen je organisatie is iets dat ieder bedrijf nu al kan doen."

Lees ook:

- TU Delft start ICAI lab AI for Software Engineering Lab (AI4SE)
- Hoe voorkom je dat jouw organisatie slachtoffer wordt van ransomware?