INNOVATIE & STRATEGIE

SECURITY

NIST kiest wapens tegen kwantumcomputer als cryptokraker

'Competitie' levert vier kandidaten op voor postkwantumcryptografie.

© Shutterstock, zef art

6 JULI 2022

Het Amerikaanse National Institute for Standards and Technology (NIST) heeft gisteren een selectie gemaakt uit de vele voorstellen ter vervanging van huidige encryptiemethoden die straks eenvoudig zijn te kraken met een kwantumcomputer.

Op deze zogeheten postkwantumcryptografische methoden wordt met smart gewacht. Een aantal huidige cryptografische technieken biedt nu weliswaar nog voldoende bescherming. Echter gegevens die nu worden versleuteld en bewaard, kunnen straks kinderlijk eenvoudig openbaar gemaakt worden. De nieuwe methoden zijn dus belangrijk voor geheimen - zoals bedrijfs- en staatsgeheimen - die over een aantal jaar nog steeds begerenswaardig zijn voor criminelen, spionnen en vreemde mogendheden.

Vooral het nu versturen van die informatie, maakt ze kwetsbaar omdat juist de encryptie voor data in transit weinig weerstand biedt tegen het rekengeweld dat de kwantumcomputer in stelling kan brengen. En van alle data die verstuurd worden, komen ongewild ergens kopieën in een opslag te staan, al zijn de gegevens versleuteld, verzekeren securityexperts. Die informatie komt dan over een paar jaar beschikbaar.

Al enkele jaren doen verschillende onderzoeksinstituten daarom onderzoek naar het verbeteren en marktrijp maken van nieuwe, maar ook al langer bestaande cryptografische methoden die niet vatbaar zijn voor dat kwantumrekengeweld. NIST heeft de onderzoekers uitgedaagd hun beste oplossingen te delen zodat de wereld kan standaardiseren op deze methoden en ze verder doorontwikkelen.

GERELATEERDE ARTIKELEN


0~ Kwantumcomputer bedreigt straks encryptie: kom nu in actie


Podcast: Waarom moet je nu echt al rekening houden met de kwantumcomputer?


13 vragen over Elliptic Curve Encryptie


Dataverkeer krijgt bescherming tegen 'kwantum'-aanvallen

De keuze is daar

De selectie van de vier veelbelovende kandidaten werd al zeker een half jaar verwacht. Nu heeft NIST ze bekend gemaakt: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON en SPHINCS+. De eerste twee zullen waarschijnlijk de meestgebruikte standaarden worden.

CRYSTALS-Kyber is bedoeld om encryptiesleutels te maken en CRYSTALS-Dilithium is vooral voor het vaststellen wie digitaal ondertekende versleutelde informatie heeft verstuurd. Overigens vallen ook FALCON en SPHINCS+ in die laatstgenoemde categorie. CRYSTALS-Kyber is dus typisch voor het veilig versturen van informatie tussen twee computers die elkaar niet eerder versleutelde informatie hebben toegestuurd. De andere drie zijn steeds opnieuw van toepassing wanneer een nieuwe gegevensoverdracht wordt gestart.

Nu beginnen met vervanging

Cryptografie-hoogleraar Ronald Cramer en TNO-kwantumspecialist Maran van Heesch legden vorig jaar in AG Connect al uit waarom het zo belangrijk is dat organisaties nu al aan de slag gaan met deze dreiging van de kwantumcomputer voor een aantal veelgebruikte cryptografische databeveiligingsmethoden. Niet alleen is de kans groot dat bedrijfs- en staatsgeheimen op straat komen, maar het zorgvuldig en grondig vervangen van cryptografische technieken in de systemen van een organisatie, kost vaak jaren. "Dat kan een heel lastig en tijdrovend proces zijn", zei Cramer in dat interview. "We hebben dat eerder gezien toen de MD5 en later SHA-1-hashfuncties werden gekraakt. Ze worden jaren daarna nog steeds gebruikt in organisaties."

Het is daarom essentieel nu al te beginnen, bijvoorbeeld met de inventarisatie welke encryptie waar wordt gebruikt en hoe kwetsbaar de organisatie zich daarmee maakt als deze encryptie waardeloos zou worden. Een tweede stap zou kunnen zijn vast in te zetten op een combinatie van de traditionele cryptografie en de nieuwe - nog niet volledig uitontwikkelde - postkwantummethoden.

THIJS DOORENBOSCH
is redacteur, coördinator printeditie en heeft als belangrijkste aandachtspunt Innovatie en Strategie, Artificial Intelligence, Datascience, Netwerken, Process Automation.

Telefoon: +31 (0)202467225 of +31(0)618868529
E-mail: t.doorenbosch@agconnect.nl

VOLGORDE NIEUWSTE EERST OUDSTE EERST

REACTIE TOEVOEGEN

UW NAAM *

E-MAIL *

De inhoud van dit veld is privé en zal niet openbaar worden gemaakt.

VOORPAGINA

Uw reactie

PLAATS REACTIE

VAN ONZE PARTNERS


EXCLUSIVE NETWORKS
Fortinet lanceert een nieuwe netwerk detectie & respons (NDR)-oplossing


DELL TECHNOLOGIES
Cybersecurity is essentieel voor economisch herstel


EXCALIER
Wat blijft hetzelfde als je geconfronteerd wordt met constante verandering?


TREND MICRO
Meer dan de helft van de supply chains gecompromitteerd door ransomware


KNOWBE4
KnowBe4 organiseert tweede editie van KB4-CON EMEA

GERELATEERDE WHITEPAPERS


Global Threat Report 2022


De 13 minimale security-eisen waaraan elke IT-omgeving moet voldoen en waarom


Implementeer DMARC om phishing-aanvallen uit je inbox te houden


Webinar Multifactor Authenticatie hacken


Leg de basis voor een veilige IT-infrastructuur met Security by Design

MEER WHITEPAPERS

LEES OOK


Oekraïne waarschuwt voor Russische cyberaanvallen


PARTNERBIJDRAGE
PODCAST 'SECURITY...


D66 wil lokale verschillen in regelgeving datacenters gelijktrekken


PARTNERBIJDRAGE
EEN SNUFJE JAMES BOND:...


'Ziekenhuizen moeten in 2023 voldoen aan wet informatiebeveiliging'

NIEUWSOVERZICHT


Mag LinkedIn experimenteren met gebruikers zonder hun toestemming?


Blik op tech: Beroepen die door IT zijn weggevaagd


'Biden-deal voor TikTok nabij, Oracle weer in beeld'