GOVERNANCE

Grapperhaus zoekt tevergeefs naar alternatief voor encryptie-backdoor

Zoektocht schadelijk voor reputatie Nederland als encryptie-innovatieland.

2

Ferd Grapperhaus © Shutterstock, Nancy Beijersbergen

8 JANUARI 2021

Vlak voor de Kerstdagen kondigde minister van Justitie en Veiligheid Ferd Grapperhaus aan een opdracht te hebben gegeven voor een "Inventarisatie naar technische mogelijkheden voor rechtmatige toegang tot versleuteld bewijs". In feite gaat hij dus op zoek naar alternatieven voor een achterdeurtje in encryptie om politie en opsporingsdiensten meer mogelijkheden te geven om efficiënt bij versleutelde communicatie te komen.

Nederland heeft een vooraanstaande positie als het gaat om onderzoek naar cryptografische technologie. Daartoe behoort onder meer Ronald Cramer, hoogleraar Cryptologie aan de Universiteit Leiden en groepsleider Cryptology bij het Centrum Wiskunde & Informatica (CWI). Hij vindt het initiatief hoogst verbazingwekkend. "Alle argumenten tegen zo'n aanpak zijn al zo vaak de revue gepasseerd. De Tweede Kamer heeft zich duidelijk uitgesproken en toch blijft de minister het maar proberen."

Alternatieven zijn er niet en dat weet niet alleen hij, maar ook de Europese Raad, vult Tanja Lange - hoogleraar Cryptologie aan de TU Eindhoven - aan. "Toch blijven ze proberen. We herhalen steeds maar dezelfde discussie als in de eerste crypto-oorlogen in de 90'er jaren. Zelfs toen waren de argumenten niet nieuw, want de meeste werden al naar voren gebracht toen Diffie en Hellman er op stonden hun artikel te publiceren waarin de public key cryptografie werd geïntroduceerd en wat de start betekende van het academisch onderzoek op dit gebied."

Ook Pieter van Boheemen en Jurriën Hamer, beiden onderzoekers van het Rathenau Instituut dat de overheid gevraagd en ongevraagd adviseert, tonen zich uiterst kritisch over deze hernieuwde zoektocht. "Veiligheid in de digitale samenleving is al een groot probleem vanwege lekken in protocollen en software. Encryptie is nou net een manier om die veiligheid flink te verhogen. Door daar weer verzwakking in aan te brengen, ondermijn je die veiligheid", stelt Hamer.

GERELATEERDE ARTIKELEN


Grapperhaus geeft verkenningsopdracht voor encryptiebackdoor 2


VS: grote overheidshack ook zónder SolarWinds-backdoor


Woordenwisseling over encryptie-backdoor laait (weer) op


EU-ministers willen Amerikaanse backdoor in encryptie 1


Privacybescherming sleepwet nog altijd onvoldoende

Cramer vreest dat de politiek op een gegeven moment toch overstag gaat voor de pleidooien van Justitie. "Dat heb je ook gezien met de Wet op de inlichtingen- en veiligheidsdiensten (Wiv)." Ondanks veel protest van onder meer wetenschappelijke en maatschappelijke hoek, hebben de opsporingsdiensten toch ruime bevoegdheden gekregen om organisaties binnen te dringen en netwerkverkeer af te tappen. "Die maatregelen worden in de politiek gebracht met het argument dat daarmee efficiënt grootschalige criminaliteit en kinderpornonetwerken kunnen worden opgespoord. Maar zijn zulke mogelijkheden er eenmaal, worden ze gaandeweg voor steeds minder zware zaken ingezet."

Van Boheemen bevestigt dat. "Als je een hamer in handen hebt, zie je overal spijkers. We hebben dat gezien met de nummerplaatherkenning. Die is bedacht voor het opsporen van snelheidsovertredingen en ontduiken van wegenbelasting.

Daarna volgde de discussie over hoe lang die gegevens bewaard mogen worden en waarvoor ze mogen worden gebruikt. Inmiddels is het systeem uitgegroeid tot een veel bredere monitoring bijvoorbeeld voor de handhaving van milieuzones."

Hamer: "Je moet kijken naar de totale gereedschapskist van de opsporingsdiensten en de effectiviteit. De capaciteit van de recherche is al jaren een probleem. Hoeveel zaken worden uiteindelijk opgelost? De discussie in de politiek verengt zich tot het verruimen van bevoegdheden terwijl er weinig aandacht is voor het oplossen van het capaciteitsprobleem. Zorg er eerst voor dat er meer rechercheurs komen en de pakkans bij misdaden wordt vergroot. Maar het is politiek haalbaarder om over verzwakking van encryptie te beginnen. Met zo'n voorstel laat je als minister makkelijk zien dat je 'tough on crime' bent."

Alternatieven zijn er voldoende in het meer klassieke recherchewerk bijvoorbeeld door te infiltreren in criminele organisaties. Een andere mogelijkheid is het wettelijk afdwingen dat iemand bij gerede verdenking toegang moet geven tot zijn smartphone. De mogelijkheid om aan massasurveillance te kunnen doen door bijvoorbeeld al het Whatsapp-verkeer door filters te halen voor het versleuteld wordt, is niet de goede weg.

Schade aan reputatie Nederland

Hamer: "Er wordt te veel gekeken naar kortetermijngewin. Wat ik mis in de discussie is de schade die het voorstel van minister Grapperhaus zou toebrengen aan de reputatie als democratisch land dat zich in de wereld juist heeft geprofileerd als voorstander van het gebruik van encryptie. We hebben hier topwetenschappers die wereldwijd toonaangevend werk verrichten op het gebied van post kwantum encryptie [die veiligheid waarborgt wanneer mogelijk over tien jaar kwantumcomputers de huidige encryptie makkelijk kunnen breken, red]. Nederland kan die leidende positie ook economisch benutten. Maar wanneer de Nederlandse overheid pleit voor het gebruik van achterdeurtjes, maak je je ongeloofwaardig. Bovendien verlies je het recht op morele verontwaardiging ten aanzien van minder democratische landen die lak hebben aan privacy. Er staat dus veel meer op het spel dan het oprollen van een paar criminele organisaties. "

Het creëren van "technische mogelijkheden voor rechtmatige toegang tot versleuteld bewijs", zoals Grapperhaus de middelen omschrijft waar hij naar op zoek is, leidt er vervolgens toe dat de zware criminaliteit snel op zoek gaan naar alternatieven. Van Boheemen: "Er ontstaat een waterbed-effect. Wat overblijft is een verzwakte beveiliging van goedwillende burgers." Die technische mogelijkheden bieden de misdaad, economische en militaire spionnen en buitenlandse opsporingsdiensten juist wel weer een nieuwe honingpot. "In het theoretisch geval van een achterdeur moet er een sleutel zijn. Wie gaat die beheren? Zelfs bij de Amerikaanse overheid is zo'n sleutel niet veilig. Er zijn heel gênante voorbeelden van hacks bij de NSA waar allerlei geheime informatie over zeroday-lekken is buitgemaakt en daarna misbruikt. Denk aan de ransomware-aanval op de ECT-terminal in de Rotterdamse haven. Maar recent zijn hackers via de achterdeur in de SolarWinds-software bij het Amerikaanse ministerie van Energie doorgedrongen tot de informatie over de kernwapens. Als die codes al niet veilig zijn."

Lees meer over: backdoor, Ferd Grapperhaus, encryptie

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