Spionage Er zijn toch nog een paar vormen van versleuteling die niet te kraken zijn door de NSA

Onzichtbaar op het web: het kan nog

Achtergrond
Crypto-oorlog

Er is hoop: niet het hele internet is af te luisteren door geheime diensten. Het slechte nieuws? Het meeste al wel.

Door onze redacteur
Carola Houtekamer

AMSTERDAM. Niet het hele internet is stuk. Geheime diensten kunnen niet alles afluisteren. Voor wie al murw is geslagen door de stroom onthullingen van NSA-klokkenluider Edward Snowden en denkt dat privacy is uit het verleden is - een fossiel uit de tijd van knipperende hyperlinks en bulletin boards: anonimiteit en privacy bestaan nog op het web. Een beetje.

Dat was de kerstboodschap van journalisten Laura Poitras, Jacob Appelbaum en collega's van het Duitse weekblad *Der Spiegel*. Dit weekeinde presenteerden ze welke vormen van versleuteling niet of nauwelijks te kraken zijn door de Amerikaanse inlichtingendienst NSA en bondgenoten. Vooralsnog.

Want het zijn er inmiddels niet zo veel meer, blijkt uit documenten die door Snowden zijn gelekt. Dat was de donkere rand rond het blijde nieuws dat de journalisten op de hackersconferentie van de Chaos Computer Club in Hamburg brachten, tegelijk met het artikel. Inlichtingendiensten kunnen al heel veel versleutelde communicatie wél ontcijferen. Dat was al bekend, maar nu is duidelijker welke sleutels zijn gekraakt.

Met encryptie kun je je mail, gesprek of surfgedrag onleesbaar maken voor derden. Alleen wie de juiste sleutel heeft, kan de informatie ontcijferen. Heel vervelend voor inlichtingendiensten die graag meelezen. Encryptie kraken zit daarom standaard in de gereedschapskist van cyberspionnen, net als hacken, wachtwoorden stelen en zeekabels aftappen.

Wat de NSA en het Britse GCHQ al is gelukt: het afluisteren van internetverkeer via https, wat je gebruikt als je telebankiert of je creditcard bij een webshop invult. De NSA was van plan om eind 2012 tien miljoen https-verbindingen *per dag* te kraken.

Ook gelukt: het afluisteren van beveiligde VPN-verbindingen die je bijvoorbeeld opzet als je vanuit huis inlogt op het kantoorsysteem. De NSA claimt VPN's van luchtvaartmaatschappijen, telecombedrijven en diplomaten te hebben gekraakt.

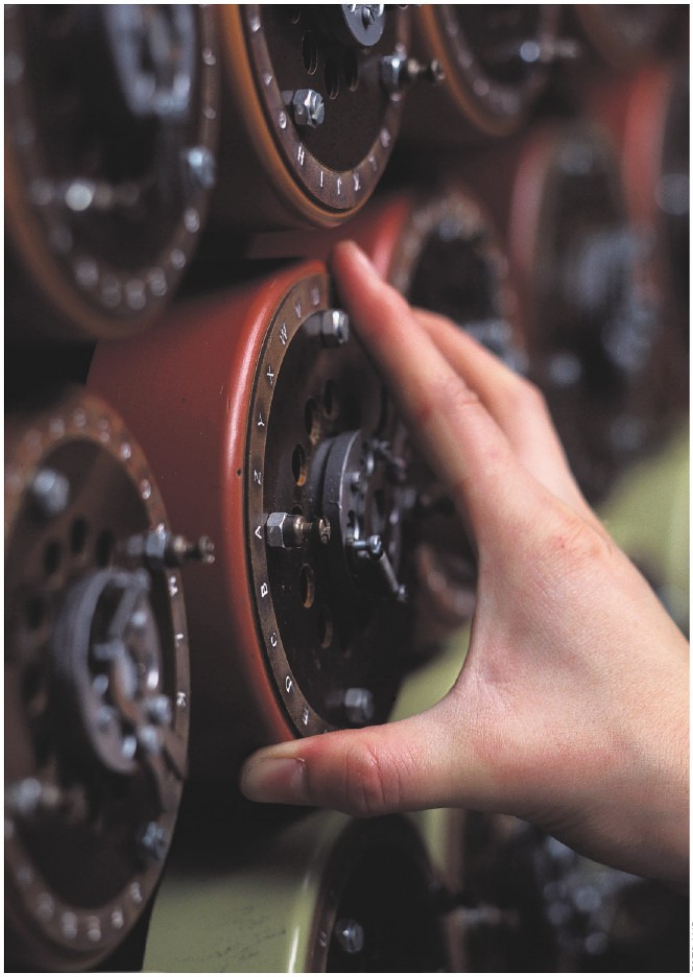

FOTO ANP

Computers begonnen met encryptie. **Hierboven een replica van de Bombemachine**, het apparaat dat in de Tweede Wereldoorlog voor de Britten Duitse codes hielp ontcijferen die versleuteld waren met de Enigma-machine. De Bombe werd bedacht door de wiskundige Alan Turing en was de voorloper van de moderne computer.

Encryptie ontcijferen staat hoog op de agenda van NSA en partners, nu iedereen het mag gebruiken. „Encryptie was altijd het domein van inlichtingendiensten", zegt hoogleraar computerbeveiliging Bart Jacobs van de Radboud Universiteit. „Het komt uit oorlogsvoering. Eerst het kraken van Enigma van de Duitsers in de Tweede Wereldoorlog, toen het onderscheppen van communicatie in de Koude Oorlog."

In de jaren 70 gingen academici met versleuteling aan de slag. Jacobs: „Opeens gingen anderen met het speelgoed van inlichtingendiensten spelen. Dat gaf heftige reacties." De *crypto wars* braken uit. Burgers wilden versleuteling waar niemand bij kan - *niemand*. Spionnen noemden dat bedreigend voor de staatsveiligheid. De Amerikaanse overheid probeerde achterdeurtjes in software te krijgen en eiste dat de FBI altijd een reservesleutel mocht opvragen.

In het begin van de eeuw leek de oorlog beslecht: iedereen kon en mocht sterke encryptie gebruiken. Maar in 2013 maakte *The New York Times* bekend dat de NSA actief versleutelstandaarden probeert te verzwakken door lobby, hacks en geheime achterdeurtjes in software van *„industry partners"*. Dat geeft inlichtingendiensten het voordeel, burgers en bedrijven die gevoelige informatie willen beschermen het nadeel. „Als de crypto-oorlog niet al verloren is", zei Appelbaum, „dan is hij nog steeds gaande".

Wat blijft er over? In documenten die in 2012 gelekt zijn, staat dat inlichtingendiensten TOR lastig vinden. TOR wordt volgens GCHQ gebruikt door *„very naughty people"* die anoniem willen surfen. Voor mails die met de *open source* versleuteling PGP zijn beschermd, is *„no decrypt available"*, vermelden documenten. Blijkbaar te moeilijk. Sommige sleutels voor chat en internetbellen lijken ook veilig. En als die allemaal tegelijkertijd worden gebruikt, verliest de NSA helemaal het overzicht.

Een goede zaak, vindt Jacobs, die zelf anoniem surft als hij bijvoorbeeld iets medisch opzoekt en niet wil dat „de Googles der aarde" meekijken. „Encryptie verbieden is zoiets als burgers verbieden een brandkast te gebruiken. Als je een agent vraagt: moeten mensen hun huis beter beschermen tegen inbraak, of minder goed, voor het geval jullie een keer binnen willen vallen, wat zegt hij dan? Beter beschermen, toch?"