Wie krijgt de sleutel van versleuteling?

Encryptie In de nasleep van het NSA-schandaal hebben Apple en Google hun diensten versleuteld. Amerikaanse en Europese opsporingsdiensten eisen nu toegang via 'achterdeurtjes'.

Door **Herbert Blankesteijn**

AMSTERDAM. Veilige, versleutelde communicatie, met een sleutel voor de overheid om mee te lezen als dat nodig is. Is dat mogelijk? In de VS en Europa woedt de discussie: opsporingsdiensten willen een 'achterdeurtje', maar experts zijn tegen.

Een half jaar terug sloegen FBI en Europol alarm: diverse internetbedrijven boden klanten versleuteling waar de bedrijven zelf de sleutel niet meer van hadden. Apple, Google en WhatsApp zijn de bekendste.

Het was een reactie op het NSA-schandaal in 2013, onthuld door Edward Snowden. Bedrijven waarvan was gebleken dat ze data deelden met inlichtingendienst NSA, hoopten zo vertrouwen van het publiek terug te winnen. Een sleutel die je niet hebt, kun je niet delen. Jammer voor politie en diensten, die zo een belangrijke informatiebron kwijtraakten.

Europa en VS vechten terug

Politici proberen nu het verloren terrein voor de overheid te heroveren. In het Verenigd Koninkrijk wil premier David Cameron bedrijven verplichten de overheid in bepaalde gevallen een sleutel te geven. Ook Europol-directeur Rob Wainwright klaagde onlangs over het toenemen van encryptie.

In de VS hield het Congres deze maand hoorzittingen over de vraag of een 'achterdeur' in versleutelingssoftware wenselijk is. FBI-directeur James Comey verklaarde dat alle communicatie leesbaar zou moeten zijn, eventueel na een gerechtelijk bevel. Het eerdere advies van de FBI aan bezitters van smartphones encryptie te gebruiken als beveiliging tegen diefstal is van de FBI-site gehaald.

Deze roep om achterdeurtjes stuit op één probleem: experts zeggen dat het niet kan. Vijftien cryptografen publiceerden tijdens de hoorzittingen een manifest vol bezwaren.

Kan het praktisch wel?

De belangrijkste betreffen de veiligheid zelf. De beste encryptietechnieken wissen een sleutel na gebruik, zodat hij niet misbruikt kan worden. Als de sleutels bewaard moeten worden ontstaat een zwakke plek. Mensen die toegang hebben tot de sleutels kunnen er misbruik van maken, de informatie kan per ongeluk op straat belanden of hackers kunnen hun slag slaan.

Al deze mogelijkheden hebben zich in het verleden wel eens voorgedaan. NSA-werknemers zochten in afgetapte informatie naar personen voor wie ze persoonlijk belangstelling hadden, zoals ex-geliefden. Laptops en usb-sticks met gevoelige informatie zijn verloren of gestolen. De vijftien experts noemen een database van Google met personen die voor de NSA in de gaten moesten worden gehouden, waar Chinese hackers in wisten door te dringen.

Verder wijzen de vijftien erop dat beheer van al die sleutels in juridisch opzicht een onontwarbare kluwen dreigt op te leveren. Als het Verenigd Koninkrijk en China allebei zo'n beleid in de wet opnemen, aan welk land moet een Britse app-bouwer met Chinese gebruikers dan zijn sleutels ter beschikking stellen? Moet hij China toegang geven tot versleutelde communicatie tussen een Chinees en een Brit?

Ook zijn er principiële bezwaren. „De regeringen van de VS en het Verenigd Koninkrijk hebben lang en hard gevochten om het beheer van internet open te houden, in weerwil van de eisen van autoritaire landen om staatscontrole in te voeren", schrijven ze. „Betekent de roep om dit soort toegang geen ommekeer in het beleid?"

Als westerse overheden achterdeuren afdwingen, zullen andere landen dit ook doen, zegt Bart Jacobs, informaticahoogleraar in Nijmegen. „Fabrikanten moeten dan tientallen achterdeuren inbouwen. Dan kun je net zo goed niet beveiligen."

Achterdeurtjes werken alleen als concurrerende diensten en software uit landen zonder dergelijke wetgeving worden verboden, zegt Jacobs. „Bovendien bestaat er zoveel gratis *open source*-software voor beveiligd communiceren dat zulke maatregelen makkelijk omzeild kunnen worden."

Nationale veiligheid

Niet alle politici maken zich zorgen over juridische *collateral damage*. „Volgens mij is onze eerste plicht om burgers te beschermen tegen aanvallen", zei ex-presidentskandidaat John McCain bij de hoorzittingen. Privacy en grondwettelijke rechten komen volgens hem op de tweede plaats.

Ook *The Washington Post* stelde in een commentaar dat softwareontwikkelaars naast bescherming van privacy ook hun verantwoordelijkheid moeten nemen voor bestrijding van criminaliteit en terrorisme. De krant pleit voor een „soort veilige gouden sleutel" waarmee veiligheidsdiensten alleen met toestemming van de rechter zich toegang kunnen verschaffen tot versleutelde informatie. „Alle vrijheid komt met beperkingen. Het lijkt alleen maar gepast dat de grote vrijheden van internet worden onderworpen aan dezelfde wettelijke grenzen en bescherming die we voor de rest van de samenleving accepteren."

Het commentaar van de krant ontlokte schampere opmerkingen van beveiligingsexperts. Natuurlijk hebben terroristen profijt van encryptie, aldus Bruce Schneier, een van de manifestondertekenaars, tegen *Business Insider*. „De voordelen van encryptie zijn voor de *good guys* én de *bad guys*. Cameron vraagt ook niet of auto's nog maar zestig kilometer per uur kunnen rijden, zodat bankrovers minder snel kunnen vluchten. Je moet niet een overweldigend aantal eerlijke mensen benadelen in een poging een paar slechte mensen dwars te zitten."

DE 'TERUGHACKWET'

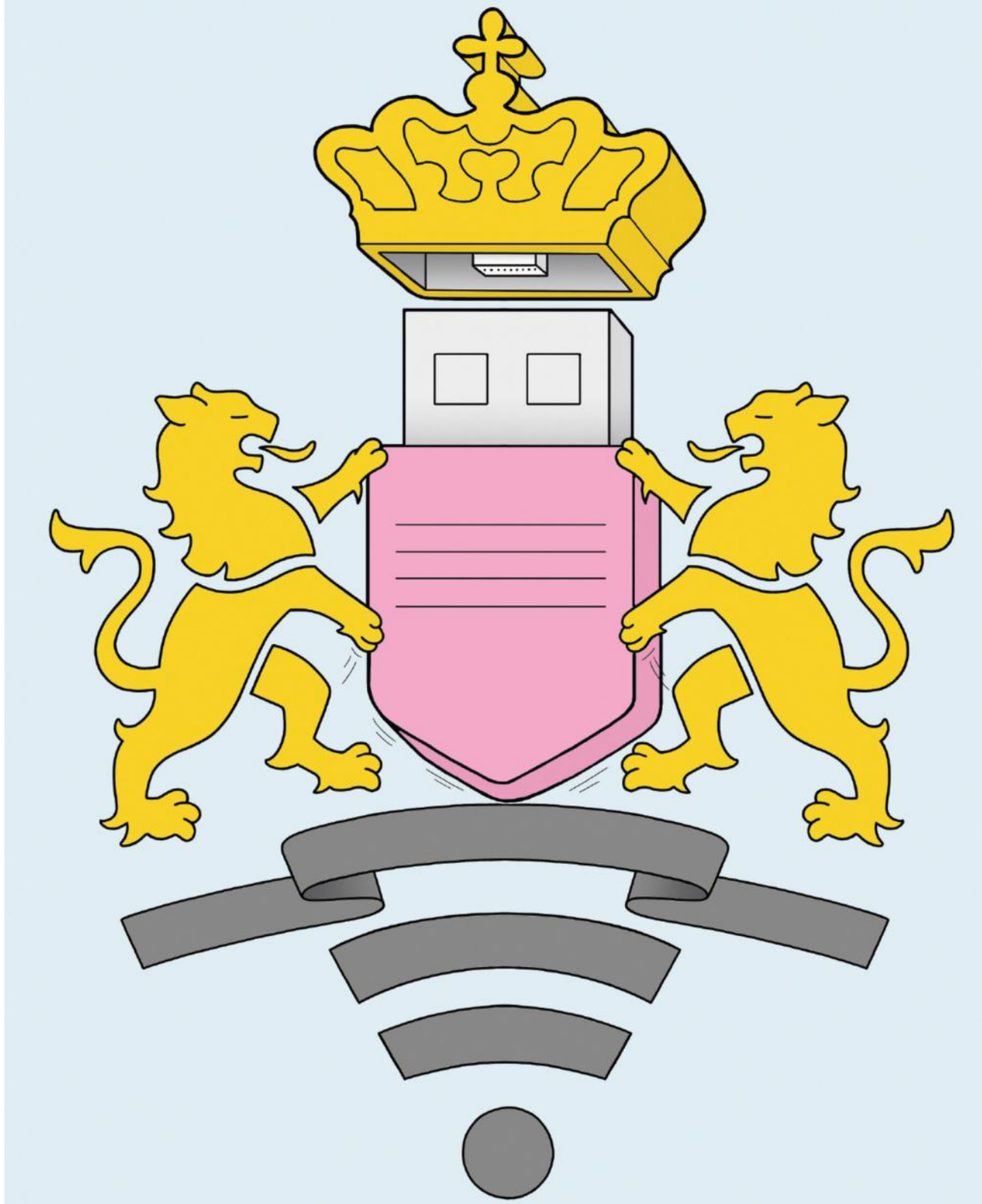
In Nederland is de zogeheten 'terughackwet' in de maak, een geesteskind van ex-minister Opstelten. De politie krijgt daarin vergaande bevoegdheden om in te breken in computers van vermeende criminelen.

Deze wet creëert onder andere de mogelijkheid van een zogeheten 'decryptiebevel', dat verdachten verplicht hun versleutelde gegevens te ontsleutelen voor de politie, op straffe van een zwaardere sanctie dan staat op het vergrijp waarvan ze worden verdacht.

Volgens veel juristen staat deze wet op gespannen voet met het principe dat verdachten geen bewijsmateriaal tegen zichzelf hoeven aan te dragen. Maar in ieder geval is deze wet alleen van toepassing in individuele gevallen.

De terughackwet ligt momenteel bij de Raad van State. In het opzettelijk verzwakken van de bescherming van informatie voorziet de wet niet.

> Als fabrikanten tientallen 'achterdeuren' moeten inbouwen, dan kun je net zo goed niet beveiligen
>
> **Bart Jacobs**
> Hoogleraar informatica over versleuteling van digitale informatie



ILLUSTRATIE TOMAS SCHATS