Mens versus machine: maatregelen tegen massasurveillance

Welke maatregelen kunnen overheden nemen om burgers beter te wapenen tegen massasurveillance?

Om de beveiliging tegen spionerende overheden (en bedrijven) beter te regelen, zal komende jaren veel worden geïnvesteerd in concrete technische maatregelen. Nederland, en de Nederlandse overheid, kan hierin voorop lopen.

Highlights

- Privacy is geen gegeven, maar iets dat zeker moet worden gesteld.
- De Nederlandse overheid kan een prominentere rol nemen bij het bevorderen van privacy.
- Het stimuleren van technische maatregelen als encryptie is een grote stap in de goede richting.
- Burgers kunnen zelf ook beveiligingsmaatregelen nemen tegen massasurveillance.

De afgelopen jaren hebben duidelijk gemaakt dat overheden en bedrijven bij het dataverkeer van burgers en bedrijven over de schouder meekijken. Hoewel het recht op privacy al decennialang is verankerd in allerlei wetten en verdragen, blijkt hiervan in het geval van digitale communicatie minder sprake van te zijn: bedrijven koppelen en verkopen persoonsgegevens en overheden ontsluiten en koppelen gegevens van verschillende bronnen. Het koppelen van data kan veel waarde leveren, echter de privacy van burgers kan in het gedrang komen.

Op het moment dat toezicht op grote schaal wordt toegepast om burgers en bedrijven te monitoren zonder duidelijk gedefinieerde en controleerbare doelbinding, spreken wij in dit artikel van ‘massasurveillance’.

In het digitale tijdperk is het delen van (persoonlijke) gegevens bij het gebruiken van webapplicaties vaak een vereiste voor het kunnen uitvoeren van transacties. Hierbij is het doorgaans onduidelijk welke (meta)informatie gebruikers met wie delen. Dit (gepercipieerde) verlies van controle over de eigen data voedt de discussie of privacy nog wel bestaat.

Om de beveiliging tegen ongewenste dataverzameling te verbeteren, zal de komende jaren veel moeten worden geïnvesteerd in concrete (technische) maatregelen. De overheid kan binnen deze ontwikkeling een doorslaggevende rol spelen, bijvoorbeeld door burgers te stimuleren om technische maatregelen zoals encryptie te gebruiken. Tevens dient de overheid zelf het goede voorbeeld uit te dragen door technieken tegen massasurveillance zelf te gebruiken.

Privacy en recht

Het recht op privacy is historisch gezien ontwikkeld als het ‘recht om met rust gelaten te worden’. Een recht om je, in de eigen levenssfeer, te kunnen onttrekken aan de spiedende ogen van andere burgers en, tot op zekere hoogte, de overheid. Dit begrip van privacy is lastig verenigbaar met de huidige digitale communicatiemiddelen en levensstijl.

Uit de discussie zoals die in de afgelopen jaren is gevoerd over het krachtenveld tussen veiligheid en privacy, worden de contouren zichtbaar van een nieuwe notie van privacy. Eén die het individu ondersteunt in het veilig delen van persoonlijke informatie en tevens beschermt tegen het onrechtmatig en buitenproportioneel gebruik van deze informatie. Privacy moet daarbij niet zozeer worden gezien als een recht (een gegeven), maar iets dat zeker moet worden gesteld.

Deze kijk op privacy richt zich op het creëren van meer controle en transparantie over wat er met gegevens gebeurt, in plaats van afscherming. Diverse wetenschappelijke onderzoeken tonen aan dat voor het individu een gevoel van controle over de eigen datastroom een positieve benadering van privacy bevordert[1]. Wet- en regelgeving op het gebied van privacy en databescherming biedt deze controle onvoldoende. De ervaring leert dat wetgeving op dit gebied achterloopt bij de technologie: op het moment dat nieuwe privacywetgeving wordt geïmplementeerd,

is deze vaak al achterhaald. Daarom is het van groot belang om juist de concrete technische mogelijkheden tegen meekijken uit te lichten, in plaats van te veel te kijken naar wetgeving.

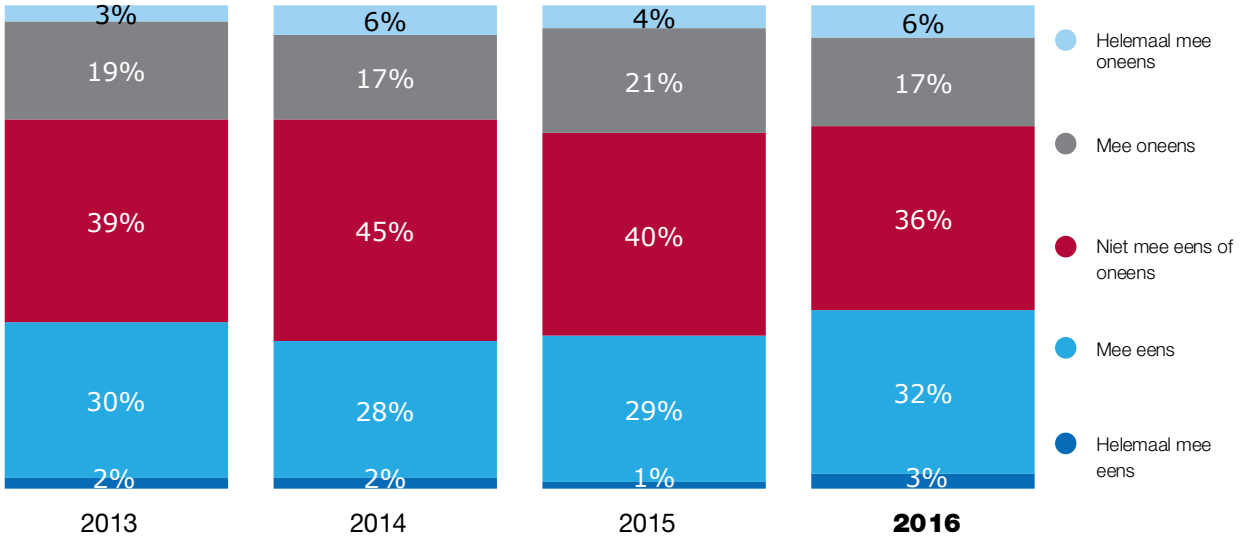
Het stimuleren van wijdverbreid gebruik van technische maatregelen

Om te verzekeren dat toegang tot data alleen mogelijk is door personen en instanties die er verantwoordelijk voor zijn of er het recht toe hebben, is het noodzakelijk om naast wet- en regelgeving technische waarborgen in te bouwen. De offline en de online wereld versmelten met elkaar. Deze versmelting biedt de mogelijkheid om offline maatregelen onder de loep te nemen om hier een online les uit te halen. De offline notie van de toepassing van concrete, vaak technische, maatregelen richt zich op het uitsluiten van onbevoegde personen.
Een van deze technische (online) maatregelen die zich richt op deze notie van uitsluiting is encryptie. Encryptie is een methode om met behulp van een speciaal algoritme gegevens te coderen zodat ze niet leesbaar zijn voor onbevoegde personen. Alleen met de juiste elektronische sleutel - een geheime reeks cijfers - kunnen de gegevens leesbaar worden gemaakt. Afgelopen jaar stelde de Nederlandse overheid in een kabinetsstandpunt[2] dat encryptie essentieel is voor het waarborgen van de vrijheid en privacy van haar burgers, mede daarom investeerde zij in diverse encryptieprojecten voor de burger.
Tevens zijn diverse gemeentes onlangs gestart met een pilot die burgers op DigiD laat inloggen met een chipkaart en kaartlezer, om zo burgers en bedrijven makkelijk en betrouwbaar zaken te laten doen via internet[3]. De techniek is gebaseerd op het inlogproces dat wordt toegepast bij online bankieren.

Kortom, het gebruik van technieken als encryptie wordt in toenemende mate gestimuleerd door de Nederlandse overheid. Naast een investering in deze technieken, kan de overheid ook het voortouw nemen door duidelijker de kaders aan te geven van wat wenselijk is, bijvoorbeeld door het neerleggen van baselines voor veilige digitale communicatie.
Daarnaast dient de overheid dit type technieken zelf toe te passen, juist nu de burger meer vertrouwen in de overheid heeft gekregen op het gebied van privacy. Uit het onderzoek dat door TNS NIPO in het kader van Trends in Veiligheid is uitgevoerd, komt naar voren dat 35% van de Nederlanders er vertrouwen in heeft dat de overheid zijn of haar privacy voldoende beschermt; een lichte stijging ten opzichte van 2014 en 2015.

Maar bovenal moeten er voor dienstaanbieders voldoende impulsen komen om diensten op een privacyvriendelijke manier aan te bieden. De overheid kan daarin gewenst gedrag stimuleren door het vergroten van impulsen om technologie te verbeteren. Het feit dat telefoonnetwerken nog steeds kunnen terugvallen op (onveilige) 2g-technologie is een voorbeeld van een (relatief) makkelijk te verhelpen probleem[4].

Figuur 1: Ik heb er vertouwen in dat de overheid mijn privacy voldoende beschermt.



[1]Zie onder andere: TNO, Privacybeleving op het internet in Nederland (2015), te vinden op https://www.rijksoverheid.nl/documenten/rapporten/2015/02/01/privacybeleving-op-het-internet-in-nederland, Solove, D., Understanding privacy (2010) Harvard, MA: Harvard University Press en Nissenbaum, H., Privacy in Context: Technology, Policy, and the Integrity of Social Life (2009) Palo Alto, CA: Stanford University Press
[2]Te vinden op http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015.
[3]Te vinden op https://www.digid.nl/over-digid/kaartlezer-pilot/over-de-pilot-met-kaartlezer/.
[4]Zie voor een beschrijving van het commercieel exploiteren van deze kwestbaarheid voor $1500 dit artikel: http://www.bloomberg.com/news/articles/2016-03-10/what-happens-when-the-surveillance-state-becomes-an-affordable-gadget.

Geven van het goede voorbeeld

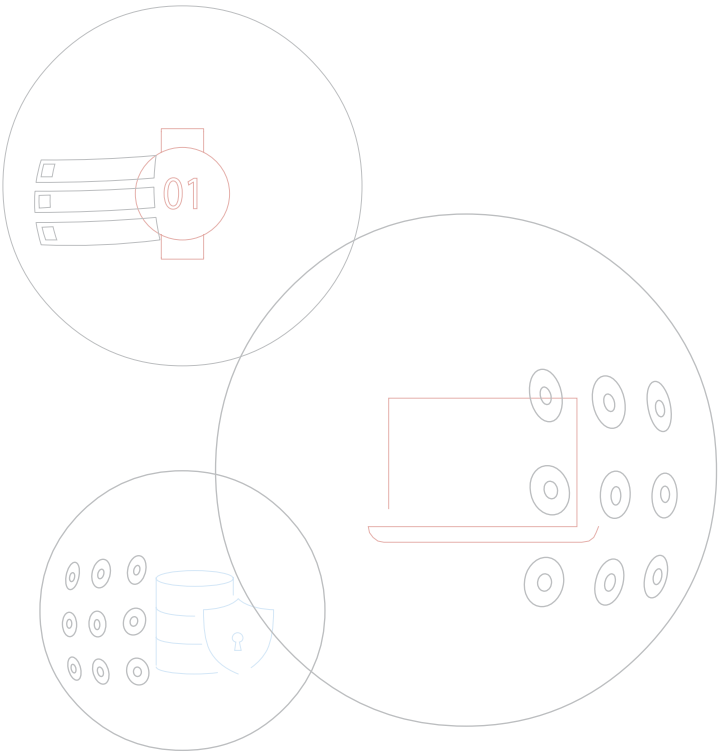
Waar burgers zelf hun gegevens moeten beschermen met technische maatregelen, is dit ook het geval voor de overheid. De overheid communiceert in toenemende mate digitaal met haar burgers waarbij online vertrouwelijke gegevens worden uitgewisseld. Een goed voorbeeld van deze digitale transformatie binnen de overheid is het verdwijnen van de blauwe envelop. De Belastingdienst wil tegenwoordig niet meer per brief, maar enkel online met de burger communiceren[5].
Daarom is het van buitengewoon belang dat de overheid het goede voorbeeld geeft en met technische en procedurele maatregelen haar gegevens (en dus indirect van de burgers) afschermt voor onbevoegden.
Hierbij kan worden gedacht aan het volgen van de eigen richtlijnen op het gebied van veilig webverkeer (denk aan Richtlijnen voor TLS[6]), maar ook in de eisen aan de eigen infrastructuur. Daarnaast kan in aanbestedingen meer aandacht besteed worden aan veiligheid. In het zogenaamde 'Forum Standaardisatie' beheert de overheid de lijst met verplichte open standaarden die gelden voor de gehele publieke sector. Deze standaarden zijn echter nog altijd in hoge mate onbekend en, indien bekend, onbemind bij overheden[7]. Consequenter vasthouden aan de eigen standaarden kan al een aanmerkelijke verbetering van digitale veiligheid tot stand brengen, ook al omdat het leveranciers en burgers kan dwingen om veiliger te werken.

Eigen verantwoordelijkheid van de burger

Natuurlijk moet niet alleen de overheid goede adviezen geven, het goede voorbeeld geven en een gedragscode opstellen. Burgers moeten zelf ook maatregelen nemen om hun persoonlijke gegevens te beschermen. Ruim 90% van de Nederlanders neemt maatregelen om zijn of haar privacy te waarborgen. Er zijn veel hulpmiddelen die de privacy beschermen. Veel van dit soort hulpmiddelen worden steeds gebruikersvriendelijker maar zijn niet allemaal standaard geïnstalleerd op de gebruikte apparatuur. Voorbeelden hiervan zijn apps die het mogelijk maken om beveiligd te bellen en berichten te sturen (zoals Signal), mailprogramma's die gebruik maken van PGP (Pretty Good Privacy), browsers die minder digitale sporen achterlaten en een zoekmachine als Duckduckgo die niet zoals Google je zoekgedrag monitort. Lang niet altijd doet men de moeite om deze hulpmiddelen op te zoeken en te installeren, terwijl dat wel een substantiële bijdrage aan meer privacy geeft[8].

Verder moeten burgers ook begrijpen wat de consequenties zijn van het delen van persoonlijke gegevens. Vooral de jongere generatie deelt vaak foto's en video's van intieme momenten. Het is wel makkelijker geworden om gegevens van internet te verwijderen, door minimaal de link naar gevoelige gegevens vanuit een zoekmachine te laten verwijderen (het zogenaamde 'recht om vergeten te worden').

[5]Dit lukt nog niet geheel, zie http://www.elsevier.nl/economie/article/2015/12/de-blauwe-envelop-nog-geen-volledig-vaarwel-2736197W/
[6]Te vinden op https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html
[7]Zie bijvoorbeeld Cybersecuritybeeld Nederland 2015, p. 51
[8]Zie onder andere: https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/



Conclusie

Techniek kan worden ingezet om massasurveillance tegen te gaan. De Nederlandse overheid geeft het goede voorbeeld, onder andere door encryptie te stimuleren. Het toepassen van technische maatregelen kan verder bevorderd worden door het goede voorbeeld te geven. Daarnaast kan de burger ook zelf diverse technische maatregelen nemen om zijn of haar privacy te waarborgen.
Als technische maatregelen worden geïmplementeerd en gestimuleerd, kan privacybevordering voor alle partijen (burgers, overheden en bedrijven) gerealiseerd worden.

Over de auteurs

Drs. Melle van den Berg en Daphne Gerritsen MA zijn consultant Security en Privacy bij Capgemini Consulting. Ton Slewe MBA is consultant bij Capgemini. Hij richt zich op cybersecurityvraagstukken bij publieke en private organisaties.

Voor meer informatie kunt u contact opnemen met de auteurs via: melle.vanden.berg@capgemini.com, daphne.gerritsen@capgemini.com en ton.slewe@capgemini.com