Rathenau Instituut

Hand-out privacywetgeving

Deskundigenbijeenkomst Eerste Kamer 20 juni 2017

De focus van de bijdrage van het Rathenau Instituut ligt op het wetsvoorstel Computercriminaliteit III.

Noodzaak en belang
Het wetsvoorstel Computercriminaliteit III maakt het voor opsporingsdiensten mogelijk om op afstand heimelijk te kunnen binnendringen in ICT-systemen van verdachte personen: van computers en mobiele telefoons tot webcams, routers en met het internet verbonden smart devices zoals 'slimme' thermostaten, auto's of medische apparatuur. Hierbij wordt gebruikgemaakt van nog niet verholpen kwetsbaarheden in hard- of software (zero-day kwetsbaarheden). Vanwege de toenemende dreiging die uitgaat van steeds professionelere cybercriminelen, valt er veel voor te zeggen dat politie en justitie de bevoegdheid krijgen om binnen te dringen in met het internet verbonden apparatuur van verdachte personen.

Randvoorwaarden
De voorgestelde uitbreiding van opsporingsbevoegdheden gaat ver, omdat politie en justitie hiermee in staat worden gesteld binnen te dringen in vrijwel alle vormen van elektronische communicatie. Deze bevoegdheidsuitbreiding dient dan ook aan strikte voorwaarden te zijn gebonden. Gebeurt dat niet, dan dreigt een disbalans te ontstaan tussen wat de overheid vermag en wat de burger daar tegenover kan stellen. De bevoegdheidsuitbreiding dient dan ook gepaard te gaan met kritisch en onafhankelijk toezicht op het gebruik dat de opsporingsdiensten maken van hun (ruimere) bevoegdheden en met waarborgen voor de rechtspositie van de burger.

Toezicht
Volgens het wetsvoorstel dient het gebruik door opsporingsdiensten van zero-day kwetsbaarheden vooraf door de Centrale Toetsingscommissie van het openbaar ministerie en een rechter-commissaris te worden getoetst. De Inspectie Veiligheid en Justitie ziet achteraf toe op een rechtmatig gebruik door opsporingsdiensten van hun bevoegdheden. Een belangrijke vraag is of dit toezicht volstaan. Hierbij is een vergelijking op zijn plaats met het toezicht door de CTIVD op het functioneren van de inlichtingen- en veiligheidsdiensten. De Inspectie lijkt minder onafhankelijk te opereren dan de CTIVD, omdat ze deel uitmaakt van het Ministerie van Veiligheid en Justitie. Ook beschikt de Inspectie over minder bevoegdheden dan de CTIVD. Zo kan ze personen niet onder ede verhoren. Dit roept de vraag op of het wetsvoorstel in voldoende mate voorziet in een kritisch en onafhankelijk toezicht op het gebruik dat opsporingsdiensten maken van hun (ruimere) bevoegdheden.

Rechtspositie burger
Het is van groot belang dat burgers over voldoende juridische mogelijkheden beschikken om zich te verweren tegen onterechte verdenkingen die voortvloeien uit het gebruik van de voorgestelde uitbreiding van opsporingsbevoegdheden. Ook hier is een vergelijking met het mandaat van de CTIVD op zijn plaats. In het wetsvoorstel voor modernisering van de Wet op de inlichtingen- en veiligheidsdiensten wordt voorzien in een klachtenfunctie van de CTIVD. Conform het wetsvoorstel, kan de CTIVD bindende uitspraken doen over klachten van burgers. Het wetsvoorstel Computercriminaliteit III voorziet niet in een vergelijkbare klachtenregeling voor burgers met betrekking tot het gebruik dat opsporingsdiensten maken van hun (ruimere) bevoegdheden. Burgers kunnen met klachten terecht bij de Nationale ombudsman. Deze beschikt echter over minder bevoegdheden dan de CTIVD en kan geen bindende uitspraken doen. Dat lijkt ons een omissie.

Aantasting cyberveiligheid door gebruik zero-day kwetsbaarheden
Daarnaast vormt een belangrijk punt van aandacht de aantasting van cyberveiligheid door het gebruik door opsporingsdiensten van zero-day kwetsbaarheden. Zolang deze kwetsbaarheden niet gemeld worden bij en verholpen zijn door de softwareproducent, kunnen bijvoorbeeld ook criminelen gebruikmaken van deze kwetsbaarheden. Het gebruik van zero-day kwetsbaarheden door opsporingsdiensten dient dan ook aan strikte voorwaarden te zijn gebonden. Andere partijen, zoals Bits of Freedom, hebben hiervoor reeds de nodige aandacht gevraagd.

Monitoring
Het wetsvoorstel Computercriminaliteit III voorziet in een evaluatietermijn van vijf jaar. Gezien de snelle technologische ontwikkelingen op het gebied van ICT, en in het bijzonder op het gebied van cyberdreigingen en cyberveiligheid, lijkt het raadzaam om deze termijn te bekorten. Het is in onze ogen nodig om de belangrijkste ontwikkelingen op het gebied van cyber(on)veiligheid, het gebruik dat opsporingsdiensten in de praktijk maken van hun bevoegdheden en de op dit gebruik betrekking hebbende rechtstatelijke ‘checks and balances’ (onafhankelijk toezicht en borging rechtspositie burger) periodiek te monitoren. Hiervoor valt te denken aan een periode van twee à drie jaar.

Cumulatieve effecten
Voor iedere uitbreiding van de bevoegdheden van opsporingsdiensten met een mogelijke impact op de persoonlijke levenssfeer, dient een zorgvuldige afweging te worden gemaakt tussen het opsporingsbelang en het belang van privacybescherming. Ook als deze afweging per dossier zorgvuldig gebeurt, kan het zijn dat het totaal aan opsporingsbevoegdheden, en het gebruik dat daarvan in de praktijk wordt gemaakt, leidt tot een ongewenste ‘surveillancecultuur’. Het is dan ook van belang om de effecten op de privacy van burgers van het geheel aan opsporings- en veiligheidsmaatregelen in samenhang en met een kritische blik te bezien. Hierbij is een belangrijke rol weggelegd voor het parlement. Periodiek en commissie-overstijgend debat draagt bij aan een betere borging van publieke waarden als privacy en daarvoor benodigde governance.

Relevante rapporten Rathenau Instituut
Een nooit gelopen race – Over cyberdreigingen en versterking van weerbaarheid (2017), https://www.rathenau.nl/nl/publicatie/een-nooit-gelopen-race
Opwaarderen - Borgen van publieke waarden in de digitale samenleving (2017), https://www.rathenau.nl/nl/publicatie/opwaarderen-borgen-van-publieke-waarden-de-digitale-samenleving