Wetsvoorstel computercriminaliteit III

Hieronder vind u mijn mening over twee punten uit het wetsvoorstel computercriminaliteit III, namelijk het verplicht meewerken van verdachten bij hun eigen veroordeling door het toegankelijk maken van versleutelde informatie en het binnendringen van computersystemen van verdachten door de overheid.

Verplichte ontsleuteling van gegevens

Bij het verplicht afstaan van encryptiesleutels wordt kinderporno en terrorisme als excuus gebruikt. Echter, uit niks blijkt dat het verplicht afstaan van deze sleutels kinderporno en terrorisme kunnen terugdringen.

Het feitelijke probleem met kinderporno zit hem in het maken van kinderporno waarbij kinderen misbruikt worden. Het verspreiden en bekijken van kinderporno voegt nauwelijks iets toe aan het misbruik. Wil je kinderporno bestrijden, dan moet je de vervaardiging aanpakken. Het verspreiden en verbergen van kinderporno is namelijk met een beetje kennis van het internet en computers dusdanig eenvoudig, dat het tegengaan hiervan eigenlijk zinloos is. Het is dweilen met de kraan open. En de bron van het probleem, namelijk pedofilie, gaat niet weg met dit soort wetten. Het bestrijden van kinderporno is dus geen valide argument voor het goedpraten van deze wet.

Een fout in de toelichting van deze wet is dat alleen maar wordt gesproken over wachtwoorden die moeten worden afgestaan. Versleuteling van informatie kan ook zonder wachtwoord gebeuren. De gebruikte encryptiesleutel kan bijvoorbeeld ook op een USB-stick geplaatst worden. Een gebruiker kan deze USB-stick verstoppen waardoor hij na aanhouding niet meer in staat is om deze af te staan. De wet is zelfs te omzeilen door bij de computer een kapotte USB-stick te bewaren, te zeggen dat de encryptiesleutel op deze kapotte USB-stick staat en vervolgens de schuld van het kapot-zijn leggen bij de politie die bij de aanhouding te onvoorzichtig is geweest met de UBS-stick.

Ik ben op zich niet tegen het verplicht afstaan van encryptiesleutels door pedofielen en terroristen, maar ik heb te weinig vertrouwen in dat deze wet niet op een later moment misbruikt zal gaan worden om ook op anderen momenten mensen te dwingen om inzage te geven in hun vertrouwelijke privéinformatie. Het grootste gevaar van deze wet voor mij is dus de function creep die op de loer ligt.

Terughacken

Terughacken is niet iets dat even gedaan wordt. Het vereist dat het doelsysteem een kwetsbaarheid bevat welke misbruikt kan worden om toegang te verkrijgen of dat de gebruikers misleidt worden tot het geven van die toegang.

In het geval van een kwetsbaarheid betekent dit dat de overheid weet moet hebben van zo'n kwetsbaarheid en dat deze kwetsbaarheid bij voorkeur niet bij anderen bekend is om de effectiviteit van het gebruik ervan te vergroten. Persoonlijk zie ik het niet gebeuren dat de overheid zelf kwetsbaarheden gaat zoeken. Deze zullen dus op de een of andere manier van anderen verkregen moeten worden. De overheid zal (met belastinggeld!) kwetsbaarheden moeten kopen. Daarbij is de vraag met welke zekerheid de overheid de enige partij is die vervolgens over deze kwetsbaarheid beschikt. Dit zal zeker niet het geval zijn want er is altijd minimaal een verkopende partij die ook over de kwetsbaarheid beschikt. Gezien het feit dat de partijen die kwetsbaarheden zoeken en verkopen over het algemeen geen eerlijke zakenmensen zijn is het niet aannemelijk dat deze kwetsbaarheden daarnaast niet aan andere partijen verkocht zullen worden. Door kwetsbaarheden te gaan gebruiken in plaats van mee te werken om ze te verhelpen, is de overheid met dit wetsvoorstel dus van plan actief mee te werken aan het onveilig houden van computersystemen.

Deze wet richt zich niet alleen op verdachten binnen Nederland, maar ook in het buitenland. Dit kan voor andere landen een excuus vormen om een eigen wet te maken die hen toestaat om ook systemen in andere landen aan te vallen. Het lijkt mij niet acceptabel als overheden van landen als China, Rusland en Iran onder hun voorwaarden systemen in Nederland gaan aanvallen.

Het wetsvoorstel richt zich op verdachten. Verdachten kunnen ook onschuldige mensen zijn. Het wetsvoorstel zegt over situaties waarbij de overheid ten onrechte inbreekt op de computer van een onschuldige. Gezien de aard van de techniek zal deze onschuldige persoon ook geen weet hebben van het feit dat de overheid zich onterecht toegang heeft verschaft tot zijn of haar privéinformatie.

Geen oplossing voor het probleem

Het wetsvoorstel computercriminaliteit III zal best kunnen leiden tot het oplossen van een aantal computercriminaliteitszaken, maar zal het feitelijke probleem niet verkleinen. Het internet is namelijk voortgekomen uit een netwerk dat meer gebouwd is op een basis van vertrouwen dan op een basis van veiligheid. En daar plukken we nu de zure vruchten van. De reden waarom computercriminaliteit bestaat is omdat het internet en veel van de daarop aangesloten systemen zijn gebouwd met te weinig aandacht voor beveiliging. Internetcriminaliteit bestaat in feite dus omdat wij het toestaan. Zo bestaan spam en phishing vanwege het ontbreken van ook maar enige vorm van beveiliging in het protocol dat gebruikt wordt voor het versturen van e-mail, wat desondanks is uitgegroeid tot een van de meest gebruikte diensten van het internet.

In plaats van je te richten op het achteraf pakken van internetcriminelen is het verstandiger om je te richten op het ontnemen van de mogelijkheid tot het plegen van computercriminaliteit. Als landen bijvoorbeeld gaan samenwerken om een veilig alternatief voor e-mail te maken zal dat meer bijdragen aan het terugdringen van computercriminaliteit dan welke wet dan ook.

Tendens

Los van wat ik zelf van deze wet vind is het wederom een wet die invloed heeft op de privacy van de burgers. Nederlandse burgers worden nu al gevolgd door middel van hun mobiele telefoon, camera's op straat, de OV-chipkaart en ANPR-systemen. Telefoons worden op grote schaal afgetapt en het internetverkeer wordt vastgelegd. Van onschuldige burgers worden vingerafdrukken afgenomen en zij dienen zich te laten fouilleren als zij daartoe worden opgedragen. Een overheid *voor* de burger lijkt steeds meer een overheid *tegen* de burger te worden. Bij alle maatregelen die de laatste jaren zijn ingevoerd is de veiligheid nauwelijks veranderd. Want voor de ene afnemende vorm van criminaliteit komt een andere in de plaats.

De overheid moet zich eens gaan afvragen hoe de Nederlandse burger naar de overheid gaat kijken nu de overheid de Nederlandse burger meer en meer als potentiële crimineel gaat zien en behandelen.