Het sleepnet

Ik maak me uitgebreid zorgen over het wetsvoorstel dat er een sleepnet kan worden ingezet door inlichtingendiensten.

Waar Nederland hoog in aanzien stond met betrekking tot privacy en beveiligingsperpectief kan dat na invoering van dit wetsvoorstel dit als positie verliezen met economische schade van Nederlandse bedrijven als gevolg.

Veel kleine Nederlandse netwerken zullen niet de kosten kunnen bewerkstelligen om het netwerk makkelijk aftapbaar te maken en zullen de deuren moeten sluiten.

De proportinaliteit van het wetsvoorstel dat er zomaar data kan worden afgetapt van international en nationaal verkeer lijkt niet in contrast te staan met een redelijke verdenking van bijvoorbeeld terroristische daden of spionage door staten.

De impact van een daadwerkelijk sleepnet zal zijn dat bronnen binnen de overheid en in andere kritieke pilaren van de samenleving stil zullen zijn. Journalisten zich zorgen moeten maken of de bron niet kan worden achterhaald via het sleepnet, ook als de data wordt verwerkt.

Toen het Amerikaanse NSA zogenaamde malware data[1] ging verzamelen en dat ging delen met het bedrijfsleven, denk hierbij aan banken en internet service providers, kwamen ze er al gauw achter dat ze de dezelfde informatie leverde als de fox-it's van deze wereld. Bedrijven op de hoogte stellen van spionage gaat ten kosten van de privacy van de rest van Nederland. Als de Nederlande overheid dit tegen zou willen gaan is een grotere investering in het gebruik van open source technologie een beter hulpmiddel net als educatie in veilig gebruik maken van het internet.

Tevens maak ik me zo grote zorgen over het feit dat er derde partijen gehacked kunnen worden om bij het daadwerkelijke doelwit te komen. Zo is er niet bekend of deze derde partijen ooit op de hoogte zullen worden gebracht dat er op op een digitaal apparaat is ingebroken door een van de inlichtingendiensten. Hoeveel informatie mag de inlichtingendienst van de derde partij opslurpen? Er zijn onvoldoende waarborgen om een derde partij slachtoffer te laten worden van de surveillance van het daadwerkelijke doelwit van de operatie.

In artikel 41 wordt er gesproken over het forceren van internet service providers om internetverkeer te ontsleutelen als dat wordt gewenst mochten ze toegang hebben tot de sleutels. Er is geen gerechtelijke toetsing die hieraan vooraf gaat.

De e-mail provider Lavabit in de Verenigde Staten heeft zijn deuren gesloten omdat het geforceerd werd door de autoriteiten encryptie sleutels te overhandigen om zo te kunnen spioneren

Dit heeft in Frankrijk geleid tot diverse internetbedrijven die zeiden de deuren te willen sluiten en naar een ander land te verhuizen waar dit niet het geval is.

Ik heb mijn vraagtekens bij de proportinaliteit van de voorgestelde artikel 41 van de wiv en zou het niet geimplementeerd zien worden.

[1] @War: The Rise of the Military-Internet Complex [boek]

Toezicht

Het is een onverstandige keuze om beslissing of een specifieke inzet terecht of onterecht genomen is bij de commissie Stiekem neer te leggen. Een gerechtelijke toetsing en onafhankelijke toetsing van NGO's als Fair Trials, Amnesty International, Human Rights Watch en Privacy international neer te leggen. Zo is er een scheiding van machten zoals we kennen van de Trias Politica en is er een mogelijkheid van NGO's om hier over te rapporteren en onafhankelijk een mening te geven over de inzet van de beslissingen.

Uitwisseling met buitenlandse diensten

Het is belangrijk dat er data wordt uitgewisseld met buitenlandse diensten dit moet alleen wel zorgvuldig gebeuren en alleen gericht.

Met gericht zou het zo moeten zijn dat wanneer we buitenlandse diensten toegang geven om iemand te targetten en deze bepaalde "selectors" gebruikt om deze persoon te volgen, dit moet worden gekeurd via een gerechtelijkse toetsing of dit proportioneel is om toe te passen en of dit valt binnen de Nederlandse wet.

Deze persoon zou ook op de hoogte moeten kunnen worden gesteld als deze nog op een manier gecontacteerd kan worden binnen het Koninkrijk der Nederlanden.

Er wordt in het voorstel niet gerept over de plaatsing van technologie van buitenlandse diensten in Nederland. Edward Snowden, de NSA klokkenluider heeft doormiddel van artikelen in gerespecteerde media in binnen en buitenland laten weten dat er technologieen worden toegepast op alle metadata welke wordt afgetapt door diensten en deze onderling uit wisselen via het quid pro quo stelsel. Hoe gaat hier mee worden omgegaan? En krijgen buitenlandse diensten zomaar de data als ze de technologie laten gebruiken door onze nationale diensten?