Inbreng Ronald Prins voor rondetafelgesprek Tijdelijke wet Cyberoperaties

Introductie

Vanaf het moment dat de huidige wet op Inlichtingen- en Veiligheidsdiensten actief werd heb ik twee jaar gewerkt als het Technisch Lid van de Toetsingscommissie Inzet Bevoegdheden (TIB). Ondanks dat ik met veel plezier het werk gedaan heb, ging het me wel steeds meer tegenzitten dat we zeer relevante en legitieme aanvragen van de diensten moeten afkeuren.

Waar oorspronkelijk voorzien was in een wet die redelijk abstract was en ruimte bood aan de toezichthouder om deze praktisch in te vullen, is door de uitgebreide wetsbehandeling de keuzevrijheid op een aantal cruciale punten heel erg beperkt. Je zou ook achteraf kunnen zeggen dat we als toezichthouder te veel naar de letter van de wet gekeken hebben en niet naar de geest van de wet.

Ik lees in de media nogal eens dat met de tijdelijke wet sprake is van uitbreiding van de bevoegdheden van de diensten. Ik zie het eerder als een reparatie van de wet zoals die eigenlijk bedoeld was.

Twee hoofdzaken uit de Tijdelijke wet zou ik graag vooraf toelichten aan u.

Kabeltap

Het belangrijkste doel van de WIV2017 was de inzet van wat ik noem de kabeltap voor de diensten. Met de kabeltap is het mogelijk om niet gericht op 1 persoon een tap te zetten maar op een kabel waarvan een hele grote groep computers de data doorheen stroomt.

In de vijf jaar dat de wet bestaat, is het nog niet gelukt de kabeltap daadwerkelijk op een serieuze manier in te zetten. De reden is omdat de wet vereist dat de tap zo gericht mogelijk moet zijn. Als je dat strikt interpreteert sluit dat nooit aan bij waar het middel voor bedoeld is, en zal je als toezichthouder elke aanvraag moeten afwijzen.

Ik denk dat de voorgestelde weg in de Tijdelijke wet, waarbij er eerst door technisch specialisten onderzoek gedaan mag worden aan wat voor soort verkeer over de kabels gaat, en daarna pas een gerichte aanvraag gedaan wordt, een goede reparatie is.

De aard van het internet brengt met zich mee dat er geen ‘telefoonboekjes” bestaan waarin te vinden is wat er op de internetkabels te vinden zal zijn. De diensten zullen deze telefoonboekjes zelf moeten maken. Als die informatie eenmaal bekend is, kan de dienst pas een daadwerkelijk zo gerichte mogelijke aanvraag indienen. Omdat de lat laag ligt om een voorverkenning te mogen uitvoeren, is het gepast dat de hiermee verkregen informatie niet doorgezet naar analisten van de diensten.

Graag breng ik ook nog onder de aandacht dat de waarde van een kabeltap zeer groot is voor de veiligheid van Nederland. De cybersecurity bedrijven in Nederland hebben op dit

moment hun handen vol aan het stoppen van digitale aanvallen. Wij doen dit op de eindpunten van de internet infrastructuur bij een zeer beperkt aantal bedrijven en overheidsorganisaties. Met de kabeltap kunnen de diensten, laten we zeggen bij de landsgrenzen, al vaststellen welke organisaties in Nederland worden aangevallen.

Hacken en technische risico's

Op dit moment wordt van de diensten verwacht dat ze van tevoren aangeven aan de TIB welke technische risico's mogelijk ontstaan bij een door hun uitgevoerde hackoperatie. Het idee hierbij is dat de hackers mogelijk schade veroorzaken aan computers waardoor deze uitvallen.

Het is goed om te begrijpen dat de aard van het werk van geheime diensten al met zich meebrengt dat ze hun werk zo onopvallend mogelijk willen doen. Ze zullen zo min mogelijk sporen achterlaten en computers laten crashen, is zeker iets dat ze willen voorkomen. Dit brengt met zich mee dat ook een andere vorm van toezicht mogelijk is, dan waar het gaat om de diensten kort te houden bij het verzamelen van inlichtingen.

Een hackoperatie van de diensten is een project dat zo maar meerdere weken inneemt waarbij door meerdere lagen beveiliging heen ingebroken wordt. Pas onderweg tijdens het hacken ontdekken ze welke apparatuur bij de targets geïnstalleerd staat en kunnen ze daadwerkelijk pas wat zeggen over eventuele risico's. Daarmee past het beter dat het aspect van de technische risico's tijdens de hackoperatie wordt beschouwd.

Daarnaast is tijdens hackoperaties haast geboden. Zeker bij het digitaal volgen van Russische en Chinese hackersgroepen die zich online zeer snel verplaatsen. De diensten vragen terecht om ruimte om mee te bewegen en niet telkens terug te moeten naar de TIB voor elke nieuwe computer die ze ontdekken. De suggestie wordt wel eens gedaan om daarvoor de reeds bestaande spoed mogelijkheid in te zetten waarmee in noodgevallen de TIB omzeild kan worden. Ik denk echter dat dat juist een stap achteruit is. De spoed mogelijkheid moet een uitzondering blijven en niet iets wat structureel ingezet wordt.

Ik kijk uit naar uw vragen.