Bezoekadres
Turfmarkt 147
2511 DP Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

I www.cybersecurityraad.nl
T 070 751 5333 (secretariaat)
E info@cybersecurityraad.nl

Datum
23 augustus 2022

Onderwerp
Adviesbrief inzake reële alternatieven voor rechtmatige toegang tot end-to-end versleutelde communicatie, anders dan inperking van encryptie.

Ministerie van Economische Zaken en Klimaat
T.a.v. Mw. Mr. Drs. M.A.M. Adriaansens
Postbus 20401
2500 EK Den Haag

Excellentie,

De beschikbaarheid en het gebruik van end-to-end encryptie[1] is de laatste jaren sterk toegenomen. Elektronische communicatiediensten, zoals WhatsApp, Signal of Telegram, zetten met de implementatie van deze vorm van encryptie sterk in op het beschermen van de privacy van gebruikers en op het waarborgen van de vertrouwelijkheid van hun communicatie. Een goede zaak, maar zoals vaak in de complexe digitale wereld heeft dit ook een keerzijde: sterke encryptie bemoeilijkt de werkzaamheden van inlichtingen- en opsporingsdiensten, waardoor andere veiligheidsrisico's in brede zin ontstaan. Het gebruik van dergelijke encryptie heeft impact op de opsporing, die steeds complexer wordt[2] door de kansen die digitalisering helaas ook aan criminelen biedt. Dit wordt zichtbaar door de toename van gedigitaliseerde criminaliteit en cybercrime.

De problematiek rond het behouden van rechtmatige toegang door inlichtingen- en opsporingsdiensten tot (beveiligde) communicatie en digitaal opgeslagen informatie van verdachten of slachtoffers heeft op dit moment uw aandacht. Zo lopen er verschillende nationale (wetenschappelijke) onderzoeken en inventarisaties rond dit onderwerp. Op deze wijze kunnen argumenten verzameld worden langs verschillende thema's en vraagstukken, om een goed geïnformeerd publiek debat te kunnen voeren en beleidskeuzes te kunnen maken. De Cyber Security Raad (hierna: de raad) juicht deze initiatieven toe.

Ook de Europese Unie ziet de ontwikkeling van sterke encryptie van elektronische communicatie enerzijds als randvoorwaarde om de grondrechten van burgers en hun digitale beveiliging te waarborgen, waarbij het anderzijds noodzakelijk is dat daartoe bevoegde opsporings- en inlichtingendiensten hun werkzaamheden zowel online als offline adequaat kunnen blijven uitvoeren. Hiermee staan we opnieuw voor een dilemma omtrent encryptie, waarvoor op korte dan wel middellange termijn geen oplossingen te verwachten zijn die aan alle verschillende belangen volledig tegemoet kunnen komen.

De raad dringt er daarom op aan dat er - vooruitlopend op bovengenoemde discussies en onderzoeken en zonder stellingname over de (on-)wenselijkheid van functionele of technische inperkingen van encryptie - gekeken wordt naar reële alternatieve mogelijkheden die nodig zijn voor het uitvoeren van inlichtingen- en opsporingstaken. De overheid heeft immers een inspanningsverplichting jegens haar burgers om de maatschappelijke veiligheid en orde te bewerkstelligen.

[1] Bij end-to-end encryptie kunnen alleen de zender en ontvanger de betreffende informatie lezen of beluisteren.
[2] Zie bijvoorbeeld Politiefunctie in een veranderende omgeving | Working Paper | WRR

De raad adviseert in deze brief over reële alternatieven voor rechtmatige toegang tot end-to-end versleutelde communicatie, anders dan inperking van encryptie. Daarbij wil de raad benadrukken dat het niet om alternatieven gaat die tot een volwaardige vervanging zullen kunnen leiden, maar de raad is wel van mening dat een brede, andere benadering van dit vraagstuk *waardevol én noodzakelijk* is.

Achtergrond

Bij traditionele telefonie is er sprake van centrale knooppunten, onder controle van (nationale) telecomaanbieders, waar de betreffende communicatie beschikbaar is en waar taps geplaatst kunnen worden, onder nationale jurisdictie. De commercieel beschikbare telecominfrastructuur is daarop ingericht, via technisch, juridisch en organisatorisch gestandaardiseerde interceptiefunctionaliteit. Echter, moderne elektronische communicatiediensten werken via internet, en veelal buiten het domein van telecomaanbieders, waardoor er geen vaste nationale tappunten zijn. Dergelijke over-the-top (OTT) diensten maken steeds vaker gebruik van end-to-end encryptie. Hierdoor zijn de gangbare interceptiemethoden voor deze OTT-diensten niet meer effectief en is de toegankelijkheid van veel inhoudelijke communicatie verdwenen.

Niet alleen de rechtmatige toegang tot versleutelde communicatie bij OTT-diensten staat onder druk; ook bij de 5G-telecominfrastructuur die momenteel uitgerold wordt, zijn er aanpassingen nodig. Hiervoor worden momenteel oplossingsrichtingen gezocht. Door encryptie van signaleringsinformatie bij 5G, kan een buitenlandse 5G-telefoon in Nederland namelijk in beginsel niet getapt worden, en vice versa. Overigens wordt ook hier gesproken over het behoud van de (huidige) mogelijkheden, teneinde het nationaal tappen van internationale telefoons mogelijk te (blijven) maken.

Om tot oplossingen te komen voor de geschetste OTT-interceptieproblematiek zal een gezamenlijke Europese aanpak noodzakelijk zijn; het betreft hier immers wereldwijd opererende aanbieders. Dit geldt eveneens voor 5G-oplossingen, waarbij er nieuwe internationale afspraken tussen telecomaanbieders en overheden over rechtmatige toegang nodig zijn, zowel ten aanzien van technische standaarden als synchronisatie van wetgeving.

Verkenning van alternatieven voor rechtmatige toegang door inlichtingen- en opsporingsdiensten

De raad heeft een korte inventariserende verkenning uitgevoerd naar alternatieven voor het inperken van encryptie. De raad heeft dit primair vanuit een technische invalshoek gedaan, waarbij gebruik is gemaakt van de inventarisatie en aanbevelingen van een technische werkgroep. Twee onderwerpen blijken goede aanknopingspunten te bieden, te weten (A.) het optimaliseren van hackactiviteiten en (B.) het intensiever gebruikmaken van bedrijfsvoeringsgegevens (hierna: bedrijfslogs). In de bijlage[3] bij deze brief treft u het rapport van de hiervoor genoemde technische werkgroep aan, waarin een meer uitgebreide toelichting op beide onderwerpen is gegeven. Op basis daarvan trekt de raad de volgende conclusies:

A. *Optimaliseren van hackactiviteiten*

   De raad concludeert dat hacken weliswaar een zeer waardevol instrument is voor de inlichtingen- en opsporingsdiensten, maar qua schaalbaarheid en voorspelbaarheid van de opbrengst niet te vergelijken is met het aftappen van reguliere telefonie via medewerking van aanbieders van openbare telecommunicatienetwerken en –diensten, hetgeen volgens de Telecommunicatiewet verplicht is. De praktische inzetbaarheid van de hackbevoegdheden zou verbeterd kunnen worden via beter passende juridische kaders en toezicht, in combinatie met technische optimalisatie. Door verankering en stroomlijning van hacken als opsporingsmiddel kan dit middel sneller en efficiënter worden ingezet en daarmee laagdrempeliger in gebruik zijn.

[3] Eindverslag technisch-inhoudelijke werkgroep 'reële alternatieven voor encryptie', Den Haag, 25 maart 2022

B. *Intensiever gebruikmaken van bedrijfslogs*

De raad concludeert dat er nog veel winst te behalen valt op dit gebied; bedrijven voldoen nu vaak erg langzaam en incompleet aan de wettelijke plicht om bedrijfslogs te leveren in reactie op wettelijke vorderingen van overheden in het opsporings- en veiligheidsdomein. Ten eerste is het mogelijk om binnen de huidige kaders assertiever te opereren en daarmee jurisprudentie te creëren, waardoor de gerichtheid en voorspelbaarheid van dergelijke trajecten toeneemt. Ten tweede kunnen door nieuwe wetgevingstrajecten, waaronder de versterking van de wettelijke basis voor (internationale) vorderingen, obstakels en onduidelijkheden verder worden weggenomen en ontstaat er een betere samenwerking en kaderstelling.

Adviezen

Als mogelijke alternatieven voor het verkrijgen van rechtmatige toegang tot versleutelde elektronische communicatie adviseert de raad om in te zetten op het optimaliseren van hackactiviteiten en het intensiever gebruikmaken van bedrijfslogs. Dit kan gerealiseerd worden door opvolging te geven aan de aanbevelingen van de technische werkgroep. Deze alternatieven zullen echter niet leiden tot een volwaardige vervanging van de bestaande interceptiebevoegdheden, zodat de teloorgang van aftapbaarheid gevoeld zal blijven worden.

Het is de verwachting dat onder andere door synchronisatie en interpretatie van wetgeving op Europees niveau adequate opvolging van de adviezen mogelijk is. Daarvoor is inzet van Europese gremia voor standaardisatie noodzakelijk, waarbij er binnen Nederland een gezamenlijke ministeriële verantwoordelijkheid ligt. Zo zou het ministerie van Economische Zaken en Klimaat de voortgang kunnen monitoren en zouden experts vanuit de inlichtingen- en opsporingsdiensten inhoudelijke bijdragen kunnen leveren, onder aansturing van de ministeries van Justitie en Veiligheid, Binnenlandse Zaken en Koninkrijksrelaties, en Defensie.

Hieronder volgt een opsomming van de verschillende adviezen.

Algemene adviezen aan de minister van Justitie en Veiligheid en de minister van Economische Zaken en Klimaat gezamenlijk:

1. *Probeer de verminderde tapmogelijkheden niet op één enkele wijze op te vangen, maar bekijk het geheel, als spectrum van mogelijke alternatieve middelen.*
2. *Bewerkstellig in een Europees kader voor het tappen van 5G-verbindingen eenzelfde transparantie, uniformiteit en rechtszekerheid, als nu gangbaar is in de telecomwereld.*

Advies ten aanzien van het intensiveren van hackactiviteiten aan de minister van Justitie en Veiligheid en de minister van Economische Zaken en Klimaat gezamenlijk:

3. *Onderzoek de mogelijkheid van een transparante wettelijke regeling voor versterkte toegang bij telecomproviders, teneinde een betere uitgangspositie te hebben om specifieke mobiele telefoons te kunnen hacken.*

Advies ten aanzien van het intensiveren van hackactiviteiten aan de minister van Justitie en Veiligheid:

4. *Zorg voor beter passende juridische kaders en toezicht, in combinatie met technische optimalisatie, om zo het hacken als opsporingsmiddel bij de politie te verankeren en te stroomlijnen. Daarbij horen de kanttekeningen dat hacken een hoge drempel kent, slecht schaalt, maatwerk vraagt, vooral geschikt is voor grote zaken en geen gegarandeerde opbrengst biedt.*

Adviezen ten aanzien van gebruik van bedrijfslogs aan de minister van Justitie en Veiligheid en de minister van Economische Zaken en Klimaat gezamenlijk:

5. *Beweeg aanbieders van online diensten tot verbeterde medewerking met de inlichtingen- en opsporingsdiensten bij het leveren van bedrijfslogs. Neem eventuele obstakels en onduidelijkheden weg door enerzijds in te zetten op nauwere samenwerking en afstemming en anderzijds parallel daaraan beter gebruik te maken van reeds bestaande juridische mogelijkheden om tot punctuele levering te komen. Dit kan op korte termijn via jurisprudentie en op langere termijn via (internationale) wetgeving.*
6. *Benader deze vordering van gegevens meer vanuit Nederlands/Europees perspectief, om interpretatiekwesties onder Amerikaans recht te vermijden. Het opvragen zou zoveel mogelijk via de Nederlandse/Europese vestigingen van de betrokken bedrijven moeten lopen, met gebruik van Europese wet- en regelgeving.*
7. *Zet meer in op publiek-private samenwerking met leveranciers van diensten in de informatiesamenleving en benadruk de maatschappelijke zorgplicht die grote ICT-partijen daarbij hebben.*

Dit advies is ook schriftelijk aangeboden aan de minister van Justitie en Veiligheid. Daarnaast is een afschrift van dit advies ter kennisgeving gestuurd naar:

- De staatssecretaris Koninkrijksrelaties en Digitalisering van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties;
- De minister van Binnenlandse Zaken en Koninkrijksrelaties;
- De minister van Defensie.

Namens de Cyber Security Raad,

Sylvia van Es
Covoorzitter CSR

Bijlage: Eindverslag bevindingen technisch-inhoudelijke werkgroep encryptie