Verslag bevindingen technisch-inhoudelijk werkgroep Encryptie

Definitief vastgesteld: 25 maart 2022

Inleiding

Het onderstaande is een verslag van een ad hoc werkgroep die samen met leden Jacobs en Van Eeten van de Cyber Security Raad (CSR) in de drie maanden Nov'21 – Jan'22 een aantal maal (online) samengekomen is. Aan deze werkgroep werd (verder) deelgenomen door:

- Twee operationeel specialisten-digitaal vanuit het Team High Tech Crime van de politie;
- Een persoon vanuit de AIVD, met een technische/beleidsmatige achtergrond;
- Een senior adviseur bij het Platform Interceptie Decryptie & Signaalanalyse (PIDS) van het Ministerie van Justitie en Veiligheid;
- Een senior beleidsadviseur bij de Directie Digitale Economie / Directoraat-Generaal Bedrijfsleven en Innovatie, Ministerie van Economische Zaken en Klimaat;
- Een Adviseur Strategie en Beleid, vanuit KPN CISO Office.

De werkgroep werd begeleid door een senior adviseur bij Bureau Secretaris van de CSR.

De vraag/opdracht waarmee de werkgroep aan de slag is gegaan luidt als volgt.

> *Welke reële alternatieven zijn er om rechtmatige toegang tot end-to-end versleutelde communicatie te krijgen, anders dan verzwakking van encryptie?*

De werkgroep had dus nadrukkelijk *niet* de opdracht om te kijken naar mogelijkheden om encryptie te doorbreken, maar juist om alternatieven daarvoor te onderzoeken. De werkgroep heeft in een aantal interne expertsessies in de breedte naar de vraagstelling gekeken en is uitgekomen bij twee belangrijke onderwerpen: (1) **hacken**, door politie en inlichtingendiensten, en (2) **vordering van bedrijfslogs**, d.w.z. van gegevens die bedrijven verzamelen voor hun bedrijfsvoering. Dit verslag gaat, na een korte inleiding, nader in op deze twee onderwerpen en komt dan tot enkele aanbevelingen.

Wanneer in het onderstaande gesproken wordt over interceptie (tappen) van telefoonverkeer en van andere vormen van communicatie is de aanname steeds dat dit slechts plaatsvindt door de daartoe bevoegde instanties (met name: politie en inlichtingen & veiligheidsdiensten) binnen de daarvoor bestaande wettelijke kaders, met de juiste toestemmingen en de verschillende vormen van toezicht. Hetzelfde geldt voor inzet van de hackbevoegdheid. Onder deze bevoegdheid wordt een grote verscheidenheid aan activiteiten uitgevoerd. Deze variëren van het (forensisch) kopiëren van een USB-stick of harde schijf, tot het uitvoeren van een gecompliceerde hack-operatie op grote netwerken. Als er gesproken wordt over de handeling 'hacken' wordt eigenlijk altijd het op afstand binnendringen in computers bedoeld. Die interpretatie wordt hier ook gevolgd.

Het tappen is de afgelopen tientallen jaren internationaal uitgekristalliseerd, zowel technisch, als organisatorisch en juridisch. Deze (publieke) standaardisatie van interfaces en architectuur voor interceptie biedt veel voordelen: enerzijds rechtszekerheid voor burgers en anderzijds professionele duidelijkheid en uitvoerbaarheid voor de opdrachtgevers en uitvoerders. Commercieel beschikbare telecom infrastructuur omvat deze gestandaardiseerde tap functionaliteit.

Met de *end-to-end* (E2E) versleuteling van moderne, populaire *over-the-top* (OTT) berichtendiensten (zoals: Whatsapp, Signal, Telegram) is deze toegankelijkheid en overzichtelijkheid (voorgoed) verdwenen. Omdat een

heldere structuur zoals die voor het tappen van telefoons gefunctioneerd heeft niet bestaat voor OTT-diensten – en op korte en middellange termijn ook niet te verwachten is – is het belangrijk om zicht te hebben op het spectrum aan alternatieven dat voor handen is. Deze notitie heeft een technische focus en bespreekt bijv. niet de juridische alternatieven, zoals verruiming van de mogelijkheden voor online infiltratie. Deze notitie is in korte tijd tot stand gekomen, gebaseerd op zeer beperkt onderzoek, en heeft geen pretentie van volledigheid.

Overigens staat het tappen niet alleen door de beschikbaarheid van deze OTT-diensten onder druk. Ook bij de 5G infrastructuur die nu uitgerold wordt is er nog geen internationale helderheid. Door de versleuteling van signaleringsinformatie bij 5G kan een buitenlandse 5G telefoon in Nederland in beginsel niet getapt worden. Andersom bestaat dit probleem ook. Alleen in het land van herkomst kan de ontsleuteling van de signaleringsgegevens, en daarmee de tap, plaatsvinden. Om nationaal tappen van internationale telefoons wel mogelijk te maken moet in de (honderden) roamingsovereenkomsten tussen telecomaanbieders afgesproken worden om deze versleuteling uit te zetten. Aanbieders staan enerzijds onder druk van hun klanten (en van de AVG) om *wel* te versleutelen en anderzijds onder druk van justitiële autoriteiten (in Europa) om *niet* te versleutelen, om internationale taps mogelijk te maken. Deze discussie loopt nog, waarbij Nederland in Europa een actieve rol speelt. Op deze discussie zelf wordt hier niet verder ingegaan.

1. Hacken

Inlichtingen & veiligheidsdiensten hebben sinds de WiV 2002 de wettelijke basis om computers (van targets) te kunnen binnendringen, ofwel rechtstreeks, ofwel indirect. De wet CC III geeft de politie sinds 2019 een vergelijkbare bevoegdheid om op afstand computers binnen te dringen. Bij de inlichtingen & veiligheidsdiensten is hacken een standaard onderdeel van de werkwijze geworden. Bij de politie is het middel nog niet zo ver ingedaald en uitgekristalliseerd (zie het rapport Verslag toezicht wettelijke hackbevoegdheid politie 2020 en een nog te verschijnen rapport van het WODC). De politie heeft te maken met zwaardere beperkingen bij het uitvoeren van hacks, met name op het gebied van de tools en de kwetsbaarheden die ingezet mogen worden.

Bij hacken kan tot op zekere hoogte gebruik gemaakt worden van tools (of scripts) die ofwel aangekocht ofwel zelf opgezet zijn. De markt voor deze tools is omstreden, zie de discussie rond het Israëlische bedrijf NSO, dat nu uitgesloten is in de V.S. Zulke tools zouden hacken makkelijker kunnen maken, maar hebben als nadeel dat ze, op basis van hun uniforme werkwijze, door targets herkend kunnen worden. Ook is de effectiviteit op de langere termijn van deze tools onzeker, omdat de kwetsbaarheden waar ze nu gebruik van maken, op een goed moment onbruikbaar kunnen worden, typisch door een patch.

Hacken is voor een groot deel maatwerk en handwerk. Het middel is niet (internationaal) technisch/ organisatorisch/juridisch gestandaardiseerd. De kosten zijn hoog, zowel administratief en operationeel, en de capaciteit is beperkt, waardoor de drempel hoog is. Het is bovendien niet schaalbaar: als je een twee keer zo grote hack-opbrengst wil, heb je twee keer zo veel hackers nodig.

Met hacken zijn de laatste jaren indrukwekkende resultaten behaald, zoals de ontmanteling van verschillende beveiligde communicatienetwerken van criminelen. Juist voor dit soort grote zaken, met een lange adem, is hacken een geschikt middel gebleken. Maar ook daar is de opbrengst vooraf onzeker.

Hacken kan gericht zijn op (hosting) infrastructuur en tegen de daar actieve verdachten/targets. Het hacken van mobiele telefoons is trager van de grond gekomen omdat een daarvoor geschikte uitgangspositie minder vanzelfsprekend voorhanden is. Op dit punt is verbetering voorstelbaar, via een nieuwe wettelijke en technische regeling, waarbij politie en inlichtingen & veiligheidsdiensten een betere uitgangspositie krijgen bij telecomproviders, zodat ze directe toegang hebben tot de verkeersstromen van-en-naar een specifieke telefoon. Daarbij blijft *end-2-end* versleuteling (noodzakelijkerwijs) onaangetast, maar is er wel een betere toegang om via een hackoperatie op een specifiek telefoontoestel binnen te dringen.

2. Bedrijfslogs

Omdat OTT-diensten *end-2-end* versleuteld zijn hebben de bedrijven die deze diensten aanbieden zelf geen toegang tot de inhoud van de communicatie. Wel slaan ze met betrekking tot deze communicatie allerlei bedrijfsvoeringsgegevens (logs) op, o.a. voor het kunnen uitvoeren van de dienst, voor fraude-detectie, voor profilering en marketing. Het gaat dan om de identiteit van de betrokkenen, de contacten, tijdstippen, locaties, duur, omvang en aard van de berichten, etc. Ook kunnen deze bedrijven op de toestellen zelf controles uitvoeren, in hun eigen apps, en kunnen ze daar de mogelijkheid bieden tot een (versleutelde) backup van het berichtenverkeer. Wat precies bijgehouden en opgeslagen wordt is in het algemeen niet bekend.

De Nederlandse politie en inlichtingen & veiligheidsdiensten vragen met enige regelmaat gegevens op bij (vaak Amerikaanse) aanbieders van OTT-diensten. Daarbij spelen de verschillen een rol tussen de rechtssystemen van Nederland/Europa en van de V.S., en tussen de daarin gebruikte begrippen en interpretaties. In Nederland wordt gewoonlijk een onderscheid gemaakt tussen identificerende en niet-identificerende gegevens, in lijn met de AVG. In de V.S. is het onderscheid tussen inhoud en meta-data van groter belang. Deze onderscheidingen sluiten niet op elkaar aan. Zo worden locatiegegevens in Nederland als meta-data gezien, maar in de V.S. als inhoud. In de praktijk kunnen account-gegevens (geregistreerd bij het aanmaken van het account) rechtstreeks bij het bedrijf zelf opgevraagd; ze worden dan relatief snel geleverd (in de orde van weken). Andere (gebruiks)gegevens moeten via het Amerikaanse ministerie van Justitie opgevraagd worden. Die procedure duurt langer (in de orde van maanden), waarbij niet altijd alle gegevens geleverd worden. De betrokken bedrijven houden de boot nogal eens af met als verweer dat ze niet weten waar de gevraagde gegevens staan. Het merendeel van de Nederlandse opvragingen betreft daarom accountgegevens.

Onderzoekers bij politie en inlichtingen & veiligheidsdiensten zijn vaak zaak-gedreven, zonder strategisch lange-termijn perspectief. Ze zijn gewend verschillende routes te bewandelen en schakelen makkelijk over van de ene route naar de andere wanneer bepaalde opbrengst tegenvalt. Hierdoor is van gebrekkige levering van bedrijfslogs nooit een fundamentele zaak gemaakt en is er ook nog nooit een juridische procedure gestart om (snellere, uitgebreidere) levering af te dwingen. Ook is, zover bekend, niet geprobeerd om betrokken bedrijven via hun vestigingen in Nederland aan te spreken onder Nederlands recht. Hier ligt ruimte voor verbetering. Ook zou de wettelijke basis voor (internationale) vorderingen versterkt kunnen worden. Daarnaast biedt publiek-private samenwerking bij fraude-bestrijding ruimte voor een meer effectieve aanpak, inclusief hulp aan slachtoffers.

3. Aanbevelingen

1. Probeer de verminderde opbrengst van de traditionele goedgeorganiseerde telefoontaps niet op één enkele wijze op te vangen, maar bekijk het geheel, als spectrum van mogelijke alternatieve middelen.

2. Veranker en stroomlijn het hacken als opsporingsmiddel bij de politie, in lijn met het aanstaande WODC-rapport, maar erken dat hacken een hoge drempel kent, slecht schaalt, maatwerk is, vooral geschikt is voor grote zaken, en geen gegarandeerde opbrengst biedt.

3. Bewerkstelling in een Europees kader voor het tappen van 5G verbindingen eenzelfde transparantie, uniformiteit en rechtszekerheid als nu gangbaar is in de telecomwereld.

4. 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.

5. Dwing aanbieders van online diensten tot nauwere samenwerking en levering van bedrijfsvoeringsgegevens (logs). 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. Mogelijke aanknopingspunten zijn hierbij: de

Nederlandse/Europese vestigingen van de betrokken bedrijven en ook de eigen Europese kijk op gegevens, waarbij de zeggenschap bij data-subjecten ligt en niet bij verwerkende organisaties.

7. Organiseer nauwere publiek-private samenwerking met de fraude-afdelingen van deze leveranciers van diensten in de informatiesamenleving. Benadruk hierbij de maatschappelijke zorgplichten die grote ICT-partijen hebben.