Aan: mr. F.B.J. Grapperhaus,
Minister van Justitie en Veiligheid.
Turfmarkt 147,
2511 DP Den Haag

Nijmegen, 2 april 2019

Betreft: Advisering m.b.t. vernieuwing C2000

Geachte Heer Grapperhaus,

Op Uw verzoek heb ik verschillende recente rapporten (waaronder het advies van de AIVD, de security audit van Xebia, het aanvullend technisch onderzoek door Valori en door FOX-IT) bestudeerd over het lopende vernieuwingstraject C2000, met bijzondere nadruk op eventuele risico's m.b.t. betrokkenheid vanuit China. Hierbij is het doel U van advies te voorzien over de genomen maatregelen en over het vervolgtraject.

Werkwijze en positionering

Uw ministerie heeft mij in de laatste week van maart 2019 inzage gegeven in honderden pagina's aan (vertrouwelijke) rapporten, waarbij de context van Uw adviesverzoek is uitgelegd. Tijdens en na de bestudering heb ik uitgebreid gesproken met inhoudelijk betrokkenen, waarbij ik zelf heb kunnen aangeven met wie ik nader wilde overleggen. Bij die gesprekken is de contactpersoon vanuit het ministerie niet aanwezig geweest. Ik heb daarbij alle vragen kunnen stellen die ik had en heb daar ook adequaat antwoord op gekregen. Mijn bevindingen zijn gebaseerd op de informatie uit deze rapporten en gesprekken. Ik heb geen zelfstandig onderzoek gedaan naar de juistheid van (de uitgangspunten van) deze informatie.

Mijn advies heb ik naar eer en geweten opgesteld, op persoonlijke titel, uitgaande van mijn eigen wetenschappelijke expertise (computerbeveiliging) en ervaring. Zaken die buiten mijn expertise liggen, zoals bijvoorbeeld ondernemingsrechtelijke aspecten, komen hierbij niet aan de orde.

Bevindingen

Het huidige C2000 communicatiesysteem voor hulpdiensten is dringend aan vervanging toe, niet alleen m.b.t. de functionaliteit, maar zeker ook m.b.t. beveiliging. Dit systeem draait bijvoorbeeld nog grotendeels op het besturingssysteem Windows XP dat sinds april 2014 niet langer ondersteund wordt door Microsoft en waarvoor sindsdien geen *security patches* meer geleverd worden. Alleen al hierom dient de

vernieuwing krachtdadig en met afgewogen spoed voortgezet te worden: er is geen weg terug.

Het vernieuwde C2000 zal, net als andere moderne ICT-systemen, door de hoge mate van verbondenheid en verwevenheid met andere digitale systemen een zekere mate van kwetsbaarheid kennen voor fouten of niet-uitgevoerde updates elders. Mede door zulke afhankelijkheden zijn er geen absolute garanties te geven.

De belangrijkste leverancier van het nieuwe C2000 is het Duitse bedrijf Hytera Mobilfunk, met Chinese eigenaar Hytera. Uit de stukken blijkt dat dit bedrijf het C2000 project gestart is zonder sterke security cultuur en zonder bewustzijn van de gevoeligheid van Chinese betrokkenheid. Deze cultuur en dit bewustzijn zijn gedurende het project verbeterd, vooral onder druk van de Nederlandse projectleiding. Het Duitse bedrijf Hytera Mobilfunk scheidt de Duitse activiteiten t.b.v. C2000 strikt van het Chinese moederbedrijf. Daarbij zijn de twee in China ontwikkelde software componenten — van beperkte omvang en functionaliteit — zowel door het Duitse bedrijf zelf, als door een Nederlandse partij, kritisch bekeken.

Leidend bij mijn oordeelsvorming is de rapportage van de AIVD, waarin gesteld wordt dat vanuit hun perspectief China weliswaar actief is met cyberaanvallen tegen Nederlandse belangen — zie ook de publieke jaarverslagen van de AIVD — maar dat C2000 niet past bij de waargenomen doelwitten: China lijkt vooral uit te zijn op het vergaren van economisch relevante informatie. Daarvoor is C2000 niet direct interessant. C2000 kan wel een relevant doelwit zijn van landen die proberen via digitale aanvallen posities op te bouwen in de Nederlands ICT-infrastructuur; de beveiliging van C2000 dient tegen zulke aanvallen bestand te zijn.

Daarnaast heb ik met waardering kunnen constateren dat bij de C2000 projectleiding de vereiste kennis en bewustzijn m.b.t. beveiling ruim voldoende aanwezig zijn. De leiding stuurt hier op, toetst regelmatig en eist aanpassingen van geconstateerde tekortkomingen.

Op grond hiervan adviseer ik U voort te gaan met de vernieuwing van C2000, op de ingeslagen weg, met de betrokken partijen, met voortdurende krachtige focus op beveiligingsaspecten, en met inachtneming van de onderstaande aanvullende opmerkingen.

Verbeterpunten

Graag voeg ik de volgende opmerkingen toe.

1. Een groot deel van de onderzoeken die ik ingezien heb richten zich, terecht, op het Duitse bedrijf Hytera Mobilfunk en op het verhogen van het beveiligingsniveau binnen dat bedrijf. Het beveiligingsniveau binnen de Nederlandse hulpdiensten verdient vergelijkbare aandacht. Met name dienen meldkamers

goed afgeschermd te zijn, zodat van daaruit niet binnengedrongen kan worden in de C2000 infrastructuur. Deze afscherming heeft niet alleen technische aspecten, maar omvat nadrukkelijk ook het beveiligingsbewustzijn van eenieder die daar werkt. De nadruk ligt daar, begrijpelijkerwijs, sterk op operationele functionaliteit, waardoor cruciale beveiligingssignalen genegeerd kunnen worden en noodzakelijke procedures in de praktijk mogelijk omzeild worden. Dat laatste kan door interne operationele druk plaatsvinden, maar ook door externe misleiding. Continue training en opleiding zijn hierbij van belang.

2. De leiding van het vernieuwingstraject is in handen van extern ingehuurde experts die gedurende langere tijd aan dit project werken. Hiermee worden de broodnodige kennis en expertise niet verankerd binnen de overheid in het algemeen, en in het bijzonder niet binnen de betrokken hulpdiensten. Ik acht het van wezenlijk belang dat de kennis van, en gerichtheid op, beveiling een integraal onderdeel uitmaakt van deze organisaties, met een hoog niveau van expertise en analytisch/strategisch denkvermogen.

3. De AIVD wijst op het belang van het monitoren van de internationale ontwikkelingen en dreigingsbeelden. Concreet wil ik daarom aandringen op het uitwerken van draaiboeken om in situaties van internationale spanning — met name met China, maar ook met andere landen — het operationele C2000 systeem van de buitenwereld te isoleren, waardoor tijdelijk geen updates van buitenaf geïnstalleerd kunnen worden. Concreet gaat het dan om het dichtzetten van de zogeheten RAS-interface.

4. Bij de verdere ontwikkeling van C2000 wil ik verder nog aanraden om systematischer gebruik te maken van open source software, in afzonderlijke componenten en ook in de infrastructuur zelf. Ik begrijp dat het in een kleine markt moeilijk kan zijn om een leverancier te vinden die open source software wil leveren, maar ik wijs er ook graag op dat open source steeds gebruikelijker is bij cruciale software componenten voor beveiliging. Zo zijn er verschillende voorbeelden van beveiligingsproducten, zoals OpenVPN-NL[1], die vanuit de Nederlandse overheid in samenwerking met bedrijven en wetenschappers ontwikkeld zijn. Om een concreet voorbeeld te noemen: de end-to-end versleuteling die door sommige diensten bovenop C2000 wordt gebruikt kan bijvoorbeeld via open source ontwikkeld worden. Zulke open source software vermindert enerzijds de afhankelijkheid van een specifieke leverancier (*vendor-lockin*) en reduceert anderzijds het risico op kwaadaardige achterdeurtjes in

[1] Zie https://openvpn.fox-it.com/about.html

de software. Daarbovenop leidt openheid van software in de praktijk vaak tot hogere kwaliteit omdat de hele wereld mee kan kijken en producenten kritiek willen vermijden.

Breder perspectief

Ik ben mij bewust van de huidige discussie over 5G en in het bijzonder over 5G van de Chinese leverancier Huawei. Ik wil graag benadrukken dat C2000 en 5G slecht vergelijkbaar zijn. Bij C2000 gaat het om een heel specifieke dienst — communicatie voor hulpdiensten — terwijl het bij 5G gaat om generieke basisinfrastructuur voor velerlei publieke en private diensten. Daarbij wordt C2000 geleverd door een Duits bedrijf met een Chinese eigenaar, terwijl Huawei's 5G volledig van Chinese makelij is. In dit kader ben ik zo vrij hier een vrijblijvende suggestie aan toe te voegen, in lijn met het bovenstaande vierde punt: Nederland en Europa zouden er goed aan doen om collectief m.b.t. 5G open source software van (alle) leveranciers te verlangen. Dit is een heldere eis, die geen onderscheid maakt tussen leveranciers, die een helder doel heeft, en die goed past in een Europese traditie van openheid en transparantie. Hiermee zou de huidige impasse mogelijk doorbroken kunnen worden.

Desgewenst ben ik gaarne bereid het bovenstaande nader toe te lichten en te bespreken.

Met vriendelijke groet,

Prof. dr. B. Jacobs,

Institute for Computing and Information Sciences,
Radboud Universiteit Nijmegen
Toernooiveld 212,
6525 EC Nijmegen