Xebia

Ministerie van Justitie en Veiligheid
T.a.v. Minister Grapperhaus
Turfmarkt 147
2511 DP Den Haag

Hilversum, 28 maart 2019

Betreft: *Samenvatting security onderzoek Hytera Duitsland*

Geachte heer Grapperhaus,

In het najaar van 2018 heeft het Ministerie van Justitie en Veiligheid de hulp van Xebia ingeroepen ter beoordeling en advisering rondom de vernieuwing van C2000. Xebia heeft hiertoe een onderzoek uitgevoerd en de resultaten aan u opgeleverd. In deze notitie geven wij een samenvatting van de aanleiding, aanpak, belangrijkste resultaten, conclusies en aanbevelingen van het onderzoek.

Aanleiding voor het onderzoek

Door toenemende (inter-)nationale druk op de mogelijke invloed van statelijke actoren in onze maatschappij in het algemeen en in door de overheid geïmplementeerde en beheerde IT-infrastructuren in het bijzonder, heeft het Ministerie van Justitie en Veiligheid aan Xebia gevraagd een onderzoek in te stellen naar een van de leveranciers van de geïntegreerde C2000-oplossing; Hytera Mobilfunk GmbH (vanaf hier: Hytera Duitsland). Eind 2018 heeft Xebia zich bij Hytera Duitsland een beeld gevormd van mogelijke aanvalsvectoren die binnen de huidige aangegane verplichtingen een rol kunnen spelen.

Aanpak van het onderzoek

Op basis van veelvoorkomende aanvalsscenario's hebben een security expert en een technisch expert van Xebia verschillende werknemers van Hytera Duitsland geïnterviewd. De bij het onderzoek betrokken werknemers vervullen verschillende sleutelrollen binnen Hytera Duitsland. Zij hebben de benodigde informatie aan Xebia verschaft waarmee Xebia potentiële kwetsbaarheden heeft kunnen identificeren. Hytera Duitsland was tijdens het onderzoek zeer meewerkend en transparant richting Xebia.

Op basis van de gevoerde gesprekken heeft Xebia een conclusie getrokken over het volwassenheidsniveau van de informatiebeveiliging bij Hytera Duitsland en heeft Xebia verschillende aanbevelingen gedaan.

Over Hytera Duitsland

Uit het onderzoek blijkt dat Hytera Duitsland zichzelf ziet als een Duits bedrijf uit Bad Münder, met een rijke geschiedenis in de elektro- en communicatietechniek. Het bedrijf heeft een Chinese eigenaar/aandeelhouder die op afstand opereert. Het management van Hytera Duitsland geeft aan grotendeels autonoom te opereren ten opzichte van Hytera China. De bij dit onderzoek betrokken Hytera-medewerkers lijken zich ervan bewust dat het bestaansrecht van het bedrijf afhangt van het vertrouwen dat klanten in hen hebben. Volgens het managementteam van Hytera Duitsland erkent Hytera China dit belang, en houdt Hytera China daarom gepaste afstand.

Het personeel van Hytera Duitsland

De aard van de projecten die Hytera Duitsland uitvoert en het type klanten (verschillende Europese veiligheidsdiensten, hulpdiensten en defensie-eenheden) van Hytera Duitsland, vereisen speciale aandacht voor informatiebeveiliging. De door Hytera Duitsland aangegeven genomen maatregelen wijzen erop dat de dreiging van statelijke actoren serieus wordt genomen. Zo ook de dreiging van Chinese statelijke actoren, die potentieel via Hytera China toegang tot – of invloed over – het C2000-netwerk proberen te verkrijgen. De medewerkers van Hytera Duitsland zijn zich ervan bewust dat informatiebeveiliging een onderwerp is dat altijd aandacht nodig heeft en waarin continu gecontroleerd, geïnnoveerd en verbeterd moet worden.

De bij dit onderzoek betrokken medewerkers maken duidelijk dat de hiërarchische aard van Hytera Duitsland ervoor zorgt dat men instructies of opdrachten vanuit Hytera China direct ter discussie stelt en betwist; dit scenario wordt als zo absurd gezien, dat men het direct zal melden aan een leidinggevende of Hytera Duitsland managementteamlid. De bij dit onderzoek betrokken medewerkers geven aan dat instructies of opdrachten altijd van een directe leidinggevende of van een Hytera Duitsland managementteamlid komen.

Bedrijfsprocessen

Hytera Duitsland heeft stappen ondernomen om invloed op organisatorisch, proces- en technisch gebied door Hytera China te voorkomen. Ook in de statuten van Hytera Duitsland is hier een en ander over vastgelegd.

Online samenwerking tussen Hytera China en Hytera Duitsland

Hytera Duitsland benoemt dat ten behoeve van de digitale samenwerking met medewerkers van Hytera China een specifiek netwerksegment is gerealiseerd door Hytera Duitsland.

Samenstelling van C2000 Voice Network

Vanwege een capaciteitsprobleem bij Hytera Duitsland is besloten de bouw van twee onderdelen (applicaties) van het C2000-systeem uit te besteden aan Hytera China. De door Hytera China opgeleverde programmacode wordt door Hytera Duitsland gecontroleerd. De kwaliteit wordt vastgesteld en eventuele risico's en zwakheden worden geïdentificeerd. Tevens wordt de code gecompileerd en getest door Hytera Duitsland voordat het wordt geïmplementeerd in het C2000 Voice Network. Het betreft de volgende applicaties:

- Normaliter kunnen er geen tekstberichten verstuurd worden naar communicatieapparatuur die uitstaat. Hytera China heeft een applicatie ontwikkeld die het tekstbericht in deze gevallen bewaart.
- De locatie van de mobiele communicatieapparatuur wordt in de meldkamer op een kaart weergegeven. Hytera China heeft de applicatie ontwikkeld die de GPS-coördinaten van de communicatieapparatuur vertaalt naar een hiervoor bruikbaar formaat.

De door Hytera China opgeleverde applicaties zullen volgens Hytera Duitsland geïsoleerd in het C2000 Voice Network worden geïmplementeerd. In geval van gecompromitteerde (Chinese) software beperkt deze maatregel de mogelijkheden om het C2000-netwerk ermee te beschadigen, uit te schakelen of af te luisteren. De betreffende applicaties kunnen uitgeschakeld worden. Het netwerk blijft dan operationeel, echter is het dan niet meer mogelijk om tekstberichten te versturen naar apparaten die uitgeschakeld zijn. Wel is het mogelijk om via een omweg de locatie van de portofoons te achterhalen. Deze locaties zijn veel minder nauwkeurig dan de locaties die de Chinese software verstrekt.

Met uitzondering van kant-en-klare commerciële softwareproducten en de twee bovengenoemde, door Hytera China geleverde, applicaties, is alle software die Hytera Duitsland levert ontwikkeld door Hytera Duitsland.

De base stations worden door Hytera China geassembleerd. Dit werd gaandeweg het onderzoek duidelijk. Assemblage van de base stations viel buiten de scope van dit onderzoek, en is daardoor niet verder onderzocht. Een AIVD-onderzoek naar de mogelijke risico's van statelijke actoren heeft dit onderwerp binnen scope gehad.

Adviezen

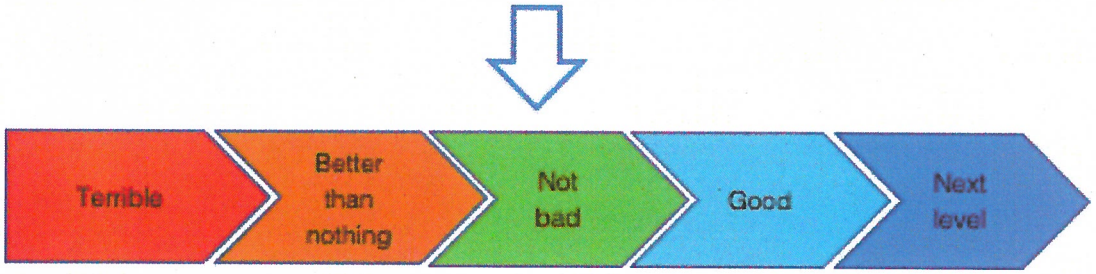
In het onderzoeksrapport doet Xebia diverse gedetailleerde adviezen. Deze adviezen bestaan uit twee soorten:

- Adviezen ter verbetering van informatiebeveiliging bij Hytera Duitsland, specifiek als tegenmaatregelen tegen Chinese statelijke actoren die de samenwerking tussen Hytera China en Hytera Duitsland trachten te misbruiken om toegang tot, invloed over, of controle over het C2000 Voice Network te verkrijgen.
- Adviezen ter verbetering van informatiebeveiliging bij Hytera Duitsland in het algemeen.

Details over deze adviezen zijn te vinden in de rapportage van het onderzoek.

Conclusies

Tijdens het onderzoek is geen compleet volwassenheidsonderzoek op het gebied van informatiebeveiliging uitgevoerd. Echter, gebaseerd op de scope van dit onderzoek, waardeert Xebia Hytera Duitsland met de score 'Not Bad' op het gebied van informatiebeveiliging.



Xebia karakteriseert dit als een gemiddelde score; dit betekent dat een basisniveau bereikt is, maar dat verbeteringen mogelijk zijn om de informatiebeveiliging bij Hytera Duitsland op een hoger niveau te brengen. Nadere details zijn te vinden in de rapportage van het onderzoek.

Met vriendelijke groet, namens Xebia Nederland B.V.,