Algemene Inlichtingen- en
Veiligheidsdienst
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

> Retouradres: Postbus 20010 2500 EA Den Haag

Ministerie van Justitie en Veiligheid
Directoraat-Generaal Politie
Directeur Meldkamer, C2000, 112
T.a.v. de heer ir. P.T. Gelton
Postbus 20301
2500 EH DEN HAAG

Europaweg 4
2711 AH Zoetermeer
Postbus 20010
2500 EA Den Haag
www.aivd.nl

Contact

T 079 320 50 50
F 070 320 07 33

Ons kenmerk
90307c1f-or1-3.0

Uw kenmerk

Bijlagen
1

Datum 17 januari 2019
Betreft Beantwoording adviesopdracht C2000

Geachte heer Gelton,

Op 1 november 2018 heeft uw voorganger advies gevraagd over C2000 (briefkenmerk 2400598) aan het Nationaal Bureau Verbindingsbeveiliging (NBV) van de Algemene Inlichtingen en Veiligheidsdienst (AIVD). C2000 is het communicatiesysteem voor de reguliere communicatie tussen hulpverleningsdiensten (zoals politie, brandweer en ambulance) en meldkamers bij de uitvoering van hun operationele taken. De communicatie die over C2000 loopt heeft Departementaal VERTROUWELIJK als maximaal rubriceringsniveau.

De adviesopdracht bestaat uit drie vragen. Kort weergegeven vraagt u als eerste of de betrokkenheid van Hytera Mobilfunk GmbH bij de vernieuwing van C2000 nieuwe of hogere veiligheidsrisico's oplevert. Uw tweede vraag gaat over de noodzaak van additionele beveiligingsmaatregelen en uw derde vraag betreft de uitvoering van een pentest.

Om de adviesopdracht te beantwoorden hebben wij analysesessies gehouden met uw specialisten op het gebied van C2000 en hebben aanwezige documentatie hierover bestudeerd. Daarnaast hebben wij analysesessies gehouden met onze specialisten op het gebied van statelijke actoren, cyberdreiging en informatiebeveiliging. Hierbij is gebruik gemaakt van informatie uit inlichtingenonderzoek. Ook is informatie gewonnen uit open bronnen en vergelijkbare internationale casussen.

De AIVD heeft vastgesteld dat statelijke actoren hun offensieve cyberprogramma's steeds meer richten op vitale processen. Voor de rijksoverheid is het daarom onwenselijk dat voor gevoelige informatie of vitale processen afhankelijkheid is van ICT-systemen uit landen waarvan is vastgesteld dat ze een offensief cyberprogramma tegen Nederlandse belangen voeren, zoals China en Rusland.

Het advies van de AIVD is om zo snel mogelijk over te gaan naar een oplossing waarbij de afhankelijkheid van landen met een offensief cyberprogramma gericht tegen Nederlandse belangen is geminimaliseerd. Zoals door uw organisatie aangegeven, is het voor de betrouwbaarheid en beschikbaarheid van het huidige C2000 van belang dat de migratie doorgaat. De AIVD adviseert om parallel aan de migratie te starten met een vervangingstraject. Daarboven adviseert de AIVD voor verantwoord gebruik van C2000 tijdens en na de migratie extra beveiligingsmaatregelen te treffen bij de leverancier en bij uw beheerorganisatie.

Uitgaande van het geplande beveiligingsniveau van het vernieuwde C2000 en de daarin voorgenomen beveiligingsmaatregelen, zijn de antwoorden op de gestelde vragen als volgt.

1. Conclusie over de betrokkenheid van Hytera Mobilfunk GmbH:
   De betrokkenheid van Hytera Mobilfunk GmbH bij de vernieuwing van C2000 geeft op dit moment een *laag*[1] risico op misbruik door de Chinese overheid. De Chinese overheid heeft diverse mogelijkheden om toegang te krijgen tot Chinese bedrijven. Echter, C2000 komt momenteel slechts beperkt overeen met gekende Chinese spionage-interesses. Hierdoor is C2000 een minder aannemelijk doelwit. De dreiging vanuit China is afhankelijk van de geopolitieke situatie, die onvoorspelbaar is. De onderbouwing van deze risico-inschatting staat in de bijlage;

2. Conclusie over additionele beveiligingsmaatregelen:
   Naast China vormen andere landen met een offensief cyberprogramma op dit moment een *matig* risico voor C2000. Om de risico's voor C2000 van deze landen te minimaliseren bevelen wij additionele beveiligingsmaatregelen aan. Op hoofdlijnen betreffen deze maatregelen het verhogen van de weerstand tegen statelijke actoren en het versterken van de rol als buffer van Hytera Mobilfunk GmbH tegen invloed van de Chinese eigenaars. Deze beveiligingsmaatregelen staan uitgewerkt in de bijlage;

3. Conclusie over de pentest:
   De uitvoering van een pentest waarbij voorstelbare aanvalsscenario's worden gesimuleerd is nuttig om beveiligingsmaatregelen te testen. De te testen aanvalsscenario's staan in de bijlage.

Bovenstaande conclusies zijn ongerubriceerd. De onderbouwing van deze conclusies staat in de bijlage. Deze is gerubriceerd omdat verspreiding ervan inzage geeft in de beveiligingsmaatregelen rond C2000 en in de werkwijze en het kennisniveau van de AIVD.

Deze conclusies en de uitwerking in de bijlage stelt u in staat uw eigen risico-appreciatie te maken en vervolgstappen te bepalen. De AIVD blijft u ook in het vervolg graag van dienst met advies.

Hoogachtend,
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties,

J.L.M. Kuijpers
Hoofd Nationaal Bureau voor Verbindingsbeveiliging van de Algemene Inlichtingen- en Veiligheidsdienst

1 Hierbij wordt uitgegaan van de volgende risicoschaal: onbekend, verwaarloosbaar, laag, matig, significant en hoog.