FOX IT
part of nccgroup

CLASSIFICATIE
COMMERCIAL.RESTRICTED

Toets op cyberrisico

Onderdeel van het programma ERTMS

Datum	14 mei 2020
Referentie	-
Opdrachtgever	Ministerie van Infrastructuur en Waterstaat
Auteur(s)	
Versie	1.0

FOR A MORE SECURE SOCIETY

DOCUMENT CLASSIFICATIE

Dit document is geclassificeerd als COMMERCIAL.RESTRICTED. De informatie die in dit document en bijbehorende bijlagen gepubliceerd is, is alleen bedoeld voor de geadresseerde(n) in de distributielijst op de pagina Document Management. Het gebruik van het document door een andere partij dan de geadresseerde(n) is niet toegestaan, tenzij deze partij hiertoe expliciet geautoriseerd is door een geadresseerde. De informatie in dit document is mogelijkerwijs vertrouwelijk van aard en valt eventueel onder de bepalingen van een geheimhoudingsverklaring of -plicht.

Indien u het voorliggende document foutief heeft ontvangen en/of geen toestemming heeft tot inzage van het document, verzoekt Fox-IT u om het document direct te sluiten en te retourneren aan Fox-IT.

Enig misbruik van dit document of de informatie in het document is niet toegestaan. Fox-IT aanvaardt geen aansprakelijkheid voor enig ongeautoriseerd gebruik of misbruik van voorliggend document door een derde partij of schade ontstaan door de inhoud van het document.

Fox-IT B.V.
Olof Palmestraat 6
2616 LM Delft
Postbus Box 638
2600 AP Delft
Nederland

T +31 (0)15 284 79 99
F +31 (0)15 284 79 90
fox@fox-it.com
www.fox-it.com

Document management

Versie management	
Projectnaam	Toets op cyberrisico, onderdeel van het programma ERTMS
Referentie	-
Opdrachtgever	Ministerie van Infrastructuur en Waterstaat
Onderwerp	Rapport
Datum	14 mei 2020
Versie	1.0
Status	Definitief
Auteur(s)	

Deze versie vervangt alle voorgaande versies van dit document. Vernietig alle voorgaande exemplaren!

Distributie lijst

Versie	Datum	Verspreidingsvorm	Naam/functie/opmerking
0.1	20 april 2020	Digitaal (intern binnen Fox-IT)	
0.2	22 april 2020	Digitaal (intern binnen Fox-IT)	
0.3	22 april 2020	Digitaal (intern binnen Fox-IT)	
0.4	28 april 2020	Digitaal (intern binnen Fox-IT)	
0.9	1 mei 2020	Digitaal via Clientportal	
1.0	14 mei 2020	Digitaal via Clientportal	

Reviews

Versie	Datum	Naam	Functie
0.1	20 april 2020		Directie, Regional Head RM&G
0.2	22 april 2020		Directie, Regional Head RM&G
0.3	24 april 2020		Senior beleidsmedewerker, Ministerie van Infrastructuur en Waterstaat
0.4	30 april 2020		Director Professional Services
0.9	12 mei 2020	Diverse	Wederhoor meeting met inhoudelijk betrokkenen

Wijzigingen

Versie	Datum	Naam	Opmerkingen
0.1	20 april 2020		Eerste opzet
0.2	22 april 2020		Tweede versie na review
0.3	22 april 2020		Derde versie na review
0.4	29 april 2020		Vierde versie na review
0.9	1 mei 2020		Vijfde versie na review
1.0	14 mei 2020		Zesde versie na inhoudelijke wederhoor

Management samenvatting

Tussen oktober 2018 en januari 2019 heeft het Bureau ICT-toetsing (BIT), op verzoek van het ministerie van IenW, onderzoek verricht naar de aanpak van de IT-gerelateerde werkzaamheden voor realisatie van het ERTMS. Naar oordeel van het BIT is de aanpak van het programma op belangrijke onderdelen onvoldoende gedegen. Om de kans op succesvolle invoering van ERTMS te vergroten, heeft het BIT vier aanbevelingen voorgesteld, waaronder het doorvoeren van verbeteringen in de ERTMS-specificaties op het gebied van cybersecurity. Als reactie op het BIT-advies, heeft het MT ERTMS bij de cybersecurity-aanbeveling acht actiepunten geformuleerd om cybersecurityrisico's te verkleinen.

In opdracht van het ministerie van IenW heeft Fox-IT voor drie van deze acht actiepunten onderzocht **in welke mate de drie acties voor de start van de aanbesteding voltooid zijn** en of er met de voltooiing sprake is van een **gedegen cybersecurity-aanpak**, waaruit de eventueel te implementeren maatregelen zijn af te leiden. In zijn algemeenheid heeft Fox-IT vastgesteld dat er stappen zijn gezet in het oppakken van de BIT-acties. Op het moment van schrijven zijn geen van de drie acties volledig afgerond. Voor de drie acties hebben wij de volgende status kunnen vaststellen:

- 3.2: Document "Rules and regulations"
  De structuur van het handboek is vastgesteld op het moment van schrijven. De start van de aanbesteding is onafhankelijk van de realisatie van deze actie. De input uit de dialoogfase van de aanbestedingen en de spoorstelsel input, zijn noodzakelijk voor het volledig afronden van dit document. Deze bijdragen zullen grotendeels pas na de deadline van december 2020 beschikbaar komen. De volledigheid van het handboek kan pas worden vastgesteld, wanneer dit aantoonbaar te relateren is aan maatregelen uit een standaard risicomanagement framework.
- 3.7: Gebruik van cryptografische hardware
  Er wordt binnen Europa aangedrongen op het ontwikkelen van een Europese standaard wat betreft cryptografie, maar dit heeft nog niet tot een concreet resultaat geleid. De eisen voor cryptografisch hardware of alternatieven zijn opgenomen in de PvE's. Uit de gevoerde gesprekken blijkt dat de kans klein is dat er door leveranciers wordt voldaan aan de gestelde cryptografische hardware-eisen. Een alternatieve implementatie van het gebruik van cryptografische hardware is nog onvoldoende onderzocht.
- 3.8: Fysieke beveiliging
  NS en ProRail hebben beide de fysieke toegangsbeveiligingseisen opgenomen in hun PvE's. De consequenties van de eisen voor internationale vervoerders en overige Nederlandse vervoerders zijn niet duidelijk.

De acties 3.7 en 3.8 zijn gereed als voor de definitieve vaststelling van de specificaties voor de aanbesteding ProRail zijn alternatieve benadering ten opzichte van NIST-norm FIPS 140-2 of vergelijkbaar ter beoordeling voorlegt aan de stuurgroep. Zodat deze kan beoordelen of dit voldoende conform het BIT-advies is. Ook dient de adaptiviteit zeker gesteld te worden voor nieuwe en alternatieve standaarden volgend op NIST-norm FIPS 140-2 of vergelijkbaar.

Aanvullend aan de scope van de opdracht hebben we geconstateerd dat er **geen consultatie** is geweest bij het BIT om hun advies te verduidelijken en er **geen cybersecurity roadmap** beschikbaar is waarin de strategische doelen op het gebied van cyber binnen het programma zijn vastgesteld. Zorg dat de expliciete verantwoordelijkheid en mandaat van de uitvoering van deze roadmap expliciet wordt belegd. Ook de consequenties van benoeming van de spoorsector als **vitale infrastructuur** dienen opgenomen te worden in de cybersecurity roadmap.

Inhoudsopgave

1 Introductie

Het programma ERTMS (European Rail Traffic Management System) is een samenwerkingsprogramma tussen het ministerie van Infrastructuur en Waterstaat, ProRail en NS. Zij werken samen met andere stakeholders aan het uitwerken van de invoeringsplannen voor ERTMS. Dit opgestelde programma is beoordeeld door het BIT (Bureau ICT-toetsing), waarna op 26 maart 2019 een advies is uitgebracht. In dit advies werd de nadruk gelegd op de aanpak van de IT-gerelateerde werkzaamheden voor realisatie van het ERTMS. Naar oordeel van het BIT is de aanpak van het programma op belangrijke onderdelen onvoldoende gedegen. Om de kans op succesvolle invoering van ERTMS te vergroten, heeft het BIT vier aanbevelingen voorgesteld, waaronder het doorvoeren van verbeteringen in de ERTMS-specificaties op het gebied van cybersecurity.

Met betrekking tot de BIT conclusie van een onderontwikkelde aanpak voor cybersecurity, worden er acht concrete maatregelen door ERTMS programma geïnitieerd. Hieronder de voorgestelde maatregelen.

Nr.	Korte omschrijving van de actie
3.1	Aanvullende expertise cybersecurity verwerven.
3.2	**Document “Rules and regulations” opstellen, daarbij aansluitend bij beleid cybersecuritysector-partijen.**
3.3	Het inrichten van een centrale organisatie voor cybersecurity aansluitend op centrale organisaties bij sectorpartijen en IenW.
3.4	Tooling implementeren bij sectorpartijen en de centrale organisatie ten behoeve van detectie en cyberincidenten.
3.5	Actieplan cybersecurity uit 2017 actualiseren op basis van nieuwe inzichten.
3.6	Dreigingsanalyses ERTMS jaarlijks actualiseren en n.a.v. beheersmaatregelen doorvoeren.
3.7	**Aandringen op het opnemen van eisen voor het gebruik van cryptografische hardware in de Europese specificaties en parallel daaraan leveranciers vragen, waar mogelijk al gebruik te maken van cryptografische hardware. Mocht dit niet mogelijk zijn dan zal het programma andere beveiligingsmaatregelen laten toepassen.**
3.8	**Strenge eisen stellen ten aanzien van fysieke beveiliging van en toegang tot de apparatuur waarin de sleutels worden opgeslagen (spoorvoertuig, RBC, KMC).**

Het ministerie van Infrastructuur en Waterstaat, DGMo, Directie Openbaar Vervoer en Spoor heeft Fox-IT verzocht een onderzoek uit te voeren. Dit onderzoek richtte zich op de reactie van het ERTMS programma op de BIT-toets.

Fox-IT is gevraagd om zich te richten in haar onderzoek op de acties 3.2, 3.7 en 3.8. De volgende hoofdvraag is centraal gesteld in het onderzoek:

“Zijn de doelstellingen van het programma voldoende vertaald naar de onderliggende specificaties, zijn deze specificaties voldoende helder en is de integraliteit tussen verschillende deelsystemen geborgd?”

De hoofdvraag is door ministerie uitgesplitst in de onderstaande twee onderzoeksvragen:

“In welke mate zijn de acties ten aanzien van cybersecurity zoals opgenomen in de managementreactie van het MT ERTMS, welke als geheel of gedeeltelijk als randvoorwaardelijk voor de start van de aanbestedingen zijn aangemerkt, voltooid?”

“In welke mate zijn deze drie acties ten aanzien van cybersecurity op zodanige wijze voltooid dat er ten aanzien van de drie acties een gedegen cybersecurity-aanpak is en er ten aanzien van deze drie acties concrete maatregelen afgeleid zijn die geïmplementeerd moeten worden?

Dit rapport gaat in op de drie acties in relatie tot de onderzoeksvragen en zal afsluiten met een overall beeld dat is verkregen door middel van:

- Introductie in de opdracht ten kantore van ERTMS in de achtergrond van het onderzoek;
- Interview met twee ERTMS leden (enerzijds de kwartiermaker systems engineering, die ook coördinator van de BIT-acties is en anderzijds de aspectmanager cybersecurity);
- Interview met twee vertegenwoordigers van ProRail (de manager projecten en de aspectmanager cybersecurity);
- Interview met een vertegenwoordiger van NS (de aspectmanager cybersecurity);
- Een afsluitend kort gesprek met de twee ERTMS leden die eerder waren gesproken.

In de volgende hoofdstukken zal worden ingegaan op de acties 3.2, 3.7 en 3.8, waar bij iedere actie de constateringen zijn weergeven. Vervolgens worden de constateringen en verkregen informatie geanalyseerd en wordt er afgesloten met conclusies en aanbevelingen.
Dit rapport sluit tenslotte af bevindingen die Fox-IT gedaan heeft naast de drie BIT-acties. Ook dit hoofdstuk wordt afgesloten met conclusies en aanbevelingen.

2 Rules and regulations

De omschrijving van de concrete maatregel zoals gedefinieerd door MT ERTMS op basis van het BIT-advies luidt:

“Document ‘Rules & regulations’ opstellen, daarbij aansluiten bij beleid cybersecuritysector-partijen”.

Doel einddatum: December 2020

2.1 Constateringen

Om invulling te geven aan het document ‘Rules & regulations’ (ook wel handboek genoemd), heeft ERTMS samengewerkt met NS en ProRail. Dit heeft geresulteerd in een inhoudsopgave met onderwerpen die gerelateerd zijn aan verschillende risicomanagement frameworks en de deelsystemen van de verschillend partijen. De aanpak van Translink Systems is geëvalueerd. Er heeft geen onderzoek naar Europese best-practices op dit gebied plaats gevonden; er is geen Europese kring van kennisspecialisten op het gebied van ERTMS implementatie, dan wel cyber specialisten.
Er is voor gekozen om de invulling van het handboek volgend te laten zijn op het aanbestedingstraject.

2.2 Analyse

De inhoudsopgave van het document ‘Rules & regulations’ is in samenspraak met NS, ProRail en IEMeV (Implementatie team ERTMS Materieeleigenaren en Vervoerders) gerealiseerd. Het is de verwachting dat er een zogenaamd spoorstelsel ingericht gaat worden en hieruit kunnen aanvullende onderwerpen en afspraken tussen partijen komen. Daarnaast is het waarschijnlijk dat er na de selectie van de leveranciers aanvullende input komt.

Er is geen volledig overzicht van hoe de maatregelen uit een risicomanagement framework zich direct of indirect vertalen naar de inhoudsopgave. Hierdoor is de compleetheid van de ‘Rules & regulations’ inhoudsopgave niet vast te stellen.

Er is geen gebruik gemaakt van een marktconforme standaard om tot de opzet van het handboek te komen. Het is niet duidelijk wat de doorslaggevende argumenten zijn geweest om niet te kiezen voor een standaard. Doordat er gekozen is voor een zelf samengestelde inhoudsopgave, zullen wijzigingen in de gebruikte frameworks gemonitord moeten worden en verwerkt moeten worden. En aangezien de levensduur van ERTMS tientalen jaren is, is het zeer waarschijnlijk dat ook de onderliggend frameworks zullen wijzigen.

Deelnemers in het ERTMS programma zijn betrokken bij initiatieven op het gebied van Europese samenwerking en het programma zelf is hier niet bij betrokken omdat dit alleen toegankelijk is voor vervoerders en beheerders.

De relevantie van dit handboek (en de eisen die daar in komen) voor de buitenlandse ERTMS gecertificeerde vervoerders is beperkt (of juridisch gecompliceerd) omdat het een Nederlandse afspraak tussen partijen is.

2.3 Conclusies en aanbevelingen

Het document "Rules & regulations" is in ontwikkeling en er is samen met sector-partijen een inhoudsopgave vastgesteld. Dit handboek zal pas afgerond kunnen worden als de spoorstelsel input verwerkt is en als de definitieve keuze voor leveranciers gemaakt is. Deze bijdragen zullen grotendeels pas na december 2020 beschikbaar komen. De einddatum voor deze BIT-actie is december 2020 en er lijkt voldoende tijd om voor de deadline een versie met de dan bekende eisen te maken. De volledigheid van de inhoudsopgave is niet vast te stellen, want deze is sterk verbonden met de inhoudelijke uitwerking.

Aanvullend hebben we de volgende aanbevelingen:

1. Heroverweeg om te kiezen voor een standaard risicomanagement framework. Als het eigen framework behouden wordt, stel dan zeker dat dit zelfgemaakte framework volledig en onderhoudbaar is en blijft.
2. Stel zeker dat de kennis die opgedaan wordt binnen de Europese samenwerking op het gebied van "Rules & regulations, op het niveau boven de specialisten gebruikt wordt. Dit is mede van belang omdat cyberaanvallen zich niet per definitie beperken tot een aanval binnen landsgrenzen.
3. Overweeg een nieuwe deadline voor de volledige versie van het document "Rules & regulations", waarin dan ook de input vanuit het spoorstelsel en van de geselecteerde leveranciers opgenomen is.

3 EU specificaties cryptografie

De omschrijving van de concrete maatregel zoals gedefinieerd door MT ERTMS op basis van het BIT-advies:

"Aandringen op het opnemen van eisen voor het gebruik van cryptografische hardware in de Europese specificaties en parallel daaraan leveranciers vragen, waar mogelijk al gebruik te maken van cryptografische hardware. Mocht dit niet mogelijk zijn dan zal het programma andere beveiligingsmaatregelen laten toepassen".

In de verdere uitwerking door MT ERTMS is bovenstaande gesplitst in twee afzonderlijke acties namelijk:

3.7a: EU specificaties cryptografie – Programma ERTMS roept EU op om de specificaties t.a.v. cybersecurity qua cryptografie te verbeteren.

3.7b: cryptografische hardware – Programma ERTMS eist cryptografische hardware te specificeren of oplossingen met dezelfde functionaliteit.

3.1 EU specificaties cryptografie

3.1.1 Constateringen

Het BIT-advies voor aanscherping van het cybersecurity gedeelte van de implementatie van ERTMS tot het niveau van cryptografische ERTMS-hardware in treinen en infrastructuur, heeft onder andere geleid tot een oproep aan de EC om de specificaties ten aanzien van cybersecurity qua cryptografie te verbeteren. Dit is gedaan door middel van een brief van de staatssecretaris van Infrastructuur en Waterstaat aan de Eurocommissaris voor Vervoer, mevrouw V. Bulc (d.d. 14 juni 2019). In deze brief wordt in de context van ERTMS opgeroepen tot de upgrade van GSM-R naar Future Railway Mobile Communication System (FRMCS) hardware en software, met de toelichting dat "Secure storage and distribution of the keys" nog niet gestandaardiseerd zijn. Daarnaast is er ondersteuning uitgesproken voor het ENISA Working Group Cyber Security for the Railways initiatief en is er een oproep voor EU Rules en Regulations aan ERTMS gebruikers. In juli 2019 stuurt de EC een reactie waarin ze toelichten een aantal cybersecurity initiatieven nauwkeurig te volgen (waaronder ERTMS) en bezig zijn met een interne review van de noodzaak tot een update van de "Technical Specifications for Interoperability and Common Safety Methods" op het gebied van Cybersecurity. In de brief wordt ook een oproep gedaan om contact op te nemen met de Europese coördinatoren om bij te dragen.

3.1.2 Analyse

Standaardisatie is een goede manier om toekomstvast de veiligheid te verhogen in de context van de Europese doelen van ERTMS. Echter standaardisatie is een specialistische activiteit die zwaar leunt op de bijdrage van de deelnemers. Door het verhogen van de inzet en deelname van partners neemt de snelheid van de standaardisatie toe. De oproep aan de Europese Commissie heeft nog niet geleid tot het versnellen van de noodzakelijke nieuwe ERTMS standaarden.

3.1.3 Conclusies en aanbevelingen

Er is een oproep naar de EC gedaan op om de specificaties ten aanzien van cybersecurity qua cryptografie te verbeteren. En hierop is ook een reactie gekomen. Deze actie is dus in formele zin afgerond. Echter dit heeft niet geleid tot de beoogde versnelling van de noodzakelijke standaardisatie. Daarom adviseren we om de bijdrage (bestuurlijk en in mankracht) aan de nieuwe Europese ERTMS veiligheidsstandaarden te verhogen.

3.2 Cryptografische hardware

3.2.1 Constateringen

Als opvolging van het BIT-advies voor de aanscherping van het cybersecurity gedeelte van de implementatie van ERTMS tot het niveau van cryptografische ERTMS-hardware in treinen en infrastructuur, heeft de NS de cryptografische hardware eisen opgenomen in haar aanbestedingsdossier. Als blijkt dat leveranciers hier niet aan kunnen voldoen, zal er naar andere methoden gezocht worden om wel aan de eisen te kunnen voldoen.

ProRail heeft er voor gekozen om geen dedicated cryptografische hardware voor in het datacenter voor te schrijven in de aanbestedingsdocumentatie; ze gaan hierover in de consultatiefase met de leveranciers in gesprek. Wel zullen ze aanvullende maatregelen nemen om de veiligheid van de sleutels zeker te stellen.

3.2.2 Analyse

In het BIT-advies wordt gesproken over "NIST-norm FIPS 140-2 of vergelijkbaar". Uit de ERTMS documentatie kwam deze standaard bij deze BIT-actie summier naar voren. In de interviews werd dit als een gegeven beschouwd. Er was niet bekend dat er een aanstaande mogelijke opvolger in ontwikkeling is (FIPS 140-3).

De maatregel omtrent de cryptografische hardware is procesmatig goed ingericht door de NS voor de VIRM. ProRail kiest er voor om voor het sleutelbeheer in het datacenter geen dedicated cryptografische hardware voor te schrijven. Hierbij is er geen volledig overzicht van hoe de maatregelen uit "NIST-norm FIPS 140-2 of vergelijkbaar", geleid hebben tot de PvE eisen. Daarom is het niet aantoonbaar dat de juiste eisen in het PvE opgenomen zijn.

Uit de interviews werd duidelijk dat de leveranciers een sterke positie hebben voor wat betreft het bieden van een oplossing. Er is weinig ruimte om hier eisen aan te stellen. De kans dat zij een cryptografische hardware oplossing gaan bieden is niet erg waarschijnlijk. Het is vrijwel zeker dat een andere oplossing kostenverhogend zal zijn.

Buitenlands materieel dat voldoet aan de ERTMS-specificaties, maar niet beschikt over cryptografische hardware, kan bij de huidige wet- en regelgeving niet geweigerd worden. Hierdoor zullen mogelijke kwetsbaarheden blijven bestaan. Het is niet duidelijk geworden hoe overige Nederlandse vervoerders om zullen gaan met de cryptografische hardware eis.

3.2.3 Conclusies en Aanbevelingen

NS heeft de cryptografische eisen volgens NIST-norm FIPS 140-2 (of vergelijkbaar) opgenomen in hun Programma van Eisen. ProRail heeft er voor gekozen om de eisen op een andere manier in hun PvE op te nemen. Aan de overige vervoerders zijn deze eisen niet op te leggen, dan wel nog niet opgelegd. Hiermee is deze BIT-actie voor NS en ProRail gerealiseerd, maar niet voor de overige vervoerders. Daarnaast hebben we de volgende aanbevelingen:

1. Laat ProRail voor de definitieve vaststelling van de specificaties de aanvullende maatregelen ter beoordeling voorleggen aan de stuurgroep, zodat deze kan (laten) beoordelen of dit voldoende is in relatie tot de door BIT gesuggereerde "NIST-norm FIPS 140-2 of vergelijkbaar".
2. Stel voor de definitieve vaststelling van de specificaties de adaptiviteit zeker voor nieuwe en alternatieve standaarden volgend op NIST-norm FIPS 140-2. Stel in ieder geval de wenselijkheid van NIST-norm FIPS 140-3 vast, met de bijbehorende consequenties.
3. Laat de NS het scenario uitwerken voor de situatie waarin leveranciers niet (tijdig) de cryptografische hardware conform "NIST-norm FIPS 140-2 of vergelijkbaar" kunnen leveren. Cruciaal hierbij is de aantoonbaarheid van het scenario op maatregelniveau ten opzichte van de "NIST-norm FIPS 140-2 of vergelijkbaar".
4. Maak de risico's van buitenlandse vervoerders zonder cryptografische hardware inzichtelijk en formaliseer de besluitvorming hierover.
5. Maak inzichtelijk hoe er met Nederlandse vervoerders niet-zijnde NS omgegaan zal worden in de context van cryptografische hardware.

4 Fysieke toegangsbeveiliging

De omschrijving van de concrete maatregel zoals gedefinieerd door MT ERTMS op basis van het BIT-advies:

“Strenge eisen stellen ten aanzien van fysieke beveiliging van en toegang tot de apparatuur waarin de sleutels worden opgeslagen (spoorvoertuig, RBC, KMC)”.

4.1 Constateringen

De actie tot het verbeteren van de fysieke toegangsbeveiliging, door het stellen van strenge eisen hieraan, is door het ERTMS programma gekoppeld aan het verbeteren van de Cybersecurity zoals door het BIT is geadviseerd. Procesmatig hebben NS en ProRail de fysieke toegangsbeveiliging toegevoegd aan hun Programma van Eisen.

4.2 Analyse

Het is vastgesteld NS beleid om toegang tot apparatuur te beveiligen en de door de NS genomen actie is breder dan het BIT-advies. Uit de verschillende gesprekken is niet duidelijk geworden wat deze actie toevoegt aan het BIT-advies "NIST-norm FIPS 140-2 of vergelijkbaar". In deze norm zijn namelijk al fysieke beveiligingsmaatregelen van de cryptografische hardware gespecificeerd.

Buitenlands materieel dat voldoet aan de ERTMS-specificaties, maar niet beschikt over deze aanvullende fysieke toegangsbeveiliging eisen, kan bij de huidige wet- en regelgeving niet geweigerd worden. Hierdoor zullen mogelijke kwetsbaarheden voor dit buitenlandse materieel blijven bestaan. Het is niet duidelijk hoe de overige Nederlandse vervoerders om zullen gaan met de strengere fysieke toegangsbeveiligingseisen.

4.3 Conclusies en aanbevelingen

NS en ProRail hebben beide de fysieke toegangsbeveiligingseisen opgenomen in hun PvE’s. Aan de overige vervoerders zijn deze eisen niet op te leggen, dan wel nog niet opgelegd. Hiermee is deze BIT-actie voor de NS en ProRail gerealiseerd, maar voor de overige vervoerders niet.
Daarnaast hebben we de volgende aanbevelingen:

1. Maak expliciet inzichtelijk waarom de fysieke toegangsbeveiligingseisen noodzakelijk zijn in aanvulling op de fysieke beveiligingsmaatregelen in NIST-norm FIPS 140-2 of vergelijkbaar.
2. Maak de risico's van buitenlandse vervoerders die geen aanvullende fysieke toegangsbeveiligingsmaatregelen genomen hebben inzichtelijk en formaliseer de besluitvorming hierover.
3. Maak inzichtelijk hoe er met Nederlandse vervoerders niet-zijnde NS omgegaan zal worden in de context van fysieke toegangsbeveiliging.

5 Overige bevindingen

Uit de documentatie alsmede de interviews is er informatie ontvangen, die niet alleen betrekking heeft op de drie actiepunten en dus de scope van het onderzoek. De conclusies en aanbevelingen uit deze informatie hebben wij niet willen vermengen met de drie actiepunten en worden dus afzonderlijk vermeld in dit hoofdstuk.

5.1 Constateringen

Tussen het in ontvangst nemen van het BIT-advies en het verzenden van de managementreactie vanuit MT ERTMS heeft er geen consultatie plaatsgevonden bij het BIT om beter te begrijpen wat er exact werd bedoeld met het advies. Ook de achtergrond en de rationale achter het advies om bijvoorbeeld te gaan werken met een handboek en met een NIST-norm FIPS 140-2 of vergelijkbaar is niet opgehaald.

Om doelen te bereiken is het gebruikelijk om die uit te werken in een roadmap. Er zijn meerdere pogingen gedaan om een Cybersecurity roadmap vast te stellen, echter tot op heden is deze er niet.

5.2 Analyse

Het BIT heeft adviezen gegeven zoals het document ‘Rules & regulations’ en ‘NIST-norm FIPS 140-2 of vergelijkbaar’, maar er heeft geen consultatie bij het BIT hierover plaats gevonden. Het opvragen van meer toelichting bij BIT zou de reden van dit advies duidelijker hebben kunnen maken, waarmee ook een toets zou kunnen worden gedaan of de oplossingen zoals die er nu liggen recht doen aan hetgeen is geconstateerd.

In de regel wordt een cybersecurity roadmap geschreven gebaseerd op de gewenste inrichting op het gebied van Governance, Prevent, Detect en Response en de geïnventariseerde risico’s. Een cybersecurity roadmap maakt inzichtelijk wat de ambities zijn op het steeds belangrijker wordende cybersecurity gebied. Daarnaast wordt met de specifieke cybersecurity roadmap zeker gesteld dat de noodzakelijke cybersecurity acties voldoende aandacht krijgen. Er is geen cybersecurity roadmap vastgesteld en hiermee lijkt cybersecurity nog niet de aandacht te krijgen binnen het programma die het wellicht zou moeten hebben.

5.3 Conclusies en aanbevelingen

Doordat er geen consultatie bij het BIT plaats gevonden heeft over de rapportage, is feitelijk niet vast te stellen of de door het MT ERTMS benoemde BIT-acties, wel in voldoende mate de zorgen van het BIT adresseren.
Het ontbreken van een onderbouwde cybersecurity roadmap is een belangrijke indicatie dat er op management niveau meer aandacht op nodig is voor cybersecurity.

In aanvulling hierop adviseren we:

1. Consulteer alsnog het BIT om op deze manier duiding te krijgen wat de achtergronden zijn bij hun advies. Op die manier kan het programma ERTMS beter sturing geven aan de noodzakelijke acties.
2. Maak een roadmap van de te behalen doelen op het gebied van ERTMS cybersecurity en voer deze roadmap uit. Zorg dat de expliciete verantwoordelijkheid en mandaat van de uitvoering van de roadmap wordt belegd bij de programmadirecteur en de directies van de implementerende organisaties.

Tot slot willen we vermelden dat op 10 maart 2020 de minister van Justitie en Veiligheid in een brief aan de Tweede Kamer heeft aangegeven dat hij heeft besloten de spoorsector als vitaal B aan te merken. Door deze benoeming zullen de aanbieders van essentiële diensten binnen de spoorsector onder Wbni geplaatst worden. Deze wet verplicht aanbieders van essentiële diensten om maatregelen te nemen voor de beveiliging van hun ICT en ernstige incidenten te melden. Logischerwijs zal dit ook voor ERTMS consequenties hebben. Dit versterkt de noodzaak tot een cybersecurity roadmap, waarbij zowel de realisatie van de maatregelen die horen bij essentiële diensten als ook de aanbevelingen uit dit rapport worden meegenomen. Dit lijkt ons essentieel voor een goede, duurzame cybersecurity op het spoor.

Fox-IT

Fox-IT voorkomt, onderzoekt en beperkt de meest serieuze dreigingen door cyberaanvallen, datalekken of fraude met innovatieve oplossingen voor overheid, defensie, politie, vitale infrastructuur, banken en grote bedrijven wereldwijd. In zijn aanpak combineert het bedrijf slimme ideeën met technologie om hiermee innovatieve oplossingen te bieden die zorgen voor een veilige maatschappij. Fox-IT ontwikkelt producten en maatwerkoplossingen om de beveiliging van gevoelige overheidssystemen te garanderen, industriële netwerken te beschermen, online bankiersystemen te verdedigen en strikt vertrouwelijke data te beveiligen.

Bezoek onze website voor meer informatie over Fox-IT en onze partners.

FOX IT
part of nccgroup

fox-it.com

Fox-IT
Olof Palmestraat 6, Delft
Postbus 638, 2600 AP Delft
Nederland

T +31 (0)15 284 7999
F +31 (0)15 284 7990
fox@fox-it.com