startdocument

Cyberawareness in de ERTMS-operatie

Versie	V 1.0
Kenmerk	[E_Kenmerk]
Classificatie	Intern

Colofon

Kenmerk	[E_Kenmerk]
Titel	Cyberawareness in de ERTMS-operatie
Documenttype	startdocument
Auteur	John Boss Eelco Maatman Kees van der Blom
Eigenaar	Arjo van Loo

Revisiehistorie

Versie	Datum	Wijziging
V0.9	21-1-2022	1e eindredactie door Arjo van Loo
V0.10	25-1-2022	2e redactieslag door Kees van der Blom
V1.0	01-03-2022	Vastgesteld bij SI Tafel

Inhoud

1 Inleiding

Het Programma ERTMS wil in 2022 het bewustzijn omtrent cybersecurity in de spoorsector vergroten. De komst van ERTMS maakt cybersecurity urgenter dan het al was doordat de operatie een grotere afhankelijkheid gaat krijgen van de IT- en OT-systemen. Zowel de implementerende organisaties (vervoerders en ProRail) als de opdrachtgever van het Programma ERTMS (ministerie I&W) zien hierin een rol en verantwoordelijkheid voor het programma.

In 2021 zijn de specialisten binnen het programma samen met het Operationeel Kenniscentrum ERTMS zich gaan oriënteren op een aanpak. Het voorliggende document is hiervan het resultaat. De actuele kennis en inzichten over cyberawareness zijn hierin samengebracht en daarmee kan het document fungeren als een referentiedocument voor een nog te ontwikkelen aanpak voor het vergroten van cyberawareness in relatie tot ERTMS. Dit document heeft als doel:

- Het duidelijk maken van nut en de noodzaak van cyberawareness in de ERTMS-context
- Het identificeren van bronnen die gebruikt kunnen worden voor cyberawareness-programma's voor de ERTMS-operatie en voor machinisten.
- Het in kaart brengen van de onderwerpen die geadresseerd moeten worden in cyberawarenessprogramma's
- Het vaststellen van criteria voor opnemen van informatie in de cybersecurity-bewustzijnsprogramma's

1.1 Cybersecurity

Cybersecurity bestaat uit een reeks technologieën, processen en praktijken die gericht zijn op het beschermen van netwerken, computers en gegevens tegen aanvallen (hacking), het toebrengen van schade en het zich toe-eigenen van ongeoorloofde toegang tot digitale systemen. De wereld van cybersecurity is niet zoals je dit in Hollywood-films ziet. Er is (meestal) geen schurk aanwezig die op een toets van een computer drukt waarna er vervolgens een trein ontploft. Een cyber-aanval zal een reeks fasen doorlopen. De aanpak van cybersecurity is om barrières te implementeren om daarmee hackers te stoppen (of op zijn minst de uitgevoerde aanval te vertragen). Veel van deze barrières zijn ingebouwd binnen het systeem. Andere barrières kunnen bestaan uit het toepassen van procedures en processen. Bij aanvallen op (ERTMS) spoorwegsystemen zal de effectiviteit van de barrières (deels) afhangen van het cyberawareness van de mensen die deze ERTMS beveiligingssystemen (gaan) gebruiken. Cyberawareness is intussen een geaccepteerd onderwerp in de gangbare industrienormen, zie hiervoor bijlage A.

1.2 Cybersecurity in de spoorsector

Cybersecurity heeft zich binnen de spoorwegsector al heeft ontwikkeld en krijgt meer urgentie door de introductie van ERTMS. Operationele werknemers zijn belast met de uitvoering van veiligheidskritische taken en moeten steeds vaker digitale systemen gebruiken om hun werk uit te kunnen voeren. Waar sprake is van een digitaal systeem (bv een computer) bestaat de mogelijkheid dat er een cyberaanval plaatsvindt. ERTMS is zo'n digitaal systeem waardoor de mogelijkheid voor cyberaanvallen op het ERTMS beveiligingssysteem aanwezig is.

1.3 Cyberawareness

Gebruikers die zich bewust zijn van het potentieel gevaar van cyberaanvallen kunnen helpen om de beveiliging ertegen te verbeteren. Een gebruiker die zich bewust is van het potentieel gevaar van cyberaanvallen heeft meer kans om 'iets verdachts' te identificeren om op deze wijze te voorkomen dat een cyberaanval slaagt.

Er zijn campagnes ontwikkeld voor consumenten om cyberawareness te vergroten. Een voorbeeld is de informatie die door banken wordt verstrekt met betrekking tot het veilig gebruik van pinpassen of het verstrekken van wachtwoorden (https://www.veiligbankieren.nl/). De risico's van industriële automatisering (OT) in het algemeen en ERTMS in het bijzonder verschillen echter van de risico's binnen het consumentendomein. Het creëren van cyberawareness bij het gebruik van het ERTMS beveiligingssysteem vereist daarom een op maat gemaakt programma.

Er bestaat een groot aantal rollen die betrokken zijn bij de ERTMS-operatie. De vereisten voor cyberawareness zullen per rol verschillen. Een senior-manager moet zich bewust zijn van andere facetten van cyberbeveiliging dan een onderhoudsmonteur of een machinist. Dit vereist per groep een andere aanpak voor het vergroten van de cyberawareness.

1.4 Focus op de machinist

De aanpak voor dit rapport is om zich te focussen op een kleine, goed gedefinieerde groep (machinisten) om een beeld te vormen om daarna dit beeld uit te breiden voor andere doelgroepen. Focus op de groep machinisten betekent eveneens dat we ons moeten richten op de groep die leidinggeeft aan de machinisten en hen ondersteunt. Deze aanpak ondersteunt meer diepgang bij de analyse en biedt daarbij ook een basis voor het uitrollen ervan voor andere doelgroepen.

De voordelen van het creëren van cyberawareness voor machinisten zijn:

- Machinisten zullen zich comfortabeler voelen bij het werken onder ERTMS, waardoor stress wordt verminderd;
- Een cyberbewuste machinist zal iets gemakkelijker afwijkingen als ‘verdacht’ identificeren waardoor de kans op het afbreken van een cyberaanval toeneemt;
- Een breder cyberawareness zal de machinisten helpen bij het op een eenduidige en consistentere manier toepassen van regels en procedures;
- Het aan de orde stellen van het onderwerp cybersecurity maakt het makkelijker om zorgen en/of ervaringen te bespreken en deze te delen

2 Waarom is cyberawareness belangrijk voor ERTMS?

De cyberaanvallen op spoorsystemen zijn tot op heden spaarzaam. Waarom moeten we ons dan druk maken over cyberawareness bij het gebruik van het ERTMS beveiligingssysteem? Drie aspecten van cybersecurity zijn relevant voor het begrijpen van de relevantie van cyberawareness in relatie tot het ERTMS-programma:

Ten eerste betekent de afwezigheid van een aanval in het verleden niet dat een aanval in de toekomst niet zal plaatsvinden. Aanvalsmethoden zijn altijd in ontwikkeling. Iedereen was verrast toen de Amerikaanse presidentsverkiezingen werden gehackt. SQL-aanvallen waren ook ooit nieuw, Er zijn hordes aanvallers (hackers) die druk op zoek zijn naar kwetsbaarheden binnen een digitaal systeem en een leger belangstellende partijen op de achtergrond met het motief om op zoek te gaan naar manieren om deze kwetsbaarheden te gaan misbruiken. Het is dus geen kwestie van ‘als’ maar ‘wanneer’ er een aanval op het ERTMS beveiligingssysteem in gang wordt gezet.

Ten tweede zijn cyberaanvallen moeilijk te voorspellen. Cybersecurityrisico’s ontstaan vanuit zowel opzettelijke aanvallen als vanuit toevallige gebeurtenissen (bijvoorbeeld het achterlaten van een laptop in een trein). Terwijl de MTBF (Mean Time Between Failures) van een veiligheidskritisch onderdeel kan worden vastgesteld, is het minder gemakkelijk om de interesse (het waarom van de aanval) en de timing van een aanvaller (hacker) in te schatten.

Tot slot zijn er tot op heden geen kwaadwillende aanvallen op het ERTMS beveiligingssysteem bekend, maar dat kan worden veroorzaakt doordat spoorwegorganisaties deze informatie niet delen of dat ze zich er gewoon niet van bewust zijn dat ze zijn aangevallen. Het feit is echter dat het ERTMS beveiligingssysteem kan worden aangevallen. Er zijn meerdere succesvolle aanvallen uitgevoerd in bv ERTMS-laboratoriumomgevingen.

Als de werknemers die het systeem gebruiken zich bewust zijn van cybersecurity-risico's, dan:

- is de kans groter dat ze een cyberaanval herkennen en op de juiste wijze reageren en
- kan op deze wijze meer van deze werknemers worden geleerd (over kwetsbaarheden en hoe deze te verhelpen).

3 Cyberawareness in de ERTMS-operatie

Er bestaat veel informatie over cybersecurity. De uitdaging bestaat er echter uit om op de juiste manier informatie aan de juiste groep te koppelen en wel zodanig dat men die informatie begrijpt en dat men deze informatie ook als nuttig ervaart.

Hieronder is een (voorbeeld van) algemene matrix voor cybersecurity-bewustzijnsprogramma's weergegeven. Doelgroepen en onderwerpen zijn hierbij aan elkaar gekoppeld. Het doel daarvan is om in een helder overzicht eenvoudig aan te geven welke informatie voor welke doelgroep relevant is,

Uitgangpunt hierbij is: 'Als men geen invloed op het systeem(onderdeel) heeft dan hoeft men daarover niets te weten'.

3.1 Doelgroepen

Deelnemers aan een cyberawarenessprogramma kunnen zijn:

1. **Operationele gebruikers**
    a. Monteurs / Technici
    b. Machinisten
    c. Treindienstleiders

2. **Management**
    a. Operationele managers
    b. Productie / Techniek
    c. Senior operators

3. **Ingenieurs**

4. **Security Technici** (waarschijnlijk weinig werknemers van deze groep aangezien zij al van veel onderwerpen op de hoogte zijn)
    a. IT-architecten
    b. CISO (Chief Information Security Officer)

3.2 Onderwerpen

De programinhoud kan worden onderverdeeld in algemene onderwerpen, met daarbij een onderverdeling naar een verder niveau van gedetailleerdheid (dat van toepassing is voor de verschillende deelnemersgroepen). Onderstaande onderwerpen worden beschreven in termen van verschillende toepassingsniveaus. Van (a) de meest algemene informatie tot aan (b en c) een geleidelijk verdiepende context.

1. **Actoren en cyber-aanvallen**
    a. Algemene achtergrond over cyberaanvallen: wat voor soort mensen zijn de aanvallers (hackers) en hoe zou een cyberaanval eruit kunnen zien? Dit is het basisuitgangspunt voor alle andere onderwerpen die daarna volgen. Cybersecurity gaat over risico's die een relatie met digitale objecten hebben (operationele systemen, computers, etc.).

2. **ERTMS – als digitaal beveiligingssysteem**
    a. Over ERTMS, de digitale aspecten van ERTMS en bekende, succesvolle hacks op het ERTMS beveiligingssysteem.

3. **Cybersecurity Management Systems (CSMS, het gebruikte management-proces binnen de sector)**
    a. ISMS / BIO (WBNI, NIB Richtlijn, standaarden) – Wat is een ISMS (Information Security Management System) - Doel van de normen bij het beheer van cybersecurity-risico's: wie gebruikt welke normen?
    Het verband tussen wetgeving en ISMS.
    b. Applicatie specifiek: De implementatie van ISMS/CSMS.

4. **Riskmanagement**
    a. Risk-management: Risk-managementproces en de verantwoordelijkheden binnen de organisatie, het aanpakken van risico's en het vaststellen van controlemechanismen. Risico's die tussen organisaties kunnen worden overgedragen en het kunnen aantonen dat risico's zijn 'aangepakt'.
    b. Risk-management in relatie tot CMSM/ISMS: het risicoregister, het Zwitserse kaas-analyse model waarbij barrières in kaart worden gebracht (als voorbeeld, maar het kan ook een andere methode zijn), het in kaart brengen van aanvalsvectoren (attack vectors) en de toepassing van de vereiste controles.

5. **Architectuur en controles** (een niveau van controles inbouwen)
    a. Zones en doorvoer-infrastructuur, zoals concepten van zonale segregatie, verdediging in de diepte (defense in depth), beveiliging d.m.v. het ontwerp
    b. Security Architectuur – Shift2Rail architectuur-paper, Veiligheidsbeleid - controles - toepassing van BIO / 62443-3-3, zones en de infrastructuur.

6. **Monitoring en SOC's** (een niveau van controles inbouwen)
    a. Wat is een SOC (Security Operation Center)? Waarom is monitoring belangrijk? Waarom ERTMS-monitoring niet zo eenvoudig is als algemene IT-monitoring. Vormen van escalatie benoemen.
    b. (Technical) SOC en CSIRT. Risk analyses t.b.v. de SOC-functionaliteit (actie tussen gebruiker en het systeem). Data-bronnen benoemen. Applicatie voor het z.g. 'machine-learning' aspect. SIEM/Tooling (Security Information & Event Management gereedschap).
    c. (Management) SOC en CSIRT, SOC functionaliteit, incident-management en incident reportages.

7. **Operationeel**
    a. Hoe ziet een hack er operationeel uit?
    b. Wijzigingen binnen de operationele procedures (het onderhoud ervan)
    c. Risico's in kaart brengen
    d. Configuratie-controle en procedures

8. **Onderhoud**
    a. Onderhoud aan het ERTMS-beveiligingssysteem (on-board)
    b. Onderhoud aan het ERTMS-beveiligingssysteem (on-track)

9. **Cyber hygiëne**
    a. De mate van (juist) werknemersgedrag bij het toepassen/bedienen van digitale systemen. Dit noemen we *cyber-hygiëne*

3.3 Doelgroepen – onderwerpen matrix

De correlatie tussen deelnemers en de programmainhoud is in onderstaande matrix inzichtelijk gemaakt

Onderwerp	Machinisten	Management	Engineer	IT / CISO
1 Actoren en cyber-aanvallen	a	a	a	
2 ERTMS als digitaal beveiligingssysteem	a	a	a	
3 CSMS (Cybersecurity Management System)		a	a, b	
4 Risk management		a	a, c	
5 Architectuur en controles		a	a, b	
6 Monitoring en SOC's		a, c	a, b	
7 Operationeel	a, b			
8 Onderhoud			a, b	
9 Cyberhygiène	a	a	a	

3.4 Programmavorm

Bewustwording wordt gecreëerd door een initiële training en ‘follow-on’ activiteiten, of dat nu trainingen of andere campagnes zijn dat maakt niet uit. Het profiel van het cybersecurity-bewustzijnsprogramma zou het volgende dienen te omvatten:

- Training, conform de inhoud zoals hierboven beschreven
- Jaarlijkse opfriscursussen
- Integratie van cyberevenementen binnen andere trainingen en oefeningen
- Regelmatige reclamecampagnes (m.b.v. posters, etc.)

4 Cyberawareness voor machinisten

Om te komen tot uitgangspunten voor een het vergroten van cyberawareness bij machinisten zijn meerdere bronnen bestudeerd en gesprekken gevoerd. Dit leverde het inzicht op dat er veel voorkomende aandachtspunten zijn en mogelijkheden om beproefde concepten over te nemen. In dit hoofdstuk worden de belangrijkste aspecten van de bewustzijnstraining (voor machinisten) die zijn geïdentificeerd benoemd. De geraadpleegde bronnen zijn terug te vinden in bijlage B, C, en D,

Er is een enorme hoeveelheid informatie over cybersecurity beschikbaar. Niet alles is relevant voor een cybersecurity-bewustzijnsprogramma. Verschillende bronnen zijn geanalyseerd. Het doel van de reviews was om te begrijpen of de bron relevant was voor een cyberawareness en om, indien mogelijk, lessen over te nemen aangaande wat werkt (en wat niet).

Opgemerkt moet worden dat veel van de onderzochte bronnen uitstekende informatie bevatten die relevant is voor verschillende aspecten van cyberbeveiligingsbeheer. Ten behoeve van dit rapport is echter alleen gekeken naar de relevantie en toepasbaarheid van de informatie voor een cybersecurity-bewustzijnsprogramma voor machinisten.

Onderstaande aspecten kunnen worden opgenomen in een cybersecurity-bewustzijnsprogramma voor machinisten:

Onderwerp	De definitie en de context van cybersecurity
Advies	Geeft een heldere definitie voor cybersecurity in relatie tot ERTMS. Biedt ter ondersteuning informatie over *waar men publiek beschikbare informatie kan vinden*. Leg het onderscheid uit dat bestaat tussen *cyberbewustzijn binnen het consumentendomein* (hoe beschermt men bancaire informatie) en *het cyberbewustzijn binnen het industriële domein* (zoals het gereedmaken en besturen van een trein).
Achtergrond	Dit biedt informatie op t.b.v. het communiceren over ‘cyberbeveiliging voor machinisten’.

Onderwerp	De wet- en regelgeving m.b.t. cybersecurity (Nationaal en Europees)
Advies	Biedt een overzicht van beschikbare wet- en regelgeving. Laat zien hoe de EU- en de Nationale wet- en regelgeving is uitgewerkt in operationele regels en procedures die de machinist helpen bij het begrijpen van de noodzaak om cybersecurity serieus te nemen.
Achtergrond	Dit geeft een onderbouwing m.b.t. het feit dat de regels en procedures hun basis hebben in wet- en regelgeving. Het helpt bij het beantwoorden van de vraag ‘waarom cybersecurity belangrijk is’.

Onderwerp	Het digitaal karakter van het ERTMS-beveiligingssysteem
Advies	Leg uit in welke mate ERTMS digitaal is en wat het verschil met andere (analoge) systemen is. Leg uit wat een IT- en een OT systeem is (met voorbeelden), leg de verschillen tussen beide systemen uit en wat het doel van de toepassing van deze IT- en OT systemen is.
Achtergrond	Het duidelijk maken dat ERTMS een digitaal systeem is dat wezenlijk verschilt met het bestaande analoge beveiligingssysteem.

Onderwerp	Een omschrijving schetsen van de ERTMS omgeving met daarbinnen de cyberdreigingen
Advies	definities voor cyberbedreigingsactoren en cyberaanvallen: *Wat is een cyberbedreigingsactor?* *Wat is een cyberaanval?* Biedt een overzicht aan met voorbeelden van deze actoren en aanvallen, zowel uit de ERTMS omgeving als uit de omgeving buiten de spoorsector.
Achtergrond	Het ontwikkelen van het begrip m.b.t. de omgeving waarbinnen de treinen rijden. Deze is niet vrij van cyberbedreigingsactoren en cyberaanvallen. Het duidelijk maken dat een digitaal systeem (zoals ERTMS) kan worden 'gehacked'. Op deze wijze kunnen machinisten 'digitale bedreigingen' relateren aan digitale processen (bij het gereedmaken en rijden het signaleren van afwijkingen van het 'normale' en daarop vervolgens actie ondernemen).

Onderwerp	Het beheer van cyberbeveiligingsrisico's
Advies	Biedt een overzicht van het ERTMS treinvoorbereiding- en rijproces aan. Dit helpt bij de identificatie van cyberrisico's. Hiermee kunnen controleprocedures worden opgesteld. Deze controles kunnen vervolgens binnen het ERTMS beveiligingssysteem worden geïmplementeerd (bij bv het gereedmaken van de trein/locomotief). Biedt een beschrijving van de ERTMS besturingselementen aan. (Cryptografie is bijvoorbeeld noodzakelijk om de authenticiteit van berichten te waarborgen. Denk hierbij aan de RBC- EVC-transmissie).
Achtergrond	Dit helpt bij het opbouwen van vertrouwen in het ERTMS-beveiligingssysteem. Hiermee toon je aan dat de operators (o.a. machinisten) deel uitmaken van een bredere, evenwichtige, aanpak om *cybersecurity* te beheren. Het laat zien dat er ook 'activiteiten achter de schermen t.b.v. *cybersecurity* worden uitgevoerd'. Er zijn, naast de machinisten, specialisten aan het werk die ervoor zorgen dat de trein (voor zover mogelijk en acceptabel) cyberveilig is.

Onderwerp	Het beschrijven en uitleggen van cyberaanvallen en wat de machinist er mee kan doen
Advies	Ontwikkel een presentatie van enkele aanvalsvectoren. Maak hiermee cyberdreigingen reëel en herkenbaar voor de machinisten.
Achtergrond	Op deze wijze demonstreert men wat de machinist bij een (herkende) cyberaanval allemaal kan doen en welke impact acties van de machinist op de aanval kunnen hebben (zie voorbeelden in bijlage A)

Onderwerp	Het trainen van 'herkenning' van een cyberaanval en het trainen van de reactie daarop
Advies	Ontwikkel scenario's met als thema: *hoe herken ik als machinist het aspect 'ongebruikelijk'?* (Uitgangspunt daarbij is: *Is wat ik zie datgene wat ik zou moeten zien?*) Train naast het herkennen van een cyberaanval ook wat de *reactie* van de machinist zou moeten zijn.
Achtergrond	Het laten nadenken van de machinisten over hoe het aspect *'ongewoon'* eruit zou kunnen zien. Uitgangspunt is dat de reactie, die wordt verwacht, duidelijk en eenvoudig is. Dit zou de sleutel moeten zijn om mee te nemen bij de vraag: *'wat te doen bij twijfel?!!'*

Bijlage A Acceptatie van cyberawareness in industrienormen

IEC 62443-2-1, section 4.3.2.4:

> Cyberawareness van al het personeel is een essentieel hulpmiddel om cyberbeveiligings-risico's te verminderen. Deskundig en waakzaam personeel is één van de belangrijkste verdedigingslinies bij het beveiligen van een digitaal systeem. Het is daarom belangrijk dat al het personeel het belang van beveiliging begrijpt bij het handhaven van de veilige werking van het digitale systeem.

De behoefte aan cyberawareness is geïdentificeerd voor de Nederlandse spoorsector. Het verhogen van deze bewustwording is aanbeveling 12a uit het 'Vitaal Spoor Rapport' (ISR Nederlands BV + Capgemini NV, 12 juli 2021).

Cyberawarenessstraining is ook verankerd in internationale standaarden die worden gebruikt door actoren binnen de Nederlandse spoorsector.

ISO 27002:2002 hoofdstuk 7.2.2:

> Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen met inbegrip van regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.

ISO 27002 vormt de basis voor de BIO die momenteel door ProRail wordt geïmplementeerd.

Het NIST cybersecurity-framework stelt ook expliciete eisen aan bewustwordingstraining. Vereiste PR. AT stelt:

> Awareness en Training (PR.AT): Het personeel en de partners van de organisatie krijgen voorlichting over cyberbeveiliging en zijn adequaat opgeleid om hun informatiebeveiligingsgerelateerde taken en verantwoordelijkheden uit te voeren in overeenstemming met gerelateerd beleid, procedures en overeenkomsten.

Het NIST cybersecurity-framework is een belangrijk aspect van het NS cybersecurity beleid.

IEC 62443-2-1 definieert 'training van personeel en veiligheids-bewustzijn' als een element van een programma voor cyberbeveiligingsbeheer. Het element wordt beschreven als:

> **Doelstelling:**
> Al het personeel (inclusief werknemers, contractmedewerkers en externe contractanten) voorzien van de informatie die nodig is om kwetsbaarheden en bedreigingen voor het GBCS (*Geïntegreerd Beheers en Controle Systeem*) te identificeren, te beoordelen, aan te pakken en waar nodig te verhelpen en om ervoor te zorgen dat hun eigen werkpraktijken effectieve tegenmaatregelen omvatten.
>
> **Beschrijving:**
> Al het personeel moet een adequate technische training krijgen in verband met de bekende bedreigingen en kwetsbaarheden van hardware, software en social engineering.

IEC 62443 wordt gebruikt als basis voor de TS 50702, een cybersecurity-standaard voor spoorwegen.

Elk van deze normen stelt in een aantal eisen onder deze rubrieken. De eisen uit deze normen moeten in samenhang worden geanalyseerd tijdens de ontwikkeling van de bewustzijnstraining voor cybersecurity-ERTMS. Dit zal IO's '(Implementatie Organisaties) in staat stellen om te voldoen aan de vereisten uit hun eigen ISMS/CSMS om hen zo te helpen bij het gebruik en de acceptatie van de training.

Bijlage B Analyse van beschikbare documenten

B.1 ERA documenten

Zie de link naar: https://www.era.europa.eu/search/site/cybersecurity_en

De ERA stelt interessante documenten beschikbaar die als achtergrondinformatie voor een bewustwordingsprogramma kunnen worden gebruikt. De informatie wordt voornamelijk aangeboden in de vorm van rapporten over specifieke onderwerpen.

B.2 EC Transport Cybersecurity Toolkit

Gepubliceerd door EC 2020 (DG MOVE)

Dit document bevat informatie die specifiek gericht is op het verbeteren van het bewustzijn van cybersecurity. Het document onderkent twee afzonderlijke profielen voor cybersecurity-bewustzijn, namelijk:

- Alle transportmedewerkers; en
- Beslissers op het gebied van cybersecurity binnen het vervoersproces.

De informatie die wordt aangeboden voor "Alle transportmedewerkers" is bedoeld om ‘ondersteuning te bieden voor een beter begrip en bewustzijn van de meest voorkomende cyberdreigingen, gericht op vervoersdiensten en vervoerssystemen’. De informatie omvat twee onderdelen, namelijk een discussie over het dreigingslandschap en specifieke aandachtspunten voor de groepen ‘*Alle transportmedewerkers’* en *‘Beslissers’*.

Het hoofdstuk over het dreigingslandschap van de transportwereld biedt een kort overzicht van bedreigingsactoren en bedreigingen. Dit hoofdstuk is rechtstreeks van toepassing op het cybersecurity-bewustzijnsprogramma voor machinisten.

Het hoofdstuk behandelt:

- Bedreigingsactoren: een beschrijving van verschillende categorieën bedreigingsactoren; en
- Cyberbedreigingen: een beschrijving van vier bedreigingen (Malware, DDOS, toegang/diefstal, en Software-manipulatie).

Het daaropvolgende hoofdstuk is gericht op twee specifieke groepen. Dit gedeelte is echter minder van toepassing op het cybersecurity-bewustzijnsprogramma voor machinisten. De inhoud aangaande: ‘alle transportmedewerkers’ gaat over ‘begeleiding naar een beter begrip voor en bewustzijn van de meest voorkomende cyberbeveiligingsdreigingen gericht op deze transportdiensten’. In dit gedeelte worden de ‘best-practices’ beschreven. Het is een verzameling van tips die binnen de categorie ‘*cyberhygiëne’* zouden kunnen vallen. De tips zijn niet direct toepasbaar voor een operationele omgeving maar kunnen nuttig zijn bij het opbouwen van een basislijn voor *cyberhygiëne*.

Het document *‘Decision makers in transport-cybersecurity’* bestaat uit informatie op hoog niveau over het beheer van cybersecurity-risico's. Het is geschikt als introductiemateriaal voor managers die in aanraking komen met cybersecurity. De informatie biedt geen diepgaande inzichten die nodig zijn om cybersecurity-beveiligingsbeheersystemen te definiëren of te implementeren noch is het materiaal direct relevant voor operators. De informatie biedt een voorbeeld van *‘hoe cybersecurity binnen de organisatie wordt beheerd’*.

B.3 DfT rapport: Rail Cybersecurity – Gids voor de industrie

Gepubliceerd door UK Department for Transport 2016 (DfT United Kingdom, February 2016)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/897091/rail-cyber-security-guidance-to-industry-document.pdf

Het rapport is gericht op de railsector en omvat als zodanig veel details over de processen t.b.v. implementatie van cybersecurity binnen de organisatie en in processen. Eén van de gestelde doelen is om *'het bewustzijn van cybersecurity in de organisatie te vergroten'*. Hoewel dit rapport van belang zou kunnen zijn voor managers en ingenieurs is het van minder belang voor machinisten.

Er zijn onderdelen van dit rapport die nuttig zouden kunnen zijn bij het ontwikkelen van een cybersecurity-bewustzijnsprogramma voor machinisten, in het bijzonder paragraaf 2.16: *'Defence in Depth'* en 2.17: *'Protect, Detect, Respond'*.

Deze paragrafen bieden inzicht in de algemene aanpak van cyberbeveiliging. Het is van belang om deze items over te nemen om hiermee de machinisten een beeld te bieden in relatie tot waar deze onderwerpen passen binnen de algemene aanpak.

Paragraaf 2.24 omvat een lijst van onderwerpen die in de opleiding aan de orde zouden moeten komen. De lijst moet echter zodanig worden gelezen dat rekening wordt gehouden met het niveau en de reikwijdte van de vereiste kennis. Toch biedt de lijst wel een goed referentiekader voor wat naar verwachting zou moeten worden behandeld bij cybersecurity-bewustzijnscursussen voor operators.

Deze lijst is hieronder in zijn geheel weergegeven:

- Awareness van cybersecurity
- Begrijpen wat de problemen kunnen zijn
- Begrijpen waarom we aan zowel cybersecurity-beveiliging ***(Security)*** als veiligheid ***(Safety)*** aandacht moeten besteden
- Begrijpen waarom beveiliging van besturingssystemen ***(OT)*** verschilt van beveiliging van informatiesystemen ***(IT)***
- De noodzaak om rekening te houden met de gehele levenscyclus van het systeem. Dus niet alleen de operatie van het systeem, maar ook de werking en het onderhoud ervan
- De voortdurend aanwezige eisen die gelden voor het beheersen van cyber-aanvallen
- Het minimaliseren van de impact op het veiligheidssysteem
- Vergelijkingen met andere sectoren maken
- Kwetsbaarheidsbeheer (inclusief 'patching', het besturingssysteem (OT), firmware en applicatiecodes)
- Het belang van het testen van apparatuur van de fabrikant voordat deze wordt geïnstalleerd (AV), de controle ervan, de problemen die er zijn bij systeemverandering en het zich bewust zijn van systeem-/netwerkgrenzen

B.4 Training Department of Homeland Security

Een aantal online trainingsmodules worden aangeboden door het 'Department of Homeland Security' in de Verenigde Staten van Amerika. Deze zijn over het algemeen erg lang en niet specifiek relevant voor de spoorwegsector. Het geeft wel enig inzicht in hoe bepaalde aspecten van het opleidingsmateriaal op een andere wijze in de training worden behandeld.

(referentie: https://us-cert.cisa.gov/ics/Training-Available-Through-ICS-CERT)

B.5 Infographic NCSC Cybersecurity beeld Nederland

Dit ‘infographic’ biedt een context voor cyberdreigingen binnen de Nederlandse context. Het CSBN (Cybersecurity Beeld Nederland) is een jaarlijkse publicatie van het NCSC (National Cybersecurity Centrum) die zich richt op het nationale cybersecurity aspect. Het is een informatief document voor de cybersecurity-industrie. Het is de vraag of een bewustwordingscursus voor operators enige meerwaarde zou vinden in dit document. De ‘infographic’ geeft op een ‘licht verteerbare’ manier inzicht in de belangrijkste punten waar het CSBN zich mee bezig houdt.

B.6 Digital Trust Centre

Het ‘Digital Trust Centre’ is een initiatief van het Ministerie van Economische Zaken en Klimaat. Het geeft advies aan bedrijven met betrekking tot cybersecurity. Een relevant onderdeel van dat advies is het aspect ‘cybersecurity-bewustzijn’.

https://www.digitaltrustcenter.nl/informatie-advies/cyberbewustwording

Het advies van het ‘Digital Trust Centre’ biedt een aanpak voor cybersecurity-bewustzijnscampagnes en biedt ‘testimonials’ (bv over Schiphol). De adviespagina is van belang voor degenen die een bewustzijnstraining willen implementeren. Het advies is niet noodzakelijkerwijs bedoeld voor degenen die zelf het onderwerp zouden kunnen zijn van een cybersecurity-bewustzijnstraining. Hoewel er een hoofdstuk is dat over *OT* gaat ligt de focus van ‘DTC’ duidelijk op *IT- en kantoorsystemen*. ‘DTC’ geeft echter wel een aanzienlijke hoeveelheid details over veel van de onderwerpen die in een bewustzijnscampagne zouden kunnen worden opgenomen. Daarom dient het ‘DTC’ toch te worden gekenmerkt als een nuttige bron.

B.7 Centrum voor Ondergrounds Bouwen (COB)

COB (Centrum voor Ondergrounds Bouwen, 25-05-2021). Het doel van dit document is het verbeteren van cybersecurity-bewustzijn ten behoeve van alle partijen die betrokken zijn bij de oplevering en het beheer van infrastructurele projecten (tunnels).

Het document bevat een breed scala aan cybergerelateerde onderwerpen, waaronder de juridische basis, het V&V-assetmanagement, cyberincident-response en cybersecurity-management. Het document bespreekt verder de relatie tussen het cyberbeveiligingsontwerp van objecten en de ontwikkeling van de levenscyclus ervan, het risicobeheer, de defensiestrategieën en de SOC-inrichting. (Security Operation Center).

Het document is geschreven in de vorm van een algemeen kennisdocument en is niet geschikt voor een cybersecurity-bewustzijnsprogramma voor machinisten.

B.8 Het ENISA rapport over railway cybersecurity

(ENISA, November 2020)
Deze studie gaat over de mate van implementatie van cybersecurity-maatregelen binnen de (Europese) railsector. Dit in het kader van de handhaving van de ‘NIS-richtlijn’ die in elke Europese lidstaat plaats moet vinden (NIS: Netwerk en Informatie Systemen). De doelstelling van de studie wordt als volgt gekenmerkt:

> ‘Het belangrijkste doel van de studie is om een voorlopige analyse te delen aangaande het vaststellen van het volwassenheidsniveau van de railsector m.b.t. de implementatie van veiligheidsmaatregelen die worden afgedwongen door deze NIS-richtlijn’.

Het rapport is niet geschikt voor een cybersecurity-bewustzijnsprogramma voor machinisten. Ondanks de feitelijke doelstelling van het rapport zijn er echter wel enkele nuttige elementen vermeld die informatie kunnen bieden. Deze informatie kan vervolgens weer worden gebruikt ten behoeve van de opzet van een cybersecurity-bewustzijnsprogramma. Onderstaand een overzicht van deze informatie:

- Een lijst met cyberincidenten (de eerste pagina van paragraaf 2) kan nuttig zijn om achtergrondinformatie te bieden
- Tabel 3 kan van belang zijn om aan te tonen dat Nederland een van de weinige landen is in relatie tot het definiëren van het spoorwegsysteem als essentieel (vitaal). Alhoewel dit nu reeds achterhaald is door de recente wijziging van het BBNI (Besluit Beveiliging Netwerk en Informatiesystemen).

Bijlage C Interviews gehouden bij organisaties

Een cybersecurity-bewustzijnstraining is geen nieuw fenomeen. Er zijn interviews gehouden met mensen die betrokken zijn bij cybersecurity-bewustzijnstrainingen die binnen de industriesector worden toegepast. Het doel van deze interviews was om te kunnen leren van de ervaringen die zij daarbij hebben opgedaan.

C.1 NS (Reizigers)

De medewerker van NSR gaf aan dat er geen speciaal programma bestaat voor het ontwikkelen van het cybersecurity-veiligheidsbewustzijn van hun machinisten. Het beheer van cybersecurity-incidenten is opgenomen binnen de bestaande processen. Er wordt een procedure gehanteerd voor het beheren van cybersecurity-incidenten. Dit aspect vormt een onderdeel van de gebruikelijke training.

Er wordt enige aandacht besteed aan het algemeen bewustzijn tijdens de training, maar (naar de mening van NSR) onvoldoende. Er wordt onderkend dat het zich bewust zijn van cyberbeveiliging bij machinisten kan worden verbeterd.

C.2 RWS (Rijkswaterstaat)

Cybersecurity-bewustzijn is een belangrijke aandachtspunt bij RWS. Er wordt een training gegeven om *het zich bewust zijn van cyberbeveiliging* te verbeteren. Dit wordt op drie niveaus aangepakt:

- Het algemene cybersecurity-bewustzijn. Dit behandelt de generieke onderwerpen van cybersecurity en is gericht op de klassieke IT-gebeurtenissen en IT-processen.
- *OT* e-learning: Er is een specifieke OT cybersecurity-module gemaakt. Deze is ontworpen voor iedereen die betrokken is bij OT en is dus niet specifiek voor de operators.
- Crisis- en operationele testen. Cybersecurity-scenario's worden opgenomen als onderdeel van de normale crisis- en operationele tests. De cyber-scenario's bieden de operators een idee van hoe een cyberaanval eruit zou kunnen zien. Er werd besloten om cybersecurity op te nemen als onderdeel van de normale training. Dit om afstand te nemen van elk *vooroordeel* waarbij gedacht wordt dat cyberaanvallen zich in een andere vorm voordoen dan een operationeel probleem.

C.3 Interview bij een petrochemisch bedrijf

De belangrijkste punten die door de vakspecialist naar voren werden gebracht, waren de volgende:

- Het is noodzakelijk om operators eerst te overtuigen dat er een (cybersecurity) risico is en te laten begrijpen (in hun eigen taal) wat er allemaal mis kan gaan. Hiermee leert men inzien waarom cybersecurity zo belangrijk voor hen (en het bedrijf) is.
- Op het moment dat de gebruikelijke veiligheidscampagnes begonnen kostte het veel energie om de operators te begrijpen. Hetzelfde bleek bij het aspect ‘cybersecurity’ aan de orde te zijn. Het is een fenomeen waar in de loop van de tijd aan gewerkt moet worden.
- Als de operators afwijkingen niet kunnen voorkomen, mitigeren of detecteren dan heeft het geen zin om ze ermee te belasten.
- Er ligt een focus op het aspect waarom IT zich niet mengt met OT en waarom deze twee zaken moeten worden gescheiden. We hebben voorbeelden gehad waarbij printers waren aangesloten tussen de IT- en OT-netwerken. Het resulteerde in het ongelukkige feit dat deze printers het OT-netwerk deden uitvallen.
- Het is noodzakelijk om het verschil tussen OT en IT uit te leggen. Het lijkt op een Windows-computer, maar achter de schermen ziet het er anders uit.
- Leg de nadruk op hoe het systeem, dat wordt besproken, eruit ziet, hoe het systeem werkt en hoe het systeem zou kunnen falen. Merk daarbij op dat de verstoringen te wijten kunnen zijn aan de volgende aspecten (twee zijn er belangrijk):
- Doe geen dingen die het systeem in gevaar kunnen brengen (apparaten verbinden, ‘repareren’, zaken omzeilen, actie nemen m.b.t. overschrijven van informatie, een waarschuwing negeren, etc.).
- Als er iets mis lijkt te zijn, vraag dan om advies. Deze eerste reactie moet worden getraind en vormt een belangrijk onderdeel van de training.

- ‘Situationeel bewustzijn’ helpt te begrijpen hoe het aspect *‘verkeerd’* eruit zou kunnen zien. *Laat je eigen oordeel over wat je zelf ziet* dus niet overschaduwen door datgene wat men normaal gesproken als ‘gebruikelijk’ ziet en men het dus ‘niet relevant’ vindt.

Bijlage D Normen en richtlijnen

Internationale normen bieden richtlijnen voor specifieke aspecten van cyberbeveiligingsbeheer. Deze zijn over het algemeen niet geschikt voor een cybersecurity-bewustzijnsprogramma voor machinisten. Sommige onderdelen zijn echter wel van belang bij het *ontwikkelen* van dit cybersecurity-bewustzijnsprogramma. ISO 27002, paragraaf 7.2.2 omvat onderstaande lijst met onderwerpen:

Binnen het opleidings- en trainingspakket (met betrekking tot informatiebeveiliging) dienen ook algemene aspecten te worden opgenomen, zoals:

a) het aangeven van de betrokkenheid van de directie bij informatiebeveiliging binnen de gehele organisatie
b) de noodzaak om bekend te worden met en het voldoen aan de van toepassing zijnde regels en verplichtingen met betrekking tot informatiebeveiliging zoals gedefinieerd in beleidsregels, normen, wetten, regelgeving, contracten en overeenkomsten
c) persoonlijke verantwoordelijkheid nemen voor het eigen doen en laten en algemene verantwoordelijkheden nemen ten opzichte van het beveiligen of beschermen van informatie die eigendom is van de organisatie en van externe partijen
d) basisprocedures inzake informatiebeveiliging vaststellen (zoals het melden van informatiebeveiligingsincidenten) en basisbeheersmaatregelen ontwikkelen (zoals wachtwoordbeveiliging, malwarecontroles en het toezien op opgeruimde bureaus)
e) contactorganen en bronnen voor aanvullende informatie kenbaar maken en advies over informatiebeveiligingsaangelegenheden bieden (met inbegrip van aanvullend opleidings- en trainingsinformatie m.b.t. informatiebeveiliging)

Verder worden er nog andere richtlijnen (zie ook paragraaf 7.2.2) verstrekt.

Bij het opstellen van een cybersecurity-bewustzijnsprogramma is het belangrijk om niet alleen de aandacht te richten op het *'wat'* en *'hoe'*, maar ook op het '*waarom'*. Het is belangrijk dat medewerkers het ***doel*** van informatiebeveiliging en de ***potentiële impact*** (positief en negatief), in relatie tot hun eigen gedrag, op de organisatie begrijpen.

Opgemerkt moet worden dat ISO 27002 betrekking heeft op IT (*en OT volledig negeert*).