ProRail

Informatiebeveiligingsbeleid

Externe Connecties, Standaarden

Eigenaar	ICT – CIO Office / Operations
Auteur	Marco de Heuvel / Kelvin Rorive
Kenmerk	IBB-2.5
Versie	2.6
Datum	Juli 2016
Bestand	IBB-2.5 Externe connectie standaarden v2.6
Status	Definitief
Informatieclassificatie	Intern

INHOUDSOPGAVE

ProRail

1 Inleiding

1.1 Introductie

Het informatiebeveiligingsbeleid van ProRail is er op gericht om aan de hand van risicoanalyses de beveiligingsbehoeften te bepalen. Hierdoor zorgt men ervoor dat de beveiliging aansluit bij de behoefte van de business. Per business proces wordt gekeken naar de beveiligingsbehoeften (IB-functie) met betrekking tot de aspecten beschikbaarheid, integriteit en vertrouwelijkheid (BIV). Vervolgens worden deze IB-functies vertaald naar standaarden de *IB-mechanismen*.

Met het ProRail informatiebeveiligingsbeleid en de handleiding classificering ICT Informatie als uitgangspunt wordt in dit document ingegaan op de standaarden voor *externe connecties*. Dit document richt zich expliciet op de *externe connecties*. Dit betreft het uitwisselen van gegevens tussen externe en interne systemen of gebruikers.

1.2 Afbakening

Dit document beschrijft de Informatiebeveiligingsstandaarden voor de *externe connecties*. Waarbij wordt ingegaan op de communicatie tussen externe netwerken en de interne ProRail *domeinen*.
Dit document gaat niet in op de beveiligingsstandaarden voor de communicatie tussen interne ProRail *domeinen*. Deze beveiligingstandaarden staat beschreven in het document (IBB-26 Interne Connectie standaard ProRail).

1.3 Doel

In dit document zijn de mogelijkheden en maatregelen voor externe connecties beschreven. Het doel van dit document is het bieden van Informatiebeveiligingsstandaarden voor deze externe connecties en dient als input voor zowel de infra architectuur van Prorail als de controlerende instanties.

1.4 Positionering

Dit document vormt een onderdeel van het stelsel van informatiebeveiliging bij ProRail. Onderstaand figuur geeft inzicht in de positionering van deze standaard door de relaties met andere documenten inzichtelijk te maken.

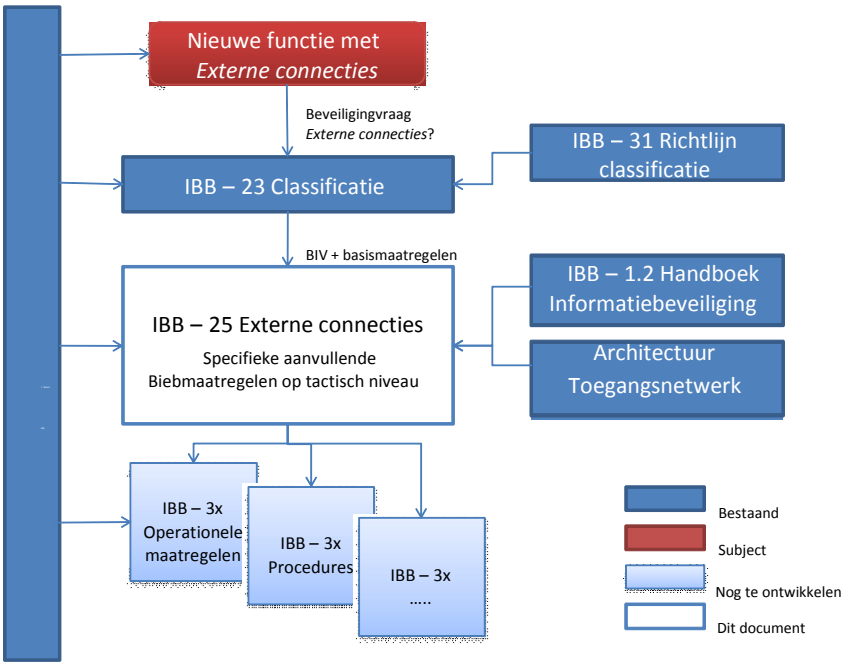


Figure 1

1.5 Uitgangspunten bij deze standaard

Bij het opstellen van deze standaard zijn de volgende uitgangspunten gehanteerd:

- Maatregelen in deze standaard zijn functioneel beschreven. Een functioneel beschreven maatregel is een *technisch* concept, voorbeeld: 'Een end2end koppeling is versleuteld'. Hoe deze versleuteling wordt gerealiseerd (het fysieke object, protocollen e.d.) is beschreven in operationele beleidsnotities;
- De beschreven maatregelen in deze standaard zullen vaak niet gerelateerd zijn aan een classificatie. Het toegangsnetwerk heeft een generiek karakter voor heel ProRail en dient als beveiligingslaag tussen het bedrijfsnetwerk en de externe netwerken. Te veel differentiatie (n.a.v. de classificatie) leidt tot meer complexiteit, hogere kosten en vaak niet tot betere beveiliging.

1.6 Doelgroep

Dit document is opgesteld voor de volgende doelgroepen: infrastructuur architecten, projectleiders en managers verantwoordelijk voor het ontwikkelen, aanpassen en implementeren van ICT-dienstverlening. Daarnaast diegene die verantwoordelijk zijn voor het opstellen van beveiligingskaders en de controle op de naleving hiervan. Denk hierbij aan systeemeigenaren en productmanagers die verantwoordelijk zijn voor de levering, beheer of uitbesteding van ICT-diensten.

Dit document dient tevens als referentie voor controlerende instanties.

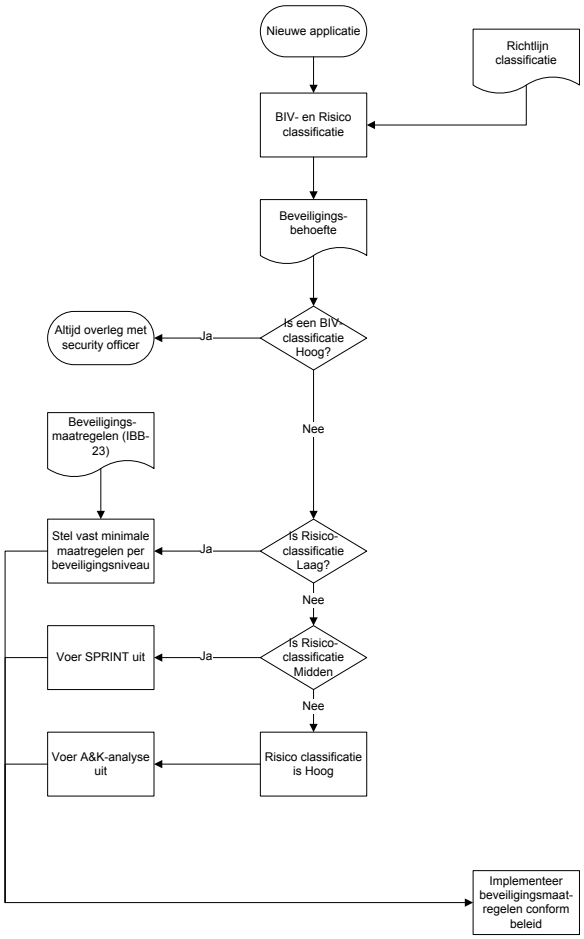
1.7 Leeswijzer

Hoofdstuk 2 beschrijft specifieke delen van de toegangsinfrastructuur van ProRail die van belang zijn bij de selectie van informatiebeveiligingsmaatregelen. Hoofdstuk 3 beschrijft de te nemen maatregelen per classificatie van informatie.

1.8 Toepassen van deze standaard

Op het moment dat er behoefte ontstaat voor het maken van een nieuwe of het wijzigen van bestaande koppelingen tussen externe en interne *domeinen*, wordt de beveiligingsbehoefte hiervan in kaart gebracht door het betrokken informatiesystemen te classificeren op basis van de kwaliteitskenmerken beschikbaarheid, integriteit en vertrouwelijkheid. Hierbij worden de niveaus B (basaal), L (laag), M (midden) en H (hoog) gehanteerd. De eigenaar van het betreffende informatiesysteem is hiervoor verantwoordelijk zoals beschreven in het document Ref [4].

Aan de hand van de classificatie per informatiebeveiligingsaspect kunnen vervolgens maatregelen worden gekoppeld, zoals in het onderstaande schema wordt weergegeven.



Het volgende tabel geeft een voorbeeld van de manier waarop de maatregelen in dit document zijn vastgelegd. Aan de hand van de classificering (beveiligingsbehoefte) dienen de maatregelen worden gekoppeld aan de voorgestelde oplossing.

Maatregel	B	I	V	Opmerkingen
maatregel 1	-	-	-	
maatregel 2		M	L	
maatregel 3	M			

1. Indien onder één van de B.I.V. aspecten een "-" staat dan betreft het een maatregel die onafhankelijk van de classificatie moet worden ingevoerd;
2. Indien onder één van de B.I.V. aspecten een lege cel staat dan betreft het een aspect dat niet van toepassing is voor de maatregel;
3. Indien een van de B.I.V. aspecten een classificering heeft, dan geldt deze maatregel ook voor de bovenliggende niveaus. Een classificatie ´L´ betekent ook dat deze maatregel geldt voor classificatie ´M´ en 'H'.

Uitzondering
In het geval dat één van beveiligingsaspecten (B.I.V) een classificering Hoog (H) heeft of indien het ICT-vraagstuk niet binnen de kaders van dit document kan worden ingedeeld dient in alle gevallen te worden overlegd met de security officer over de te nemen maatregelen.

1.9 Definities

Term	Definitie
Applicatieve ontkoppeling	Applicatieve ontkoppeling is een techniek waarbij een sessie op een ontkoppelingssysteem wordt afgesloten om vervolgens vanaf dit systeem de sessie weer op te bouwen.
Besloten netwerken	Onder de besloten netwerken vallen NIS, Hermes en Corporate UMTS.
Derde partijen	Partners in de spoorbranche.
DMZ	Een verbijzonderde zone (met specifieke beveiligingsmaatregelen) tussen onvertrouwde en vertrouwde zones.
Domein	Een logische groepering van systemen die samen een infrastructuur vormen voor een specifiek toepassingsgebied.
Externe koppeling(en)	De functionaliteit om te kunnen communiceren tussen gebruikers en systemen van interne ProRail-domeinen met externe domeinen die niet in beheer of onder controle van ProRail zijn.
HOP-server	Een server waar vanaf een geautoriseerde gebruiker een sessie kan opzetten naar een specifiek domein of systeem.
IB-functies	Geautomatiseerde activiteiten gericht op beschikbaarheid, controleerbaarheid, integriteit en vertrouwelijkheid.
IB-mechanismen	Dit zijn technische concepten die de *IB-Functies* invullen. Denk hierbij aan begrippen als encryptie en redundancy.
Inbound verkeer	Dit betreft verkeer waarbij het initiatief van de datakoppeling bij een gebruiker of systeem buiten het ProRail netwerk ligt.
Koppelvlak	Het gecontroleerd uitwisselvlak van informatie tussen gekoppelde zones/netwerken.
Outbound verkeer	Dit betreft verkeer waarbij het initiatief van de datakoppeling bij een gebruiker of systeem binnen het ProRail netwerk ligt.
Publieke netwerken	Het Internet valt onder publieke netwerken, net zoals het PSTN netwerk.
Semi- publieke netwerken	Besloten netwerken met partners in de spoorbranche. NIS valt onder de Semi-publieke netwerken.

Trust Koppeling	In de context van koppeling van verschillende Windows domeinen. In geval van een vertrouwde relatie biedt een dergelijke koppeling toegang voor gebruikers uit het vertrouwde domein.
Two-sided SSL	Bij Two-sided SSL wordt aan de hand van SSL zowel de identiteit van de server als de cliënt gecontroleerd.
Zone	De logische verzameling van ICT-componenten met hetzelfde beveiligingsniveau, die via beveiligde *koppelvlakken* gegevens kunnen uitwisselen met andere zones.

1.10 Referenties

[1] IBB-1 Informatiebeveiligingsbeleid ProRail
[2] IBB-1.2 Handboek voor Informatiebeveiliging ProRail
[3] IBB-2.3 Risicobeheersing en classificatie bij Informatievoorziening ProRail
[4] IBB-3.1 Handleiding ICT Beveiligingsbehoefte classificering
[5] ProRail Toegangsnetwerk
[6] NORA Dossier Informatiebeveiliging – Normen IT-voorzieningen

2 Toegangsnetwerk ProRail

2.1 Algemeen

Voor het koppelen van externe partijen en systemen maakt ProRail gebruik van een toegangsnetwerk dat het *koppelvlak* vormt tussen de interne netwerken en de niet of minder vertrouwde externe netwerken.

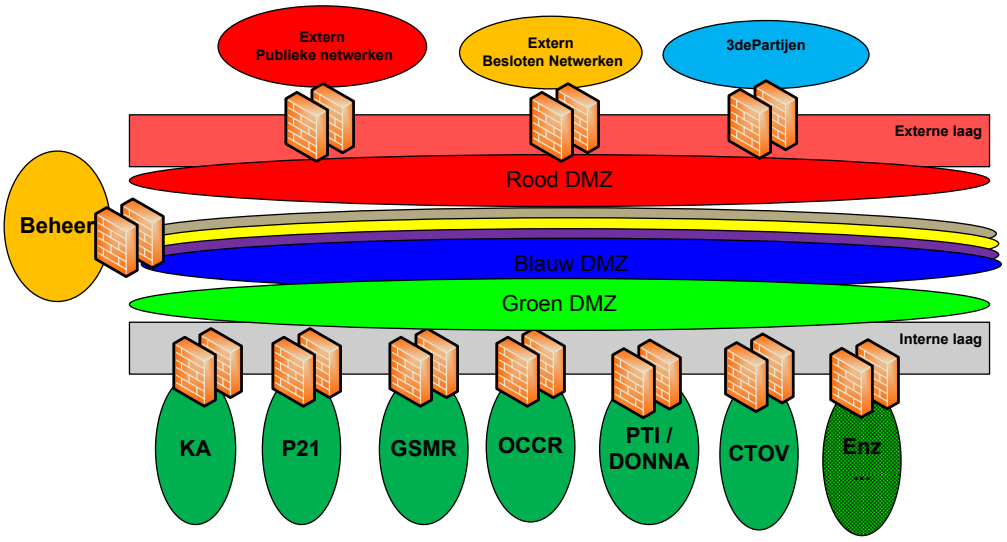
2.2 Architectuurprincipes

Uitgangspunt bij het opstellen van basis informatiebeveiligingsmaatregelen zijn de architectuurprincipes. De onderstaande architectuurprincipes zijn vastgesteld ten aanzien van *externe connecties*. Deze principes zijn vastgelegd in het architectuurdocument Ref. [5]:

1. Het toegangsnetwerk is de enige manier om ProRail netwerken van buitenaf te bereiken;
2. Het toegangsnetwerk is de enige manier om een extern netwerk te bereiken;
3. Het toegangsnetwerk is de enige manier om tussen ProRail netwerken koppelingen te leggen;
4. Het toegangsnetwerk is de preferente plaats voor generieke systemen;
5. Dezelfde functionaliteiten gebruiken zoveel mogelijk dezelfde systemen;
6. Dezelfde functionaliteiten hebben dezelfde beheerder;
7. Er is een dubbele firewall laag;
8. Routeringsinformatie op de buitenste firewalls is zo beperkt mogelijk;
9. Verkeer binnen ProRail gaat nooit via een buitenste firewall;
10. Er wordt niet geNAT op de binnenste firewalls;
11. Er zijn verschillende firewalls voor besloten en publieke externe netwerken;
12. Inkomend en uitgaand verkeer gaat altijd via een systeem in een *DMZ*;
13. Systemen in een *DMZ* kunnen logisch gescheiden worden;
14. Het is mogelijk om systemen redundant aan te sluiten;
15. “Best practices” worden zoveel mogelijk gevolgd.

2.3 Architectuur toegangsnetwerk

De toegangsinfrastructuur zoals toegepast bij ProRail is op abstract niveau samengevat in onderstaand figuur.



2.4 *Zone*-indeling toegangsnetwerk

Het toegangsnetwerk is verdeeld in beveiligingszones. Het doel hiervan is om risico's te isoleren zodat bedreigingen of incidenten niet doorwerken in de andere *zones*. Onderdelen met verschillende betrouwbaarheidseisen worden door de zonering van elkaar gescheiden. Iedere beveiligingszone heeft een eigen functie en beveiligingsniveau. Een *zone* heeft een gedefinieerd beveiligingsniveau, dit betekent dat binnen de *zone* samenhangende beveiligingsmaatregelen gelden. Op de *koppelvlakken* en binnen deze zones worden beheersmaatregelen toegepast. Hiermee worden de informatiestromen tussen interne en externe netwerken gecontroleerd. De verschillende functies van de zones worden met een kleur aangeduid en uiteengezet in het onderstaande tabel.

Zone	Functie	Voorbeeld
Rood	*DMZ* voor toegang vanaf externe *publieke netwerken*.	Citrix access gateway, VPN Concentrators, mail relay.
Bruin	*DMZ* voor toegang naar extern *publieke netwerken.*	Forward proxy, DNS Relay.
Geel	Transit *zone* van extern publiek en besloten naar intern.	Verkeer vanaf VPN concentrator naar een interne *zone.*
Paars	*DMZ* voor toegang van of naar externe *Besloten netwerken.*	Communicatie met NIS, HERMES en Vodafone APN.
Blauw	Standaard *DMZ* omgeving.	Content systemen, Citrix servers.
Groen	Interne *DMZ* ten behoeve van generieke beheersystemen en generieke services.	AAA, NTP, RSA, NSM.

Tabel 1, zone-indeling toegangsnetwerk

2.5 Gebruikersgroepen

Binnen de ProRail infrastructuur zijn aan de hand van de informatiebehoeften verschillende gebruikersgroepen gedefinieerd. De informatiebehoefte is datgene wat een gebruiker of gebruikersgroep met het oog op een bepaalde toepassing wenst. Denk hierbij aan het raadplegen, verwerken of uitwisselen van informatie. Door gebruikersgroepen te definiëren is het mogelijk om naast de indeling per koppeling ook te specificeren naar een gebruikersgroep. Hierdoor kan er onderscheid worden gemaakt bij het definiëren van maatregelen over een zelfde type koppeling bij gebruik door verschillende gebruikersgroepen.

Een voorbeeld hiervan is het gebruik van een virtuele werkplek door medewerkers voor KA functionaliteit en door beheerders voor beheerwerkzaamheden.

Gebruikersgroep	Gebruikers	Toepassingen
Publiek	- Reizigers - Leveranciers - Medewerkers	Reisinformatie, Projectinformatie, Algemene informatie
Medewerker buiten	- Medewerkers - Beheerders - Ingehuurd personeel - Contractpartijen	Remote werken (thuiswerken)
ProRail beheerders	- Beheerders	Remote werken, Remote beheer
Contractpartij beheer	- Externe dienstverlener - Leverancier van systemen - Netwerkleverancier	Remote beheer, Statusberichten
Contractpartij informatievoorziening		Verbruiksinformatie, Capaciteitsplanning

Tabel 2, gebruikersgroepen

3 Informatiebeveiligingsmaatregelen

3.1 Inleiding

In dit hoofdstuk worden de IB-maatregelen beschreven die van toepassing zijn bij het gebruiken van het toegangsnetwerk van ProRail. De architectuur van het toegangsnetwerk is beschreven in document Ref. [5]. In deze architectuur is een zonering beschreven waarbij elke zoneovergang minimaal netwerkfiltering wordt gehanteerd (firewalling). Bij de uitwerking van de maatregelen is dit als uitgangspunt gehanteerd.

Voor het toegangsnetwerk gelden algemene beveiligingseisen, onafhankelijk van het soort koppeling met het toegangsnetwerk. Daarnaast worden een aantal type koppelingen onderkend waarvoor specifieke aanvullende beveiligingseisen zijn gesteld.

Bij het beschrijven van de maatregelen wordt uitgegaan van de verschillende koppelingen die ProRail beschikbaar heeft binnen het toegangsnetwerk.

De maatregelen zijn op functioneel niveau beschreven waarbij is toegelicht welk risico wordt geadresseerd met de maatregel. De lezer van deze standaard kan de beschreven IB-maatregel vertalen naar een concrete en passende technische oplossingen.

3.2 Algemene Maatregelen

Het toegangsnetwerk is het enige *koppelvlak* van ProRail met externe netwerken of -gebruikers. Het toegangsnetwerk is een generieke dienst waarmee informatie wordt uitgewisseld met verschillende classificaties. Het toegangsnetwerk dient een basisbeveiliging te hebben die met aanvullende specifieke maatregelen eenvoudig voor een hogere classificatie van informatie kan worden toegepast.

Ten aanzien van de beschikbaarheid, integriteit en vertrouwelijkheid zijn de minimale maatregelen per beveiligingsniveau van toepassing zie Ref [3]. Deze hebben voornamelijk betrekking op continuïteitsvoorzieningen, herstelbaarheid, verwerking en bewaking. Hierbij voorziet de architectuur van het toegangsnetwerk in de mogelijkheid dat systemen met een hoge B(IV) classificatie, redundant kunnen worden aangesloten.

Aanvullend op de minimale maatregelen uit Ref [3] zijn onafhankelijk van het beveiligingsniveau voor het toegangsnetwerk algemene maatregelen van kracht. Deze maatregelen hebben betrekking op verschillende *IB-functies* binnen het toegangsnetwerk denk hierbij aan zonering, filtering, systeem integriteit, controleerbaarheid en bewaking.

Maatregelen
Voor het toegangsnetwerk gelden de volgende algemene maatregelen.

ID	Maatregel	B	I	V	Opmerkingen
Algemeen					
IBB-25_3.2-1	Alle Netwerken aangesloten op het toegangsnetwerk worden geclassificeerd zoals beschreven in Ref. [4] Handleiding classificering ICT Informatie beveiligingsbehoeften IBB-31.	-	-	-	

ID	Maatregel	B	I	V	Opmerkingen
IBB-25_3.2-2	Voor het koppelen van partners wordt in alle gevallen een overeenkomst getekend waarin duidelijke voorwaarden voor het aansluiten van netwerken en systemen zijn opgesteld.	-	-	-	
IBB-25_3.2-3	Er zijn voorzieningen geïmplementeerd om de beschikbaarheid van het toegangsnetwerk te bewaken.	-			
IBB-25_3.2-4	Datacommunicatievoorzieningen beschikken over automatisch werkende alternatieve routeringsmechanismen om uitval van fysieke verbindingen op te vangen.	-			
IBB-25_3.2-5	Toegangsnetwerk is volledig redundant uitgevoerd.	M			Uitval van hardware of verbinding leidt niet tot onbeschikbaarheid.
Firewalling en *zones*					
IBB-25_3.2-6	Bij elke zoneovergang zoals gedefinieerd in de architectuur ref. [5] wordt netwerkfiltering (firewalling) toegepast. Logische scheiding is toegestaan indien routering via de Firewalls verloopt.		-	-	
IBB-25_3.2-7	Met filtering wordt er minstens gecontroleerd op protocol en richting. Niet toegestane verbindingen worden geblokkeerd.	-	-	-	
IBB-25_3.2-8	Besloten en publieke infrastructuur is minimaal logisch gescheiden middels separate firewalls.		-	-	
IBB-25_3.2-9	*Zones* en systemen die vanaf de *publieke netwerken* bereikbaar zijn dienen geen verbindingen naar het publieke netwerk op te kunnen zetten.	-	-	-	toelichting *
IBB-25_3.2-10	NAT wordt alleen uitgevoerd op firewalls in de buitenste laag.			-	
DMZ					
IBB-25_3.2-11	In een *DMZ* zijn maatregelen getroffen om aanvallen te signaleren en te kunnen blokkeren die een bedreiging vormen voor de betrouwbaarheid van de infrastructuur van ProRail.	-	-	-	
IBB-25_3.2-12	Inbound informatiestromen vanaf *publieke netwerken* worden applicatief ontkoppeld in het externe *DMZ* (rood).	-	-	-	
IBB-25_3.2-13	Inbound informatiestromen vanaf *besloten netwerken* worden applicatief ontkoppeld in het externe *DMZ* (paars).	-	-	-	

ID	Maatregel	B	I	V	Opmerkingen
IBB-25_3.2-14	Het interne AD-domein is alleen gecontroleerd beschikbaar in de rode of paarse *DMZ*. Applicatieservers in het DMZ zijn nooit onderdeel van een intern AD-domein.	-	-	-	Zie voor toelichting **
IBB-25_3.2-15	Servers in de *DMZ* hebben zo beperkt mogelijk Internet toegang.	-	-	-	
IBB-25_3.2-16	Routering op servers in een *DMZ* is alleen statisch toegestaan bij *applicatieve ontkoppeling* (o.a. proxies). Alle overige routering op servers is niet toegestaan.	-	-	-	
IBB-25_3.2-17	Binnen de *DMZ* worden alleen protocollen gebruikt die nodig zijn voor de benodigde functies. Overige protocollen worden niet toegestaan.	-	-	-	
IBB-25_3.2-18	De *DMZ* wordt ingericht met IT-voorzieningen, waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening). Elk systeem in een *DMZ* is voorzien van een actuele security configuratie conform ProRail ontwerpvoorschrift (OVS) of voldoet minimaal aan de NIST[1]standaard.	-	-	-	

Tabel 3, algemene maatregelen

* Om te voorkomen dat ProRail-systemen misbruikt worden voor staging mogen systemen in een *DMZ* die vanaf een publiek netwerk bereikbaar zijn, geen verbinding naar dat *publieke netwerk* kunnen opzetten. Een uitzondering hiervan is de Mail-relay. Hiervoor zijn specifieke maatregelen beschreven in paragraaf 3.6

**** Indien één van de *DMZ* servers wordt gecompromitteerd dan mag het niet mogelijk zijn om via deze server direct op het interne *domein* te kunnen komen. Daarom dienen servers in een rode of paarse *DMZ* alleen op gecontroleerde wijze en zo beperkt mogelijk een onderdeel te zijn van het interne AD-*domein*.
Als alternatief en waar mogelijk kan er een gescheiden AD-domein worden opgezet in de *DMZ* omgeving en wordt er gesynchroniseerd vanuit het interne AD-domein. Hierbij is de communicatie beperkt tot alleen het benodigde protocol en richting. Er zijn verschillende oplossingen beschikbaar waaronder het gebruik van een read only Domain controllers(RODC) waarbij alleen de benodigde informatie wordt gesynchroniseerd en er geen wijzigingen vanuit de DMZ kunnen worden doorgevoerd in de AD.

3.3 Soorten netwerkkoppelingen

Afhankelijk van het soort netwerkkoppeling waarvoor het toegangsnetwerk wordt gebruikt moeten bovenop de algemene maatregelen aanvullende maatregelen worden getroffen.

Het NIST (National Institute of Standards and Technology) onderhoud lijst met definities en regels van alle bij een automatiseringsproces betrokken middelen en componenten waarin per operatingsysteem en applicatie gedetailleerde security configuratie setting worden bijhouden. Deze lijst dient als referentie voor het beveiligen en harden van systemen. De lijst is te vinden via de volgende link; http://checklists.nist.gov/ .

In de navolgende paragrafen worden aanvullende maatregelen beschreven afhankelijk van het soort koppeling.
De volgende koppelingen worden onderscheiden bij ProRail:
Koppeling ter ondersteuning van:

- Remote werken;
  Het beschikbaar hebben van KA functies en faciliteiten buiten het gecontroleerde ProRail netwerk;
- Publicatie van informatie
  Het beschikbaar stellen van informatie vanuit ProRail aan gebruikers op onvertrouwde netwerken met behulp van webfunctionaliteiten. Een voorbeeld is de ProRail website.
- Datakoppeling
  Het uitwisselen van bedrijfsgegevens van en naar het ProRail netwerk met niet bekende partijen of netwerken. Een voorbeeld hiervan is e-mail verkeer.
- Interconnecties
  Het koppelen van netwerken en systemen van ProRail met partners in de spoorbranche (bekende partijen) waarmee een overeenkomst is afgesloten. Voorbeelden hiervan zijn het uitwisselen van reis- en planningsinformatie.
- Servicebus
  Uitwisseling van informatie met derden op basis van onder andere XML-gebaseerde technologieën.

Netwerkkoppelingen in relatie met gebruikersgroepen
De netwerkkoppelingen kunnen worden gerelateerd aan de gebruikersgroepen zoals in Tabel 2 staat weergegeven. Hierdoor kan er onderscheid worden gemaakt bij het definiëren van maatregelen over een zelfde type netwerkkoppeling bij gebruik door verschillende gebruikersgroepen.

Gebruikersgroep	Koppelingen
Publiek	- Publicatie van informatie
Medewerker buiten	- Remote werken
ProRail beheerders	- Remote werken - Beheer
Contractpartij beheer	- Servicebus - Datakoppeling
Contractpartij informatievoorziening	- Servicebus - Datakoppeling

Tabel 4, Netwerkkoppelingen in relatie met gebruikersgroepen

3.4 Remote werken

Toegang tot het bedrijfsnetwerk vanaf een remote werkplek wordt als volgt mogelijk gemaakt bij ProRail:

- Virtuele werkplek
- Bedrijfsapplicaties via een Portaal
- Tunneling (VPN of DirectAccess)
- Beheer

3.4.1 Virtuele werkplek

Met een virtuele werkplek wordt alleen beeldscherm informatie overgebracht naar de fysieke werkplek van de gebruiker. Er zijn meerdere technieken die dit mogelijk maken (VDI, Citrix enz). Een virtuele werkplek kan gestart worden vanaf onbekende hardware, zoals een privé pc. Een virtuele werkplek biedt een veilige vorm van ontsluiten van het bedrijfsnetwerk naar remote werkers op onbekende pc´s. Sessie hijacking is vrijwel uitgesloten waardoor kwaadaardige code vanaf de onbekende pc geen bedreiging is voor het bedrijfsnetwerk.

Het grootste risico van een virtuele werkplek is onderscheppen van inloggegevens (o.a. keyloggers). Kwaadaardige gebruikers kunnen deze inloggegevens misbruiken.
Daarom wordt voor virtuele werkplekken die vanaf een niet door ProRail gecontroleerd netwerk worden gebruikt, 2-factor authenticatie vereist.

Voor de afscherming van het bedrijfsnetwerk dient bij gebruik vanaf niet gecontroleerde netwerken, gebruik te worden gemaakt van *applicatieve ontkoppeling* in de externe *DMZ* rood (Citrix access gateway enz).

3.4.2 Bedrijfsapplicaties via portaal

Het portaal voorziet in het beschikbaar stellen van specifieke bedrijfsapplicaties, afhankelijk van de autorisaties van de gebruiker. *Applicatieve ontkoppeling* hiervoor vindt plaatst in de externe *DMZ* rood. De applicaties worden beschikbaar gesteld via de Internet browser op de werkplek. Een portaal kan in principe vanaf elke willekeurige werkplek worden benaderd zowel vanuit het interne, door ProRail gecontroleerde, *domein* als het externe *domein*. Voor het benaderen van deze toepassingen vanuit niet door ProRail gecontroleerde netwerken, is 2-factor authenticatie vereist.

3.4.3 Tunneling vanaf een werkplek

Tunneling kan gerealiseerd worden door middel van aparte VPN software op de werkplek. Ook geïntegreerde oplossingen in OS vallen in deze categorie zoals DirectAccess. In alle gevallen wordt er een sleutel (d.m.v. een certificaat) uitgewisseld waarmee het systeem zich authentiseert, waarna de gebruiker zich ook moet authentiseren. Tunneling dient alleen mogelijk te zijn vanaf bekende en gecontroleerde hardware (actuele virusscanning e.d.).

Bij de authenticatie van de remote gebruiker is 2-factor authenticatie als minimale maatregel gesteld (zie Ref [2]). Het risico voor remote gebruikers zit met name in diefstal van het device (laptop) in combinatie met een geldig gebruikersnaam en wachtwoord.
Daarnaast is vanuit het externe toegangsnetwerk niet bekend met welk systeem autorisaties een gebruiker toegang krijgt (niet overal is duidelijk onderscheid in KA-accounts en beheeraccounts).

Er dient gebruik te worden gemaakt van een *applicatieve ontkoppeling* bij het verbinden van de remote werkplek met het interne KA netwerk. De *applicatieve ontkoppeling* vindt plaats in de rode *zone*.

3.4.4 Beheer

In relatie met *externe connecties* worden in geval van beheer van de ProRail ICT-voorzieningen de volgende rollen onderkend:

- ProRail beheerders
- Contractpartij beheer

ProRail beheerders
Voor beheer wordt gebruik gemaakt van een apart beheeraccount. Via dat specifieke account worden de betreffende beheeractiviteiten uitgevoerd. Logging op beheerhandelingen zijn zo mogelijk.
Bij beheer vanuit een niet door ProRail gecontroleerde omgeving (zoals thuiswerkplek) wordt er met de reguliere 2-factor authenticatie en Citrix ingelogd voor remote werken. Op dat moment kan er met het specifieke beheeraccount ingelogd worden voor uitvoeren van beheer, alsof de beheerder vanuit het interne netwerk beheer uitvoert.

Contractpartij beheer
Onder contractpartij beheer wordt verstaan, het uitvoeren van beheerfuncties binnen de ICT-infrastructuur van ProRail door een derde partij of een derde partij biedt diensten aan op de infrastructuur van de eigen organisatie (fysiek in huis).

De risico's bij dergelijke beheerkoppelingen liggen voornamelijk bij de benodigde bevoegdheden voor het uitvoeren van dergelijke functionaliteit. Een van de risico's hierbij is het weglekken van vertrouwelijke informatie. De toegang voor contractpartijen dient daarom zoveel mogelijk beperkt te worden tot het stikt noodzakelijke (need to know). ProRail maakt gebruik van beherende partijen die op verschillende wijzen toegang hebben tot de infrastructuur, via een eigen netwerkverbinding of via openbare netwerken zoals Internet.

Ten aanzien van maatregelen kan een beheerder van een derde partij gezien worden als een eigen beheerder met dien verstande dat handelingen van externe beheerders gelogd moeten worden met daarop real-time analyse van deze logging om afwijkende acties te detecteren.

3.4.5 Maatregelen

ID	Maatregel	B	I	V	Opmerkingen
IBB-25_3.4-1	Businessapplicaties, direct benaderbaar vanuit de KA omgeving zijn gelijk beveiligd als een systeem in *DMZ,* zie o.a. maatregel IBB-25_3.2-18		M	M	
IBB-25_3.4-2	Externe toegang tot het beheersegment is alleen mogelijk via een *Hop* in de blauwe *zone*.	-	-	-	Bv. Eerst toegang tot standaard KA, daarna toegang tot beheer
IBB-25_3.4-3	Bij gebruik van niet-publieke ICT-voorzieningen vanuit een niet door ProRail gecontroleerd netwerk vindt altijd sterke authenticatie (2-factor) van gebruikers plaats.	-	-	-	
IBB-25_3.4-4	VPN Tunnels worden alleen opgezet vanaf bekende en gecontroleerde hardware.	-	-	-	
IBB-25_3.4-5	Bij het opzetten van een VPN tunnel vindt authenticatie van het systeem plaats (bijvoorbeeld door middel van het uitwisselen van certificaten).	-	-	-	
IBB-25_3.4-6	Authenticatie van een gebruiker is vereist bij VPN tunnels vanaf een werkplek.	-	-	-	
IBB-25_3.4-7	Er vindt uitsluitend informatie-uitwisseling plaats tussen een remote werkplek en ProRail via een versleuteld kanaal, voor geautoriseerde netwerk- en communicatieprotocollen.	-	-	-	
IBB-25_3.4-8	Alle handelingen van beheerders worden gelogd.		M	M	
IBB-25_3.4-9	Alle handelingen van gecontracteerde beheerders worden gelogd.		-	-	
IBB-25_3.4-9	Real-time loganalyse vindt plaats op afwijkende beheerhandelingen.		M	M	

Tabel 5, KA-maatregelen

3.5 Publicatie van informatie

ProRail publiceert, maar ontvangt ook informatie via haar websites, denk hierbij aan informatie aanvragen via invulformulieren of klachtenformulieren. Er wordt onderscheid gemaakt tussen anonieme en geauthentiseerde gebruikers. Geauthentiseerde gebruikers zijn bijvoorbeeld medewerkers maar ook aannemers die specifieke informatie nodig hebben. Geauthentiseerde gebruikers kunnen informatie via de websites aanpassen of gegevens uploaden.

De risico's via deze koppeling richten zich voornamelijk op het ongeautoriseerd toegang krijgen tot vertrouwelijke informatie of het onbeschikbaar maken c.q. aanpassen van de websites. Bedreigingen zijn o.a. defacing en Ddos met als gevolg een reputatieschade die gezien het maatschappelijk belang van de organisatie van groot belang is. Integriteit van de ProRail websites is hierdoor van zeer groot belang.

Voor veilige verstrekking van informatie via publiek beschikbare websites is het van belang dat er een scheiding op verschillende beveiligingsniveaus (Tiering) wordt toegepast (presentatie / applicatie / gegevens). De presentatielaag wordt in de externe *DMZ* (rood) geplaatst, in de vorm van een reverse-proxy (*applicatieve ontkoppeling*). De reverse-proxy vormt een beveiligingslaag waarmee externe aanvallen afgevangen kunnen worden. De beveiliging van de overige lagen valt buiten het bereik van deze standaard.

Vertrouwelijke informatie is alleen beschikbaar voor geauthentiseerde gebruikers. Naarmate de vertrouwelijkheid van de informatie stijgt, dienen er zwaardere beveiligingsmaatregelen te worden getroffen, zie maatregelen.

ID	Maatregel	B	I	V	Opmerkingen
IBB-25_3.5-1	Websites van ProRail worden alleen publiekelijk beschikbaar gesteld door middel van een reverse-proxy in de externe *DMZ* (rood) waarbij de proxy minimaal controleert op juist protocol gebruik. Indien nodig kan er verdere inspectie plaatsvinden.	-	-	-	
IBB-25_3.5-2	Webinformatie wordt versleuteld getransporteerd over het publieke netwerk.			M	
IBB-25_3.5-3	Webinformatie is alleen beschikbaar voor sterk geauthentiseerde gebruikers (2-factor authenticatie).			H	Met hoge zekerheid moet vaststaan wie informatie opvraagt.
IBB-25_3.5-4	Outbound webverkeer wordt altijd ontsloten door middel van proxies, waarbij de proxy minimaal controleert op juist protocol gebruik.	-	-	-	Hiermee wordt de mogelijkheid gecreëerd om filtering toe te passen.

Tabel 6, Maatregelen irt publicatie van informatie

3.6 Datakoppeling over *publieke netwerken*

ProRail heeft vele datakoppelingen met *derde partijen* over zowel publieke- als *semi-publieke netwerken*. Het risicoprofiel voor een datakoppeling over het publieke netwerk is anders dan bij een datakoppeling met een *semi-publiek netwerk*. In de paragraaf 3.7 ‘Interconnectie’ worden de beveiligingsmaatregelen beschreven voor het koppelen met *semi-publieke netwerken*.

Een datakoppeling betreft een server-to-serverkoppeling zonder menselijke tussenkomst. Webservices betreft ook een server-to-serverkoppeling. Dit type koppeling wordt apart beschreven in paragraaf 3.8 vanwege de brede inzetmogelijkheden en de toekomstige ontwikkelingen.

Een datakoppeling over *publieke netwerken* betreft bijvoorbeeld DNS, e-mail en specifieke applicatiekoppelingen met eigen specifieke protocollen.

De risico’s bij datakoppeling over een publiek netwerk liggen vooral bij *inbound verkeersstromen.*

De aangeboden data is veelal onbekend en kan kwaadaardige code bevatten zoals virussen. Om het interne netwerk te beschermen tegen ongewenste data, wordt een inbound datakoppeling altijd applicatief ontkoppeld in de externe *DMZ*.
Daarnaast moet voorkomen worden dat een gecompromitteerd systeem in de externe *DMZ* een bedreiging vormt voor de overige systemen in het *DMZ*. Daarom dient elk systeem of groep systemen met dezelfde functie logisch gescheiden te zijn van elkaar. Private-Vlan technologie is een voorbeeld waarmee dit te bereiken is.

Bij *outbound verkeer* bestaat het risico dat een gecompromitteerd systeem in de *DMZ* oneigenlijke datakoppelingen opzet op initiatief van de hacker. Daarnaast moet worden voorkomen dat beheerders van systemen in de externe *DMZ* oneigenlijk datakoppelingen kunnen opzetten.

Bij overdracht van informatie met classificatie intern of hoger over een publiek netwerk is versleuteling van de verbinding noodzakelijk. Een versleuteling met AES256 of vergelijkbaar wordt daarbij vereist.

ID	Maatregel	B	I	V	Opmerkingen
IBB-25_3.6-1	End-to-end versleuteling over het toegangsnetwerk is niet toegestaan. Op gedefinieerde overgangen moet het verkeer gecontroleerd kunnen worden op kwaadaardige code.	-	-	-	Ontkoppeling is altijd nodig, ook al is de data versleuteld.
IBB-25_3.6-2	*Inbound verkeer* wordt altijd gecontroleerd op kwaadaardige code in het toegangsnetwerk.	-	-	-	Hieronder valt ook intrusion detection.
IBB-25_3.6-3	Waar beschikbaar wordt gebruik gemaakt van inherent veilige protocollen.	-	-	-	Geen ftp, maar sftp of SNMPv3 ipv SNMPv2.
IBB-25_3.6-4	Een inbound datakoppeling eindigt altijd in de externe *DMZ* (rood).	-	-	-	
IBB-25_3.6-5	Filtering is afgestemd op de doelstelling van de communicatie. Hierbij vindt controle plaats op protocol en richting van de communicatie. Firewalling van *inbound verkeer* is zo expliciet mogelijk gedefinieerd in de externe *DMZ*.	-	-	-	
IBB-25_3.6-6	Outbound datakoppelingen vanuit een *DMZ* naar een publiek netwerk worden beperkt tot de noodzakelijke protocollen.	-	-	-	
IBB-25_3.6-7	In de externe *DMZ* mag routering tussen inbound datakoppelingen niet mogelijk zijn.	-	-	-	
IBB-25_3.6-8	Een datakoppeling is versleuteld met minimaal AES256, of vergelijkbaar.			L	
IBB-25_3.6-9	Authenticatie van afzender is vereist bij *inbound verkeer* doormiddel van 2-factor authenticatie bij een gebruiker of met een digitaal certificaat in andere situaties.		M	M	

ID	Maatregel	B	I	V	Opmerkingen
IBB-25_3.6-10	Er wordt actief gecontroleerd op ongewenste patronen op basis van loginformatie.	L	L	L	Bijvoorbeeld SIEM.

Tabel 7, Datakoppeling over publieke netwerken

3.7 Interconnectie

ProRail heeft naast een koppeling met *publieke netwerken* (zoals Internet) ook koppelingen met extern *Besloten netwerken* of specifiek *derde partijen* over een eigen exclusieve dataverbinding. De partijen die achter de *semi-publieke netwerken* zitten zijn bekende partijen waar afspraken mee te maken zijn. Daarmee zijn de risico's minder groot dan bij *publieke netwerken*. Maar de partijen achter de *semi-publieke netwerken* vallen buiten de verantwoordelijkheid van ProRail ten aanzien van informatiebeveiliging. Daarom moet worden voorkomen dat beveiligingsproblemen bij *derde partijen* op het *semi-publieke netwerk*, van invloed kunnen zijn op ProRail.

De architectuur van het toegangsnetwerk heeft hierin al voorzien door de *semi-publieke netwerken* te koppelen over een apart *DMZ* (paars). In deze *DMZ* kunnen passende beveiligingsmaatregelen worden getroffen, in relatie tot het risicoprofiel van *semi-publieke netwerken*.

ID	Maatregel	B	I	V	Opmerkingen
IBB-25_3.7-1	Er dient altijd een contract of overeenkomst aanwezig te zijn met de externe partij met daarin de verantwoordelijkheden op het gebied van beveiliging.	-	-	-	Zonder contract of overeenkomst moet deze partij gezien worden als een publieke partij.
IBB-25_3.7-2	Een inbound datakoppeling vanuit een *semi-publiek netwerk* eindigt altijd in de externe *DMZ* (paars).	-	-	-	
IBB-25_3.7-3	Filtering is afgestemd op de doelstelling van de communicatie. Hierbij vindt controle plaats op protocol en richting van de communicatie. Firewalling van *inbound verkeer* is zo expliciet mogelijk gedefinieerd in de externe *DMZ*.	-	-	-	
IBB-25_3.7-4	*Inbound verkeer* wordt altijd gecontroleerd op kwaadaardige code in het toegangsnetwerk	-	-	-	
IBB-25_3.7-5	Outbound datakoppelingen vanuit een *DMZ* naar een *semi-publiek netwerk* worden beperkt tot de noodzakelijke protocollen.	-	-	-	
IBB-25_3.7-6	Routering tussen inbound datakoppelingen is niet mogelijk in de externe *DMZ*.	-	-	-	
IBB-25_3.7-7	Een datakoppeling is versleuteld met minimaal AES256, of vergelijkbaar.			M	

ID	Maatregel	B	I	V	Opmerkingen
IBB-25_3.7-8	Authenticatie van afzender is vereist bij *inbound verkeer* doormiddel van 2-factor authenticatie bij een gebruiker of met een digitaal certificaat in andere situaties.		M	M	
IBB-25_3.7-9	Authenticatie van afzender is vereist bij *inbound verkeer* doormiddel van een gebruikersnaam en wachtwoord.		L	L	

Tabel 8, Interconnectie

3.8 Enterprise Service-bus (ESB)

Webservices zijn bedoeld voor het uitwisselen van informatie op gestructureerde wijze. Hier ligt een Service Oriented Architecture aan ten grondslag. Systemen die informatie uitwisselen met elkaar zijn verbonden via een service-bus. Omdat het gebruik van webservices is gestandaardiseerd (XML), wordt deze vorm van connectiviteit steeds breder geadopteerd. Zo ook bij ProRail. Het toegangsnetwerk moet deze ontwikkeling ondersteunen, zodanig dat externe partijen optimaal en veilig kunnen koppelen met de service-bus van ProRail. De maatregelen in deze paragraaf zijn specifiek gericht op de koppeling die nodig is om externe partijen te verbinden met de service-bus van ProRail.

Het toegangsnetwerk voorziet in de connectiviteit tot de interne service-bus. De risico's die daarbij spelen zijn minimaal gelijk zoals beschreven in paragraaf 3.6 en 3.7. Webservices is, bekeken vanuit netwerkbeveiliging, niet anders dan webverkeer. Toch zijn er een aantal risico´s specifiek voor webservices waarvoor beveiligingsmaatregelen getroffen moeten worden.

Het risico bij webservices ligt vooral in de juistheid van de structuur van XML berichten en dat de payload niet bedreigend is voor de interne netwerken. Bij webservices wordt ook meer gebruik gemaakt van versleuteling van de payload. De versleuteling van de netwerkkoppeling is dan niet nodig. Ook authenticatie vindt bij webservices plaats op applicatief niveau. Bij authenticatie van webservices speelt het toegangsnetwerk minder een rol. Beveiliging verschuift bij webservices meer naar applicatief niveau en is het netwerk (toegangsnetwerk) meer een betrouwbare koppeling ten diensten aan de webservices.

Het toegangsnetwerk dient webservices te controleren op juiste structuur waarmee wordt voorkomen dat een onjuist XML bericht een bedreiging vormt voor de service-bus. Daarnaast dient het toegangnetwerk te voorzien in filtering op server-niveau. Alleen extern geautoriseerde servers worden door de firewall toegelaten op de externe *DMZ*. Versleuteling van berichten wordt bij voorkeur geregeld vanuit de webservice. Indien dit niet mogelijk is, of ongewenst is, dan wordt standaard versleuteling toegepast op de verbinding met SSL.

ID	Maatregel	B	I	V	Opmerkingen
IBB-25_3.8-1	XML verkeer wordt gecontroleerd op juiste syntax in de externe *DMZ* (rood en paars).		-		
IBB-25_3.8-2	*Two-sided SSL* wordt altijd toegepast om webservices met elkaar te verbinden.		-	-	

ID	Maatregel	B	I	V	Opmerkingen
IBB-25_3.8-3	In het externe *DMZ* worden alleen specifieke server-to-server verkeerstromen toegelaten. Onbekende servers kunnen geen XML berichten aanbieden.	-	-	-	Dit volgt automatisch na uitvoeren van maatregel IBB-5_3.8-2
IBB-25_3.8-4	Filtering is afgestemd op de doelstelling van de communicatie. Hierbij vindt controle plaats op protocol en richting van de communicatie. Firewalling van *inbound verkeer* is zo expliciet mogelijk gedefinieerd in de externe *DMZ*.	-	-	-	
IBB-25_3.8-5	Authenticatie op systeem niveau van afzender is vereist bij *inbound verkeer.*		**-**	**-**	

Tabel 9, Enterprise Service-bus