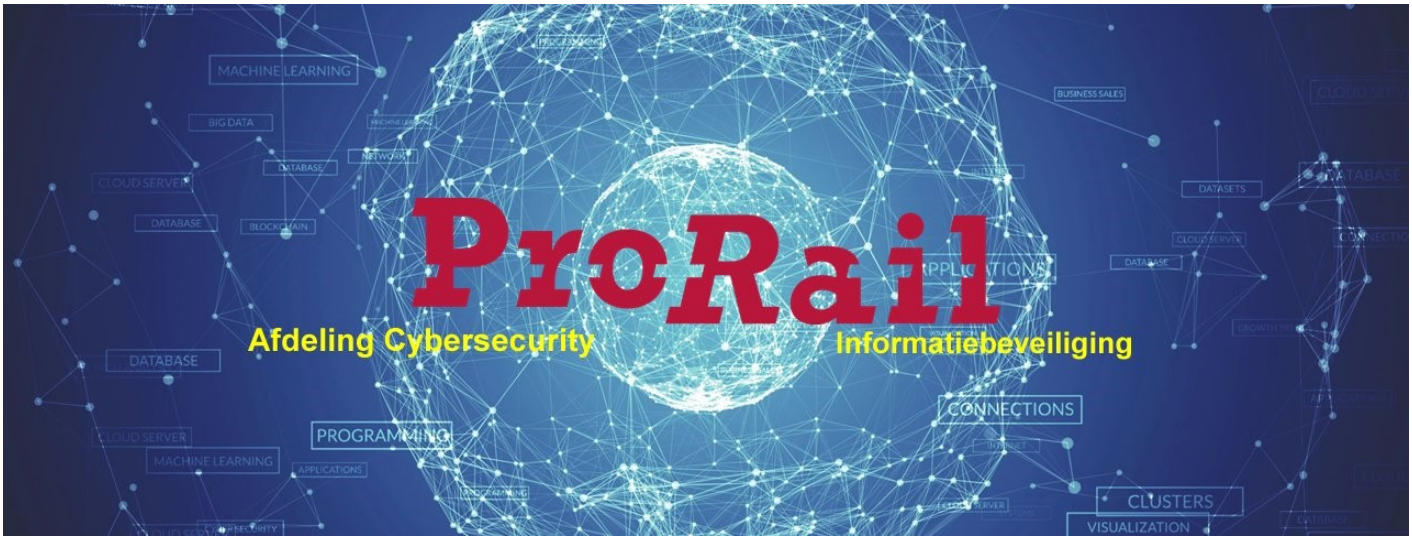
Informatiebeveiligingsbeleid

Eisen Informatiebeveiliging, aan leveranciers en onderaannemers van ProRail



Eigenaar	ExCo
Auteur	Afd. Cybersecurity
Reikwijdte	ProRail breed (incl. Leveranciers)
Kenmerk	IBB-1.6
Versie	1.2
Datum	Juli 2023
Bestand	IBB-1.6 Eisen Informatieveiligheid aan de Ondernemer 1.2.docx
Status	Definitief
Informatieclassificatie	Intern + Contractpartners

ProRail

Inhoudsopgave

Informatiebeveiligingsbeleid **1**
Inhoudsopgave **2**
1. Inleiding **2**
1.1 Doelstelling van dit document 2
2. Beveiligingsbeleid **2**
2.1 Organisatie van informatiebeveiliging bij levering/doorlevering van IT-, OT- of Clouddiensten 3
2.2 Beheer van opgeslagen informatie 3
2.3 Beheer van bedrijfsmiddelen 3
2.4 Beveiligingseisen t.a.v. personeel 3
2.5 Fysieke beveiliging en beveiliging van de omgeving 3
2.6 Beheer van communicatie- en bedieningsprocessen 3
2.7 Logische Toegangsbeveiliging 4
2.8 Ontwikkeling, Installatie en Onderhoud van IT- en OT-systemen 4
2.9 Beheer van informatiebeveiligingsincidenten 4
2.10 Naleving 4

1. Inleiding

De primaire processen van ProRail zijn zodanig afhankelijk van informatiesystemen dat uitval veelal leidt tot veiligheidsproblemen en verstoring van de treindienst met als gevolg imagoschade en grote (maatschappelijke) schade. ProRail stelt daarom doelstellingen ten aanzien van informatiebeveiliging waarmee de risico's verkleind worden.

ProRail wil daarom in control zijn over de beschikbaarheid (van processen, informatiesystemen, gegevens), integriteit en vertrouwelijkheid van gegevens, doordat ProRail een objectief beeld heeft van de risico's en zo kan kiezen voor de juiste balans tussen risico en maatregelen (kosten)'.

De Dienstverleners dienen in te stemmen met het recht van audit (op elk door ProRail gewenst moment) en te voldoen aan de aanvullende eisen die deze auditor stelt (o.a. m.b.t. rapportage).

Opmerkingen:

- Ondernemers (term Erkenninggsregeling) worden in dit stuk benoemd met de term "Dienstverlener".
- Daar waar dienstverleners wordt genoemd, geldt e.e.a. impliciet ook voor haar onderaannemers.
- Daar waar staat of wordt bedoeld 'informatiesystemen' betreft het bij ProRail àlle vormen van systemen (zoals administratief, technisch)

1.1 Doelstelling van dit document

De doelstelling van dit document is het vastleggen van de beveiligingseisen zoals gedefinieerd door ProRail, waaraan de gecontracteerde Dienstverleners moeten voldoen. De beveiligingseisen van ProRail zijn geformuleerd langs de kapstok van ISO27002. De beveiligingseisen zijn gebaseerd op een risicoanalyse. Deze risicoanalyse wordt periodiek geactualiseerd.
Op basis van deze actualisatie kunnen wijzigingen plaatsvinden in de eisen ten aanzien van informatiebeveiliging die gesteld worden door ProRail

2. Beveiligingsbeleid

- De gecontracteerde Dienstverlener dient te beschikken over een actueel, gedocumenteerd en door haar management geaccordeerde risicoanalyse, uitgevoerd voor de te leveren ICT-diensten. Bij deze risicoanalyse moeten de bedreigingen voor de bedrijfsmiddelen, kwetsbaarheden en de invloeden op de organisatie zijn vastgesteld en het bijbehorende risiconiveau te zijn bepaald.
- Het informatiebeveiligingsbeleid van ProRail is leidend. Op onderwerpen waar ProRail geen beleid heeft wordt overleg gepleegd.
- De Dienstverlener kan aansprakelijk gesteld worden voor de schade die voortvloeit uit "lekkage" van (vertrouwelijke) ProRail gerelateerde informatie die (door Dienstverlener gebruikte) systemen is opgeslagen.
- De websites, servers en databasesystemen met alle daarop opgeslagen informatie bevinden zich fysiek binnen de Europese Unie en deze mogen ook niet van uit een locatie buiten de EU toegankelijk zijn en/of bewerkt worden. Staten die zich aan de regelgeving van de EU verbonden hebben, zoals Zwitserland en Noorwegen, worden onder EU gerekend.
- De eisen in dit document zijn ook van toepassing op diensten die door de Dienstverlener worden ingekocht ten behoeve van de aan ProRail te leveren dienst.
  (Voorbeeld: Aannemers en Ontwerpbureaus gebruiken gezamenlijke tooling om een project te ondersteunen)
- De leverancier dient aan te geven hoe de data overgedragen wordt bij wisseling van leverancier.

2.1 Organisatie van informatiebeveiliging bij levering/doorlevering van IT-, OT- of Clouddiensten

- De dienstverlener, het datacentrum en de beheerprocessen moeten aan het niveau van de ISO 2700x normen-set voldoen. De Dienstverlener dient een vast aanspreekpunt voor informatiebeveiliging aan te wijzen.
- De dienstverlener dient inzicht te geven in haar welke derden mogelijk toegang kunnen hebben tot ProRail data. Denk aan hosting providers, software-leveranciers, support partijen, etc

2.2 Beheer van opgeslagen informatie

Opgeslagen informatie dient beveiligd te worden conform het veiligheidsniveau dat bij deze informatie is overeengekomen.
Dit betekent o.a. dat:

- ProRail een BIVP classificatie heeft uigevoerd en de Dienstverlener met passende beveiligingsmaatregelen komt, denk bij .vertrouwelijke informatie aan multi-factor authenticatie (is weten=logincredentials en iets bezitten=telefoon of token) en versleuteling van informatie en verbindingen.
- Persoon-gerelateerde informatie is per definitie minimaal vertrouwelijk. (Bij info over gezondheid: Geheim)

2.3 Beheer van bedrijfsmiddelen

- Alle ICT-componenten en –diensten, inclusief de onderlinge relaties en classificaties, worden vastgelegd en dit overzicht wordt permanent onderhouden door de Dienstverlener.
- De Dienstverlener draagt zorg voor het opstellen en actueel houden van de volgende documentatie, welke op verzoek aan ProRail kan worden overlegd:
  - Een lijst van contactpersonen;
  - Een lijst van ingezette beheerders, inclusief hun bevoegdheden en screening;
  - Een autorisatiematrix van de objecten (informatiesystemen) onder beheer;
  - Een lijst van objecten (informatiesystemen), inclusief merk, type, versie en (security) bijwerking (patches);
  - Een lijst van alle uitgegeven toegangstokens;
  - Een netwerk infrastructuur diagram;
  - Een lijst van firewall regels en instellingen;
  - Een lijst van alle ingaande/uitgaande (VPN) netwerkverbindingen en –protocollen.
  - Een lijst van door ProRail goedgekeurde uitsluitingen en uitzonderingen.

2.4 Beveiligingseisen t.a.v. personeel

- De gecontracteerde Dienstverlener moet zich inspannen om ervoor te zorgen dat medewerkers regelmatig op het belang van informatiebeveiliging worden gewezen (security awareness).
- De Dienstverlener is verantwoordelijk voor alle betrokken medewerkers, inclusief ingehuurde personen, met autorisatierechten op de ProRail Infrastructuur. Een Verklaring Omtrent Gedrag (VOG)[1] wordt sterk aanbevolen.
- Iedere medewerker van de gecontracteerde Dienstverlener, met toegang tot de IT-systemen van ProRail, krijgt bij aanvang schriftelijke informatie over het geldende informatiebeveiligingsbeleid.
- Iedere medewerker van de gecontracteerde Dienstverlener, met toegang tot de IT-systemen van ProRail, dient bij aanvang akkoord te gaan met de geheimhoudingsverklaring van ProRail.
- Toegangsrechten tot informatie van ProRail van medewerkers van de Dienstverlener die geen diensten verlenen aan ProRail worden per direct geblokkeerd.

2.5 Fysieke beveiliging en beveiliging van de omgeving

- In beheer zijnde apparatuur wordt in beveiligde ruimtes geplaatst. Deze beveiligde ruimtes zijn aantoonbaar alleen te benaderen door geautoriseerde personen.

2.6 Beheer van communicatie- en bedieningsprocessen

- Dienstverlener is verantwoordelijk voor het aanleveren van duidelijke instructies voor het gebruiken en onderhouden van de geleverde producten/diensten.
- Om de integriteit van programmatuur en gegevens te beschermen, zijn op alle systemen maatregelen genomen tegen kwaadaardige programmatuur e.d.
- Er dienen back-ups van informatie en programmatuur te worden gemaakt en regelmatig te worden getest overeenkomstig met het vastgestelde back-up en restore beleid.
  Verder kan ProRail er voor kiezen dat het exporteren van data moet mogelijk zijn.
- Gegevensuitwisselingen met netwerken van andere dienstverleners worden op een standaard- en beveiligde manier ingericht en onderhouden.
- Beheer-, test- en productieverkeer zijn van elkaar gescheiden.

[1] De onderneming zelf dient over een zg. ‘GedragVerklaring Aanbesteden (speciale-sectoropdrachten)’ te beschikken.

- De Dienstverlener heeft vast gehanteerde procedures voor het verwijderen van informatie van servers, werkplekken, back-ups etc, wanneer deze niet langer nodig zijn.
- Het gebruik/toegang en pogingen tot ongeautoriseerd gebruik/toegang van de ICT-middelen wordt geregistreerd. Deze registratie wordt op verzoek van ProRail, op een door ProRail te definiëren gangbare wijze beschikbaar gesteld.
- Activiteiten van gebruikers en beheerder dienen in het kader van audit trailing passend beveiligd in logbestanden vastgelegd te worden. Bijv bij een forensisch onderzoek na een cybersecurity incident.worden in logbestanden vastgelegd. Deze registratie wordt op verzoek van ProRail, op een door ProRail te definiëren wijze beschikbaar gesteld.
- Er is inzicht in sleutelbeheer. De leverancier dient aan te geven hoe het beheer van encryptiesleutels is ingericht.

2.7 Logische Toegangsbeveiliging

- De Dienstverlener volgt procedures voor het verlenen en intrekken van toegangsrechten van personeel tot systemen van ProRail. Toe te passen technologie hiervoor wordt in overleg met de ProRail architecten gekozen. Waar mogelijk doen gebruikers authentiseren via single-sign-on (SSO) tegen een ProRail (Azure) Active Directory.
- Periodiek wordt door ProRail een review uitgevoerd van de toegangsrechten van medewerkers van de gecontracteerde Dienstverlener (en de derden die de Dienstverlener inschakelt) voor de systemen bij ProRail en de Dienstverlener.
- Om toegang te krijgen tot systemen van ProRail wordt gebruik gemaakt van beveiligde verbindingen die beantwoorden aan ProRail beleid/architectuur.
- De toegang van medewerkers van de Dienstverlener is beperkt tot systemen bij ProRail, de Dienstverlener en afgenomen diensten bij Derden, die benodigd zijn voor het leveren van de dienst.
- Voor toegang op afstand tot systemen is goedkeuring van ProRail nodig. Toegang op afstand vindt altijd plaatst over beveiligde verbindingen én met twee-factor authenticatie (token).
- Toegang tot de systemen is beperkt met wachtwoorden conform de wachtwoordeisen zoals opgenomen in het informatiebeveiligingsbeleid van ProRail.
- Toegang kan alleen worden verkregen op basis van een persoonlijk gebruikersaccount. Algemene gebruikersaccounts zijn geblokkeerd.
- Voor de inrichting van servers en systemen zijn security baselines opgesteld die tijdens installatie, inrichting en/of configuratie worden toegepast.
  Minimaal jaarlijks wordt nagegaan of systeeminstellingen en beveiligingsparameters conform de geldende security baselines van ProRail zijn ingericht.
- Het is verplicht om beveiligingsadviezen (patches) van Leveranciers altijd zo spoedig mogelijk op te volgen, tenzij uitvoering van een dergelijk advies het goed functioneren van bedrijf kritische processen belemmert. Niet uitvoeren van kritische Patches op een ProRail gerelateerde omgeving dient altijd met ProRail overlegd te worden (ketenaansprakelijkheid).
- Er wordt zoveel mogelijk gebruik gemaakt van actuele versies van programmatuur die door de Dienstverlener ondersteund wordt.

2.8 Ontwikkeling, Installatie en Onderhoud van IT- en OT-systemen

- (Web) applicaties worden ontwikkeld en getest op basis van landelijke richtlijnen voor beveiliging, zoals de richtlijnen voor webapplicaties van het NCSC[2] ICT-Beveiligingsrichtlijnen voor webapplicaties.
- Er wordt tenminste getest op bekende kwetsbaarheden zoals vastgelegd in de OWASP[3] top10
- (Web) applicaties worden voor de in productie name ondermeer getest op invoer van gegevens (grenswaarden, format, inconsistentie, SQL-injectie, cross site scripting, etc.)

2.9 Beheer van informatiebeveiligingsincidenten

- Er dient een vaste procedure voor het melden van (fysieke en ICT) beveiligingsincidenten te zijn. Beveiligingsincidenten dienen onmiddellijk aan de contactpersoon van ProRail gerapporteerd te worden.

2.10 Naleving

- De Dienstverlener dient aantoonbaar in-controle te zijn over de maatregelen die getroffen worden om veel voorkomende aanvallen zoals (Distributed) Denial-of-Service-, brute force, buffer overflow, Cross-Site Scripting (XSS), SQL-injectie en andere aanvallen te voorkomen.
- Er wordt een regelmatig terugkerend overleg geagendeerd, tussen ProRail en de Dienstverlener, met als onderwerp cyber security, waarbij security gerelateerde zaken worden besproken.
- ProRail heeft de mogelijkheid om een onafhankelijk onderzoek uit te (laten) voeren naar de werking van de beveiligingsmaatregelen zoals getroffen door de gecontracteerde Dienstverlener.

[2] Nationaal Cyber Security Centrum
[3] Open Web Application Security Project