Annex 3A

Informatiebeveiligingseisen voor Leveranciers van Printapparatuur

Jurjan Rozema/Houssain Taibi
Afdeling Cybersecurity
14-03-2025

Dit document beschrijft de informatiebeveiligingseisen voor leveranciers van printapparatuur binnen ProRail. De eisen zijn gebaseerd op het document IPP-O.04 Informatiebeveiligingseisen aan leveranciersrelaties, dat als leidend kader geldt. De IT Baseline is niet opgenomen, aangezien de leverancier alleen verantwoordelijk is voor de levering, implementatie en het beheer van de printers. Brede IT-beveiligingseisen, zoals netwerkbeveiliging en infrastructuurbeheer, vallen onder de verantwoordelijkheid ProRail.

De leverancier moet zorgen voor een veilige configuratie en beheer van de printers. Dit omvat het instellen van beveiligde printprotocollen (zoals IPPS), toegangsbeveiliging via pasgebaseerd printen of multi-factor authenticatie en het beperken van ongeautoriseerde toegang. Daarnaast is de leverancier verantwoordelijk voor tijdige firmware-updates en patches, waarbij alleen digitaal gesigneerde updates worden geïnstalleerd. Ook moet logging en monitoring worden ingericht om beveiligingsincidenten te registreren en te rapporteren aan ProRail. De volgende eisen zijn van toepassing:

A. AVG
    a. Bij de verwerking van persoonsgegevens houdt de leverancier zich aan de eisen uit de Algemene Verordening Gegevensverwerking.
    b. Leveranciers dienen zich te conformeren aan de procedure Melding Datalekken van ProRail. Tijdlijnen, voorwaarden, contactpersonen, etc. worden opgenomen als onderdeel van de verwerkersovereenkomst.

B. Awareness
    a. De leverancier zorgt ervoor dat gedurende de uitvoering van het contract zijn medewerkers periodiek en aantoonbaar op het belang van informatiebeveiliging en hun rol daarin worden gewezen (security awareness).

C. Businesscontinuïteit n.v.t.

D. Certificeringen en normenkaders n.v.t.

E. Contactpersoon
    a. Zowel ProRail als de leverancier hebben een contactpersoon voor informatiebeveiligingsaspecten, vastgelegd in de SLA. Deze contactpersonen zijn adviserend en ondersteunend aan het contract- en leveranciersmanagementproces. Afstemming vindt altijd plaats onder regie van de contractmanager.

F. Escrow n.v.t.

G. Exit-strategie n.v.t.

H. Gegevensuitwisseling
    a. Digitale gegevensuitwisselingen vinden plaats conform een gestandaardiseerde en beveiligde manier, nader af te spreken.

I. Gegevensverwerking en -opslag
    a. De leverancier maakt alleen gebruik van de verstrekte en gegenereerde gegevens voor het uitvoeren van de gecontracteerde werkzaamheden.
    b. De websites, servers en databasesystemen met alle daarop opgeslagen informatie bevinden zich fysiek binnen de Europese Economische Ruimte (EER) en mogen alleen vanuit een locatie buiten de EER toegankelijk zijn en/of bewerkt worden vanaf een beveiligd ProRail werkstation waarbij lokale opslag niet mogelijk is en een beveiligde verbinding en multi-factor authenticatie gebruikt wordt. De data mogen de EER niet verlaten.
    c. Geheimhouding n.v.t.

J. Incidenten
    a. Er wordt een vaste procedure voor het melden van (IT) beveiligingsincidenten en kwetsbaarheden afgesproken tussen ProRail en de leverancier. Deze dient aan te sluiten bij de bestaande incidentmanagementprocessen binnen Prorail. En wordt vastgelegd in een DAP binnen 6 weken na start van de Implementatiefase.
    b. De leverancier meldt (beveiligings-)incidenten en kwetsbaarheden direct aan ProRail, en als dat wettelijk noodzakelijk is, ook aan de Autoriteit Persoonsgegevens. Bij niet-gemelde incidenten waar persoonsgegevens bij betrokken zijn, kan ProRail de leverancier in gebreke stellen.
    c. De leverancier geeft (beveiligings-)incidenten volgens gemaakte afspraken opvolging en rapporteert daarover aan ProRail.

K. Monitoring en loganalyse

    a. Activiteiten van beheerders dienen ten behoeve van audittrailing vastgelegd te worden in logboeken en herleidbaar tot een persoon. Deze registratie wordt op verzoek van ProRail door de leverancier op een door ProRail te definiëren wijze beschikbaar gesteld.

L. Onderaanneming en toeleveranciers
    a. Alle voorwaarden en eisen op het gebied van informatiebeveiliging die gelden voor personeel van de leverancier zijn ook van toepassing op derden, die in opdracht van de leverancier diensten verrichten voor ProRail.
    b. De leverancier moet desgevraagd inzage geven in de maatregelen die hij genomen heeft om de aan hem opgelegde eisen ook door te vertalen naar derden.
    c. Het is de leverancier niet toegestaan, zonder voorafgaande uitdrukkelijke schriftelijke toestemming van ProRail, de uitvoering van een contract geheel of gedeeltelijk aan derden over te dragen of uit te besteden. Deze toestemming zal niet op onredelijke gronden geweigerd worden.
    d. ProRail wordt zo snel mogelijk op de hoogte gebracht indien de leverancier wijzigingen aanbrengt bij het uitbesteden van zijn eigen (deel)processen. Hierdoor kan ProRail bepalen of er zwaarwegende risico's bestaan (bv. uitbesteding aan onveilige landen) en tevens inzicht verkrijgen in de wijze van beheersing van de door de leverancier uitbestede (deel)

processen. Deze inzet, beheersing en wijziging van sub verwerking wordt opgenomen in de overeenkomst met de leverancier.

M. Personeel n.v.t.

N. Retour/vernietiging bedrijfsmiddelen en informatie n.v.t.

O. Auditrecht
   a. ProRail kan op enig moment een audit, waaronder een penetratietest, (laten) uitvoeren om te controleren dat aan beveiligingseisen die van toepassing zijn wordt voldaan.

P. Security by Design
   a. De gangbare principes rondom Security by Design/Default zijn uitgangspunt voor de ontwikkeling van software en systemen. Over wat dit concreet binnen de opdracht inhoudt worden afspraken gemaakt tussen ProRail en de leverancier.
   b. De leverancier dient ervoor te zorgen dat de printapparatuur en bijbehorende systemen gedurende de gehele levenscyclus beveiligd zijn tegen malware, ongeautoriseerde toegang en andere cyberdreigingen. De firmware en software dient altijd up to date te zijn.

Q. Security testing n.v.t.

R. Toegang tot digitale infrastructuur en gegevens

   a. Er wordt een gedocumenteerde formele en actuele procedure afgesproken en vastgelegd in een DAP (binnen 6 weken na de start van de implementatiefase) voor het registreren, verlenen, wijzigen en intrekken van logische toegang tot IT-systemen. Deze procedure wordt periodiek (minimaal eens per jaar) beoordeeld en geactualiseerd.
   b. De toegang van medewerkers van de leverancier is beperkt tot systemen bij ProRail, de leverancier en afgenomen diensten bij derden, die benodigd zijn voor het leveren van de dienst (need to know principe).V. Toegang tot fysieke infrastuctuur
   c. Alle toegangsmiddelen (waaronder sleutels, pasjes, tokens) mogen uitsluitend worden gebruikt voor het doel waarvoor deze beschikbaar zijn gesteld en niet worden gedeeld met anderen.