Vraagspecificaties Cybersecurity OT

VS1- en VSP-eisen bij de inkoop/aanbesteding van OT-Systemen ter invulling van de digitale beveiliging.

Versie: 1.1

Vertrouwelijkheidsniveau: Bedrijfsvertrouwelijk

GVB Door en door Amsterdam

Colofon

Versiebeheer en status

28 september 2022, Versie 1.1, In hoofdstuk 4 zijn de eisen uit hoofdstuk 2 en 3 in één set beschrevem, waarbij de proceseisen en systeemeisen zijn samengenomen. Een project kan - afhankelijk van de manier waarop het project het bestek heeft opgesteld - beide formaten gebruiken: of de opgeslitste eisen (hoofdstuk 2 en 3) of de gecombineerde eisen (hoofdstuk 4).
23 juni 2022, Versie 1.0, De tekst in dit document is samengesteld aan de hand een eerder concrete aanbesteding van een OT-systeem en is opgesteld in samenwerking met het betrokken project door Wim van Asperen, Cybersecurity Officer OT.

Contactpersoon	Cybersecurity-officer OT, Wim van Asperen
Doorkiesnummer	0621854536
Faxnummer	

Inhoudsopgave

1 Inleiding

In dit document zijn de eisen gegeven voor cybersecurity voor OT in het kader van een aanbesteding c.q. opdrachtverlening voor het ontwerpen, realiseren, implementeren, overdragen en (laten) beheren van een OT-systeem en als onderdeel van een totale vraagspecificatie c.q. het programma van eisen.

> NB1. In hoofdstuk 2 en 3 zijn de cybersecurity gesplitst in respectievelijk de Proceseisen (VS2, of VSP) en de Systeemeisen (technisch, VS1), zodat een project bij de aanbesteding deze teksten kan integreren in de totale vraagspecificatie c.q. het programma van eisen.
>
> NB2. In hoofdstuk 4 zijn de cybersecurity-eisen als geheel gegeven en kunnen worden overgenomen voor een aanbesteding waarbij geen onderscheid wordt gemaakt tussen de proces- en systeem-eisen.
>
> Inhoudelijk zijn hoofdstuk 2 en 3 enerzijds en hoofdstuk 4 anderzijds identiek. De keuze voor het al of niet splitsen van proces- en systeemeisen is aan het projectteam.
>
> N.B. Lees eerst het Cybersecurity-voorschrift OT, zie de cybersecurity-documenten voor OT downloaden het van het intranet…
> *https://gvb939.sharepoint.com/organisatie/algemeen/informatiebeveiliging/Paginas/Cybersecurity%20OT.aspx*

Vooraf (!) aan de aanbesteding dient vastgesteld te worden of cybersecurity van toepassing is (ofwel is software in enige vorm een onderdeel van de beoogde oplossing) en zo ja dan geeft de opdrachtgever (Beheerder c.q. de Asset owner) de opdracht aan het projectmanagement om een projectcybersecurity-officer aan te wijzen en hem/haar de volgende initiële activiteiten te laten uitvoeren.

1. Uitvoeren van initiële cyberrisico-analyse voor het beoogde systeem in de beoogde operationele omgeving, ter indicatie voor de aandachtspunten in de aanpak en ter indicatie en vaststelling van specifieke cyber hazards.
2. Vaststellen van de operationele doelstellingen (kpi's) voor de doelomgeving voor fysieke veiligheid, beschikbaarheid en privacy (bedrijfswaarden)
3. Vaststellen van de vigerende kaders (wet- en regelgeving).
4. Invullen van een (eerste versie van het) cybersecurity-dossier met bovenstaande vaststellingen.
5. Opnemen van cybersecurity-eisen in de vraagspecificaties van het project.

De projectcybersecurity-officer faciliteert de projectmanager met expertise en capaciteit voor alle cybersecurity-activiteiten in het project. projectcybersecurity-officer rapporteert over de uitvoering in het project aan de Cybersecurity-officer OT. Omgekeerd helpt de Cybersecurity-officer OT de projectcybersecurity-officer bij de projectuitvoering.

De projectmanager integreert cybersecurity als systeemaspect in de projectaanpak (organisatie, financiën en activiteiten), als een (RAMSHEEP) 'systeemaspect'. Cybersecurity is dan dus ook een natuurlijk aandachtspunt in de systeemintegratie, configuratie- en wijzigingsmanagement en alle verificatie- & validiatie-activiteiten.

Cybersecurity-officer OT zal een onafhankelijke pen-testen organiseren net vooraf aan de inbedrijfsstelling en ter validatie van de cybersecurity van het systeem.

De kosten voor de cybersecurity worden expliciet opgenomen in de projectbegroting. Na de initiële stappen kan de schatting worden gemaakt voor de inbreng van de (rol) van project CS-manager en de kosten van de technische en organisatorische maatregelen tijdens het project (en daarna). Als vuistregel kan ca 10% van de totale software-kosten (eenmalig en jaarlijks) voor cybersecurity worden opgenomen in het project- en beheerbudget.

Het cybersecurity-dossier wordt tijdens de projectuitvoering aangevuld en gecompleteerd vooraf aan de overdracht naar het assetmanagement - als formeel overdrachtsstuk. Het cybersecurity-dossier vormt de handleiding voor het assetmanagement voor het beheren van de cybersecurity van het systeem, inclusief de aandacht voor de cybersecurity-processen en voorzieningen voor gebruikers en beheerders.

2 Proceseisen (VS2- of VSP-eisen)

Hieronder zijn de proceseisen gegeven die dienen te worden geïntegreerd in een programma van eisen in het kader van inkoop/aanbesteding van een OT-Systeem.

Bindende documenten

#Uitleg: De documenten op de intranet-pagina 'Cybersecurity OT' zijn alle bindende documenten.
#Neem-over: De actuele/vigerende documenten vind je op het intranet:
https://gvb939.sharepoint.com/organisatie/algemeen/informatiebeveiliging/Paginas/Cybersecurity%20OT.aspx

Cybersecuritymanagement

#Uitleg: Cybersecuritymanagement is (naast aspecten zoals risicomanagement, configuratiemanagement, financieel management, etc) een onderdeel van Projectbeheersing. Voeg daarom 'Cybersecuritymanagement' toe aan het hoofdstuk Projectbeheersing in het programma van eisen en neem de tekst hieronder over in de betrokken paragrafen.

H.n.m. Doelstelling Cybersecuritymanagement
#Neem-over: *Het doel van cybersecuritymanagement is om de operationele veiligheid, beschikbaarheid en privacy van alle stakeholders van de metro- en tramoperatie te borgen door de invloed van risico's van cyberaanvallen en cyberbesmettingen op de systemen te mitigeren.*

H.n.m. Werkzaamheden Cybersecuritymanagement
#Neem-over:
- Aanstellen van een projectcybersecurity-officer (van ON)
- Samenwerken met projectcybersecurity-officer van OG
- Opstellen van cybersecuritymanagementplan (inclusief V&V en risicomanagement voor CS) voor alle project- en beheerfase
- Uitvoeren van cyberrisico-analyses
- Ontwerpen, realiseren en implementeren van cybersecurity-maatregelen

H.n.m. Eisen en producten cybersecuritymanagement
#Neem-over:
VSP-eis-code..# Aanstellen van een projectcybersecurity-officer
Opdrachtnemer dient een projectcybersecurity-officer aan te stellen als primair contactpersoon voor (in het bijzonder) de projectcybersecurity-officer van Opdrachtgever

VSP-eis-code..# Opstellen van cybersecuritymanagementplan
De Opdrachtnemer dient een cybersecuritymanagementplan op te stellen op basis van hetgeen gesteld in het Cybersecurity-voorschrift OT (#Geef-ref #…) en de cybersecurity-eisen OT (#Geef-ref #…) en laat dit plan goedkeuren door Opdrachtgever alvorens aan het project mag worden begonnen. Het cybersecuritymanagementplan dient ook de V&V te beschrijven voor de cybersecurity gedurende alle fase van de Werkzaamheden en bevat alle formele momenten van goedkeuring door de Opdrachtgever.

VSP-eis-code..# Ontwerpen, realiseren en implementeren van CS-maatregelen

Opdrachtgever dient cybersecurity-maatregelen te ontwerpen, realiseren en implementeren gericht op de borging van de door Opdrachtgever gestelde operationele doelstellingen voor veiligheid, beschikbaarheid en privacy op basis van de cybersecurity-eisen OT (#Geef-ref #…).
Opmerking. De operationele doelstellingen voor veiligheid, beschikbaarheid en privacy worden door de Opdrachtgever ter beschikking gesteld.
Opmerking. Comply-or-explain. Er mag worden afgeweken van de Cybersecurity-eisen OT op basis van een schriftelijke door de Opdrachtgever goedgekeurde cyberrisico-analyse en een goedgekeurd voorstel voor alternatieve maatregelen.
Opmerking. De Cybersecurity-eisen OT zijn gebaseerd op weerstandsniveau-4 van de CSIR (CyberSecurity-Implementatie-Richtlijn) van Rijkswaterstaat en aangevuld met enkele specifieke maatregelen van Opdrachtgever.

VSP-eis-code..# Cyberrisicomanagementaanpak
Opdrachtnemer dient cyberrisicoanalyses uit te voeren ter onderbouwing van het afwijken van de Cybersecurity-eisen OT. Opdrachtnemer dient de cyberrisicoanalyses uit te voeren aan de hand van de Cyberrisicomanagementaanpak van Opdrachtgever (#Geef-ref #..) Deze cyberrisicoanalyses dienen expliciet door Opdrachtgever te worden goedgekeurd.
Opmerking. Het Cyberdreigingsbeeld OT (#Geef-ref #..) dient mede te worden gebruikt als input voor de risico-analyses en wordt door de Opdrachtgever ter beschikking gesteld na gunning van de opdracht (i.v.m. de vertrouwelijkheid ervan).

3 Technische eisen (VS1 of Systeemspecificatie)

Hieronder zijn de technisch- of systeemeisen gegeven die dienen te worden geïntegreerd in het programma van eisen in het kader van inkoop/aanbesteding van een OT-Systeem.

Cybersecurity is (naast functionele en realisatie-eisen) een ‘Aspecteis’ net als Betrouwbaarheid, Beschikbaarheid, Onderhoudhoudbaarheid en Veiligheid.

Neem op bij ‘definitie van eisen’ over Cybersecurity op:
‘Eisen met betrekking tot de weerbaarheid van het betrokken Systeem tegen cyberaanvallen en cyberbesmettingen.’

Referenties/bronnen:
Neem de referenties over uit het document Referenties en bronnen voor Cybersecurity OT.

Aspecteis:
Cybersecurity
Eis-code:
#... (projectafhankelijk)
Tekst:
Het betrokken systeem dient beveiligd te zijn tegen cyberaanvallen en cyberbesmettingen. Voor het betrokken systeem dienen minstens de maatregelen te zijn/worden getroffen zoals beschreven in het document Cybersecurity-Eisen OT. Herstelwerkzaamheden naar

aanleiding van de pen-test (zoals genoemd bij Verificatiemethode) zijn een verantwoordelijkheid van ON.

Toelichting:

In het document Proceseisen (VS2 of VSP) is beschreven hoe cybersecurity door de Opdrachtnemer dient te worden ingebed in de projectwerkzaamheden.

Verificatiemethode:

Aan de hand van het door OG goedgekeurde V&V-plan. Door OG wordt vooraf aan de acceptatie een pen-test uitgevoerd, ter validatie van de ingerichte en geïmplementeerde maatregelen.

Voorschrift/Normen:

Cybersecurity-Eisenset OT aangevuld met Cybersecurity-voorschrift OT.

4 Cybersecurity-eisen

Cybersecurity-eisen zijn systeem- en proces-eisen met betrekking tot de weerbaarheid van het betrokken systeem tegen cyberaanvallen en cyberbesmettingen.

Het doel van cybersecuritymanagement is om de operationele veiligheid, beschikbaarheid en privacy van alle stakeholders van de OV-operatie te borgen door de invloed van risico's van cyberaanvallen en cyberbesmettingen op de systemen te mitigeren.

Cybersecuritymanagement is (naast aspecten als risicomanagement, configuratiemanagement, financieel management, etc) een natuurlijk onderdeel van projectbeheersing.

In het kort betekent cybersecuritymanagement voor een project en voor Opdrachtnemer (ON) het volgende:
- Het aanstellen van een projectcybersecurity-officer door en van ON
- Het samenwerken met projectcybersecurity-officer van Opdrachtgever (OG)
- Opstellen van cybersecuritymanagementplan (inclusief de V&V voor cybersecurity) voor alle projectfasen én tot en met de beheerfase na het project.
- Uitvoeren van cyberrisico-analyses, indien wordt afgeweken van de eisen-set en standaard maatregelen
- Ontwerpen, realiseren en implementeren van technische en organisatorische cybersecurity-maatregelen.

Bindende/vigerende bijlagen
De bijlagen die vigerend zijn voor dit project en een onderdeel vormen van de cybersecurity-eisen per 28 september 2022, zijn de volgende:
CS-1 Cybersecurity-voorschrift OT Versie 1.7 Bedrijfsvertrouwelijk
CS-2 Cybersecurity-eisen-maatregelen voor OT Versie 1.3 Bedrijfsvertrouwelijk
CS-3 Vraagspecificaties Cybersecurity voor OT Versie 1.1 Bedrijfsvertrouwelijk
CS-4 Cybersecuritydossiersjabloon OT Versie 28 juni 2022 Bedrijfsvertrouwelijk
CS-5 Vertrouwelijkheid OT Versie 2.1 Bedrijfsvertrouwelijk
CS-6 Cyberincidentprocedure OT Versie 1.3 Bedrijfsvertrouwelijk
CS-7 Wachtwoordenbeleid OT Versie 2.11 Bedrijfsvertrouwelijk
CS-8 Hardeningvoorschrift OT Versie 0.2 Bedrijfsvertrouwelijk
CS-9 Aansluitvoorwaarden NMA-netwerk Versie 1.0 Vertrouwelijk *)
CS-10 Cyberrisicomanagement OT Versie 1.2 Bedrijfsvertrouwelijk
CS-10.1 Cyberdreigingsbeeld OT Versie 28 juni 2022 Vertrouwelijk *)
CS-10.2 Cybersecurity KPI-s OT Versie 1.1 Bedrijfsvertrouwelijk
CS-11 Cybersecurity beleid buitenlandse devices, versie 28mrt22, Bedrijfsvertrouwelijk
*) wachtwoord wordt separaat onder geheimhouding verstrekt door OG

Eis-CS-1 Cybersecurity
Het betrokken systeem dient beveiligd te zijn tegen cyberaanvallen en cyberbesmettingen. Voor het betrokken systeem dienen minstens de maatregelen te zijn getroffen zoals beschreven in het document Cybersecurity-eisen-maatregelen voor OT (CS-2).

Eis-CS-1.1 Verificatiemethode: Aan de hand van het door ON opgestelde en door OG goedgekeurde Projectcybersecuritymanagementplan (inclusief de verificatie en validatie).
Eis-CS-1.2 Validatiemethode: Door OG zal vooraf aan de acceptatie van het project een pen-test laten uitvoeren, ter validatie van de ingerichte en geïmplementeerde maatregelen. Eventuele herstelwerkzaamheden naar aanleiding van de pen-test zijn een verantwoordelijkheid van ON en dienen vooraf aan de acceptatie van het project te zijn uitgevoerd.
Eis-CS-1.3 Voorschrift/Normen: Cybersecurity-eisen-maatregelen voor OT (CS-2) aangevuld met Cybersecurity-voorschrift OT (CS-1).

Eis-CS-1: Aanstellen van een projectcybersecurity-officer
Opdrachtnemer dient een projectcybersecurity-officer aan te stellen om de projectcybersecurity-aspecten te behartigen, om de gestelde cybersecurity-eisen in te vullen en om als primair contactpersoon te fungeren voor (in het bijzonder) de projectcybersecurity-officer van OG.

Eis-CS-2: Opstellen van cybersecuritymanagementplan
De Opdrachtnemer dient een projectcybersecuritymanagementplan op te stellen op basis van hetgeen gesteld in het Cybersecurity-voorschrift OT (CS-1) en de Cybersecurity-eisen-maatregelen voor OT (CS-2) en laat dit plan goedkeuren door Opdrachtgever alvorens aan de ontwerpfase mag worden begonnen. Het projectcybersecuritymanagementplan dient ook de verificatie en validatie (V&V-plan) te beschrijven voor de cybersecurity gedurende alle fase van de Werkzaamheden en bevat alle formele momenten van goedkeuring door de Opdrachtgever.

Eis-CS-2: Ontwerpen, realiseren en implementeren
Opdrachtgever dient alle cybersecuritymaatregelen te ontwerpen, realiseren en implementeren zoals gegeven in Cybersecurity-eisen-maatregelen voor OT (CS-2). De maatregelen zijn gericht op de borging van de door Opdrachtgever gestelde/geeiste operationele doelstellingen voor Beschikbaarheid.

Eis-CS-4: Comply-or-explain
Er mag worden afgeweken van de Cybersecurity-eisen-maatregelen voor OT (CS-2) op basis van een schriftelijke door de Opdrachtgever goedgekeurde cyberrisico-analyse en een goedgekeurd voorstel voor alternatieve maatregelen. ON kan gebruik maken van de Cyberrisicomanagementaanpak (CS-10) van Opdrachtgever. De cyberrisicoanalyses en alternatieve maatregelen dienen expliciet door Opdrachtgever te worden goedgekeurd alvorens een volgende projectfase mag worden gestart. Het Cyberdreigingsbeeld OT (CS-10.1) dient mede te worden gebruikt als input voor de risico-analyses en wordt door de OG ter beschikking gesteld na gunning van de opdracht (i.v.m. de vertrouwelijkheid ervan).