

Scope Diensten voor Cyber Security van IA

Raamovereenkomst Dienstverlening Industriële Automatisering:

N.B. In dit document wordt, om de taal, zoals gebruikt in de eisen en criteria nader te duiden, gebruik gemaakt van het procesoverzicht van Fasen en Documenten zoals dit volgens Systems Engineering in RWS-projecten vaak wordt gehanteerd (zgn. V-model).

1.1.1 Terminologie

Diensten voor Cyber Security van IA

Cyber Security van een IA-keten betreft de eigenschappen van de IA-keten en/of een IA-systeem als geheel. Het cyber secure maken van een IA-keten of systeem betreft het preventief en (re)actief voorkomen en beperken van gevaar of schade¹ veroorzaakt door verstoring, uitval of misbruik van (delen) van de IA-keten of systeem en de hiermee verbonden ICT in de omgeving. Als een IA-keten of systeem cyber secure is, biedt het de gebruiker van de IA-keten of systeem digitale veiligheid en beschermt het tegen aanvallen, manipulatie en/of geweld door onbevoegden die zichzelf toegang (fysiek, ofwel digitaal) willen verschaffen tot beveiligde ruimten en informatievoorziening.

Diensten voor Cyber Security van IA betreffen specialistische diensten die gericht zijn op het (adviseren over) ontwerpen, realiseren, verifiëren, valideren, testen, monitoren, onderhouden, aanpassen en bedienen van IA-ketens met als doel dat deze ketens de eigenschap 'cyber secure' krijgen of houden.

1.1.2 Perceel 3 Diensten voor Cyber Security van IA

Dit perceel omvat de in de paragraaf 1.1.1 gedefinieerde diensten voor Cyber Security van IA. Het gaat hierbij veelal om activiteiten ter voorkoming, detectie en afhandelen van cyber security gerelateerde incidenten. Hierbij moet men denken aan het opstellen en toepassen van cyber security kaders, het beoordelen van ontwerpdocumenten, het beoordelen van cyber security beveiligingsplannen, penetratietesten, malware onderzoek, kwetsbaarheidsanalyses, analyses en rapportage over dreigingen en onderzoek na incidenten. De door RWS gehanteerde cyber security kaders omvatten de securityaspecten voor proces, mens, organisatie en techniek. Tevens omvat het perceel diensten betreffende algemene advisering en ondersteuning over Cyber Security van IA-ketens en systemen en de hiermee verbonden ICT in de omgeving binnen RWS.

Veelal worden binnen de Diensten voor Cyber Security van IA de volgende categorieën onderscheiden:

- Cyber Security advisering;
 - o Deze categorie betreft specifieke diensten voor het beoordelen van Cyber Security van IA, waaronder analyses en rapportage over bedreigingen. Tevens omvat het diensten betreffende algemene advisering rond en ondersteuning van activiteiten om IA-ketens en systemen cyber secure te maken of houden, o.a. binnen de aanleg- en onderhoudsprojecten van RWS. De Cyber Security wordt hierbij gezien vanuit de volle lifecycle en vanuit het proces, de organisatie en de techniek. Het gaat daarbij onder andere om het toepassen en vertalen van de Cyber Security kaders en richtlijnen binnen de IA in projecten voor de natte en droge objecten van RWS. Verder zijn de activiteiten gericht op het ondersteunen van de projectorganisaties door het adviseren van projecten over de toe te passen Cyber Security kaders, het toetsen van de vertaling van de securitykaders binnen ontwerpen en het testen van de beveiliging van het ontwerp en ondersteunen van projecten bij operationele vragen. Ook het adviseren over en toetsen van de organisatorische en procesmatige maatregelen maken hier onderdeel van uit.

¹ Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT/IA, schending van de vertrouwelijkheid van de ICT/IA opgeslagen informatie of schade aan de integriteit van die informatie.

- Kwetsbaarheidsanalyse van IA-ketens op Cyber Security;
 - o Deze activiteiten omvatten het uitvoeren van of ondersteunen bij kwetsbaarheidsanalyse van de IA-ketens op de eigenschap Cyber Security. Dit betreft zowel documentstudies als fysieke controles, bijvoorbeeld door:
 - Het uitvoeren van kwetsbaarheidsscans, penetratietesten, malware onderzoek;
 - Het testen van de verschillende Cyber Security beveiligingsmaatregelen;
 - Het testen van de Cyber Security bewustwording bij gebruikers en beheerders.
- Diensten in geval van een hack en/of sabotage.
 - o Het betreft activiteiten en onderzoeken als onderdeel van het incident-response proces. Deze dienst wordt afgeroepen indien RWS een vermoeden heeft van een hack of sabotage of poging daartoe. Het gaat hierbij om:
 - Het onderzoeken of er daadwerkelijk sprake is van een hack of sabotage;
 - Het ondersteunen bij het stoppen van de hack of sabotage;
 - Het ondersteunen bij het voorkomen of beperken van de gevolgschade;
 - Het uitvoeren van een forensisch onderzoek, waarbij ook het verkrijgen en vastleggen van de bewijslast.

1.1.3 *Werkzaamheden behorende bij perceel 3 Diensten voor Cyber Security van IA (niet uitputtend)*

Dit perceel omvat specialistische activiteiten op het gebied van Cyber Security binnen omgevingen waarin IA en SCADA systemen worden toegepast.

Het gaat hierbij om activiteiten ter voorkoming, detectie en afhandelen van Cyber Security gerelateerde incidenten. Hierbij moet men denken aan het opstellen en toepassen van Cyber Security kaders, het beoordelen van ontwerpdocumenten, het beoordelen van Cyber Security beveiligingsplannen, penetratietesten, malware onderzoek, kwetsbaarheidsanalyses, analyses en rapportage over dreigingen, onderzoek na incidenten. De door Rijkswaterstaat gehanteerde Cyber Security kaders omvatten de securityaspecten voor proces, mens, organisatie en techniek. Tevens omvat het diensten betreffende algemene advisering en ondersteuning over Cyber Security van IA en SCADA omgevingen van Rijkswaterstaat. Dit perceel is in de volgende drie subcategorieën verdeeld:

- CS-IA advisering;
- Kwetsbaarheidsanalyse van IA ketens op Cyber Security;
- Diensten in geval van een hack en/of sabotage.

Alle activiteiten vinden onder de regie van Rijkswaterstaat plaats.

Elke activiteit wordt afgerond met een deugdelijk en helder rapport/document conform de in een Nadere Overeenkomst aangegeven eisen. In het geval van een toets en/of een test wordt dit vooraf gegaan door een respectievelijk toetsplan of testplan. Daarnaast kan er worden gevraagd om een plan van aanpak en/of projectplan vooraf ter acceptatie aan te leveren.

1.1.3.1. *IA Cyber Security advisering*

Dit zijn activiteiten die gericht zijn op het ondersteunen van de aanleg- en onderhoudsprojecten op het gebied van CS-IA, gezien vanuit de volle lifecycle en vanuit het proces, de organisatie en de techniek. Het gaat daarbij onder andere om het toepassen en vertalen van de Cyber Security kaders en richtlijnen binnen de IA voor de natte en droge objecten van Rijkswaterstaat.

Verder zijn de activiteiten gericht op het ondersteunen van de projectorganisaties door het adviseren van projecten over de toe te passen Cyber Security kaders, het toetsen van de vertaling van de securitykaders binnen ontwerpen en het testen van de beveiliging van het ontwerp en ondersteunen van projecten bij operationele vragen. Ook het adviseren over en toetsen van de organisatorische en procesmatige maatregelen maken hier onderdeel van uit.

De activiteiten volgen het proces van systems engineering volgens het V-model, JSTD-016 en MIL-STD-498, met inachtneming van de onderstaande fasen. Hierbij zijn de genoemde activiteiten niet gelimiteerd tot de desbetreffende fase:

Fase: Algemeen en contractvoorbereiding

- Begeleiden en informeren van de projectorganisatie over de Rijkswaterstaat Cyber Security methodiek met als doel Cyber Security awareness te creëren;
- Het opstellen van en het adviseren over Cyber Security eisen en kaders in de verschillende modelcontracten voor natte en droge objecten waarbij rekening gehouden moet worden

- met het Systems Engineeringsmethodiek en de UAV-GC inkoopvoorwaarden;
- Het uitvoeren van risicoanalyses en het maken van afwegingen om tot de juiste set van Cyber Security requirements te komen;
- Het ondersteunen van de projectorganisaties bij de vertaling van Cyber Security requirements naar contracteisen voor IA;
- Het adviseren en bewaken van de integraliteit, samenhang, risico's en beheersing van het Cyber Security inhoudelijk deel van een object in een project;
- Het adviseren over en ondersteunen van Contract Beheersing op Cyber Security inhoudelijke aspecten tijdens de contractvoorbereiding.

Fase: Ontwerp

- Het adviseren over het toepassen van de kaders binnen de diverse fases van het systems engineering proces;
- Het adviseren in en ondersteunen op Cyber Security inhoudelijke aspecten tijdens de ontwerpfase;
- Het adviseren en beoordelen van de iteratieve opbouw van het Cyber Security Beveiligingsplan;
- Het ondersteunen bij verificatie- en validatieprocessen betreffende aantoonbaarheid en traceerbaarheid van de Cyber Security eisen naar de voorlopig, definitief en uitvoeringsontwerp documenten;
- Het beoordelen van Cyber Security ontwerpproducten en testplannen;
- Het adviseren over en ondersteunen van contractbeheersing op Cyber Security inhoudelijke aspecten tijdens de ontwerpfase.

Fase: Realisatie en testen

- Het beoordelen van Cyber Security testplannen en testrapportages;
- Het ondersteunen bij verificatie- en validatieprocessen betreffende aantoonbaarheid en traceerbaarheid van de Cyber Security eisen naar technische oplossingen;
- Het adviseren over en het beoordelen van de iteratieve opbouw van het Cyber Security Beveiligingsplan;
- Het adviseren en beoordelen van Cyber Security explains. Dit zijn gemotiveerde afwijkingen die autorisatie behoeven;
- Het valideren van de CS-IA uitwerking van het ontwerp;
- Het adviseren over en ondersteunen van contractbeheersing op Cyber Security-inhoudelijke aspecten tijdens de realisatie- en testfase.

Fase: Beheer en onderhoud

- Het adviseren en beoordelen vanuit de PDCA cyclus van het Cyber Security Beveiligingsplan;
- Het in het kader van assetmanagement uitvoeren van CS-IA risicoanalyses op bestaande objecten van Rijkswaterstaat en het adviseren hierover;
- Het adviseren en beoordelen van Cyber Security Beveiligingsplannen die nog ontwikkeld worden voor bestaande assets;
- Het adviseren en beoordelen en rapporteren over de status van de explains;
- Het adviseren en beoordelen van onderhoudsplannen van Opdrachtnemers voor het CS-IA aspect;
- Het adviseren en of beoordelen van het CS-IA deel van de conditieonderzoeken;
- Het adviseren over en ondersteunen van contractbeheersing op Cyber Security-inhoudelijke aspecten tijdens de beheer- en onderhoudsfase.

1.1.3.2. Kwetsbaarheidsanalyse IA ketens op cyber security

Deze activiteiten omvatten het uitvoeren van of ondersteunen bij kwetsbaarheidsanalyse van de IA ketens op Cyber Security.

Dit betreft zowel documentstudies als fysieke controles, bijvoorbeeld door:

- Het uitvoeren van kwetsbaarheidsscans, penetratietesten;
- Het testen van de verschillende Cyber Security beveiligingsmaatregelen;
- Het testen van de Cyber Security bewustwording bij gebruikers en beheerders.

Een onderdeel van deze activiteiten is een gedegen voorbereiding en afstemming met de stakeholders. Dit wordt vastgelegd in een testplan met afgewogen risico's en beheersmaatregelen.

Als resultaat van het onderzoek worden rapportages geformuleerd met realistische aanbevelingen voor verbeteringen.

1.1.3.3. Diensten in geval van hack of sabotage

Het betreft activiteiten en onderzoeken als onderdeel van het incident-response proces. Deze dienst wordt afgeroepen indien Rijkswaterstaat een vermoeden heeft van een hack of sabotage of poging daartoe.

Het gaat hierbij om:

- Het onderzoeken of er daadwerkelijk sprake is van een hack of sabotage;
- Het ondersteunen bij het stoppen van de hack of sabotage;
- Het ondersteunen bij het voorkomen of beperken van de gevolgschade;
- Het uitvoeren van een forensisch onderzoek, waarbij ook het verkrijgen en vastleggen van de bewijslast.