RWS BEDRIJFSVERTROUWELIJK
KRW WNZ

Rijkswaterstaat Centrale Informatievoorziening

Derde Werelddreef 1
2622 HA Delft
Postbus 2232
3500 GE Utrecht
T 088 797 28 00
F 088 797 29 09
civ-info@rws.nl
www.rijkswaterstaat.nl

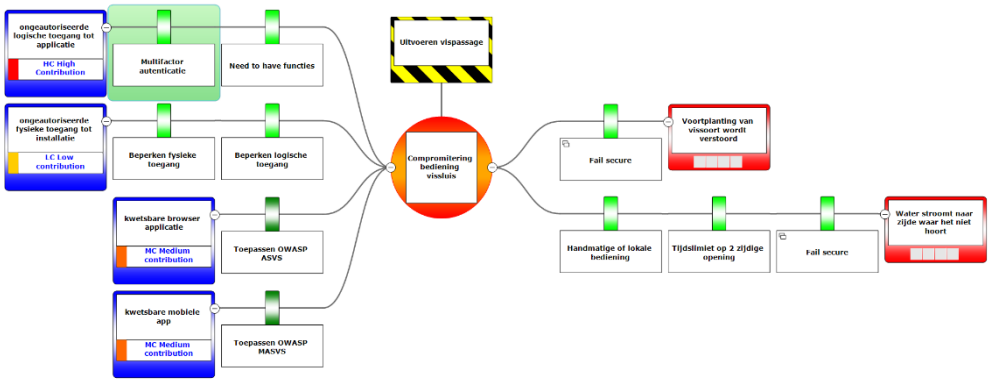
memo

Cybersecurity eisen m.b.t. vispassage Avelingen

Datum
24 april 2025

De Scope van het system under consideration(SUC)
De vispassage van het type "de Wit-sluisvispassage" bestaat uit een buis met aan weerszijde schuiven. De schuiven worden elektro-mechanisch bewogen en de aansturing wordt verzorgd door een lokale besturingsinstallatie. De bediening van de besturingsinstallatie kan worden uitgevoerd middels lokale bediening op de lokale besturingsinstallatie én via een SaaS (Software as a Service) dienst aangeboden door een externe partij. De vispassage wordt voorzien van hard en software t.b.v. de monitoring van data met betrekking tot het gebruik en effect van de vispassage, te denken valt aan monitoring van vissoorten, aantallen etc. De energievoorziening van de vispassage wordt verzorgt met zonnepanelen en accu's. Bijzonderheid van de vispassage is dat de schuiven ook aan beide zijden kunnen worden geopend. Dit om na een hoogwaterperiode water te kunnen afvoeren uit het uiterwaard.

Risicoanalyse vispassage
Voor de vispassage is een risicoanalyse uitgevoerd om het grootste risico en de dreigingen in beeld te krijgen. Zie Bijlage 1. Het risico staat hierbij centraal. Links staan de maatregelen om de kans van optreden te beperken, rechts de maatregelen op de gevolgen te beperken. De CSIR (Cybersecurity Implementatierichtlijn Objecten) voorziet al in een groot deel van de maatregelen. De risicoanalyse heeft a.g.v. de SaaS dienst tot aanvullende maatregelen geleid. Deze maatregelen zijn opgenomen in onderstaande maatregelen tabellen.



Van toepassing zijnde maatregelen:
Op basis van de risico analyse zijn onderstaande eisen m.b.t. tot cybersecurity van toepassing.

Eis nummer	Eis Titel	Eis contracttekst
VSP17	Verwerking van bewijsmateriaal	De Opdrachtnemer dient in voorkomende gevallen zijn medewerking te verlenen aan het verzamelen, bewaren en beschikbaar stellen van cybersecurity bewijsmateriaal.
VSP34	Fysieke toegangsbeveiliging IA-gerelateerde ruimten	De Opdrachtnemer dient met betrekking tot fysieke toegangsbeveiliging van de ICT en IA gerelateerde ruimten (waaronder bedien- en technische ruimten) binnen beheerobjecten cybersecuritymaatregelen te treffen conform paragraaf 2.1.1 "Maatregelen fysieke toegangsbeveiliging IA-gerelateerde ruimten" van bijlage V "Cybersecurity Implementatierichtlijn Objecten".
VSP40	Securitymaatregelen bij datanetwerkkoppelingen	De Opdrachtnemer dient met betrekking tot datanetwerkkoppelingen cybersecuritymaatregelen te treffen conform paragraaf 2.4.1 "Netwerkkoppelingen" van bijlage V “Cybersecurity Implementatierichtlijn Objecten”.
VSP50	Pentesten	De Opdrachtnemer dient zijn medewerking te verlenen aan het (laten) pentesten en (laten) uitvoeren van (geautomatiseerde) kwetsbaarheidsscans van de ICT en IA door de Opdrachtgever.
VSE04	Hardening	Maximale hardening conform de maatregelen uit paragraaf 2.5.2 “Hardening” en bijlage CSR9 “Hardening” van de [Cybersecurity Implementatierichtlijn Objecten] dient aangehouden te zijn voor de (rand)apparatuur en delen van de datanetwerkinfrastructuur van waaruit remote beheer en onderhoud wordt uitgevoerd aan de ICT en IA van het beheerobject.
VSE05	Toegangsmaatregelen beheerobject	Voor de ICT en IA van het beheerobject dienen voor de identificatie, authenticatie en autorisatie maatregelen

		geimplementeerd te worden conform paragraaf 2.2 "Maatregelen logische toegang" van de [Cybersecurity Implementatierichtlijn Objecten].
VSE06	Wachtwoordeisen beheerobject	Voor de ICT en IA van het beheerobject dienen de eisen en functionaliteit ten aanzien van wachtwoorden conform bijlage CSR 7 "Wachtwoorden" van de [Cybersecurity Implementatierichtlijn Objecten] gevolgd te worden.
VSE07	Cryptografie beheerobject	Voor de ICT en IA van het beheerobject dienen bij inzet van versleuteling ter bescherming van de vertrouwelijkheid, authenticiteit en/of integriteit maatregelen getroffen te worden conform paragraaf 2.4.2 "Cryptografie" van de [Cybersecurity Implementatierichtlijn Objecten].
VSE08	Sterke encryptie beheerobject	Voor de ICT en IA van het beheerobject dient bij inzet van versleuteling alleen gekozen te worden voor de versleuteling, de onderliggende algoritmes en instellingen met uitsluitend de duiding “goed”, zoals aangegeven in het NCSC document [Richtlijnen voor Transport Layer Security].
VSE11	Fysieke beveiliging gerelateerde ruimten beheerobject	De fysieke toegangsbeveiliging van ICT en IA gerelateerde ruimten (waaronder Bedienruimte en Technische Ruimten) van het beheerobject dient ingericht te zijn conform paragraaf 2.1.1 "Maatregelen Fysieke toegangsbeveiliging IA-gerelateerde ruimten" van de [Cybersecurity Implementatierichtlijn Objecten].
VSE17	Hardening beheeroject	De ICT en IA van het beheerobject dient gehardend te zijn conform de maatregelen uit paragraaf 2.5.2 "Hardening" en bijlage CSR 9 “Hardening” van de [Cybersecurity Implementatierichtlijn Objecten].
VSE31	Invoer/uitvoer controles beheerobject	ICT en IA van het beheerobject dient voorzien te zijn van invoer en uitvoer validatie controles om corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen traceerbaar te maken.
VSE33	Eisen aan webapplicaties voor beheer van beheerobject	Bij inzet van (web)applicaties voor beheer of onderhoud van ICT en IA van het beheerobject dient de

		beveiliging van de in te zetten (web)applicaties ingericht te zijn conform de [ICT-Beveiligingsrichtlijnen Webapplicaties] van het Nationaal Cybersecurity Centrum.
VSE39	Veilige modus beheerobject	De ICT en IA van het beheerobject dient naar een vooraf gedefinieerde veilige situatie (beide schuiven van de passage staan dicht) gestuurd te worden in geval van een aanval, incident of calamiteit conform paragraaf 2.3 "Maatregelen beveiligingsincidenten en incident response plan" van de [Cybersecurity Implementatierichtlijn Objecten].

De bovenstaande eisen verwijzen naar maatregelen in de CSIR bijlage bij de overeenkomst. De eisen verwijzen naar maatregelen uit de CSIR. In sommige gevallen is niet de gehele paragraaf van toepassing. Als dat het geval is dan staat in onderstaande tabel de maatregelen uit de CSIR die van toepassing zijn voor die specifieke eis.

Ident	Maatregel vereiste	Onderbouwing	VSE VSP ref
FR1	VRKI-referentie: 1		VSP34
FR5	Sleutel: Toegang middels een fysieke sleutel (voor normering zie Bouwkundige maatregelen/sluitwerk).	Deze eis geldt voor de (buiten)kast waar de apparatuur tbv de bediening en monitoring van de vissluis.	VSP34
FR11	BK2: Bouwkundige maatregelen met prestatie-eis van 3 minuten inbraakwerendheid.		VSP34
FR20	EL2: Grade 2		VSP34
IT3	Het ICS/SCADA systeem dient na onderbreking of falen terug te kunnen keren naar een bekende veilige staat.	1. De functionaliteit om de sluis aan 2 zijden open te zetten kan voor een maximaal ingestelde tijd worden uitgevoerd. Deze tijd is hardcoded in de lokale besturing. Na die tijd moet de handeling om aan 2 zijden te openen weer opnieuw worden uitgevoerd	VSE39

		door een geautoriseerde gebruiker. 2. Indien het niet mogelijk is om de installatie op afstand te bedienen moet de installatie lokaal naar een veilige toestand (beide schuiven dicht) worden gebracht.	
NT1	ICS/SCADA en safety systemen, de ondersteunende systemen en besloten lokale objectnetwerken mogen alleen verbindingen hebben met kantoornetwerken indien deze verlopen via de beveiligde centrale voorzieningen van de objecteigenaar.		VSP40
NT2	Communicatie en functies van safety systemen zijn afgeschermd van overige communicatie.		VSP40
NT3	De gebruikte communicatiemethoden dienen de integriteit van de gegevensoverdracht te borgen, inclusief fysieke en omgevingsinvloeden op de integriteit van de gegevensoverdracht.		VSP40
CT1	Bij inzet van versleuteling (cryptografie) dient de gekozen versleuteling en de onderliggende algoritmes en instellingen uitsluitend de duiding "goed" te hebben zoals aangegeven in de meest actuele versie van het NCSC document "Richtlijnen voor Transport Layer Security".		VSE07

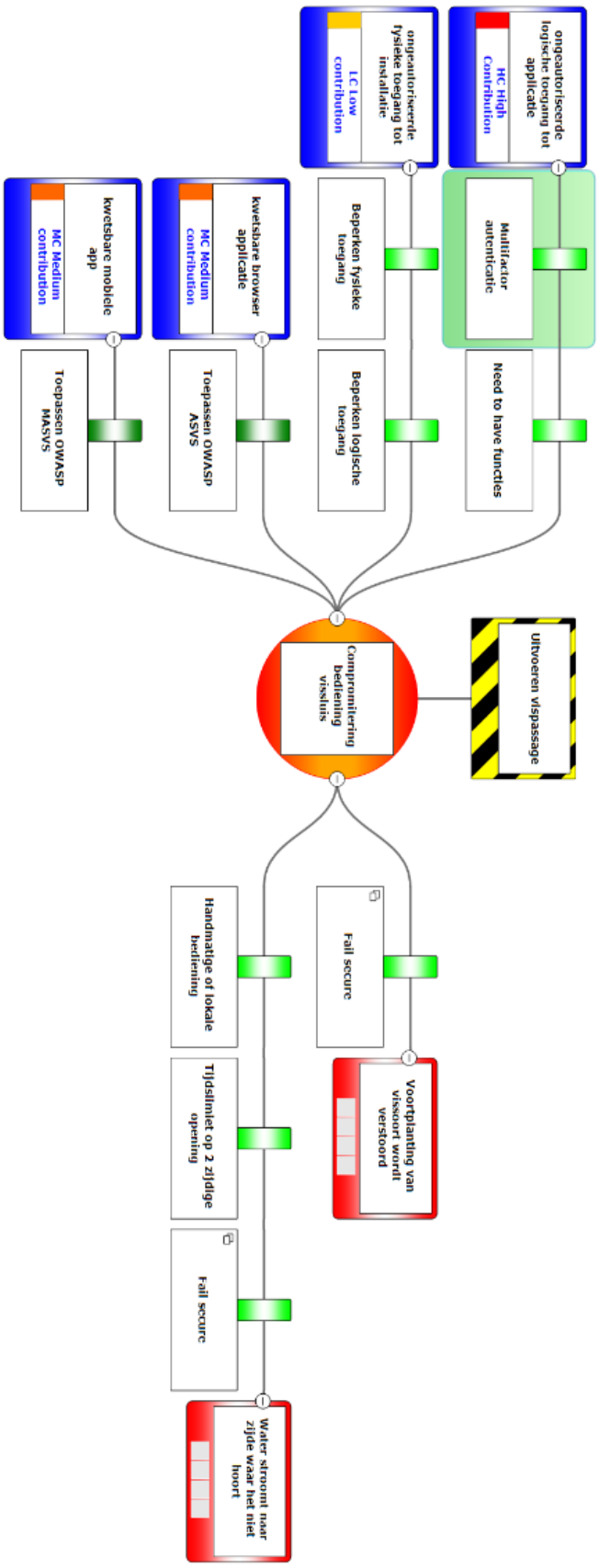
CT2	Indien het configureren van de IA/PA/OT systemen op afstand plaatsvindt, dan dient dit over beveiligde verbindingen plaats te vinden. Inzet van onveilige communicatieprotocollen (FTP, Telnet, VNC en RDP) dient daarbij vermeden te worden. Indien het Systeem geen veilig communicatieprotocol ondersteunt dan mag enkel gemotiveerd en na goedkeuring het onveilige communicatieprotocol worden ingezet, mits er een additioneel versleuteld kanaal wordt toegepast (SSL, TLS, IPSEC etc.). De gekozen versleuteling en de onderliggende algoritmes en instellingen dienen dan uitsluitend de duiding "goed" te hebben zoals aangegeven in de meest actuele versie van het NCSC document "Richtlijnen voor Transport Layer Security".		VSE07
HP2	Hardware, software en netwerkapparatuur dienen veilig geconfigureerd te worden waarbij gebruik wordt gemaakt "good practice security baselines".		VSE17
HT1	Indien mogelijk dienen ICS/SCADA-systemen zodanig te worden (her)geconfigureerd dat auto-run van USB-tokens, USB harde schijven, mounted network shares of andere removable media niet is toegestaan. Ook dient het gebruik van mobiele code beperkt te		VSE17

	worden, waarbij het uitvoeren van mobiele code niet is toegestaan, tenzij: a. de afkomst van de mobiele code op voldoende wijze is geauthentiseerd en geautoriseerd; b. het versturen van mobiele code naar/van de ICS/SCADA systemen is geblokkeerd.		
HT4	Minimale hardening maatregelen zijn: a. niet noodzakelijke datanetwerkservices uit te zetten; b. het verwijderen (patchen) van bekende kwetsbaarheden; c. alle poorten die niet nodig zijn te deactiveren/blokkeren; d. alle default "access points" te verwijderen; e. de default accounts uit te schakelen conform het wachtwoord beleid Indien uitschakelen niet mogelijk is dient het wachtwoord te worden aangepast; f. indien beschikbaar gebruik te maken van de security opties van leveranciers.		VSE17
HT5	Het aanzetten van uitgeschakelde services en/of protocollen moet mogelijk blijven.		VSE17

<u>Aanvullende maatregelen</u>
De CSIR is met name gericht op het beschermen van de IA op beheerobjecten van RWS en waarbij de bediening vanuit het eigen beschermde netwerk wordt uitgevoerd. Voor de vispassage wordt gebruik gemaakt van een dienst van derden (software as a service, SaaS) die via een publieke mobiele verbinding connectie maakt met de vispassage. Op basis van de risicoanalyse is dit mogelijk indien er een aantal maatregelen worden genomen door de SaaS provider.

Control	Control beschrijving	Onderbouwing
SaaS Provider Security Assurance & Compliance	SaaS-provider moet aantonen dat zij voldoet aan ISO 27001 en bewijs leveren van beveiligingsaudits, certificeringen en contractuele beveiligingsverplichtingen.	
Cloud Application Security (SaaS Security Hardening)	SaaS-provider moet security-by-design-principes toepassen, veilige softwareontwikkeling waarborgen en configuratie hardening afdwingen.	
OT/IoT-SaaS Configuratiebeheer & Verharding	SaaS-provider moet tools voor configuratiebeheer leveren, veilige standaardinstellingen afdwingen en misconfiguraties voorkomen.	
Sterke Authenticatie & Autorisatie (MFA & RBAC)	SaaS-provider moet Multi-Factor Authenticatie (MFA), Role based acces control (RBAC) en fijnmazige toegangsrechten tot OT/IoT-systemen ondersteunen.	voor tenminste gebruikers met rechten om de installatie te bedienen
Just-In-Time (JIT) Toegang voor SaaS-Beheerde OT/IoT-Systemen	SaaS-provider moet sessie verloop instellen en toegang door admins en beheerders traceren.	
Toegangslogging & Auditing voor SaaS-Beheerde OT/IoT-Systemen	SaaS-provider moet gedetailleerde toegangslogs bijhouden, forensische analyse ondersteunen en auditrapportages op verzoek beschikbaar stellen.	
Data-encryptie voor OT/IoT Telemetrie & Besturingssignalen	SaaS-provider moet end-to-end encryptie garanderen (AES-256 voor opslag, TLS 1.3 voor transport) en best practices voor beheer van encryptie sleutels toepassen.	
Veilige Communicatie tussen OT/IoT-Systemen & SaaS-Diensten	SaaS-provider moet gebruikmaken van veilige VPN’s, IPSec of ZTNA voor communicatie tussen SaaS en OT/IoT-systemen.	

LTE MitM-aanvalbescherming	SaaS-provider moet veilige VPN's of private APN's vereisen voor LTE-verbindingen om verkeeronderschepping te voorkomen.	
OWASP ASVS	SaaS-provider waarborgt dat de applicatie voldoet aan de OWASP Application Security Verification Standard 4.0.3 (ASVS) niveau 1 eisen.	
OWASP MASVS	SaaS-provider waarborgt dat de mobiele applicatie voldoet aan de OWASP Mobile Application Security Verification Standard v2.1.0 (MASVS).	Waar van toepassing: MASVS-CODE: Codekwaliteit; Code 2


ongeautoriseerde logische toegang tot applicatie
HC High Contribution
ongeautoriseerde fysieke toegang tot installatie
LC Low contribution
Multifactor authenticatie
Beperken fysieke toegang
kwetsbare browser applicatie
MC Medium contribution
kwetsbare mobiele app
MC Medium contribution
Need to have functies
Beperken logische toegang
Toepassen OWASP ASVS
Toepassen OWASP MASVS
Uitvoeren vispassage
Compromitering bediening visstuis
Fail secure
Voortplanting van vissoort wordt verstoord
Handmatige of lokale bediening
Tijdsslimiet op 2 zijdige opening
Fail secure
Water stroomt naar zijde waar het niet hoort