HARDENING RICHTLIJNEN PA-DOMEIN

Project: PA Beheeractiviteiten
Classificatie: Bedrijfsvertrouwelijk: Intern

Eigenaar en beheerder document

Documenteigenaar	
Functie: Manager OTI	Naam: Casper Braamse
Document beheerder	
Functie: PL beheersmaatregelen	Naam: Wim Uijtdewilligen

Versiebeheer

Versie	**Datum**	**Omschrijving**
0.1	18-11-2024	Eerste versie van het document
0.2	25-11-2024	Globale maatregelen per eis
0.3	12-12-2024	Borging maatregelen binnen Delfland
0.4	16-12-2024	Finaliseren concept ter review
0.99	19-12-2024	Review commentaar van Edwin en Hidde verwerkt

Vaststelling en periodieke validatie

Vastgestelde versie	**Datum vaststelling**	**Wie**	**Functie**
1.0		Casper Braamse	Aangewezen validator namens SG PA BIO*logisch*
Volgende validatie			
Classificatie	Vertrouwelijk		

Inhoudsopgave

1 Inleiding

1.1 Wat is hardening?

Hardening betreft het verwijderen of uitschakelen van overbodige en/of ongebruikte functionaliteit van een apparaat en is van toepassing op software, hardware en netwerk. Hardening zorgt ervoor dat systemen minder kwetsbaar worden, waardoor aanvallers en malware minder kansen krijgen om voet aan de grond te zetten. Hardening wordt toegepast op zowel ICT als PA componenten.

Er worden drie methoden van hardening toegepast, te weten software-, hardware- en netwerk-hardening:

- Software hardening is van toepassing op operating systemen (bijvoorbeeld Microsoft Windows, Active Directory) en applicaties (bijvoorbeeld HMI of engineering software, configuratietools, maar ook MS Office, Acrobat reader, Active-X controls en Adobe Flash).
- Hardware hardening is van toepassing op bijvoorbeeld firmware, alsook het uitschakelen van niet gebruikte communicatiepoorten, antennes, en overige niet gebruikte functionaliteit.
- Netwerk (Process Control Network) hardening is van toepassing op bijvoorbeeld uitschakelen van onveilige en niet gebruikte protocollen, het beperken van netwerkverkeer (firewalls) en segmentatie/zonering van het netwerk.

1.2 Aanleiding

Er zijn momenteel geen eenduidige maatregelen binnen Delfland geïmplementeerd die zorgdragen voor juiste hardening van de systemen binnen het PA-domein.

1.3 Doel

Door het opstellen en toepassen van hardening richtlijnen voor het hardenen van de systemen binnen het PA-domein hanteert Delfland in de toekomst een methodische aanpak voor het identificeren en beheersen van potentiële beveiligingskwetsbaarheden. Ook zorgt dit voor een verkleining van het aanvalsoppervlak en wordt voldaan aan wet- en regelgeving.

1.4 Scope

De hardening richtlijnen zijn opgesteld op basis van de eisen die door BIO en CSIR worden gesteld (zie hoofdstuk “6 Eisen”) en worden toegepast voor het hardenen van de systemen (software, hardware en netwerk) binnen het PA-domein.

Hierbij is het uitgangspunt dat er alleen PA-assets worden aangepakt die al in het CMDB staan. Zoniet, dan moeten deze eerst in het CMDB worden opgenomen. Een voordeel van deze werkwijze is dat ongedefinieerde hardware hiermee in het CMDB wordt opgenomen. Vanuit het project ontkomen we er niet aan om breder te kijken dan alleen zullen er ook PA-assets op het grensvlak PA / ICT liggen en die onder verantwoordelijkheid van PA door ICT worden doorgevoerd op de systemen. Dit geven we aan bij de ICT-afdeling. Andersom zal de ICT-afdeling maatregelen willen doorvoeren die effect hebben op de PA-scope, dit geven ze ook aan als input op dit project.

Onderstaande tabel geeft een compleet overzicht van de bij Delfland aanwezige productfamilies met hun omvang:

Assetsysteem	Objectgroep	PA-familie	PA-functie	PA-
Algemeen	Historian Waterketen en watersysteem	ABB SPH+	Dataopslag	1
Waterketen	AWZI DGL + Rioolgemalen	ABB 800 xA	Visualisatie	1
Waterketen	AWZI DGL	ABB 800 AC	Besturing	7
Waterketen	AWZI DGL	Siemens	Package units	
Waterketen	AWZI NWA + Rioolgemalen	ABB 800 xA	Visualisatie	1
Waterketen	AWZI NWA	ABB 800 AC	Besturing	
Waterketen	AWZI NWA	Siemens	Package units	
Waterketen	Hoofd-rioolgemalen Delfland	ABB 800 AC	Besturing	16
Waterketen	Rioolgemalen gem. Maassluis	ABB 800 AC	Besturing	15
Waterketen	Rioolgemalen gem. Maassluis	Aquaview	Visualisatie	1
Waterketen	Rioolgemalen gem. Maassluis	Flygt FGC/APP	Besturing	125
Waterketen	Houtrust	ABB Freelance	Visualisatie	1
Waterketen	Houtrust	ABB Freelance	Besturing	
Waterketen	Harnaschpolder	ABB Freelance	Visualisatie	1
Waterketen	Harnaschpolder	ABB Freelance	Besturing	
Watersysteem	WIS (Historian Watersysteem)	FEWS/Oracle	Dataopslag	1
Watersysteem	BOS (Beslissingondersteunenen systee	FEWS/Oracle	Optimalisatie	1
Watersysteem	Boezemgemalen	ABB 800 xA	Visualisatie	1
Watersysteem	Boezemgemalen	ABB 800 AC	Besturing	6
Watersysteem	Doorvoergemaal 't Westambacht	ABB 800 AC	Besturing	1
Watersysteem	Binnenstad Delft	ABB 800 AC	Besturing	6
Watersysteem	Kunstwerken waterberging Hoekpolder	ABB 800 AC	Besturing	1
Watersysteem	Waterberging Woudsepolder	ABB 800 AC	Besturing	1
Watersysteem	Poldergemalen/ stuwen/ inlaten/filter	Siemens WINCC	Visualisatie	1
Watersysteem	Poldergemalen/ stuwen/ inlaten/filter	TBox	Besturing	311
Watersysteem	Zonnestuw Vlinderstrik	Vlaar CSB	Besturing	1
Watersysteem	VisliftUP	TBox	Besturing	
Watersysteem	Peilmeting draadloos	Terratransfer (exte	Sensoren	
Watersysteem	Waterkwaliteitsmeting	diverse	Sensoren	200
Watersysteem	Waterkwaliteitsmeetnet	Telecontrolnet (ex	Dataopslag	1
Watersysteem	Waterkwaliteit	Aquadesk	Dataopslag	1
Waterveiligheid	Keersluis Maassluis		Besturing	1
Waterveiligheid	Vlaardinger Driesluizen	Zenon	Visualisatie	1
Waterveiligheid	Vlaardinger Driesluizen	Siemens Simatic	Besturing	
Waterveiligheid	Vlaardinger Buitensluis		Besturing	1
Waterveiligheid	Spuisluizen (combi boezemgemalen)	ABB 800 AC	Besturing	4
Waterveiligheid	Afsluiter persleiding gemaal Parksluizen	ABB 800 AC	Besturing	1
Waterveiligheid	Boostergemaal + 18 pompputten Grond	ABB 800 AC	Besturing	1
Algemeen	PA-netwerk	diverse	Communicatie	1

2 Maatregelen

Een gehardened systeem heeft de volgende kenmerken:

1. Alles wat nodig is voor het systeem is geactiveerd, alle onnodige diensten, poorten en componenten zijn gewist of uitgeschakeld.
2. Alle niet benodigde gebruikers accounts zijn gewist.
3. Alle niet benodigde poorten zijn gesloten.
4. Rechten zijn zoveel als mogelijk beperkt.

Om dit te bereiken passen we hardening maatregelen toe. In hoofdstuk “6 Eisen” wordt per eis de te nemen maatregelen en de borging binnen Delfland beschreven om aan deze eis te voldoen. Hierbij dient wel aangetekend te worden dat, in lijn met de BIO en CSIR proceseisen, dit document voortdurend onderhouden en waar nodig aangevuld dient te worden.

3 Werkomschrijvingen en logboek

De benoemde maatregelen in voorgaande hoofdstuk zijn globaal beschreven. Voor het daadwerkelijk doorvoeren van de hardening maatregelen is per systeem of apparaat een beknopte werkomschrijving aanwezig die de praktische omschrijving geeft van de wijzigingen. Ook is er een overkoepeld logboek hardening aanwezig waarin de genomen acties zijn vastgelegd. Alle wijzigingen lopen via het PA-wijzigingsproces van Delfland.

4 Verantwoordelijkheid

De Securityspecialist PA is verantwoordelijk voor implementeren en naleven van de hardening richtlijnen.

5 Eisen

Bron	Typering vanuit bronnorm	Categorie bron	Code bron	Beschrijving	Maatregelen	Borging binnen Delfland
TA PA domein	Hardening richtlijnen opstellen voor apparatuur en systemen			Niet gebruikte functies uitschakelen op apparatuur (onderdeel hardening).	Opstellen hardening richtlijnen.	Zie HP1 - maatregel 1
CSIR	2.4 Maatregelen netwerkkoppelingen en cryptografie	2.4.1 Netwerkkoppelingen	NP5	Objectbeheerder draagt zorg voor en ziet erop toe dat het lokale objectdatanetwerk gehardend is door niet noodzakelijke netwerkservices uit te zetten (voor hardening zie 'Maatregelen bescherming tegen kwetsbaarheden).	1. Uitschakelen niet noodzakelijke netwerkservices. 2. Documenteer alle uitgevoerde wijzigingen in netwerkconfiguraties en services 3. Voer periodieke audits uit om te controleren of ongebruikte netwerkservices uitgeschakeld blijven.	1. Zie HT4 - maatregel 1 2. Zie HP3 - maatregel 1 3. Periodieke operationele taak in TOPdesk
CSIR	2.4 Maatregelen netwerkkoppelingen en cryptografie	2.4.1 Netwerkkoppelingen	NP6	Bij afname van netwerkdiensten via providers, of in het geval van samenwerkingsverbanden, dient geëist te worden dat maximale hardening is doorgevoerd op de ingezette netwerk componenten en of apparatuur.	1. Leg vast in SLA's met providers dat maximale hardening moet worden toegepast. 2. Vraag providers bewijs (bijv. audits of rapportages) van de provider voor de geharde configuraties. 3. Controleer periodiek of de geleverde netwerkcomponenten voldoen aan de afgesproken hardening-eisen.	1. Hoofdstuk in raamcontracten 2. Toetsen tijdens afnametesten 3. Periodieke operationele taak in TOPdesk / Logboek PA-hardening
CSIR	2.5 Maatregelen bescherming tegen kwetsbaarheden	2.5.2 Hardening	HM1	Voor bewustwording, gedragsrichtlijnen en training van bedienaars, beheerders en overig ondersteunend personeel wordt verwezen naar paragraaf 2.7 de maatregelen-set "bewustwording en training" van de Cybersecurity Implementatierichtlijn Objecten.	1. Ontwikkel een trainingsprogramma voor de PA-beheerders over de hardening richtlijnen en security awareness. 2. Organiseer regelmatige sessies om personeel op de hoogte te houden van nieuwe dreigingen en best practices. 3. Voer periodieke tests uit om te controleren of het personeel de richtlijnen begrijpt en naleeft.	1. Interne / externe training 2. ARDA / interne kennissessies 3. ARDA / interne kennissessies
CSIR	2.5 Maatregelen bescherming tegen kwetsbaarheden	2.5.2 Hardening	HP1	Er dient een geborgde procedure te zijn voor het hardenen van ICS/SCADA en overige ondersteunde ICT-systemen en datanetwerkelementen.	1. Stel hardening richtlijnen voor het PA-domein op die beschrijven welke stappen moeten worden doorlopen. 2. Zorg dat de richtlijnen wordt nageleefd door middel van controles en audits. 3. Werk de richtlijnen bij op basis van nieuwe kwetsbaarheden en inzichten.	1. Dit document (Hardening richtlijnen PA-domein) 2. Periodieke ISO audits 3. Periodieke operationele taak in TOPdesk.
CSIR	2.5 Maatregelen bescherming tegen kwetsbaarheden	2.5.2 Hardening	HP2	Hardware, software en netwerkapparatuur dienen veilig geconfigureerd te worden waarbij gebruik wordt gemaakt "good practice security baselines".	1. Gebruik standaarden, zoals CIS Benchmarks, voor het configureren van systemen en netwerken. 2. Documenteer alle configuraties en implementeer versiebeheer om wijzigingen bij te houden.	1. Input voor opstellen werkomschrijvingen 2. Zie HP3 - maatregel 1
CSIR	2.5 Maatregelen bescherming tegen kwetsbaarheden	2.5.2 Hardening	HP3	Het dient aantoonbaar te zijn welke hardening-methoden zijn gebruikt en hoe deze zijn toegepast. Hierbij wordt een vooraf opgesteld protocol gevolgd en is er een registratie van de uitgevoerde hardening activiteiten.	1. Documenteer welke hardening-methoden zijn toegepast, inclusief een protocol en logboeken. 2. Bewaar rapportages van uitgevoerde hardeningactiviteiten voor audits.	1. PA-wijzigingsproces / Werkbeschrijvingen / Logboek PA-hardening 2. Logboek PA-hardening
CSIR	2.5 Maatregelen bescherming tegen kwetsbaarheden	2.5.2 Hardening	HP4	Het inschakelen van uitgezette services en/of protocollen mag alleen door geautoriseerd personeel worden uitgevoerd en dient gedocumenteerd te worden.	1. Beperk wie services en protocollen kan inschakelen. Alleen geautoriseerd personeel mag wijzigingen doorvoeren. 2. Leg elke wijziging vast in logboeken inclusief motivatie en goedkeuring. 3. Voer periodieke audits uit om ervoor te zorgen dat geen ongeautoriseerde wijzigingen zijn doorgevoerd.	1. Rechtenbeheer PA / ICT 2. Logboek PA-hardening 3. Periodieke operationele taak in TOPdesk / PA-wijzigingsproces
CSIR	2.5 Maatregelen bescherming tegen kwetsbaarheden	2.5.2 Hardening	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 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.	1. Zet automatische uitvoering van externe media uit in de systeemconfiguratie. 2. Autoriseer en verifieer mobiele code voordat deze wordt gebruikt. 3. Gebruik firewallregels om verzending van mobiele code te beperken.	1. Werkomschrijvingen 2. Werkomschrijvingen 3. Werkomschrijvingen

Bron	Typering vanuit bronnorm	Categorie bron	Code bron	Beschrijving	Maatregelen	Borging binnen Delfland
CSIR	2.5 Maatregelen bescherming tegen kwetsbaarheden	2.5.2 Hardening	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.	1. Identificeer en schakel niet noodzakelijke netwerkservices (bijv. file sharing, remote desktop, etc.) en poorten uit (eis a en c). 2. Patch, afhankelijk van het risico, bekende kwetsbaarheden zo snel mogelijk (eis b). 3. Verwijder standaard toegangen, standaard accounts en stel veilige wachtwoorden in voor alle systemen (eis d en e). 4. Activeer beschikbare beveiligingsopties van leveranciers (eis f).	1. Werkomschrijvingen 2. Risico management 3. Werkomschrijvingen 4. Werkomschrijvingen
CSIR	2.5 Maatregelen bescherming tegen kwetsbaarheden	2.5.2 Hardening	HT5	Het aanzetten van uitgeschakelde services en/of protocollen moet mogelijk blijven.	1. Definieer een goedkeuringsproces voor het inschakelen van services. 2. Documenteer alle uitgezette services en protocollen in een wijzigingslogboek, inclusief de reden voor uitschakeling en wie het heeft goedgekeurd.	1. PA-wijzigingsproces 2. Logboek PA-hardening
BIO	6. Organiseren van informatiebeveiliging		06.2.1.2	Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd: b. Het device maakt deel uit van patchmanagement en hardening.	Stel beperkingen in voor het gebruik van mobiele apparaten, zoals encryptie en het blokkeren van niet-goedgekeurde applicaties.	Werkomschrijvingen
BIO Audit '22	U.06 Netwerk en informatietransport		U.06	Stel een procedure op voor hardening van het PA netwerk en voer deze in. Pas de eisen toe in de CSIR en overweeg de toepassing van best practices in deze CSIR.	Opstellen hardening richtlijnen.	Zie HP1 - maatregel 1