Hardeningvoorschrift OT

De eisen voor het digitaal bewapenen van

de OT/Operationele Technologie van GVB

Vertrouwelijkheid.
Dit document is Bedrijfsvertrouwelijk

Colofon
Dit document beschrijft een onderdeel van de aanpak voor de digitale beveiliging van de OT van GVB, zie het top-document: Cybersecurity-voorschrift OT [11].

Documentnummer

Versie	0.2, aangepast aan de GVB-organisatie en de nieuwe OV-governance. Paragraaf Bewapenen tegen bekende kwetsbaarheden toegevoegd.
Datum	7 juli 2022
Status	Vast te stellen door de Cybersecurity-Board OT
Join	CEB/OVG/21203
Datum	20 augustus 2019
Versie	0.1
Status	concept, vast te stellen door Cybersecurity Board en DT MET

1. Inleiding

De Cybersecurity-eisen OT van GVB [12] bevat enkele concrete en vereiste hardeningsmaatregelen. Dit document geeft de referenties naar bronnen om de hardening handen en voeten te geven bij het ontwerpen van de juiste beveiligingsmaatregelen.

Document [1] geeft een definitie van hardening.

De onderwerpen in Document [1] zijn vereist voor de OT-systemen van GVB en vormen een onlosmakelijk onderdeel van de vraagspecificatie c.q. van de Cybersecurity-eisen OT van GVB [12].

Hardening is een begrip dat niet in de BIO/ISO-27001/2 wordt genoemd. Wel beschrijft de BIO/ISO-27001/2 de nodige maatregelen die als hardening gelden.

Voor het hardenen van de OT-systemen van GVB beperken we ons niet slechts tot het beperken van software en poorten; wat wel een gangbare uitleg is.

Hardening van de OT-systemen van GVB betreft de volgende onderwerpen:
- Beperken/beheersen Losse media
- Encyrptie (systemen en verbindingen) en sleutels
- Beperken/beheersen software/systeemhulpmiddelen
- Malware detectie/bescherming
- Beperken/beheersen fysieke ruimte en toegang(srechten)
- Beperken/beheersen online/IAA-toegang(srechten/gegevens *)
- Bescherming Bekabeling
- Firewall bescherming
- Intrusion detectie/bescherming
- Binary hardening
- Beheer/bescherming Broncode
- Beheer van Verwijderingen

*) IAA = identificatie, authenticatie en autorisatie

2. Wapenen tegen bekende kwetsbaarheden

Naast de bovenstaande algemene bewapeningsprincipes, geldt als eis dat de OT-systemen van GVB bewapend worden/zijn tegen bekende specifieke kwetsbaarheden. GVB wenst geen slachtoffer te worden van bekende en voorkoombare kwetsbaarheden.

Bekende kwetsbaarheden zijn kwetsbaarheden (inclusief zero-days) die via de betrokken media en/of in de Mitre-database (CVE's) algemeen bekend zijn. Voorbeelden zijn log4j, OPC-UA-protocol of betreffen het genoemde kwetsbaarheden zoals beschreven in de rapporten van cybersecurity-onderzoekers, zoals Icefall.

Bewapening betreft het implementeren van patches of het treffen van andere of extra beveiligingsmaatregelen die aantoonbaar en aannemelijk (d.m.v. een risico-analyse) voldoende zijn. De opdrachtnemer dient deze maatregelen te nemen.

Hieronder worden (niet-limitatief) een lijst gegeven van bekende kwetsbaarheden waar zeker bewapening voor nodig is, aangevuld met protocollen/systemen/software waarvan algemeen bekend is dat ze verdacht zijn van kwetsbaarheden. De opdrachtnemer dient aan te geven of de kwetsbaarheden van toepassing zijn of niet en zo ja welke beveiligingsmaatregelen geleverd worden ter mitigatie van het risico.

- Silverfish-kwetsbaarheden beschreven in het Prodaft-rapport
- Log4j
- OPC-UA-protocol
- Lapsus Okto
- IEC 61850, inclusief de gerelateerde protocollen DNP3 en IEC 60870-5-101/104
- Kwetsbaarheden beschreven in het Icefall-rapport

3. Bronnen en referenties

[1] Hardening-beleid-voor-gemeenten, Versie 1.01 of hoger, augustus 2016, Informatiebeveiligingsdienst (IBD), KING.

[2] Toegangsbeleid, versie 1.0.1 of hoger, IBD, King

[3] TR62443-3-1 Chapter 5 Authentication And authorizationTR62443-3-1 Chapter Filtering, Blocking, Access control

[4] TR62443-3-1 Chapter 7 Encryption

[5] ISO27002 12.2 Protection from malware

[6] ISO27002 12.3 Backup

[7] ISO27002 12.4 Firewall/DMZ

[8] Aanbevelingen van het NCSC voor OT systemen: https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/mei/01/checklist-beveiliging-ics-scada/FS2012-02-Checklist-beveiliging-van-ICS-SCADA-systemen.pdf

[9] Control systems security, Homeland Security, april 2011, Hoofdstuk 2.8 Systems and communication protection: https://www.us-cert.gov/sites/default/files/documents/CatalogofRecommendationsVer7.pdf

[10] Control systems security, Homeland Security, https://www.us-cert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf

[11] De meest recente versie van het Cybersecurity-voorschrift OT - inclusief de gerelateerde onderliggende documenten - zijn te vinden op de pagina ‘Cybersecurity OT’ van het intranet van GVB:
https://gvb939.sharepoint.com/organisatie/algemeen/informatiebeveiliging/Paginas/Cybersecurity%20OT.aspx

[12] De meest recente versie van de Cybersecurity-eisen OT van GVB, zie de pagina ‘Cybersecurity OT’ van het intranet van GVB:
https://gvb939.sharepoint.com/organisatie/algemeen/informatiebeveiliging/Paginas/Cybersecurity%20OT.aspx