Bijlage 2a – Relevante CSIR maatregelen (OT)

Inschrijver dient te voldoen aan de volgende relevante CSIR-maatregelen:

1. LT3: Voor bedienaars, beheerders en systemen worden unieke ID's gehanteerd zodat uitgevoerde handelingen terug te leiden zijn tot een persoon of systeem.
2. LT7: (Standaard) wachtwoorden moeten door gebruikers bij het in gebruik nemen van de systemen gewijzigd kunnen worden.
3. LT10: Alvorens aan te melden dient een systeemnotificatie op het scherm te worden weergegeven. Hierin worden restricties omtrent (on)geautoriseerd systeemgebruik aangegeven, evenals logging en monitoring van het systeemgebruik.
4. 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).
5. 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 netwerkcomponenten en of apparatuur.
6. NP7: Het koppelen van mobiele apparatuur van derden of removable media aan lokale ICS/SCADA systemen, lokale objectdatanetwerken of het overkoepelende datanetwerk van de objecteigenaar dient uitsluitend plaats te vinden na autorisatie van de hiertoe aangewezen en gemandateerde functionaris aan de kant van objectbeheerder.
7. NT3: De gebruikte communicatiemethoden dienen de integriteit van de gegevensoverdracht te borgen, inclusief fysieke en omgevingsinvloeden op de integriteit van de gegevensoverdracht.
8. CP1: Bij gebruik van cryptografie dienen uitsluitend PKI-Overheid certificaten te worden ingezet voor communicatie met (externe) netwerken buiten de eigen infrastructuur.
9. CP4: Bij gebruik van cryptografie dient te worden gekozen voor cryptografische toepassingen die voldoen aan passende standaarden en is dit gedocumenteerd.
10. 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".
11. 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".
12. 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."