Handreiking cybersecurity voor (tunnel)beheerders

De handreiking is gratis online te raadplegen op www.cob.nl/groeiboek/cybersecurity

1. Wet- en regelgeving

- EU-richtlijn 2016/1148: *Directive on security of network and information systems* (*NIS Directive*)
- EU-richtlijn 2016/679: *General data protection regulation* (GDPR)
- Cybersecuritywet (Csw)
- Algemene verordening gegevensbescherming (AVG)

2. Fysieke beveiliging

- Hekwerk
- Terreinbeveiliging
- Hang- en sluitwerk (NEN5096)
- Inbraakwerende kast
- Toegangscontrole
- Inbraakalarm-, brandmeldinstallatie

3. Mens

- *Cyber security awareness*: mensen bewust maken en houden van digitale beveiliging (ook ingehuurd personeel!) door middel van training en instructie.
- Specifieke functionarissen benoemen: functionaris informatiebeveiliging, waaronder ook cybersecurity valt, en een incidentmanager.
- Specifieke eisen stellen aan medewerkers die operationeel zijn bij het beheer van de tunnel:
  - » Verklaring omtrent het gedrag (VOG)
  - » Geheimhoudingsverklaring
  - » Aantoonbaar cybersecurity bewustzijn, bv. door training en instructie

4. Organisatie

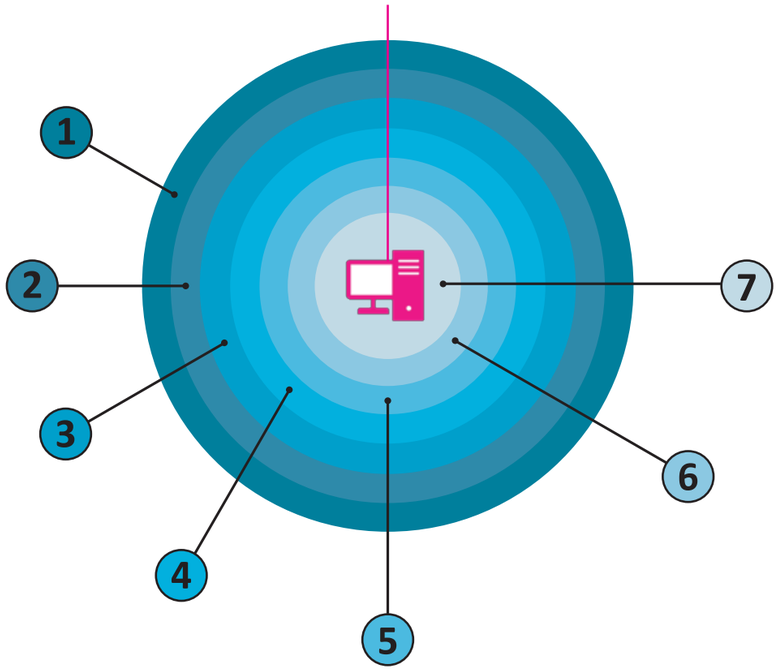
Ervoor zorgen dat de beheerder beschikt over een overzicht van:

- » Onder zijn beheer vallende assets
- » Processen en procedures
- » De rollen die er zijn en wie hiervoor zijn benoemd

Gelaagde beveiliging

Defense in depth

Supervisory control and data acquisition (SCADA)



5. Processen en documenten

- Personeel trainen (bewustwording).
- Maandelijkse rapportage cybersecurity.
- Jaarlijkse risicoanalyse cybersecurity.
- Op basis van de risicoanalyse maatregelen nemen tegen spionage, zodanig dat de documenten met betrekking tot OT en IT zijn beveiligd tegen verlies en ongeautoriseerde kennisname en wijziging.
- Jaarlijks de toegangsrechten van alle medewerkers beoordelen en actualiseren.
- Actuele registratie bijhouden van de toegang tot OT en IT gerelateerde ruimten.
- Een procedure opstellen voor de toegang tot OT en IT gerelateerde ruimten.
- Cybersecurity-beveiligingsplan opstellen.
- Herstelplan opstellen voor een besmetting met malware, waaronder alle nodige voorzieningen voor back-up, kopieën van gegevens en programmatuur evenals herstelmaatregelen.
- Documenten opstellen en onderhouden voor de bediening, het beheer, het onderhoud en de technische ondersteuning van OT en IT.
- Logboeken bijhouden voor wijzigingen op systemen, netwerken en assets.

6. Beheer en onderhoud

- Periodiek toepassen beveiligingsupdates en patches ICS/SCADA, ondersteunende ICT-systemen en netwerkomgeving; ook van de verwijderbare apparatuur en ICT-systemen.
- Patches en anti-virusupdates die vanaf internet worden gedownload: controleren op juistheid van de internetsite waarmee contact is gelegd en/of op gebruik van een betrouwbare *certificate authority* geverifieerde digitale handtekening.
- Koppelen van mobiele apparatuur of verwijderbare media aan ICS/SCADA en overige ondersteunende ICT-systemen en netwerken alleen toestaan na autorisatie van de hiertoe gemandateerde functionaris.
- *Hardenen* van ICS/SCADA, overige ondersteunende ICT-systemen en datanetwerkelementen.
- Toegang tot internet en het gebruik van e-mail vanaf ICS/SCADA en overige ondersteunende ICT-systemen verbieden.
- Accountgegevens als strikt geheim behandelden.
- Voor wijzigingen aan ICS/SCADA en overige ondersteunende ICT-systemen altijd een risicoafweging maken.
- Voordat uitvoering van werkzaamheden plaatsvindt, de risicoafweging en de hieruit voortvloeiende maatregelen laten goedkeuren door de objectverantwoordelijke/-beheerder.
- Wijzigingen bijwerken in de *configuration management database* (CMDB).
- Jaarlijks de effectiviteit van getroffen maatregelen en kwetsbaarheden in het netwerk en in systemen evalueren.
- Jaarlijks de instellingen/configuraties van ICS/SCADA en overige ondersteunende ICT-systemen in de CMDB vergelijken met de daadwerkelijke instellingen/configuraties en indien nodig bijwerken.
- Wijzigingen in ICS/SCADA en overige ondersteunende ICT-systemen indien mogelijk testen voordat de implementatie in productie gaat.
- Na noodwijzigingen die buiten het reguliere wijzigingsproces om zijn aangebracht, als gevolg van incidenten met een bijzonder (urgent) karakter, alsnog de gebruikelijke procedures volgen en in de CMDB-administratie bijwerken.
- Voor elke wijziging een terugvalscenario opstellen waarin is vastgelegd waaruit de terugval bestaat, onder welke condities tot een terugval wordt overgegaan en wie daartoe kan besluiten.Kort na de implementatie van een wijziging met een test verifiëren dat de wijziging is gelukt of dat op het terugvalscenario moet worden overgegaan.

7. Netwerkkoppelingen, apparatuur, software

- Als beheerder erop toezien dat alle netwerkkoppelingen met het lokale objectnetwerk strikt en uitsluitend plaatsvinden via de beveiligde centrale netwerkvoorzieningen en koppelpunten van de voor het tunnelbeheer verantwoordelijke organisatie.
- ICS/SCADA-systemen zodanig configureren dat *mounted network shares* en *auto-run* van verwijderbare media niet worden toegestaan.
- Niet toestaan dat besloten (lokale) objectdatanetwerken directe internetverbindingen hebben. Dit geldt ook voor draadloze verbindingen en inbelvoorzieningen.
- Intern ontworpen en ingekochte systemen/applicaties jaarlijks testen op fouten in code, op malware en op generieke beveiligingskwetsbaarheden.
- Gegevensdragers altijd controleren op virussen voordat deze worden gekoppeld aan ICS/SCADA of overige ondersteunende ICT-systemen en netwerken.
- Indien derden toegang tot OT en/of IT op afstand (*remote access*) wensen, deze toegang via de centrale, beveiligde en gemonitorde voorzieningen van de (tunnel)beheerder laten verlopen.
- Toegang tot ICS/SCADA en overige ondersteunende ICT-systemen blokkeren, tenzij het expliciet is toegestaan.
- Ongeautoriseerd aan- of afkoppelen van verwijderbare apparatuur of USB-sticks aan het netwerk of ICS/SCADA-systemen verbieden.
- Voorzie verwijderbare apparatuur en systemen die gekoppeld worden aan ICS/SCADA en ondersteunende ICT-systemen en netwerkomgeving van alle recente beveiligingsupdates en patches.
- Onbeheerde ICS/SCADA-systemen en overige ondersteunende ICT-apparatuur – zo mogelijk – locken.
- De handelingen van medewerkers, meldingen vanuit systemen en eventlogs vastleggen in auditlogbestanden.
- Voor kritieke ICS/SCADA en overige ondersteunende ICT-systemen in afstemming met en/of op verzoek van de (tunnel)beheerder specifieke logsystemen inzetten.
- In geen geval gevoelige gegevens opnemen in logregels; dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden, zoals wachtwoorden en inbelnummers.
- Periodiek (bij voorkeur dagelijks) automatisch een back-up maken van alle in het systeem aanwezige dynamische en configuratiegegevens.
- De juiste verwerking van de back-up bewaken op basis van een back-uplog. Deze back-uplogs minstens een week bewaren.