

Onderstaande tekst geeft de essentie uit een e-mail weer.

Inrichting datacommunicatieapparatuur

Hieronder staat het lijstje met aandachtspunten die van belang zijn voor de keuze en inrichting van datacommunicatie apparatuur.

Identiteiten

- Rollen
- Rechten
- Wachtwoordbeleid (wisselen, complexiteit, uniek etc)
- Centrale authenticatie, lokaal minimaal

Logging

- In- en uitloggen
- Niet standaard gedrag (DOS attack bijv.)
- Opstarten van het apparaat
- Activeren en de-activeren van poorten
- Wijzigingen aan de configuratie
- Logging naar centrale server (syslog)

Attack surface verkleinen

- Niet gebruikte poorten uit of in een dood VLAN
- Default dicht, alleen open zetten wat nodig is
- Niet gebruikte functionaliteit uit
- Kabels wegwerken en/of fysiek afschermen
- Fysieke toegang tot device, in het bijzonder console poorten, afschermen
- Geen stickers of andere netwerkinfo op de apparatuur plakken
- DHCP uitzetten voor statische apparatuur
- TLS verbindingen

Onderhoud

- Periodieke firmware updates
- Jaarlijkse audits
- Apparaat tijdig vervangen (meestal 5-8 jaar levensduur) i.v.m. toenemende eisen (technische levensduur kan veel langer zijn)
- Onderhoudsafspraken duidelijker vastleggen.

Privacy

- iVRI's worden onder specifieke omstandigheden als verwerkers van persoonsdata gezien.
- Privacy aspect verhoogt de eisen aan informatiebeveiliging.
- Sla geen gegevens op het apparaat op als dat niet strikt noodzakelijk is. (stuur bijv. de CAM berichten van de weggebruikers dus alleen door naar TLEX/UDAP, VLOG alleen als stream uitsturen etc.)

In het algemeen:

BIO framework is een hoog-over beschrijving. Bovenstaande punten komen voort uit eerdere ervaringen met audits op technische aspecten. De BIO stelt ook eisen aan procedurele aspecten ten aanzien van veilige omgang met referenties en bijvoorbeeld zaken als sleutelbeheer.