

Reactie op aanvullende technische vragen D66 – Raadsvoorstel Vaststellen Beleids- en beheerplan Civiele Kunstwerken 2026-2030

Vraag:

1. Is er een risicoanalyse uitgevoerd specifiek gericht op de potentiële kwetsbaarheden van deze installaties?
2. Welke maatregelen zijn er momenteel getroffen om de cybersecurity van e-installaties in civiele kunstwerken binnen onze gemeente/organisatie te waarborgen?
3. Worden de leveranciers en beheerders van deze installaties getoetst op hun cybersecurity expertise en maatregelen?

Antwoord:

Vitale infrastructuur zijn volgens de wet verplicht om de digitale weerbaarheid te verhogen. Voor overheidsinstanties is dit vastgelegd in de BIO, die steeds vaker wordt aangevuld met de IEC 62443.

Dit is de internationale standaard voor cybersecurity binnen Industrial Automation en deze geeft een praktische invulling aan digitale beveiliging tegen cyberaanvallen. Onze leveranciers van de hard-, software bij de beweegbare civiele kunstwerken werkt volgens beide en heeft hiervoor een gecertificeerd consultant in huis en zij informeren gebruikers over beveiligingslekken en -incidenten en de daarmee gepaarde oplossing.

Onderstaand een opsomming van de Cybersecurity-features systemen zoals die door de leverancier van de hard-, software worden toegepast.

- Voorzien van ingebouwde firewall
- Toegangsbeveiliging
- DoS (Denial of Service)
- Data Encryption
- OpenVPN
- Syslog
- Brut Force Protection
- Secure communicatie (OPC UA, DNP3-secure, IEC 60870-5-104-secure)
- Best Practise Guideline
- Security Response Center (adviezen, updates, e-mailnotificaties)

Vraag 4.

Is er budget gereserveerd voor het verbeteren van de cybersecurity van deze kunstwerken in de toekomst indien nodig?

Antwoord:

De eisen over onder andere de cybersecurity worden beschreven bij de aanbestedingen die eens in de vier jaar wordt gedaan. De inschrijvers berekenen dit dan ook door bij hun inschrijfprijs.

Financieel is dit bij inkoop van de betreffende hardware en software dus al afgedekt in de begroting.