Basismaatregelen voor cybersecurity van industriële automatisering & control systems (BIACS)

Handvatten voor digitale weerbaarheid essentiële installaties

Veel organisaties maken in hun installaties gebruik van industriële automatisering of andere gebouwgebonden besturingssystemen voor het aansturen van hun primaire processen. De weg- en waterinfrasector is daar geen uitzondering op. Dergelijke systemen zijn echter lang niet altijd goed beveiligd tegen cybercriminaliteit. Reden voor het ministerie van Infrastructuur en Waterstaat (IenW) om Hudson Cybertec te vragen een basiskader op te stellen, aan de hand waarvan organisaties hun cyberveiligheid op een gestructureerde wijze kunnen vormgeven. Dit resulteerde in de Basismaatregelen voor cybersecurity van industriële automatisering & control systems (BIACS).

De samenwerking tussen IenW en Hudson Cybertec dateert al van een aantal jaar geleden. “In 2019 hebben we voor Rijkswaterstaat de Cyber Security Implementatie Richtlijn (CSIR) geactualiseerd. Dit in lijn met de geldende normenkaders waar Rijkswaterstaat aan moest voldoen. Van daaruit is bij IenW de vraag ontstaan om ondersteuning bij het opstellen van een basiskader voor partijen voor wie bestaande richtlijnen rond cyberveiligheid nog een brug te ver zijn”, aldus Michael Theuerzeit, lead consultant bij Hudson Cybertec in Den Haag. Het bedrijf is onderdeel van de Kiwa groep, een Nederlandse test-, inspectie- en certificeringsspecialist die wereldwijd actief is en circa 12.000 medewerkers telt.

Grotere reikwijdte

Hudson Cybertec, opgericht in 2012, is geworteld in de operationele technologie (OT) en OT-security is dan ook de core business van het bedrijf. “De markt ziet ons als subject matter expert als het gaat om de IEC 62443, het internationale normenkader voor cybersecurity rond industriële automatisering en control systems (IACS) en OT-security”, vertelt Theuerzeit. “Cybersecurity is booming, ook gezien de nieuwe Europese richtlijn NIS2 (Network and Information Security directive, red.), die volgend jaar van kracht wordt, en de nationale wetgeving die hieruit zal voortvloeien. Daar moeten bedrijven wat mee, want in vergelijking met de NIS vallen straks duizenden in plaats van tientallen bedrijven binnen de scope van deze richtlijn.”

Breed toepassingsgebied

IACS is van toepassing op een breed scala aan organisaties, uiteenlopend van een nucleaire faciliteit tot een koekjesfabriek. “Zowel asset owners als leveranciers van PLC’s, sensoren, actuatoren en DCS-systemen om processen te volgen, te sturen en te controleren, dienen aantoonbaar cybersecure te zijn. Kijkend naar de weg- en waterinfra valt bijvoorbeeld te denken aan tunnelbeheersystemen, gemalen en afvalwaterzuiveringsinstallaties, maar ook aan wegkantsystemen en verkeerslichtinstallaties”, schetst Theuerzeit. Onder de NIS2 wordt de range aan bedrijven die aantoonbaar in control moeten zijn op dit gebied uitgebreid. “In lijn met die nieuwe Europese richtlijn wordt momenteel ook de Wet beveiliging netwerk- en informatiesystemen (Wbni) aangepast.”

Fysieke consequenties

Door incidenten met cryptolockers, malware en hackers zijn steeds meer organisaties doordrongen van het belang serieus werk te maken van de cybersecurity van hun operationele, c.q. gebouwgebonden systemen die op het netwerk zijn aangesloten. “Want als er iets met de OT gebeurt, kan dit onmiddellijk fysieke consequenties hebben: een brug die niet meer beweegbaar is, een pompinstallatie die niet meer werkt, wegkantsystemen of verkeersregelinstallaties die uitvallen of een tunnelbuis die ineens dichtgaat”, stelt Theuerzeit. “Om organisaties te helpen hun cyberveiligheid op een gestructureerde wijze vorm te geven, hebben we daarom in opdracht van IenW de BIACS opgesteld.”

Moeilijk tastbaar

Doel van de BIACS is organisaties in staat te stellen de juiste basismaatregelen te nemen om hun cyberweerbaarheid omhoog te brengen. De focus ligt daarbij op organisaties waarvoor voldoen aan andere normen, zoals IEC 62443 of CSIR, nog een brug te ver is. Theuerzeit: “Niet elke norm is voor elke organisatie geschikt en bestaande normen zijn soms voor organisaties moeilijk tastbaar te maken. Denk aan kleinere gemeenten, die immers ook verkeersregelinstallaties hebben staan en eveneens bruggen in beheer hebben. Dan kan dit kader met basismaatregelen handvatten bieden, ook voor bijvoorbeeld provincies, het mkb en de maakindustrie.”

> “Als er iets met de OT gebeurt, kan dit onmiddellijk fysieke consequenties hebben: een brug die niet meer beweegbaar is, een pompinstallatie die niet meer werkt, wegkantsystemen of verkeersregelinstallaties die uitvallen of een tunnelbuis die ineens dichtgaat”

Michael Theuerzeit van Hudson Cybertec over het belang van cybersecurity. (Foto: Hudson Cybertec)

‘Een grove verdeling is: 50% mens, 30% beleid en 20% techniek’

Drie pijlers

Bij de BIACS gaat Hudson Cybertec uit van drie pijlers – mens, organisatie en techniek – vervat in tien thema’s. “Met technische maatregelen alleen ben je er niet, er zijn altijd aanvullende organisatorische maatregelen nodig. En de factor mens is heel belangrijk. Een grove verdeling is: 50% mens, 30% beleid en 20% techniek. Als je alleen technische maatregelen neemt, heb je dus een blinde vlek van 80% waar het gaat om mens en beleid. Doordat de BIACS alle belangrijke thema’s op het vlak van mens, beleid en techniek benoemt, vergeet je niets.”

Nulmeting

Op basis van jarenlange kennis en ervaring inzake cybersecurity – en als auteur van de BIACS – adviseert Hudson Cybertec organisaties over de implementatie van dit normenkader dan wel van de CSIR, de IEC 62443 en andere, meer sectorspecifieke normen. “Doel is steeds hun digitale weerbaarheid te verbeteren. Hiervoor doen we vaak eerst een nulmeting om te inventariseren hoe een bedrijf ervoor staat. Vervolgens kijken we wat er moet gebeuren om een minimumniveau van cybersecurity te bereiken”, zegt Theuerzeit. “Daarna helpen we organisaties een implementatieplan op te stellen op basis van de gebruikte norm.”

Noodzakelijke investering

Tot slot wijst de consultant nogmaals op het belang van cybersecurity voor organisaties. “In feite is het net als met een brandblusinstallatie: je hoopt deze nooit nodig te hebben, maar noodzakelijk is zo’n installatie wel. Cybersecurity is minder tastbaar, maar bedenk dat het net zo lang goed gaat tot het een keer fout gaat. Dus investeer in cyberveiligheid en voorkom dat je operationele installaties doelwit worden en wellicht wekenlang uit de running zijn.”

Meer informaite

www.hudsoncybertec.com