

PA Roadmap

Project PA BIO logisch

Aanleiding voor de PA Roadmap

In het kader van het verbeteren van de cybersecurity van de procesautomatisering (PA) is onder regie van het project PA BIO logisch, eind 2021 een Technische Assessment op het PA-domein uitgevoerd door Hudson Cybertec. De resultaten hiervan zijn onder meer in november 2021 gedeeld met de commissie BFO en de VV.

De belangrijkste aanbeveling van Hudson was:

1. Het aanbrengen van fysieke scheiding tussen de KA en PA;
2. Het dieper segmenteren van de PA.

Voor beide aanbevelingen geldt, dat het gegeven advies nog veel ruimte laat voor de wijze van uitvoering. Daarom is er ervoor gekozen (zie memo aan Commissie BFO en VV) een *detail* PA Roadmap te maken en ook een ontwerp van de wijze waarop de diepere segmentering van de PA moet plaatsvinden. Dit is het zogenaamde '*zone en conduit model*', dit is in lijn met Waterschapsbrede architectuur afspraken en de zogenaamde IEC62443 norm (een meer specifieke invulling van de BIO voor PA).

Huidige stand van zaken

Inmiddels is de PA Roadmap en het *zone en conduit model* afgerond en is de implementatie hiervan gestart. Het ontwikkelen van de roadmap heeft plaatsgevonden in de eerste helft van dit jaar en is uitgevoerd door bureau Kienia in samenwerking met Delfland experts.

Om de adviezen van Hudson Cybertec te implementeren op een wijze die past bij Delfland is een afweging gemaakt tussen:

- Het belang van een object voor het primair proces;
- In welke mate de security risico's gemitigeerd moeten worden, hiervoor is een risicoanalyse gemaakt met als uitgangspunt de risicomatrix van Delfland;
- De kosten van implementatie van een maatregel.

In de PA Roadmap worden vijf plateaus onderscheiden. Met de implementatie van de maatregelen per plateau, verbetert de cybersecurity van de PA. Voor het eerste plateau is een detail Projectplan gemaakt, de uitvoering daarvan is inmiddels gestart.

Inhoud van de PA Roadmap

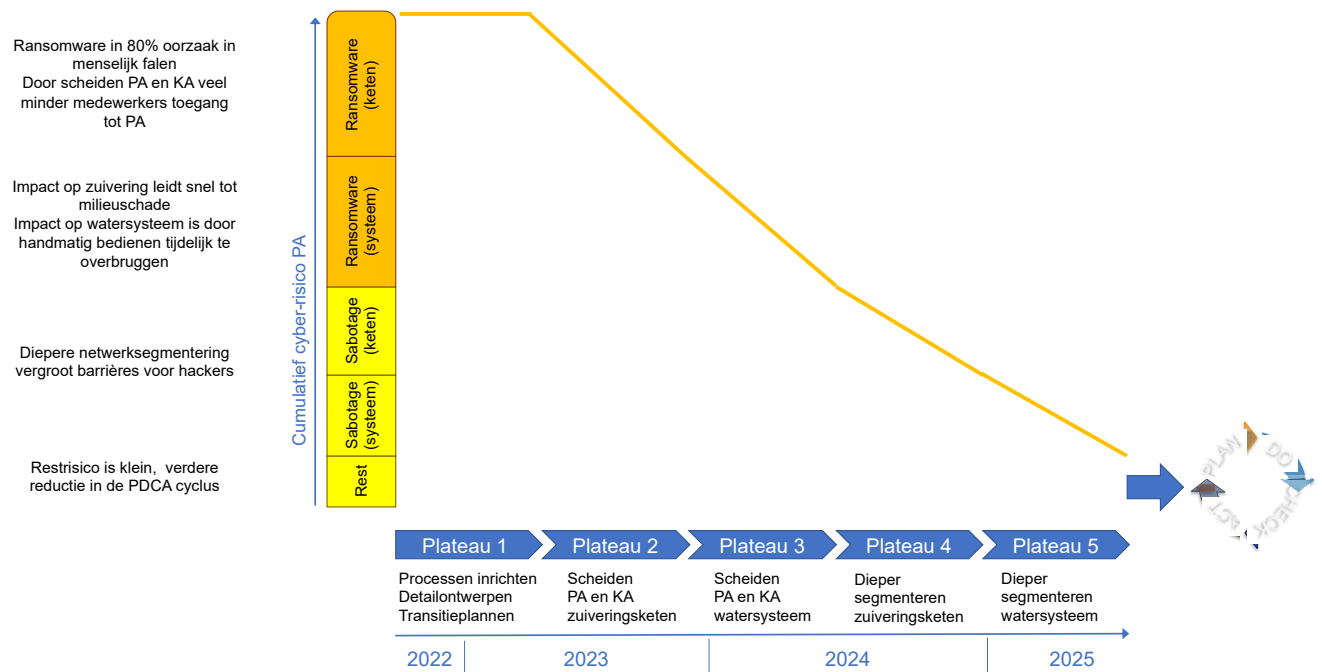
De PA Roadmap heeft drie essentiële onderdelen:

- A. De *scheiding* van het PA- en KA-verkeer op de zogenaamde *backbone* tussen de locaties van Delfland, door het aanbrengen van gescheiden netwerkdiensten tussen deze locaties. Het niveau van scheiding komt overeen met het niveau van scheiding dat door netwerk serviceproviders (zoals bijvoorbeeld KPN, Vodafone, etc.) wordt gehanteerd om verkeer van verschillende klanten te scheiden. Dit is voldoende veilig gezien het risicoprofiel van Delfland.
- B. Het *ontvlechten* van PA en KA (computer)systemen en services, zodat in geval een cyberdreiging de PA autonoom door kan blijven draaien, ook al is de KA uitgevallen.

- C. De diepere *segmentering* in het PA-domein (volgens het *zone en conduit model*), waardoor wordt bereikt dat een cyberincident binnen de PA zich niet zomaar over het gehele areaal van Delfland kan verspreiden. De opdeling die daarbij gemaakt wordt zorgt ervoor dat er logische functionele eenheden ontstaan, die in 'eilandbedrijf' door kunnen blijven functioneren. Daarnaast worden door een hiërarchische architectuur de meest kritieke besturingsfuncties op de grootst mogelijk afstand geplaatst van het Internet.

Risico Afweging

Zoals gezegd is de PA Roadmap ingedeeld in vijf plateaus. Per plateau verbetert de cybersecurity. Dat is in de onderstaande figuur te zien. Deze figuur is een illustratie, omdat de schalen van de HDD-risicomatrix (Ernst categorie: Zeer Klein, Klein, Matig, Behoorlijk, Ernstig, Extreem) niet lineair (eerder logaritmisch) zijn. De risico's in de PA zijn daarvan afgeleid en kunnen daarom niet in een zuiver meetbare schaal worden geplaatst. De illustratie is door experts gevalideerd ('*expert opinion*').



Figuur 1: Risicoverlaging door netwerkscheiding en -segmentering & Planning per plateau

Veruit de grootste veiligheidswinst voor de PA-systemen is te behalen door de *scheiding* van PA en KA. Het grootste risico dat Delfland nu loopt is uitval van systemen door *ransomware*. In ca. 80% van de gevallen blijkt (onbewust) onveilig gedrag van medewerkers bepalend. Door de scheiding van PA en KA wordt het aantal medewerkers met toegang tot PA beperkt, waardoor de kans op ransomware op de PA-systemen afneemt.

De diepere *segmentering* binnen de PA verhoogt het aantal barrières die een hacker moet overwinnen voor hij op afstand een besturings- of bewakingssysteem in de PA kan bereiken. Dit verlaagt de kans op sabotage van de waterveiligheid of -kwaliteit.

Daarom wordt qua volgorde, in plateau 1, 2 en 3 de focus gelegd op het realiseren van de *scheiding* van de PA en KA. En volgt de diepere *segmentering* in plateau 4 en 5.

De waterketen wordt als eerste geïmplementeerd, omdat daar de impact van een cyber-incident minder makkelijk is op te vangen door handmatige bediening. In het watersysteem is dit makkelijker. De impact op het watersysteem uit zich vooral in financiële schade doordat langere tijd meer mensen ingezet moeten worden voor handmatige bediening en reparatie van getroffen systemen. Bij de waterketen is ook milieuschade te verwachten door overstort van vuil water.

Figuur 1 hierboven illustreert de risicoverlaging en geeft per plateau ook de planning in de tijd aan.

Bij de afronding van ieder plateau en voor de start van ieder volgend plateau, zal een herijking plaatsvinden. Dit is nodig, omdat gedurende de looptijd situaties, dreigingen en risico's kunnen veranderen, waardoor bijsturing nodig is. Een voorbeeld hiervan zou kunnen zijn, dat de plannen rondom de vernieuwing van AWZI De Grote Lucht conflicteren met de werkzaamheden in plateau 4. Een aanpassing zou dan kunnen zijn om plateau 4 en 5 in de tijd te verwisselen of om de scope van plateau 4 te beperken tot de zuiveringskring van de Nieuwe Waterweg.

Kosten

In onderstaande tabel zijn de kosten per jaar voor de implementatie van de PA Roadmap te zien. De totale kosten voor de vijf plateaus bedragen euro 1,1 miljoen. Daarbovenop komt de inzet van interne capaciteit van Delfland, die uren zijn niet in euro's vertaald.

	2022	2023	2024	2025
Kosten PA Roadmap	110k€	425k€	365k€	195k€

Het budget voor de kosten is opgenomen in de Kadernota 2023 en zal tevens worden opgenomen in de Begroting 2023 en de Meerjarenraming 2024-2027.

26 augustus 2022

Jaap den Haan

Afdelingsmanager Onderhoud Technische Installaties & Procesautomatisering