-Vertrouwelijk-

Hoogheemraadschap van Delfland

Samenvatting validatie
Versterking Informatiebeveiliging
Week 34/2022

HUDSON CYBERTEC
Cyber Security - Technical Automation

Contactgegevens:

Hoogheemraadschap van Delfland

Phoenixstraat 32
2611 AL Delft

Mevrouw Jolanda Riel

Hudson Cybertec

Laan van ’s-Gravenmade 74
2495 AJ Den Haag

De heer Marcel Jutte

Opleverdatum: 30 augustus 2022

Inhoud

1 Introductie

1.1 Vraagstelling Hoogheemraadschap van Delfland

Het Hoogheemraadschap van Delfland (hierna te noemen Delfland) heeft een pentest laten uitvoeren. Er is een pentest rapport, een Advies verbeterpunten en een Plan van Aanpak opgeleverd. In december 2020 heeft Delfland aan Hudson Cybertec gevraagd de acties van het project, zoals gedefinieerd in het Plan van Aanpak, te valideren.

Het plan is opgedeeld in fasen. Eind februari 2021 is fase 1 afgerond en heeft Hudson Cybertec een eindrapport opgeleverd. In het eindrapport stonden restpunten die in de periode tot 19 april 2021 zijn opgelost en door Hudson Cybertec gevalideerd.

Half mei 2021 is het Plan van Aanpak Versterking Informatiebeveiliging (VIB) gepresenteerd en is Hudson Cybertec gevraagd ook de uitvoering van dit plan te valideren.

1.2 Doel

Dit dashboard heeft tot doel inzicht te geven in de kwaliteit en volledigheid waarmee binnen het project het Plan van Aanpak wordt uitgevoerd en of het doel van het project, i.c. het verminderen van risico's, daadwerkelijk wordt bereikt.

1.3 Scope

Dit validatierapport heeft betrekking op het project "Versterking Informatiebeveiliging", tot en met week 34 (24 augustus) van 2022.

1.4 Totstandkoming van dit document

Dit rapport is tot stand gekomen op basis van de beschikbare informatie die via email en Teams van Delfland is verstrekt en (telefonische) interviews met projectmedewerkers. De validatie is uitgevoerd door Hudson Cybertec, met uitzondering van de validatie van deelproject 8. Dit deelproject is uitgevoerd door Hudson Cybertec en gevalideerd door VKA.

2 Dashboard week 34/2022

Onderdeel	Opzet	Bestaan	Werking
Deelproject 1: Afronding Fase			
Deelproject 2: Segmentatie (KA)			
Deelproject 3: Vulnerability management			
Deelproject 4: Privileged Access Management (PAM II)			
Deelproject 5: Logging en monitoring			
Deelproject 6: Organisatie	Wordt niet gevalideerd		
Deelproject 7: Netwerkscheiding KA/PA			
Deelproject 8: Netwerkmonitoring van de PA-omgeving			
Deelproject 9: Opdracht advies technische security PA	Wordt niet gevalideerd		
deelproject 10.1: PA VMware platform			
Deelproject 10.2: PA-KA Werkplekscheiding			
Deelproject 10.3: MAC filtering op routers			
Deelproject 10.4: Patchmanagement			
Deelproject 10.5: Calamiteitscenario Cyber Security Incident	Wordt niet gevalideerd		
Deelproject 10.6: Logging en monitoring II			
Deelproject 10.7: Aanbesteding SOC en CERT	Wordt niet gevalideerd		

Kleurcodes:

- groen is ‘ok en gereed’.
- oranje is ‘nog niet gereed’;
- wit is ‘nog niet gereed of niet beoordeeld’.

De werkprocessen van de deelprojecten 2, 3, 4, 5, 7, 8 10.1, 10.2, 10.3, 10.4 en 10.6 maken formeel onderdeel uit van deelproject 6. De werkprocessen beschrijven het gebruik en beheer van het projectresultaat door de staande organisatie. Validatie van de processen is echter toegelicht onder het betreffende deelproject.

Deelproject 8 is door een andere validator beoordeeld, waarbij andere criteria zijn gehanteerd, dan bij de overige validaties. De validator van deelproject 8 heeft bijvoorbeeld de opzet als ‘nog niet gereed’ beoordeeld, terwijl de ontwerpen op advies van de Design Authority (DA) in de stuurgroep zijn goedgekeurd. De validatie van deelproject 8 is opgeleverd op 13 juli en geeft de status weer tot week 28. Het systeem is operationeel, maar nog niet formeel opgeleverd.

3 Risico

Het project heeft een groot deel van de cybersecurity risico's weggenomen, maar er blijven nog substantiële risico's over. In dit hoofdstuk zijn observaties opgenomen die betrekking hebben op het resterende cybersecurity risico.

3.1 Situatie ten opzichte van de start van het project

In het "Advies verbeterpunten netwerkinfrastructuur Hoogheemraadschap Delfland" van 13 november 2020 zijn drie problemen beschreven.

1. **Vulnerabilities** 🟡

   In het advies werd geconstateerd dat er veel oude, kwetsbare, software werd gebruikt en dat security-patches ontbraken. In fase 1 zijn veel van deze vulnerabilities opgelost. In fase 2 is een structureel proces ingericht. Delfland heeft door de implementatie van een eigen vulnerability scanner continu inzicht in de vulnerabilities. De cijfers laten nog steeds een groot aantal 'critical' vulnerabilities zien. Dit komt met name door de aanwezigheid van verouderde software.

2. **Accounts** 🔴

   In het advies werd geconstateerd dat accounts zwakke wachtwoorden hadden en dat (te) veel medewerkers toegang hadden tot (te) veel accounts met verhoogde rechten. In fase 1 zijn de wachtwoorden vervangen door sterke wachtwoorden en is een deel van de accounts met verhoogde rechten opgeruimd. Het aantal "domain admin" accounts blijft echter toenemen (nu 78, op 10 september 2021 waren het er nog 34, Microsoft adviseert "zo weinig mogelijk"). In fase 2 was het beoogde doel van deelproject 4 (privileged access management) het verder beperken van het gebruik van accounts met verhoogde rechten. Dit doel is nog niet bereikt, omdat deelproject 4 niet is afgerond.

3. **Netwerk** 🔴

   In het advies werd geconstateerd dat het netwerk onvoldoende is gesegmenteerd en dat er geen beperkingen waren op aan te sluiten apparaten. Dit laatste punt is grotendeels opgelost, maar van segmentatie is nog geen sprake. De Kantoorautomatiseringswerkplekken (KA werkplekken) zijn ondergebracht in een eigen segment, waardoor deze geen toegang meer hebben tot de Procesautomatiseringsomgeving (PA). Er zijn echter nog 150 werkplekken die wel toegang hebben tot PA, het ontwerp is niet formeel goedgekeurd en de werkprocessen zijn niet vastgesteld. Binnen de PA is geen netwerksegmentatie aangebracht.