Managementsamenvatting validatie Versterking Informatiebeveiliging

Week 23/2022

HUDSON CYBERTEC
Cyber Security - Technical Automation

Hudson Cybertec
Laan van 's-Gravenmade 74
2495 AJ Den Haag

www.hudsoncybertec.com
info@hudsoncybertec.com
tel.: 070-2500717

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: 15 juni 2022

1 Managementsamenvatting validatie

1.1 Introductie

Het Hoogheemraadschap van Delfland (hierna te noemen Delfland) heeft in 2020 een pentest laten uitvoeren. Er is een pentest rapport, een Advies verbeterpunten en een Plan van Aanpak opgeleverd. Het aanbrengen van de verbeteringen is projectmatig aangepakt. Hudson Cybertec is gevraagd de uitvoering te valideren.

Deze samenvatting 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. Dit document heeft betrekking op het project "Versterking Informatiebeveiliging", tot en met week 23 (10 juni) van 2022. En is tot stand gekomen op basis van de beschikbare informatie die via email en Teams van Delfland is verstrekt en (telefonische) interviews met projectmedewerkers.

1.2 Dashboard week 23/2022

Onderstaande tabel geeft aan welke onderdelen van het project "Versterking Informatiebeveiliging" zijn gevalideerd (groen). Gevalideerd wil zeggen dat de kwaliteit van uitvoering van het deelproject is gecontroleerd en als voldoende is beoordeeld, en dat het beoogde resultaat is gerealiseerd. Deelprojecten 6, 9 en 10.7 worden niet gevalideerd.

Onderdeel	Opzet	Bestaan	Werking
Deelproject 1: Afronding Fase 1			
Deelproject 2: Segmentatie (KA)			
Deelproject 3: Vulnerability management			
Deelproject 4: Privileged Access Management (PAM II)			
Deelproject 5: Logging en monitoring			
Deelproject 6: Organisatie			
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		

1.3 Stand van zaken

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

1. **Vulnerabilities (kwetsbaarheden)**
   In het advies werd geconstateerd dat er veel oude, kwetsbare, software werd gebruikt en dat security-patches ontbraken. Het project heeft een structureel proces ingericht om vulnerabilities op te lossen. Delfland heeft door de implementatie van een eigen vulnerability scanner continu inzicht in de vulnerabilities. Het oplossen daarvan is deels geautomatiseerd. 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. Wachtwoorden zijn vervangen door sterke wachtwoorden. Het deelproject om beheer-accounts met verhoogde rechten te beheren met een software-tool is nog niet afgerond. Het aantal "domain admin" accounts (accounts met alle rechten) is nog hoog.
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 en Delfland voldoet nog niet aan de eigen richtlijn. Er is onvoldoende segmentatie in de kantoorautomatiseringsomgeving (KA), geen segmentatie in de procesautomatiseringsomgeving (PA) en er is geen scheiding tussen KA en PA.

Naast de onderwerpen uit het advies verbeterpunten speelt er nog een aantal problemen:

1. **Off-line back-up**
   Een off-line back-up is een back-up die niet is gekoppeld aan het netwerk, waardoor deze back-up onbereikbaar blijft voor een aanvaller ("hacker") die zich in het netwerk bevindt. Op dit moment heeft Delfland geen off-line back-up en bestaat de kans dat een aanvaller de back-up onbruikbaar maakt in geval van, bijvoorbeeld, een ransomware-aanval. Het traject om off-line back-ups te realiseren is opgepakt door het project en verkeert in een afrondende fase.
2. **Gereed zijn voor eventuele calamiteit**
   Het project heeft onderkend dat er onvoldoende voorbereiding is op problemen. Er is daarom een deelproject toegevoegd om een calamiteitenplan op te stellen. Daarnaast is een deelproject toegevoegd om afspraken te maken met leveranciers die in geval van een calamiteit (een "hack") Delfland kunnen helpen bij het herstellen van de bedrijfsprocessen.

Een belangrijke verbetering die is gerealiseerd is de inrichting van het Security Operation Center (SOC). Het SOC heeft verschillende monitoring-systemen tot zijn beschikking en is hierdoor in staat om problemen snel te detecteren en in te grijpen. Het SOC meet en rapporteert daarnaast de status van cybersecurity.