Hoogheemraadschap van Delfland

Aan:
De leden van de verenigde vergadering

ONS KENMERK
2084401
DELFT
26 april 2022

Onderwerp: Voortgang Informatiebeveiliging

Geachte leden,

Volgens afspraak spreken wij met u over de versterking van de informatiebeveiliging in openbare beraadslagingen en informeren wij u daartoe via een brief. In de vergadering van uw commissie BFO van 22 februari 2021 bespraken wij met u de stand van zaken per 8 februari 2022. Met deze brief informeren wij u over de stand van zaken van het project Versterking Informatiebeveiliging (VIB) per 26 april 2022.

Algemeen beeld

De algehele voortgang op het totale VIB-project is per saldo op hoofdlijnen als volgt. Het oorspronkelijke plan van het project bestond uit negen deelprojecten. Behoudens formele acceptaties zijn zeven van die negen deelprojecten afgerond. De deelprojecten Privileged accesmanagement (PAM) en monitoring van de procesautomatisering (PA-monitoring) hebben extra vertraging opgelopen en zullen in juni operationeel zijn.

Daarnaast zijn aan de scope van het VIB-project gedurende fase 2 zeven deelprojecten toegevoegd. Dit betrof enkele projecten ter aanvulling op de oorspronkelijk geplande projecten, zoals de scheiding van werkplekken voor kantoorautomatisering en procesautomatisering (KA-PA werkplekscheiding), alsmede projecten op het gebied van reguliere beheer- en onderhoudstaken, die worden overgenomen door de eigen organisatie. De laatste projecten behoren daarmee feitelijk tot de volgende fase van de versterking van de informatiebeveiliging, namelijk de fase waarin de reguliere organisatie de informatiebeveiligingswerkzaamheden zelfstandig gaat uitvoeren. Behoudens formele acceptaties is één van de zeven aanvullende deelprojecten afgerond. Vier deelprojecten zitten in de realisatiefase en zullen allen in juni gereed zijn. Twee deelprojecten zitten nog in de planfase.

Doordat nog niet alle projecten zijn afgerond kan in uw commissie van 10 mei 2022 nog geen definitieve afronding van het VIB-project fase 2 worden gerapporteerd. Wij plannen om dit in de commissie van 21 juni 2022 plaats te laten vinden. We plannen dan tevens aan u een validatie-eindrapport voor het gehele VIB-project voor te leggen, mogelijk met uitzondering van de eindvalidatie van het deelproject PA-Monitoring. Omdat het deelproject PA-monitoring wordt uitgevoerd met projectinzet van de huidige validator, moet voor de validatie een derde onafhankelijke partij worden gecontracteerd. Dat lukt waarschijnlijk niet vóór de deadline van vergaderstukken voor de commissie in juni. Dit betekent dat u dit rapport in dat geval pas enkele dagen voorafgaand aan uw vergadering ontvangt.

Nog niet afgeronde projecten

Planningsonzekerheden blijven ons parten spelen en zijn ook niet volledig uit te sluiten ondanks de onverminderd enorm grote inzet van medewerkers. Immers wij blijven prioriteren op de aanpak van de grootste risico's ook als dat tot vertraging leidt van de realisatie van oorspronkelijke mijlpalen. Daarnaast is dit werk verre van routinematig en gaat dus niet alles de eerste keer helemaal goed. Ook blijven wij afhankelijk van leveringsprestaties van onze leveranciers.

In onze brief van 8 februari 2022 hebben wij gemeld dat als gevolg van het Log4Shell beveiligingslek van eind 2021 vertraging was opgelopen in het VIB-project. De nog niet afgeronde projecten zouden ongeveer 1 maand later afgerond worden dan eerder was afgegeven: begin april in plaats van eind februari. Dit betrof de deelprojecten PAM, PA-monitoring en KA-PA werkplekscheiding. Naar aanleiding van het Log4Shell beveiligingslek waren diverse extra maatregelen uitgevoerd om de informatiebeveiliging op een hoger niveau te brengen, zoals beveiliging tegen DDOS-aanvallen, Intrusion Detection op de Firewall, uitbreiding van het aantal virusscanners en de inrichting van een Computer Emergency Respons Team (CERT). Door deze extra maatregelen was het risico van de vertraging van de deelprojecten beheersbaar. Het beveiligingslek zelf kon dankzij de investeringen in de informatiebeveiliging van het afgelopen jaar effectief worden geadresseerd en we konden concluderen dat de Log4Shell-dreiging onder controle is.

Sinds 8 februari is bij de genoemde drie deelprojecten extra vertraging opgetreden. Het risico van deze extra vertraging is nog steeds beheersbaar. Bij PAM kwam de extra vertraging door latere levering van software dan voorzien. In plaats van begin april zal dit project in mei operationeel zijn. Bij PA-monitoring is een fout in het ontwerp gemaakt. Deze fout is medio februari in de implementatiefase ontdekt en heeft geleid tot extra vertraging. De fout is hersteld en het project zal in mei alsnog afgerond worden. Het aanvullende project KA-PA werkplekscheiding kon niet worden uitgevoerd door een tussenkomende update van de basis-werkplekomgeving. De update was nodig vanwege een nieuwe Windows-versie en noopte tot een versnelde vernieuwing, met de bijbehorende testinspanningen om vast te stellen of alle applicaties onder de nieuwe Windows-versie werken. De vernieuwing wordt in mei afgerond, waarna de KA-PA werkplekscheiding op basis van de nieuwe basis-werkplekomgeving in de maand juni alsnog wordt uitgevoerd.

Security operations center en CERT partner

Wij dringen bij collega-waterschappen aan op de inrichting van een gezamenlijk Security Operations Center (SOC) via het Waterschapshuis en het vinden van een gezamenlijke partner ter versterking van het CERT. Zolang deze initiatieven nog niet in werking zijn getreden hebben we zelf maatregelen getroffen. We hebben tijdelijk, met hulp van een externe partner ons eigen SOC ingericht. Dit kan nog niet worden overgedragen aan onze reguliere organisatie. De noodzakelijke personele uitbreiding is daarvoor nog niet gereed. Het tijdelijke contract is daarom verlengd tot eind 2022. Intussen bereiden we ons voor op een aanbesteding voor nog eens 1 jaar, zodat er voldoende ruimte is om de overgang naar een gezamenlijk SOC goed voor te bereiden en te implementeren. Ditzelfde geldt ook voor ons tijdelijke contract met de CERT-partner.

Organisatie en cultuur

Op het gebied van organisatie en cultuur zijn volgens ons plan maatregelen uitgevoerd, gericht op het ICT-team, op de IT-verantwoordelijken in de primaire processen en op de gehele organisatie van Delfland. Het ICT-team wordt door middel van casuïstiek uit het project doorlopend getraind in hun onderlinge samenwerking en bestuurlijke sensitiviteit. Bij de nieuwe, separate afdeling ICT is een vaste coördinator in dienst getreden. Tevens is een vaste afdelingsmanager geworven die medio mei in dienst treedt. Daarmee kan ook de teamontwikkeling goed geborgd worden. Voor de IT-verantwoordelijkheid van de

belangrijkste applicaties in de primaire processen is het eigenaarschap in kaart gebracht en worden de daaraan gestelde eisen vastgelegd en afgesproken. Voor de gehele organisatie zijn de communicatiestrategie en de bewustzijnscampagnes uitgevoerd. Al deze activiteiten zullen ook na mei worden voortgezet.

Procesautomatisering

Op het gebied van de PA is onder de vlag van het project PA BIO*logisch* een technisch assessment uitgevoerd. Dit assessment moet worden opgevolgd door een roadmap voor de verbetering van de PA-beveiliging. Aan deze roadmap wordt momenteel gewerkt. Het streven is deze in het najaar van 2022 gereed te hebben. Intussen wordt het project PA BIO*logisch* voortgezet. We zijn voorbereidingen aan het treffen om hierin nieuwe werkpakketten en projecten onder te brengen die, wanneer deze zullen zijn uitgevoerd, vormgeven aan onze ambities om het volwassenheidsniveau van de PA-organisatie te verhogen. Hiertoe wordt o.a. doorlopend aandacht gegeven aan het vastleggen van de beheer- en beveiligingsprocessen.

Financiën

Voor het traject tot en met december 2021 bedroegen de exploitatiekosten ca. € 1,6 miljoen. De in 2021 niet gemaakte exploitatiekosten voor inhuur zullen in 2022 alsnog worden gemaakt. Deze kosten, alsmede de aanvullende kosten voor de overbrugging tot de structurele formatie-uitbreiding volledig is gerealiseerd, voor de voortzetting van het SOC en voor de implementatie van een CERT, bedragen naar verwachting ca. € 2,4 miljoen. Naar zich nu laat aanzien zal ca. € 2 miljoen daarvan structureel benodigd zijn, dus in de jaren na 2022. Een begrotingswijziging voor 2022 zal aan u worden voorgelegd in de Bestuursrapportage 2022. De begrotingen voor 2023 en verder worden aan u in de Kadernota 2023 en de Begroting 2023 en meerjarenraming 2024-2027 voorgelegd.

De investeringskosten bedroegen tot en met december 2021 ca. € 0,4 miljoen. Voor verdere investeringen in vervanging en uitbreiding van hard- en software ten behoeve van informatiebeveiliging zal jaarlijks ca. € 1,5 miljoen nodig zijn. Concrete investeringsplannen worden in de Bestuursrapportage 2022 of de Begroting 2023 aan u voorgelegd. Wanneer afzonderlijke investeringen niet boven de activeringsgrens van € 0,1 miljoen uitkomen, worden ze in de exploitatie geboekt.
In de investeringsraming van € 1,5 zijn niet de investeringen opgenomen voor de uitbreiding en vervanging van de procesautomatisering. Deze worden in het project PA Bio*logisch* voorbereid en worden t.z.t. afzonderlijk aan u voorgelegd.

Bedragen x 1.000€	2021 INITIELE BEGROTING	2021 BIJGESTELDE BEGROTING	2022	2023
Vast personeel	0	0	700	700
Tijdelijk personeel	0	1.100	1.200	800
Materieel	0	500	500	500
Totaal exploitatie	**0**	**1.600**	**2.400**	**2.000**
Totaal investering	**0**	**400**	**1.500**	**1.500**

Conclusie

Concluderend is volgens de stand van 26 april 2022 de informatiebeveiliging van Delfland in opzet, bestaan en werking op een hoger niveau gebracht. De Cyberweerbaarheid KPI is echter nog steeds ‘zeer kwetsbaar’ omdat detectie nog onvoldoende is en er nog geen offline back-up beschikbaar is. De maatregelen die de komende twee maanden zijn gepland zullen de Cyberweerbaarheid KPI significant verbeteren. De validatie van de gerapporteerde voortgang door de onafhankelijke validator onderschrijft dit beeld.

Ook de BIO/AVG-audit die in januari 2022 is uitgevoerd onderschrijft dit beeld. Recent is het definitieve auditrapport van Delfland beschikbaar gekomen en is de sectorrapportage gepresenteerd. In de audit is gekeken naar opzet en bestaan en in hoeverre er aan niveau 3 van de BIO en de AVG wordt voldaan. Dit is het volwassenheidsniveau waarnaar de sector eind 2021 streefde op weg naar niveau 4, het uiteindelijke ambitieniveau van de sector. In de audit van 2023/2024 wordt ook gekeken naar de werking, en of de waterschappen de gewenste groeistappen hebben gemaakt en daarmee op niveau 4 komen. Waar we bij de vorige landelijke audits nog onder het gemiddelde scoorden, zitten we er nu op of (net) boven.

Qua volwassenheid scoren we gemiddeld nog onder het streefniveau 3 voor eind 2021. Voor de PDCA Informatiebeveiliging en Privacy en de BIO PA wordt door geen enkel waterschap het streefniveau 3 gehaald. Voor de BIO KA en AVG behalen slechts enkele waterschappen het streefniveau. Het samengevat oordeel van de auditor is dan ook dat Delfland goed op weg is en dat er vertrouwen is in de verder te nemen stappen.

In het tweede kwartaal 2022 zullen we een nieuwe interne PEN-test uitvoeren, gevolgd door een externe PEN-test in de maanden daarna. De testen zullen ons helpen om nieuwe of nog bestaande kwetsbaarheden aan te wijzen en daarop aanvullende of nieuwe maatregelen te nemen. Wij zullen u over de uitkomsten op hoofdlijnen informeren.

Zoals wij u al eerder hebben gemeld is informatiebeveiliging naar onze mening nooit af. Ook de validator wijst erop dat enkele projecten nog niet zijn afgerond en dat enkele belangrijke vervolgmaatregelen gewenst zijn, zoals de verdere segmentatie van het KA-netwerk en van de procesautomatisering. De structurele uitbreiding van de capaciteit van de ICT-afdeling en de roadmaps KA en PA realiseren wij in de rest van 2022. Hierin kijken we ook naar de omliggende onderdelen van de IV-keten, zoals de securityorganisatie en de architectuurorganisatie en volgen we de nieuwe technologische ontwikkelingen om deze zo nodig te implementeren bij Delfland.

Ook gedurende 2022 vullen we de bestaande capaciteit aan met tijdelijke externe expertise, om de periode waarin vast personeel nog niet is geworven te overbruggen. Daarnaast blijven wij werken aan de samenwerking met andere waterschappen en met Het Waterschapshuis.

<u>Opheffen geheimhouding</u>

Tenslotte staan wij stil bij de door u gestelde vraag of de geheime documenten, die eerder in de besloten vergaderingen van uw commissie BFO over het onderwerp informatiebeveiliging zijn besproken, openbaar gemaakt kunnen worden.

Op basis van onze analyse en het advies van de validator zijn wij voornemens aan uw Verenigde Vergadering van 2 juni 2022 het voorstel tot opheffing van de geheimhouding voor te leggen. Dit betreft alle stukken die in de besloten BFO-vergaderingen zijn ingebracht in de periode 1 december 2020 tot en met 2 november 2021. In deze documenten zullen enkele teksten die kritisch zijn voor de informatiebeveiliging, zoals de typebenaming van nieuwe servers, of privacygevoelig zijn, zoals de herleidbaarheid naar specifieke functionarissen binnen Delfland, onleesbaar worden gemaakt.

Wij vertrouwen erop u hiermee voor nu voldoende te hebben geïnformeerd.

Hoogachtend,
Dijkgraaf en Hoogheemraden van Delfland,
de Secretaris,

ir. P.C. Janssen

de Dijkgraaf,

dr. P.H.W.M. Daverveldt