STATENBRIEF

PROVINCIE :: UTRECHT

Aan Provinciale Staten

ONDERWERP	Voortgang Informatieveiligheid & Privacy	TELEFOONNUMMER	+31653265024
		E-MAILADRES	remco.ter.heijne@provincie-utrecht.nl
DATUM	26-04-2022		
DOCUMENTNUMMER	8247A28B	DOMEIN/OPGAVE	BDV
VAN	Victor Roos, Stefanie Kelterman, Remco ter Heijne	TEAM	BDV
		PORTEFEUILLEHOUDER	Strijk
NUMMER PS	PS2022BEM30		
COMMISSIE	Bestuur, Economie en Middelen		
BIJLAGEN	1. Jaarrapportage Functionaris voor Gegevensbescherming 2022 2. Samenvatting Rapport van Bevindingen AIB 2021		

Geachte dames en heren,

Essentie / samenvatting
Onlangs zijn twee rapporten opgeleverd die inzicht geven in het volwassenheidsniveau van de organisatie op het gebied van informatieveiligheid en privacy. Dit betreft het rapport Assessment Informatiebeveiliging 2021 opgesteld in opdracht van Concerncontrol en de Jaarrapportage 2021 van de Functionaris voor Gegevensbescherming (FG).

Uit de conclusies van de rapporten wordt bevestigd dat er een duidelijke groei waarneembaar is ten aanzien van de mate waarin de organisatie grip heeft op het onderwerp privacy. Daarentegen blijft de groei in volwassenheid ten aanzien van informatieveiligheid achter. We hadden dit niet verwacht, mede gezien de vele activiteiten die zijn en worden uitgevoerd en de effecten die we daarvan ervaren. Ondanks een duidelijke verbetering van de kennis en bewustwording in de organisatie heeft de inzet die hierop is gepleegd niet geleid tot een *aantoonbaar* hoger volwassenheidsniveau op het gebied van informatieveiligheid.

In deze brief worden de belangrijkste bevindingen en aanbevelingen ten aanzien van informatieveiligheid en privacy beschreven. Daarna is op basis van de managementreactie verwoord welke interventies door de organisatie worden gepleegd om tot de noodzakelijke verdere groei te komen.

Inleiding
Binnen de provincie is ervoor gekozen om de onderwerpen informatieveiligheid en privacy gezamenlijk onder te brengen in het Programma Informatieveiligheid en Privacy (IV&P). De onderwerpen kennen veel overeenkomsten, maar er is ook een belangrijk onderscheid. Daar waar informatieveiligheid zich richt op de beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van alle informatie binnen de provincie, richt privacy zich op de verantwoorde omgang met persoonsgegevens. Daarbinnen worden vragen beantwoord of bijvoorbeeld een uitwisseling van persoonsgegevens met een derde partij wel past binnen het takenpakket van de provincie. Of dat voor een bepaalde taak niet meer dan de noodzakelijke gegevens worden gebruikt. Het gaat doorgaans om de bescherming van medewerkersgegevens en gegevens van burgers en passanten (wanneer er bijvoorbeeld camera's worden geplaatst in de openbare ruimte). Privacy kent daarmee meer een juridische insteek, bij informatieveiligheid ligt meer nadruk op de techniek.

Volwassenheidsniveau's
Er worden vijf volwassenheidsniveaus onderscheiden waarop organisaties informatieveiligheid en privacy hebben ingebed in hun processen. Dit varieert grofweg van geen of versnipperde aandacht voor informatieveiligheid en privacy, tot perfecte organisatiebrede beheersing en benutting van informatieveiligheid en privacybescherming. Voor de provincie Utrecht is bepaald dat volwassenheidsniveau drie voor beide onderwerpen passend is gezien het type organisatie en de gegevensverwerking die hier plaatsvindt. Dit niveau is doorgaans voldoende om te voldoen aan de wetgeving op beide gebieden. Hieronder zijn de verschillende niveaus en hun kenmerken schematisch weergegeven:

De provincie Utrecht heeft zich tot doel gesteld op het gebied van privacy te groeien naar volwassenheidsniveau drie. Op het gebied van informatieveiligheid is gesteld eerst toe te groeien naar volwassenheidsniveau twee, en daarna door te groeien naar niveau drie. Dit omdat deze groei ten aanzien van informatieveiligheid meer met zich meebrengt dan bij privacy.

Privacy
De Functionaris voor Gegevensbescherming stelt jaarlijks een rapportage op. Deze bestaat uit twee delen:

- een overall beeld van het volwassenheidsniveau van de organisatie op het gebied van privacy, gebaseerd op het volwassenheidsmodel van het Centrum Informatiebeveiliging en Privacy (CIP).
- Inzicht in de mate waarin privacy geland is binnen de organisatie, naar aanleiding van een uitvraag aan de individuele teamleiders.

De bevindingen uit bijgaande FG-jaarrapportage maken duidelijk dat het gewenste volwassenheidsniveau drie nog niet over de hele linie is bereikt, maar dat er duidelijk zichtbaar een sterke positieve ontwikkeling plaatsvindt. De grootste uitdagingen liggen kort gezegd op de informatie-uitwisseling tussen de teams enerzijds en de privacy officers anderzijds, een risico gerichte benadering van privacy, vroegtijdige betrokkenheid van privacy bij nieuwe ontwikkelingen en op het gebied van informatiebeveiliging.

Incidenten
In 2021 hebben enkele incidenten plaatsgehad. Dat betroffen 'gangbare datalekken', zoals het verzenden van een e-mail naar een verkeerde adressant en verlies of diefstal van een laptop, maar ook incidenten met een groter risico voor de bescherming van de persoonsgegevens. Deze incidenten zagen op de wereldwijde kritieke kwetsbaarheid in Apache Log4j en een verkeerd gebruik van Sharepoint, waardoor gevoelige informatie in te zien was voor meer medewerkers dan bedoeld. Deze incidenten kunnen schadelijk zijn, maar geven ook veel inzicht in zwakheden binnen de werkprocessen, waardoor hier prioriteit aan gegeven kan worden. Ieder incident is daarmee een leerpunt.

Netwerk contactpersonen
Ten slotte is een belangrijke ontwikkeling dat er in 2021 gebouwd is aan een intern ambtelijk netwerk van contactpersonen informatieveiligheid en privacy. Zij zijn in de organisatie extra ogen en oren om knelpunten te melden en extra monden om tips en aanwijzingen binnen de organisatie te verspreiden.

Informatieveiligheid
In lijn met de afspraak in het convenant Interprovinciale Regulering Informatieveiligheid over verantwoording, heeft de eenheid Concerncontrol het assessment informatiebeveiliging gedurende september – december 2021 voor de vierde keer uitgevoerd, bijgestaan door een externe auditor. Het assessment geeft inzicht in het informatiebeveiligingsniveau en de implementatiestatus van het beleid informatiebeveiliging bij de provincie Utrecht. De bevindingen en aanbevelingen zijn hieronder samengevat. De uitwerking hiervan is opgenomen in de bijlage 'Samenvatting Rapport van bevindingen assessment informatiebeveiliging 2021'.

In de afgelopen twee jaar heeft de organisatie de aanpak van informatiebeveiliging en privacy ondergebracht bij het programma IV&P. Het programma heeft de beschikking gekregen over de beschikbare expertise (alle specialisten) en de capaciteit daarvan is in deze periode bijna verdubbeld[1]. Het programma heeft een regisseur gekregen voor versterking van de sturing en de verbinding met de lijn, het management en het bestuur. Het assessment heeft een organisatiebrede scope (programma en lijn) en de volwassenheidsniveau's en bevindingen hebben betrekking op deze scope.

Uit het onderzoek is gebleken dat er veel geïnvesteerd is in verbinding, het verbeteren van kennis en bewustwording. Dit wordt door de lijn ervaren en de bekendheid met het onderwerp en de spelers van informatiebeveiliging & privacy is duidelijk gegroeid. De oprichting van het leernetwerk heeft hieraan bijgedragen. In de afgelopen 2 jaar is het overkoepelende beleid voor informatiebeveiliging vernieuwd en zijn op verschillende onderwerpen specifieke beleidsuitwerkingen en richtlijnen opgesteld. Daarnaast werkt het programma de laatste maanden aan de versterking van de weerbaarheid door het opstellen van een incident responsplan, het organiseren van een crisisteam daarvoor ("CERT"[2]) en het oefenen met fictieve cyberaanvallen. Het programma heeft de afgelopen periode ook gestaag gewerkt aan het in kaart brengen van informatiebeveiliging- en privacyaspecten bij applicaties met het uitvoeren van korte scans.

De extra inspanning van het programma wordt ervaren door de organisatie, maar de ontwikkeling in volwassenheid van de processen op het gebied van informatiebeveiliging gaat moeizaam. De bevindingen uit het onderzoek duiden de problemen die de ontwikkeling van de volwassenheid tegenwerken. Voor een goed begrip van deze bevindingen is het van belang deze te plaatsen in de context van wat nodig is voor het vasthouden van het minimum procesvolwassenheidsniveau 2 en het bereiken van de ambitie procesvolwassenheidsniveau 3 over de volle breedte van de organisatie. De bevindingen beschrijven de belangrijkste problemen (naar de mening van de auditors de waarschijnlijke oorzaken) die –ondanks alle inspanningen- verhinderen dat de organisatie kan groeien naar niveau 3 op het gebied van informatiebeveiliging.

De belangrijkste bevindingen over het organisatiebrede beveiligingsniveau zijn:

a. Gebrek aan opvolging van aanbevelingen uit onderzoeken en aan implementatie van beveiligings-maatregelen bij risico's;
b. De lijn is verantwoordelijk voor informatiebeveiliging & privacy, maar beschikt niet over de benodigde expertise en rapporteert er niet over;
c. Plannen en rapportages zijn activiteitgericht opgesteld, niet resultaatgericht;
d. Versterking van de governance[3] van informatiebeveiliging & privacy langs managementcyclus is nog niet in gang gezet door het CMT; het programma kan slechts verleiden en faciliteren;
e. Het programma worstelt met informatiebeveiligingsvraagstukken door ontoereikende inhoudelijke aansturing;

[1] 4 information security officers, 1 technical information security officers 3 privacy officers
[2] Cyber Emergency Response Team
[3] Governance: de wijze waarop sturing, beheersing, verantwoording en toezicht is georganiseerd.

f. Onvolledig zicht en grip op incidenten, geen lering en zicht op oorzaken;
g. Onvoldoende leveranciersmanagement bij omvangrijke uitbesteding.

Per onderdeel van het dashboard informatiebeveiliging 2021 is bepaald welk niveau van procesvolwassenheid is bereikt (schaal 0 tot 5). De organisatie heeft in het plan informatiebeveiliging van 2016 en de eerste voortgangsrapportage naar GS/PS aangegeven te willen groeien naar niveau 3 met een minimumniveau van 2. De huidige status is weergegeven in het onderstaande dashboard. Uit deze status blijkt dat de provincie Utrecht de informatiebeveiliging nog niet kan reguleren zoals bedoeld in het convenant van 2014.

Dashboard informatiebeveiliging	*Volwassenheidsniveau*			
Onderwerp	*2015*	*2017*	*2019*	*2021*
Beleid & normen	1	1	1	1
Risicoanalyse	1	1	2	1 (-1)
Informatiebeveiligingsbeleid en -plan	1	1	1	1
Uitvoering	1	1	1	1
Continuïteit	1	1	1	2 (+1)
Ketens	1	1	1	1
Aansluiten	2	2	2	2
Incidentmanagement	1	1	2	1 (-1)
Toetsing en verantwoording	1	1	1	1
Evaluatie	1	1	1	1
Leerstrategie	1	2	1	2 (+1)

5 Geoptimaliseerd
4 Gemanaged
3 Gedefinieerd **<= ambitie**
2 Herhaalbaar **<= minimum**
1 Initieel
0 Niet aanwezig

De aanbevelingen voor het verbeteren van het organisatiebrede beveiligingsniveau zijn:
a. Neem de aanbevelingen en hoge risico's mee naar actiemanagement en sturingsrapportage en stuur vanuit CIO-office[4] op de opvolging en afdoening;
b. Zorg dat lijn haar verantwoordelijkheid voor informatiebeveiliging kan waarmaken door begrijpelijke kaders en expertise beschikbaar te stellen die helpt met implementeren van beveiligingsmaatregelen en/of de dienstverlener aan te sturen;
c. Transformeer de aanpak naar het inrichten en op gang brengen van informatiebeveiligingsprocessen op basis van de vereisten voor het procesvolwassenheidsniveau – eerst 2, later 3;
d. Versterk de governance van informatiebeveiliging & privacy in lijn met de toezegging aan PS[5];
e. Versterk de inhoudelijke sturing en pas die toe bij de procesgerichte aanpak;
f. Volg incidenten op met een centrale registratie en gebruik incidenten als bron om te leren;
g. Breng en houd informatiebeveiligingsafspraken in contracten met leveranciers in beeld en stuur risicogebaseerd op naleving.

Managementreactie
Wij hechten veel waarde aan informatieveiligheid en privacy. Het is noodzakelijk dat de organisatie op beide onderwerpen groeit naar een acceptabel volwassenheidsniveau. Dit is voorwaardelijk om een zorgvuldige omgang met vertrouwelijke- en/ of persoonsgegevens te waarborgen en risico's op misbruik en datalekken zoveel als mogelijk te verkleinen. Informatie is bovendien een van de belangrijkste bedrijfsmiddelen van onze organisatie en informatieveiligheid en privacy zal de komende jaren alleen maar meer gewicht en belang krijgen.

Het is van belang dat het zorgvuldig omgaan met vertrouwelijke informatie onderdeel is van ons dagelijks doen en laten. Het programmateam Informatieveiligheid en Privacy (IV&P) heeft in opdracht van het CMT de afgelopen jaren ingezet op bewustwording binnen de organisatie, het opstellen van beleid hoe om te gaan met informatie en het adviseren van de organisatie hoe technische en organisatorische maatregelen vorm te geven. De activiteiten waren en zijn gericht op het waarborgen van de vertrouwelijkheid, beschikbaarheid en integriteit van informatie en persoonsgevoelige gegevens. We moeten constateren dat het programma als buitenboordmotor onvoldoende heeft

[4] Onafhankelijke strategische eenheid onder leiding van de CIO (Chief Information Officer); zie Statenbrief 2021BEM155-01.
[5] Dit was een aanbeveling uit het assessment informatiebeveiliging 2019 dat tot noodzakelijke interventie voor de opvolging is benoemd; zie Statenbrief 2020BEM71 'Interventie binnen concernopgave Digitale Overheid'.

geleid tot de noodzakelijke inbedding binnen de reguliere processen in de lijnorganisatie noch de randvoorwaarden daarvoor volledig zijn ingevuld.

Sturing en plan-do-check-act-cyclus
Wij zijn de sturing op informatieveiligheid & privacy opnieuw aan het vormgeven en zullen daarbij deze aanbevelingen als belangrijke input meenemen. Met betrekking tot deze sturing wordt een interventie gedaan die ertoe leidt dat de lijn meer in positie komt en haar eigenaarschap ten aanzien van informatieveiligheid en privacy kan waarmaken. Om de lijn daarvoor toe te rusten, wordt zij geholpen door de Chief Information Officer (CIO) vanuit het CIO-office in wording. Daarbij is aandacht voor de benodigde ondersteuning qua:

- Instrumentarium; o.a. instrumentarium waarbij werkprocessen en datastromen worden doorgelicht op benodigde maatregelen gelet op informatieveiligheid en privacy, het uitvoeren van risicoanalyses en -classificaties om de kwetsbaarheden van systemen op het gebied van informatieveiligheid in te delen naar relevantie en urgentie en g*egevensbeschermingseffectbeoordeling* om na te gaan wat gezien de vereisten aan vertrouwelijkheid, beschikbaarheid en integriteit nodig is aan technische en organisatorische maatregelen
- Kennis; o.a. door opleidingsaanbod Utrecht Academie gericht op bewustzijn, kunnen herkennen van dreigingen en kwetsbaarheden en weten hoe te handelen en het programma digitaal slagvaardige medewerker, waarbij in bredere zin bewustwording over de mogelijkheden en gevaren van technologie en informatie aan de orde komen.
- Capaciteit o.a. operationele capaciteit, medewerkers die met focus en aandacht voor informatieveiligheid en privacy aan het werk zijn, waarbij mogelijke overdracht vanuit het programmateam IV&P naar de lijn plaats heeft.

De CIO wordt rechtstreeks aangestuurd door de algemeen directeur, kan onderwerpen agenderen voor het CMT en kan naar eigen inzicht gezien de agenda aansluiten bij het CMT. De voortgang ten aanzien van Informatieveiligheid en Privacy wordt daarmee ook vanuit de CIO gevolgd en indien nodig geagendeerd en bespreekbaar gemaakt binnen het CMT en tijdens het PO. Daarbij wordt ook gebruik gemaakt van de inzichten die de functionaris Informatieveiligheid en de functionaris gegevensbescherming als toezichthouders hebben op basis van eigen waarnemingen en het eerdergenoemde ISMS.

Informatieveiligheid & Privacy is als onderdeel opgenomen in de managementcyclus. Over de voortgang wordt gerapporteerd, gesproken en waar nodig bijgestuurd. Het programma Informatieveiligheid & Privacy levert hiervoor input uit het zogenaamde Information Security Management Systeem (ISMS) dat in uitrol is. In het ISMS staan alle maatregelen die nodig zijn om te voldoen aan de Baseline Informatieveiligheid Overheid (BIO), met daarbij eigen planningen en benoemde actiehouders. De beheerder van het systeem is de functionaris informatieveiligheid.

Groei volwassenheidsniveau
Op basis van een reëel tijdspad en de aanbevelingen uit het Assessment rapport en ook de suggestie van de functionaris informatieveiligheid willen we ons gericht zetten op het verhogen van het volwassenheidsniveau. Daarbij wordt voortgebouwd op hetgeen al in gang is gezet aan activiteiten met oog voor noodzakelijke bijsturing en intensivering. De vastlegging van het tijdspad en de voortgang draagt bij aan het aantoonbaar maken van getroffen technische en organisatorische maatregelen en de mate waarin deze effect hebben op de volwassenheid van informatieveiligheid.

Voor informatieveiligheid betreft dit tot eind 2022 gerichte inzet op het verder ontwikkelen van risicoanalyses, het opvolgen van maatregelen, incidentmanagement en leveranciersmanagement. Voor privacy betreft dit tot eind 2022 gerichte inzet op privacy by design, toezicht op de rechtmatigheid van verwerkingen en organisatorische maatregelen gericht op de beveiliging van persoonsgegevens.

De planning van de activiteiten en maatregelen die hieraan bijdragen wordt rond de zomer vastgesteld. Momenteel wordt het CIO-office ingericht, waarin ook de regie op en coördinatie van IV&P wordt ondergebracht. Hiermee wordt

weer een belangrijke vervolgstap gezet naar de organisatorische inbedding en waarmee de formele sturingslijnen op informatieveiligheid en privacy in de organisatie op orde komt.

Focus I-functie
Gezien de verschillende ambities op de I-functie ten aanzien van werken met data, digitale dienstverlening, digitaal slagvaardige medewerker en archivering stellen wij onder meer voor om allereerst de basis op orde te brengen. Dit betekent dat de prioriteit qua sturing en inspanningen ligt bij informatieveiligheid, privacy, archivering, de digitaal slagvaardige medewerker en het versterken van de centrale regie en sturing op de organisatie van informatievoorziening met het CIO-office. Op de andere onderdelen, werken met data en digitale dienstverlening doen we hetgeen minimaal nodig is, zijn we geen koploper en ook zeker geen achterloper.

Met het besef dat we een betere uitgangspositie verkrijgen op het gebied van privacy en met name informatieveiligheid kunnen we de kans op datalekken en beveiligingsincidenten verkleinen, maar niet volledig uitsluiten.

Naast bovengenoemde zaken werkt het huidige programma IV&P ondertussen door aan haar reguliere taken en aan de procesvolwassenheid van IV&P in de organisatie, met betrokkenheid van de CIO.

Vervolg
Samen met het CMT zullen wij de voortgang de komende maanden nauwgezet volgen en u hierover elk kwartaal informeren bij de voortgangsrapportage van het programma BV Beter.

Gedeputeerde Staten van Utrecht,

Voorzitter,
mr. J.H. Oosters

Secretaris,
mr. drs. A.G. Knol-van Leeuwen