JAARVERSLAG GEGEVENSBESCHERMING 2021

GEMEENTE WESTLAND

Auteur(s)	Taakveld Gegevensbescherming
Datum	19 januari 2022
Versie	1.0
Status	Definitief

ALG HS 007

21-0248688

Inhoudsopgave

21-0248688

Managementsamenvatting

Het college van B&W van gemeente Westland legt jaarlijks verantwoording aan de Raad af over de uitvoering van het gegevensbeschermingsbeleid. Dit beleid omvat zowel informatiebeveiliging als privacy. Dit jaarverslag Gegevensbescherming 2021 bevat die verantwoording.

We baseerden het jaarverslag ook op:

- een actuele meting over de BIO (Baseline Informatiebeveiliging Overheid) en de AVG (Algemene Verordening Gegevensbescherming),
- de resultaten uit de zelfevaluaties via ENSIA (**E**enduidige **N**ormatiek **S**ingle **I**nformation **A**udit) en
- de uitvoering van ons Jaarplan Gegevensbescherming 2021.

Over de voortgang hiervan rapporteerden we periodiek aan de concerndirectie via kwartaalrapportages. De vierde kwartaalrapportage komt met het uitbrengen van dit jaarverslag te vervallen.

We beoordeelden de normen uit zowel de BIO als de AVG vooral vanuit een generiek beeld. En niet specifiek toegespitst op processen en/of applicaties.
In dit jaarverslag houden we rekening met aandachtspunten die voortkomen uit de metingen over de BIO (informatiebeveiliging) en de AVG (privacy). Ook betrekken we de uitkomsten uit de zelfevaluaties via ENSIA erbij.
De aandachtspunten met de hoogste risico's vormen de basis voor ons Jaarplan Gegevensbescherming 2022.

Daar waar gegevensbescherming staat vermeld, bedoelen we zowel informatiebeveiliging als privacy.

Mijlpalen in 2021

In 2021 realiseerden we op het gebied van gegevensbescherming het volgende:

- *geactualiseerd beleid*
  - We rondden het Gegevensbeschermingsbeleid 2021-2023 af. Het college stelde het beleid vast. Het beleid is terug te vinden in het gemeenteblad.
- *geactualiseerd verwerkingsregister*
  - We actualiseerden het verwerkingsregister. We gebruikten hiervoor het model van de VNG. We publiceerden een publieksversie op de gemeente website.
- *pilot naleving verwerkersovereenkomsten*
  - We toetsten steekproefsgewijs of verwerkers hun beveiliging aantoonbaar op orde hadden. Afspraken hierover staan in de verwerkersovereenkomst. Verwerkers zijn bijvoorbeeld leveranciers van applicaties waarin persoonsgegevens voorkomen. Dit toonden de leveranciers onder andere aan door een ISO27001 certificering aan te leveren. We vervolgen de pilot in 2022 en betrekken dan de proces- of applicatie eigenaren hier ook bij.
- *GAP-analyses*
  - We voerden GAP-analyses uit. Zowel voor informatiebeveiliging als privacy. Een GAP-analyse is een methode om een vergelijking te maken tussen een bestaande en een gewenste situatie. De concerndirectie stelde de analyses vast. Verderop in dit verslag vindt u hier meer informatie over.
- *IRPA-tool*
  - We participeerden in de testfase van de IRPA-tool. De IBD (Informatie Beveiligingsdienst) ontwikkelde samen met gemeenten deze **i**ntegrale **r**isico- en **p**rivacy-**a**nalysetool. Deze nieuwe tool helpt om analyses op het gebied van privacy en informatiebeveiliging gemakkelijk, professioneel en éénduidig uit te voeren.

- *ENSIA verantwoording met DigiD en Suwinet audit*
  - Gemeenten verantwoorden zich over informatiebeveiliging via ENSIA. De focus van ENSIA ligt op verantwoording richting de gemeenteraad. En hiermee leggen gemeenten verantwoording af aan de rijksoverheid en toezichthouders waar het gaat om het gebruik van landelijke voorzieningen. We rondden met succes de zelfevaluatie over 2020 af. En leverden tijdig de verantwoording over 2021 in.
- *Afstudeeropdracht*
  - We begeleidden een afstudeerder bij zijn afstudeeropdracht. Resultaat: geslaagd!

Beveiligingsincidenten

In 2021 ontvingen we 549 meldingen over beveiligingsincidenten waarvan 343 over geconstateerde kwetsbaarheden. Het ging hierbij ook om ontdekte kwetsbaarheden die met updates van software en aanpassingen van de hardware waren op te lossen.
Van deze beveiligingsincidenten merkten we er 31 aan als datalek. Daarvan meldden we er 23 bij de AP (Autoriteit Persoonsgegevens) en informeerden we in 17 gevallen de betrokkenen.
Verderop in dit verslag vindt u hier meer informatie over.

Vooruitblik 2022 op het gebied van gegevensbescherming

Via wát we wilden bereiken:

- We dragen bij aan een risico bewuste organisatie
- Men kan en wil ons vinden
- We zijn een waardevolle vraagbaak
- We gedragen ons als een rechtvaardige toezichthouder
- We ondersteunen bij compliance aan verplichte kaders

En hóe we dat wilden bereiken:

- Proactief, kritisch maar ook dienend richting de organisatie
- Meedenkende “sta in de weg”
- Vertegenwoordiger van belangen burgers/klanten en bewaker van kaders en normen

Naar thema’s voor 2022:

- ‘DOEN!’
  - Risico gebaseerd
  - Bevindingen uit zelfevaluaties, IT-audits, rekenkameronderzoek en pentesten
  - Crisisplan
  - Klantgericht
  - Communicatie
- ‘Focus op…’
  - Bedrijfscontinuïteit
- ‘Basis op orde’
  - ISMS-/PMS-tool
  - Risicoregister
- ‘Dagelijkse bezigheden’
  - Going concern taken
  - Aanvullend beleid op onderdelen

Deze activiteiten namen we op in ons jaarplan Gegevensbescherming 2022.

1. Inleiding

Een jaarverslag Gegevensbescherming...terugkijken en vooruitkijken. Waar staat de organisatie op het gebied van gegevensbescherming? En welke rol speelden wij, taakveld Gegevensbescherming het afgelopen jaar hierin? Wat hebben we bereikt en wat niet?
Zomaar wat vragen die we in dit verslag hopen te beantwoorden.

We ondersteunden, informeerden en adviseerden medewerkers (individueel en in team- of taakveldverband), teammanagers en bestuurders met van alles en nog wat. Natuurlijk wel onderwerpen met een gegevensbeschermingsaspect. Niet alleen gemeente breed, maar ook ingezoomd op een proces, applicatie of een issue binnen een team of taakveld. Dit deden we door gevraagd en ongevraagd advies te geven, analyses uit te voeren, memo's op te stellen, pilots uit te voeren en zelfevaluaties en audits te begeleiden. We rapporteerden hierover en monitorden de voortgang van ons eigen jaarplan.

Hoe past dit binnen het gegevensbeschermingsbeleid? En wat waren de resultaten voor medewerkers, de organisatie en de inwoners van gemeente Westland?

Kijkend vanuit het beleid, geven we in dit verslag weer waar we samen met de organisatie aan werkten. Waar de organisatie nu staat op het gebied van gegevensbescherming. En waar we in 2022 verder aan willen werken.

2. Definitie, uitgangspunten en doelen gegevensbeschermingsbeleid

Met de vaststelling van het 'Gegevensbeschermingsbeleid 2021-2023 - Doorlopend: doordacht en doordrongen datagebruik' zette gemeente Westland een belangrijke vervolgstap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente op orde te houden.
Het doet recht aan de integrale verantwoordelijkheid van de lijnmanagers. Het biedt voorwaarden voor het bestuur om hun verantwoordelijkheid te kunnen dragen. En het biedt de raad een basis om haar toezichthoudende taak uit te kunnen voeren.
Het zet ook de medewerkers van het taakveld Gegevensbescherming in een goede positie als ondersteuner en adviseur van management en medewerkers.

De opzet van dit beleid is, anders dan voorheen, gericht op wat de organisatie wil bereiken: een goede borging van de gegevensbescherming in de producten en diensten. Het geeft handen en voeten aan hoe de organisatie dat wil bereiken en volgens welke meetlat: "Doorlopend: doordacht en doordrongen datagebruik".

Doorlopend:	Doordacht:	Doordrongen:
		
- Voor, tijdens en achteraf bij het verwerken - Binnen, buiten en thuis - Bewust handelen	- Weloverwogen - In juiste verhouding - Binnen de kaders	- Tot diep in onze wortels - In het hoofd en met het hart - Niet als principe maar als drijfveer

De organisatie moet blijven voldoen aan de kaders die gelden. Dit beleid kan dan ook niet los worden gezien van de AVG, de BIO, de bestuurlijke aanvulling op de BIO vanuit de VNG met de 10 bestuurlijke principes, de ISO 27001/27002 en de standaarden waar we aan moeten voldoen. ISO 27001 en ISO 27002 zijn twee normen op het gebied van informatiebeveiliging.

ISO 27001 is een wereldwijd erkende norm op het gebied van informatiebeveiliging. ISO 27002 geeft richtlijnen en principes voor het initiëren, implementeren, onderhouden en verbeteren van informatiebeveiliging binnen een organisatie.

De ISO 27001 norm is een internationaal erkende norm op het gebied van informatiebeveiliging. In deze norm staat beschreven hoe je als organisatie informatiebeveiliging procesmatig kunt inrichten. Zo kun je aantonen dat je als organisatie voldoet aan alle eisen en dat je maatregelen hebt getroffen tegen informatiebeveiligingsrisico's.

ISO 27002 is als het ware een verdieping op ISO 27001. De ISO 27002 is eigenlijk een hulpmiddel om de risicoanalyse, welke een verplicht onderdeel vormt van de ISO 27001 norm, uit te voeren. ISO 27002 bestaat namelijk uit een lijst met maatregelen waarmee je de risico's die je hebt geïdentificeerd kunt beperken of verkleinen.

Waar ISO 27001 een kort en bondig document is, biedt ISO 27002 meer informatie en details.

De 10 bestuurlijke principes voor informatiebeveiliging:

1. Bestuurders bevorderen een veilige cultuur
2. Informatiebeveiliging is van iedereen
3. Informatiebeveiliging is risicomanagement
4. Risicomanagement is onderdeel van de besluitvorming
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking
6. Informatiebeveiliging is een proces
7. Informatiebeveiliging kost geld
8. Onzekerheid dient te worden ingecalculeerd
9. Verbetering komt voort uit leren en ervaring
10. Het bestuur controleert en evalueert

21-0248688

2.1. Wat is gegevensbescherming?

Gemeente Westland is een informatie-intensieve organisatie met een sterke focus op de dienstverlening. Deze organisatiekenmerken vragen om een betrouwbare en veilige informatievoorziening. De medewerkers van de gemeente moeten beschikken over betrouwbare informatie om de klanten optimaal te helpen en te adviseren. Daarnaast moeten burgers en bedrijven erop kunnen vertrouwen dat hun gegevens in goede handen zijn bij de gemeente.
Om dit meer vorm en inhoud te geven hanteren we onderstaande definities:

- *Definitie gegevensbescherming*: Bewust en doelgericht ons denken, doen en laten richten op het zorgvuldig bewerken en verwerken van (vertrouwelijke) informatie binnen de geldende wetten, regels en normen.
- *Definitie privacy*: Centraal stellen van de belangen van betrokkenen bij het bewerken, verwerken en delen van (bijzondere) persoonsgegevens.
- *Definitie informatiebeveiliging*: Het risicobewust treffen, onderhouden en controleren van samenhangende maatregelen met betrekking tot informatieverwerking en informatiesystemen zodat het juiste niveau van beschikbaarheid, integriteit en vertrouwelijkheid is en blijft gewaarborgd.

Het gegevensbeschermingsbeleid geldt voor het complete proces van informatievoorziening en de hele levenscyclus van informatiesystemen. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politiek bestuur, alle medewerkers, burgers, bezoekers en externe relaties.

2.2. AVG en BIO

Twee belangrijke zaken vormen de basis voor het gegevensbeschermingsbeleid. De eerste is een wettelijke, de AVG die sinds 25 mei 2018 van kracht is. De tweede is de BIO die sinds 1 januari 2019 van kracht is.

AVG
De AVG regelt dat organisaties duidelijk maken waarom ze persoonsgegevens verzamelen, waarvoor ze die gebruiken en hoe lang de data wordt bewaard. Zo moet worden bepaald voor welk doel data wordt gebruikt, op basis van welke grondslag dat plaatsvindt en er wordt niet meer verzameld dan nodig voor het doel. Ook is van belang waar data wordt opgeslagen en of het met anderen wordt gedeeld. Tot slot regelt de AVG dat onze burgers en klanten rechten hebben om inzage te krijgen in de opgeslagen data, het wijzigen en soms zelfs het verwijderen daarvan.
In nagenoeg alle processen die wij als gemeente Westland kennen worden persoonsgegevens gebruikt. Dus bijna iedereen heeft hier dagelijks mee te maken.

BIO
De BIO stelt kaders en normen voor de informatieveiligheid. De BIO bevat te nemen maatregelen waarin men keuzes heeft in hoeverre die worden toegepast of niet. In alle gevallen geldt dat er risico's zijn en iedereen deze in het werk herkent. Daarnaast zijn er verplichte overheidsmaatregelen waarin er feitelijk geen keuze is. Het niet toepassen van zo'n maatregel vraagt een expliciet besluit met toelichting (pas toe of leg uit). Tot slot bevat de BIO meerdere controls aan de hand waarvan kan worden beoordeeld of er juist omgegaan wordt met de risico's en maatregelen.
De BIO is gebaseerd op de ISO 27001 en ISO 27002.

Relatie privacy en informatiebeveiliging
Met de inwerkingtreding van de AVG op 25 mei 2018 is privacy volop in de schijnwerpers komen te staan. Privacy heeft alleen betrekking op persoonsgegevens, waarbij dat begrip overigens ook

heel ruim is. Informatiebeveiliging heeft een breder aandachtsgebied. De beveiliging is bijvoorbeeld ook gericht op de bedrijfscontinuïteit en beperkt zich niet tot uitsluitend persoonsgegevens. Toch is het niet vreemd dat privacy en informatiebeveiliging vaak in één adem worden genoemd. Een aantal beveiligingsmaatregelen is van directe invloed op het waarborgen van de privacy. Omgekeerd dragen privacy vereisten zoals het afsluiten van verwerkersovereenkomsten, bij aan verhoging van de informatiebeveiliging. Informatiebeveiliging en privacy worden binnen gemeente Westland daarom in samenhang opgepakt.

2.3. Uitgangspunten en doelen van het gegevensbeschermingsbeleid

Het doel van het beleid is dat gegevensbescherming geborgd is, wordt en blijft binnen de organisatie en al haar producten en diensten. Basis daarin is het besef dat alle medewerkers een verantwoordelijkheid hebben naar de burgers, klanten en zichzelf met betrekking tot gegevensbescherming. Beginsel is dat iedereen zich bewust is dat de gemeente omgaat met vertrouwelijke data en gevoelige informatie. Daarom zijn beschermende maatregelen nodig. Om de privacy van mensen te bescherming én om de vertrouwelijkheid, beschikbaarheid en integriteit van de gegevens te garanderen.

Concreet vertaalt zich dit in de volgende strategische doelen van gegevensbescherming:

- Het managen van de gegevensbescherming.
- Het beschermen van de privacy rechten van burgers en klanten.
- Het adequate beschermen van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang tot systemen en/of informatie.
- Het garanderen van correcte, tijdige en veilige informatievoorzieningen.
- Het waarborgen van veilige informatiesystemen, processen en verwerkingen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Burgers en klanten actief informeren wat er met hun persoonsgegevens gebeurt.
- Het waarborgen van de naleving van dit beleid.

3. Samenvattend beeld en resultaten gegevensbescherming 2021

In 2018 stelde de Functionaris Gegevensbescherming (FG) een jaarverslag op. Dit in het kader van de van kracht geworden privacy wetgeving. Hierna zochten we een vorm van verslaglegging vanuit het hele (nieuw gevormde) taakveld Gegevensbescherming.
Dit is het eerste jaarverslag over zowel informatiebeveiliging als privacy (gegevensbescherming) bij gemeente Westland. De afgelopen twee jaar boden we wel kwartaalrapportages aan. Maar we voelden nu ook de behoefte om een jaarverslag te schrijven.

In 2021 is het gemeentelijk gegevensbeschermingsbeleid vastgesteld en gepubliceerd. Dit nieuwe beleid beschreven we al in hoofdstuk 2. Hiermee is het beleid actueel en voldoet aan de huidige wet- en regelgeving.

In 2021 voerden wij een GAP-analyse (light) uit. Zowel op informatiebeveiliging als op privacy. Hiermee brachten wij goed in beeld waar de verschillen zitten tussen de normenkaders en de situatie bij Gemeente Westland. We boden de rapportages hiervan aan de concerndirectie aan.

Naast de GAP-analyses legde de organisatie ook verantwoording over informatiebeveiliging (en indirect privacy) af via de zelfevaluatie ENSIA. En werden er diverse andere onderzoeken uitgevoerd (IT-audits over 2020 en 2021 door de accountants en externe en interne pentests).

Hofmann Cybersecurity startte in het vierde kwartaal van 2021 met de uitvoering van het rekenkameronderzoek naar informatiebeveiliging. Dit is een vervolg op het onderzoek uit 2019. In 2020 en 2021 werkten we er hard aan de bevindingen uit dit onderzoek op te laten pakken. Hiervan deelden we ook geregeld tussentijdse updates met de clusterdirecteur en de portefeuillehouder. We verwachten dat het rapport in het 1e kwartaal van 2022 opgeleverd wordt. En gaan daarna natuurlijk samen met de organisatie aan de slag met de aanbevelingen.

3.1. GAP-analyses (light)

We voerden in 2021 een GAP-analyse uit op de BIO (informatiebeveiliging) en de AVG (privacy). Een GAP-analyse is een methode om een vergelijking te maken tussen een bestaande en een gewenste situatie. Dit is een maatregel uit de BIO en komt ook terug in het normenkader privacy 'AVG Borgingsproduct 2.0'.

In het hoofdstuk 'Borging accountability' uit het Gegevensbeschermingsbeleid staat dat de GAP-analyse 'een belangrijk instrument is om inzicht te hebben in de status van de feitelijke situatie op het gebied van gegevensbescherming en de gewenste situatie daarvan'.
In het Jaarplan Gegevensbescherming 2021 namen we op om dit jaar een verkorte analyse, een zogenaamde lightversie, uit te voeren. We kozen voor een lightversie, omdat de organisatie nog volop bezig is met de implementatie van de vele maatregelen.

3.1.1. GAP-analyse BIO

Voor de rapportage maakten we gebruik van de door de VNG (Vereniging voor Nederlandse Gemeenten) voorgestelde consolidatie van de BIO-hoofdstukken:

BIO Hoofdstuk		Aantal controls en/of maatregelen	Consolidatie	Totaal aantal controls en/of maatregelen
H5	Informatiebeveiligingsbeleid	2	1. Beleid en organisatie	23
H6	Organiseren van informatiebeveiliging	11		
H18	Naleving	10		
H7	Veilig personeel	8	2. Personeel en toegang	55
H9	Toegangsbeveiliging	27		
H11	Fysieke beveiliging en beveiliging van de omgeving	20		
H16	Beheer van informatiebeveiligingsincidenten	14	3. Continuïteit en incidenten	20
H17	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	6		
H12	Beveiliging bedrijfsvoering	30	4. Informatiesystemen	55
H14	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	13		
H15	Leveranciersrelaties	12		
H8	Beheer van bedrijfsmiddelen	14	5. Databescherming	31
H10	Cryptografie	4		
H13	Communicatiebeveiliging	13		
				184

We bepaalden de mate van implementatie voor 184 maatregelen:

	Geïmplementeerd?				
	Ja	Deels	Nee	Nvt	
	93	52	31	8	184
1. BELEID EN ORGANISATIE Actueel beleid en organisatie van informatiebeveiliging en controle op naleving	17	5	0	1	23
2. PERSONEEL EN TOEGANG Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens	26	22	5	2	55
3. CONTINUÏTEIT EN INCIDENTEN Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten	5	11	4	0	20
4. INFORMATIESYSTEMEN Veilige omgang met informatiesystemen en afspraken hierover met onze leveranciers	30	6	15	4	55
5. DATABESCHERMING Veilige omgang met data in onze software	15	8	7	1	31
	51%	28%	17%	4%	100%

Het beeld van de feitelijke situatie uit de GAP-analyse verschilt niet wezenlijk met de constateringen uit diverse andere onderzoeken:
- het rekenkameronderzoek Informatiebeveiliging uit 2019,
- de IT-audits bij de Jaarrekeningen 2019 en 2020,
- de ENSIA-zelfevaluatie 2020 en
- de uitgevoerde interne pentest.

We vragen vanuit taakveld Gegevensbescherming regelmatig aandacht voor de bevindingen uit deze onderzoeken. We concluderen dat in 2020 en 2021 de organisatie kleine stappen heeft gezet. Wij merken dat andere prioriteiten en de waan van de dag er geregeld voor zorgen dat de bevindingen uit bovengenoemde onderzoeken naar beneden zakken op de prioriteitenlijsten. Dit is een organisatie breed fenomeen. Het management spreekt uit dat gegevensbescherming belangrijk is, maar de urgentie wordt niet altijd gevoeld.

Een groot incident, zoals de hack bij gemeente Hof van Twente, zorgt voor een korte opleving van het gevoel van urgentie, maar deze zakt ook snel weer weg. Dit heeft tot gevolg dat de te nemen maatregelen keer op keer uitgesteld worden. Hierdoor blijven de risico's voor de organisatie bestaan. We doen dit namelijk niet alleen om te voldoen aan wet- en regelgeving (compliant te zijn), maar vooral ook om onze systemen met daarin een schat aan informatie te beschermen.

Met deze GAP-light wilden wij heel specifiek in beeld brengen welke maatregelen de organisatie minstens moet nemen om de gemeente op een basisniveau te beschermen.

3.1.2. GAP-analyse AVG

Voor de rapportage maakten we gebruik van de door de VNG (Vereniging voor Nederlandse Gemeenten) voorgestelde thema-indeling privacy maatregelen:

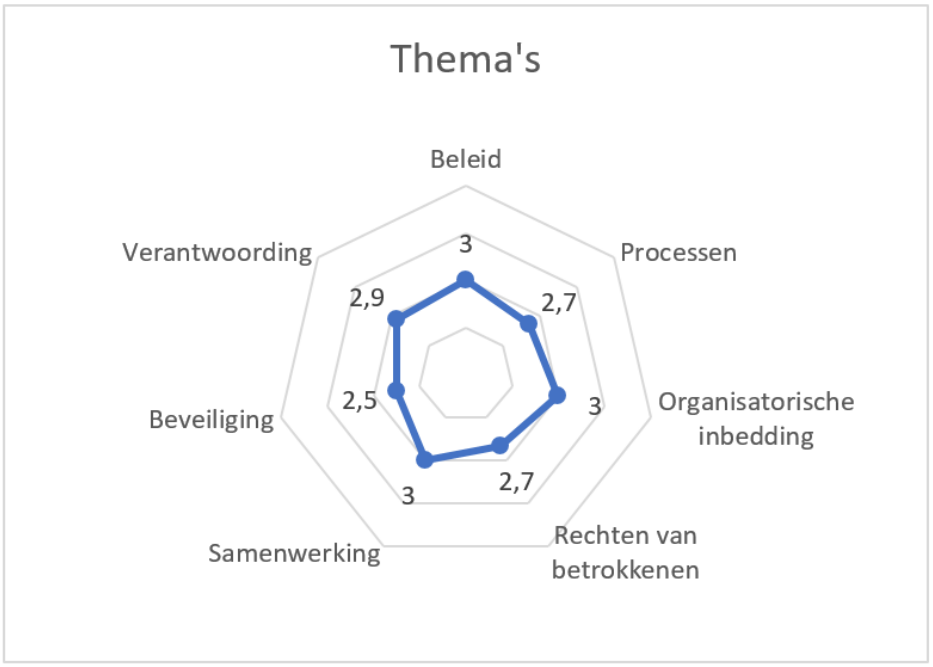
					Volwassenheidsniveau (VN)				
Thema	Aantal controls	Aantal maatregelen	Organisatie-maatregelen (O)	Proces-maatregelen (P)	1	2	3	4	5
1. Beleid	2	12	7	5	0	2	10	0	0
2. Processen	7	37	16	21	0	13	24	0	0
3. Organisatorische inbedding	4	24	17	7	0	8	16	0	0
4. Rechten van betrokkenen	6	31	11	20	2	13	16	0	0
5. Samenwerking	2	9	2	7	0	2	7	0	0
6. Beveiliging	3	29	9	20	0	12	17	0	0
7. Verantwoording	4	12	10	2	0	3	9	0	0
	28	154	72	82	2	53	99	0	0

We bepaalden de mate van implementatie voor 154 maatregelen:

	Geïmplementeerd?							
	Ja		Deels		Nee			
	O	P	O	P	O	P		VN
Thema	60	49	10	23	2	10	**154**	**2,8**
1. Beleid	7	2	0	2	0	1	12	3
2. Processen	12	12	4	5	0	4	37	2,7
3. Organisatorische inbedding	17	6	0	1	0	0	24	3
4. Rechten van betrokkenen	8	14	1	2	2	4	31	2,7
5. Samenwerking	2	6	0	1	0	0	9	3
6. Beveiliging	9	8	0	11	0	1	29	2,5
7. Verantwoording	5	1	5	1	0	0	12	2,9
	39,0%	31,8%	6,5%	14,9%	1,3%	6,5%		
	71%		**21%**		**8%**		**100%**	

En we bepaalden het volwassenheidsniveau per control en thema:

Totale volwassenheidsscore (gemiddelde van alle thema's): 2,8



Gemeente Westland is op weg om privacy goed vorm te geven. Dat is het algemene beeld van de feitelijke situatie uit de GAP-analyse, gezien vanuit taakveld Gegevensbescherming. We zien een duidelijke toename van aandacht voor dit onderwerp en ook neemt de bewustwording zichtbaar toe. Maar we zijn er nog niet.
We bepaalden het volwassenheidsniveau op 3. Niveau 3 is het minimumniveau. Dit wil niet zeggen dat de gemeente volledig compliant aan de AVG is, als bij alle controls niveau 3 is bereikt. Dit omdat de maatregelen bij een control niet uitputtend zijn.
De organisatie moet eerst binnen volwassenheidsniveau 3 groeien van organisatie breed naar inzicht in de status van de maatregelen per team of taakveld (of clusters van teams en taakvelden). Daarna kunnen we bepalen wat er nodig is om naar niveau 4 te groeien.

4. Disclaimer

Voorkomen van beveiligingsincidenten lukt helaas niet altijd. 100% beveiliging is een utopie. Privacy-incidenten vallen hier ook onder. Denk aan datalekken.
De vraag is dan ook niet óf er een beveiligingsincident met een hoge impact zal plaatsvinden, maar wannéér.
Beveiligingsincidenten kunnen leiden tot onderbreking van werkzaamheden en dienstverlening en reputatieschade. Of tot aanzienlijke financiële schade als gevolg van het bestrijden van een incident en het herstellen naar een normale situatie. Privacy-incidenten leiden tot een inbreuk op de bescherming van de persoonsgegevens van de inwoners, medewerkers of andere (externe) personen. Bij gemelde datalekken met gegevens van onze inwoners informeert de organisatie hen actief over de melding.
Als preventieve maatregel verzorgen wij bewustwording en geven gevraagd en ongevraagd advies.
De maatregelen die de organisatie neemt zijn erop gericht de risico's zoveel mogelijk te minimaliseren tegen aanvaardbare kosten. Daarnaast wordt rekening gehouden met de impact op dienstverlening en bedrijfsvoering.
Een heel effectieve maatregel is bijvoorbeeld het uitschakelen van alle internetverbindingen van het gemeentehuis. Een hacker van buiten het kantoor zou dan geen enkele kans meer hebben. Maar hoe veilig dit ook is, dit zou de bedrijfsvoering dusdanig verstoren, dat dit niet werkbaar is. Naast preventieve maatregelen richten we ons ook op procedures en maatregelen wanneer zich een incident voordoet. Zodat de gemeente met de dienstverlening en bedrijfsvoering zo snel mogelijk weer operationeel kan zijn.

5. Belangrijkste beheersmaatregelen gegevensbescherming

Zowel in de BIO als de AVG staan maatregelen. We hanteerden de BIO versie 1.4 en het Borgingsproduct AVG versie 2.0 als normenkaders.
Het vraagt meerdere jaren om deze maatregelen te implementeren in de gemeentelijke processen en systemen. Daarom is inzicht in wat er moet gebeuren met welke prioriteit belangrijk.
De uitgevoerde GAP-analyses geven inzicht in:

- De status van belangrijke gemeente brede maatregelen (zogenaamde O-maatregelen, waarbij 'O' staat voor organisatie);
- Essentiële processen;
- Kritische systemen;
- De status van systeem specifieke maatregelen.

IRPA-tool

Welke maatregelen de organisatie moet nemen hangt af van de risico's. Deze maken we inzichtelijk aan de hand van wat de kans is dat zich iets voor doet, welke impact dit heeft en welke schade er mee gemoeid is. Instrumenten hiervoor zijn bijvoorbeeld de baselinetoets BIO en de **D**ata **P**rivacy **I**mpact **A**ssessment (DPIA).
De IBD ontwikkelde samen met gemeenten een **i**ntegrale **r**isico- en **p**rivacy-**a**nalyse (IRPA) tool. Met deze nieuwe tool voeren we samen met de organisatie analyses op het gebied van privacy en informatiebeveiliging gemakkelijk, professioneel en éénduidig uit. Bij het uitvoeren van de analyses maken we gebruik van de kennis die de IBD in de tool verwerkte. De risico's die volgen uit DPIA's en risicoanalyses zijn voor veel gemeentelijke basisprocessen beschikbaar. Deze data vormen een solide basis of referentie voor de eigen analyses op nieuwe of vernieuwde processen. We participeerden in de pilot van deze tool. In het najaar namen we de tool in gebruik. Alle organisatie brede maatregelen staan standaard in de tool (O-maatregelen). Zowel op het gebied van

informatiebeveiliging (BIO versie 1.4) als op het gebied van privacy (AVG Borgingsproduct versie 2.0).
We actualiseren deze periodiek, zodat we altijd de meest recente stand van zaken gebruiken bij de analyses. Per analyse bepalen we de P-maatregelen. Dit zijn maatregelen per proces.

Baselinetoets BIO en DPIA
We voeren een baselinetoets uit om te bepalen of een proces, informatiesysteem en/of informatie een bepaald **B**asis **B**eveiligings**n**iveau (BBN) heeft binnen de BIO. De uitkomsten gebruiken we om te bepalen of er meer maatregelen nodig zijn voor een proces en onderliggende informatiesystemen. Waar nodig voeren we een aanvullende diepgaande risicoanalyse uit. Het resultaat van de baselinetoets BIO kan duiden op een zwaartepunt in het te beschermen belang. De score voor Beschikbaarheid is bijvoorbeeld een hogere dan voor Integriteit en Vertrouwelijkheid. In de daarna uit te voeren risicoanalyse leggen we dan de nadruk op verhogen van Beschikbaarheid.
Een DPIA is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen. Vervolgens kunnen we maatregelen nemen om de risico's te verkleinen.
We gebruiken de baselinetoets en (pre-)DPIA bij de fase voor het starten van een project of voor een nieuw informatiesysteem. De vragenlijst vormt input voor de eventueel te nemen aanvullende beveiligingsmaatregelen. Deze worden in de definitiefase van het project nader uitgewerkt. Bijvoorbeeld door middel van een aanvullende diepgaande risicoanalyse.

Uitgangspunten gemeente brede maatregelen
We toetsten de O-maatregelen dus al op wat is geïmplementeerd en nog actueel is volgens de BIO- en privacy normen. Bij deze gemeente brede maatregelen gaan we uit van:
- Het gemeentelijk gegevensbeschermingsbeleid, dit is gelijk voor de hele organisatie;
- Het toewijzen van de Chief Information Security Officer (CISO)-rol en de rol van Functionaris Gegevensbescherming (FG);
- Verantwoordelijkheden van de lijnmanagers (te verankeren in het beleid);
- Beheerprocessen en aandacht voor beveiliging;
- Personele beveiligingsmaatregelen;
- Fysieke toegangsbeveiligingsmaatregelen;
- Beveiligingsmaatregelen voor apparatuur en software;
- Malware scanning als generieke dienst (dus niet voor één informatiesysteem);
- Omgang met (mobiele) gegevensdragers;
- Ingerichte privacy processen (zoals verwerkingsregister, verwerkersovereenkomsten en rechten van betrokkenen);
- Het hebben van een Information Security Management System (ISMS) en Privacy Management System (PMS).

Het laatste uitgangspunt toegelicht: ISMS en PMS
Het ISMS is een proces dat de basis legt voor passende beveiligingsmaatregelen over de langere termijn. Het helpt onder andere om risico's te beheersen, passende beveiligingsmaatregelen te treffen, lering te trekken uit incidenten en daarmee de betrouwbaarheid en de kwaliteit van de informatievoorziening en bedrijfscontinuïteit te waarborgen.
Het PMS doet hetzelfde specifiek voor privacy maatregelen en processen.
Voor een overzicht van alle maatregelen en de voortgang van alle uitgezette acties gebruiken we nu verschillende Exceloverzichten. Dit geeft geen totaaloverzicht van de stand van zaken. En geeft geen inzicht in verbanden tussen nog niet geïmplementeerde maatregelen, conclusies en aanbevelingen uit audits, zelfevaluaties en onderzoeken.
Daarom dienden we eind 2019 het verzoek om de aanschaf van een ISMS-/PMS-tool in.

Zo'n tool bevat alle maatregelen om de risico's op het gebied van informatieveiligheid en privacy te beheersen. En alle acties die daarvoor zijn uitgezet, de voortgang van die activiteiten, de resultaten van uitgevoerde onderzoeken en bewakingsmogelijkheden. Met behulp van de tool kan het management en iedere proceseigenaar op elk moment zien en aantonen of zij op alle normen in control zijn.
In onze jaarplannen over 2020 en 2021 hielden we rekening met implementatie van de tool. De aanvraag resulteerde nog niet in de aanschaf van een product.
We hopen dit punt in 2022 alsnog te realiseren.

5.1. Aandachtspunten op basis van de GAP-analyse BIO

Voor de volgende thema's uit de GAP-analyse vroegen wij extra aandacht en prioriteit:
- Thema Personeel en toegang - Beperking toegang tot informatie
- Thema Continuïteit en incidenten - Informatiebeveiligingscontinuïteit
- Thema Informatiesystemen - Beveiliging van de bedrijfsvoering
    - Gebeurtenissen registreren
    - Bescherming van informatie in logbestanden
    - Monitoring en beoordeling van dienstverlening en leveranciers
- Thema Informatiesystemen - Monitoring en beoordeling van dienstverlening van leveranciers
- Thema Databescherming - Beleid inzake het gebruik van cryptografische beheersmaatregelen

We lichtten de thema's met de bijbehorende maatregelen toe in een memo (Corsanummer 21-0293024). Deze memo boden we samen met de GAP-analyse en de bijbehorende lijst met maatregelen aan de directie aan.

5.2. Aandachtspunten op basis van de GAP-analyse AVG

Voor de volgende thema's uit de GAP-analyse vroegen wij extra aandacht en prioriteit:
- Thema Processen – Verwijderen en anonimiseren
- Thema Rechten van betrokkenen – Communicatieplan privacy en invulling rechten van betrokkenen
- Thema Beveiliging – Privacy by design en default en privacy specifieke eisen in beleid en procedures
- Thema verantwoording – Periodieke evaluatie verwerkingen

We lichtten de thema's met de bijbehorende maatregelen toe in een memo (Corsanummer 21-0327170). Deze memo boden we samen met de GAP-analyse en de bijbehorende lijst met maatregelen aan de directie aan.

6. Realisatie doelstellingen Gegevensbeschermingsbeleid

Hieronder geven we aan met welke genomen maatregelen we invulling gaven aan de strategische doelen die we in hoofdstuk 2 noemden.

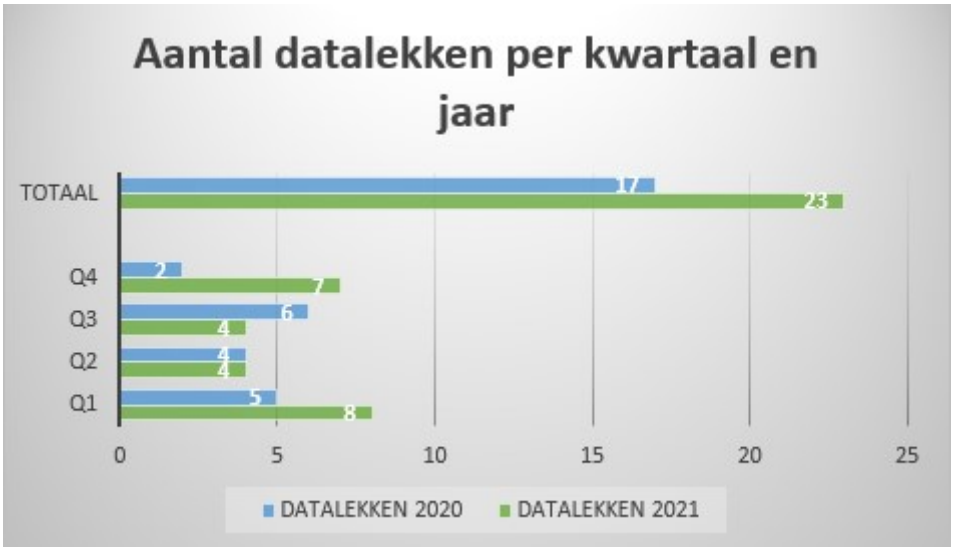
- Het managen van de gegevensbescherming.
  - We gaven gevraagd en ongevraagd advies,
  - we stelden beleid op en
  - participeerden in audits.
- Het beschermen van de privacy rechten van burgers en klanten.
  - Dit verankerden we in het beleid,
  - we voerden de processen die betrekking hebben op de rechten van betrokkenen uit,
  - we voerden een pilot uit op de naleving van verwerkersovereenkomsten en
  - werkten aan bewustwording.
- Het adequate beschermen van bedrijfsmiddelen.
  - We gaven voorlichting aan medewerkers (onder andere door het publiceren van factsheets) en
  - we adviseerden en monitorden de bevindingen uit IT-audits.
- Het minimaliseren van risico's van menselijk gedrag.
  - We zetten in op bewustwording en voorlichting via diverse kanalen. Bijvoorbeeld intranet of aansluiten bij teamoverleggen.
- Het voorkomen van ongeautoriseerde toegang tot systemen en/of informatie.
  - We begeleidden een afstudeertraject over autorisaties,
  - we gingen samen met de teams Verbijzonderede interne controle en Applicatiemanagement met dit onderwerp aan de slag (doel: borging proces periodieke controle op autorisaties),
  - we adviseerden over wachtwoordbeleid en
  - gaven adviezen hierover in diverse projecten.
- Het garanderen van correcte, tijdige en veilige informatievoorzieningen.
  - Ook hier gaven we gevraagd en ongevraagd advies en
  - participeerden we in onderzoeken en audits.
- Het waarborgen van veilige informatiesystemen, processen en verwerkingen.
  - Ook hier gaven we gevraagd en ongevraagd advies en
  - participeerden we in onderzoeken en audits.
- Het adequaat reageren op incidenten.
  - We werkten mee aan verbetering van het proces beveiligingsincidenten en
  - pasten het datalekkenprotocol toe.
- Het beschermen van kritieke bedrijfsprocessen.
  - We werkten mee aan de start van het BCM-project (**B**usiness **C**ontinuity **M**anagement).
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
  - Dit uitgangspunt verankerden we in het beleid en
  - droegen dit uit in onze werkzaamheden met betrekking tot bewustwording.
- Burgers en klanten actief informeren wat er met hun persoonsgegevens gebeurt.
  - We actualiseerden de informatie op de gemeente website,
  - we publiceerden de nieuwe versie van het verwerkingsregister en het nieuwe beleid en
  - we zorgden voor een Engelse vertaling op de gemeente website over kwetsbaarheden melden.
- Het waarborgen van de naleving van dit beleid.
  - We borgden dit verder binnen taakveld Gegevensbescherming (door bijvoorbeeld het uitvoeren van analyses).

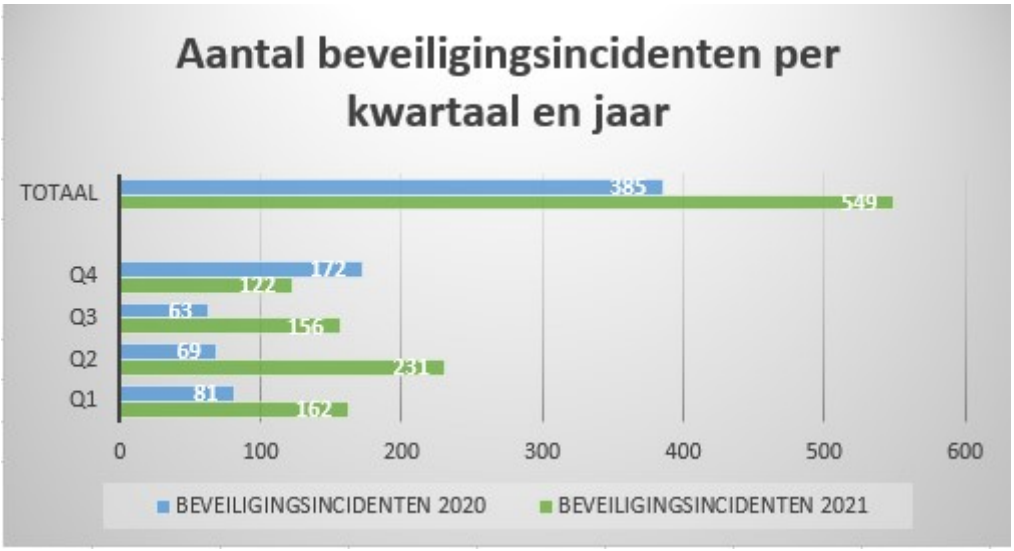
7. Incidenten en ontdekte kwetsbaarheden

In 2021 ontvingen we 549 meldingen over beveiligingsincidenten waarvan 343 over geconstateerde kwetsbaarheden. Het ging hierbij ook om ontdekte kwetsbaarheden die met updates van software en aanpassingen van de hardware waren op te lossen.
Van deze beveiligingsincidenten merkten we er 31 aan als datalek. Daarvan meldden we er 23 bij de AP (Autoriteit Persoonsgegevens) en informeerden we in 17 gevallen de betrokkenen.

Vulnerability disclosure
Nieuw dit jaar is het aantal vulnerability disclosure meldingen. Dit zijn meldingen van derden, meestal ethische hackers, die een kwetsbaarheid op onze systemen melden. Dit zijn waardevolle meldingen. Sinds het plaatsen van de Engelse tekst over onze vulnerability disclosure procedure op onze website nam het aantal melding hiervan toe. In 2021 zijn er 8 vulnerability disclosure meldingen gedaan.

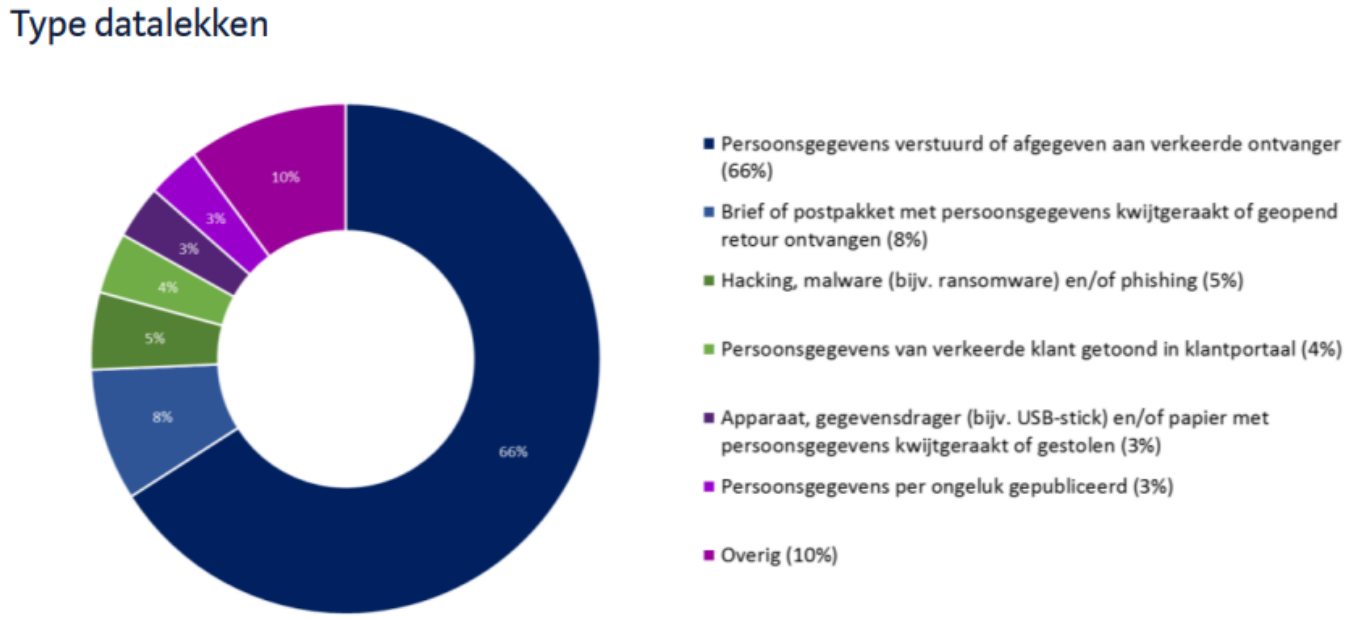
Aantallen
De afgelopen jaren steeg het aantal gemelde incidenten door het toenemende bewustzijn van medewerkers. Ook het registreren van meldingen van de Informatiebeveiligingsdienst (IBD) zorgde voor hogere aantallen. In de twee tabellen hieronder is deze ontwikkeling te zien.
Op de langere termijn verwachten we dat het aantal gemelde incidenten daalt, omdat de organisatie en ketenpartners bewuster met gevoelige informatie omgaan.





Datalekken

De gemelde incidenten delen we op diverse manieren in. De belangrijkste indeling betreft datalekken. Dit geeft invulling aan de meldplicht datalekken. Die is geregeld in de AVG.
Een beveiligingsincident valt niet per definitie onder de meldlicht. We onderzoeken bij een incident of er persoonsgegevens in verkeerde handen kwamen. Of nog zouden kunnen komen. Als dat het geval is dan wordt het incident binnen 72 uur na ontdekken gemeld bij de AP. Hierin nemen we de genomen maatregelen om het datalek te dichten op. Ook onderzoeken we direct de risico's voor personen waarvan de gegevens waren gelekt (betrokkenen). Aan de hand van de risico's bepalen we of we deze personen informeren over het datalek.
Ook de datalekken die we niet bij de AP melden, leggen we vast in het interne incidentenregister.
De AP publiceerde in 2020 onderstaand diagram over het type datalekken in Nederland. Dit komt overeen met het beeld uit onze organisatie: het overgrote deel van de datalekken in 2021 had als oorzaak 'persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger'. Aandacht voor bewustwording is vrijwel het enige waar we op in kunnen zetten om dit te voorkomen.



Kwetsbaarheden
De IBD informeert gemeenten over ontdekte kwetsbaarheden in gebruikte systemen en software. Deze meldingen komen bij gemeente Westland binnen bij de back office van taakveld I&A. Bij binnenkomst screent de back office de meldingen op urgentie. De meeste meldingen zijn met software updates snel opgelost.

Log4J
Het grootste incident van 2021 was de kwetsbaarheid op Apache Log4J. Die had en heeft wereldwijd een grote impact. Half december informeerde de IBD gemeenten over deze kwetsbaarheid. Er was nog weinig bekend over de impact binnen gemeente Westland. We wisten nog niet in welke van de applicaties en systemen Log4J zich bevond. Maar we wisten wel dat het risico erg groot was. Daarom zetten we samen met de organisatie voor dit incident een crisisorganisatie op. Deze inventariseerde in eerste instantie waar de kwetsbaarheid zich bevond. De informatie van het NCSC (**N**ationaal **C**yber **S**ecurity **C**entre) en de IBD was hierbij van onschatbare waarde. Via deze organisaties ontvingen gemeenten lijsten van de systemen en applicaties die mogelijk kwetsbaar waren. Hier kon gemeente Westland op acteren. Hierdoor schakelde de organisatie een aantal applicaties enkele dagen uit in afwachting van patches van de leveranciers.
In aanvulling hierop is forensisch onderzoek opgestart, zodat onderzocht kon worden of de gemeente op enig moment besmet is geraakt. Ook haalde de IBD een pilot om gemeentes te scannen op kwetsbaarheden, die voor 2022 gepland stond, naar voren. Hierdoor kon in de eerste week al groen licht worden gegeven: de organisatie was van buitenaf niet kwetsbaar via Log4J.
Tijdens deze crisisweken zette Bureau Vest, dat voor gemeente Westland het Business Continuity Plan schrijft, een eerste aanzet voor een crisisplan op. Met de geleerde lessen uit deze crisis wordt dit opgewerkt tot een volwaardig crisisplan voor digitale incidenten.

Afspraken en detectie
De organisatie sluit met leveranciers en ketenpartners verwerkers- of dataleveringsovereenkomsten af. In deze overeenkomsten staan eisen op het gebied van informatiebeveiliging en privacy. Dit verkleint risico’s op beveiligingsincidenten aanzienlijk.
In 2021 startten we met een uitvraag bij leveranciers waar een verwerkersovereenkomst mee was afgesloten om hun beveiligingswaarborgen aan te tonen.
Daarnaast werkt de organisatie aan het implementeren van technische maatregelen. Hiermee wordt het mogelijk om systematisch in de gaten te houden wat er gebeurt in de gemeentelijke systemen, afwijkingen te herkennen en hier vervolgens adequaat op te reageren.
Detectie zorgt voor het vroegtijdig signaleren van afwijkingen en bedreigingen en geeft daarmee ruimte om incidenten te voorkomen. Detectie zorgt dat kosten als gevolg van incidenten laag blijven. En incidenten uiteindelijk zelfs voorkomen kunnen worden. Maar ook dat zaken die niet of nooit gezien worden wel aan het licht komen en kunnen worden aangepakt. Detectie en de reactie op meldingen vereist echter tijd van beheerders, die deze tijd vaak niet beschikbaar hebben.
Als de gemeente niet weet wat er gebeurt, kan ook niet worden gestuurd op risico's. Gebrek aan inzicht in wat er feitelijk gebeurt is onwenselijk. Omdat dit het bestuur belet om adequaat te kunnen sturen op risico's, ernaar te handelen en ervan te leren.
Op de website van de gemeente is het daarom voor buitenstaanders mogelijk om op discrete en verantwoorde wijze melding te maken van een kwetsbaarheid in een ICT-systeem. Omdat melders vaak geen Nederlands spreken, zetten we in 2021 ook een Engelse versie op de site.

Het implementeren van de BIO en de AVG brengt de basis op orde. Daarmee richten we gegevensbescherming als proces in. De focus op detectie en actieve preventie zien we als de logische vervolgstap.

8. Meerjarenperspectief

In oktober 2021 stuurde Jan van Zanen vanuit de VNG een brief. Deze brief was een oproep aan alle burgemeesters in Nederland om met college, raad en ambtelijke organisatie de benodigde tijd, mensen en middelen vrij te maken om de digitale beveiliging van gemeenten in lijn te brengen met de actuele risico's van ransomware.
Deze oproep onderschrijven wij. De wil is er wel. En zeker vanuit ons taakveld adviseerden wij in 2021 geregeld over te nemen maatregelen. Maar we zien dat er een gevoel van prioriteit en urgentie mist. De waan van de dag en krapte op de arbeidsmarkt zorgt dat er sterk geprioriteerd moet worden in projecten. De security projecten zakken hierdoor doorlopend naar onderen op de prioriteitenlijsten.

Inwoners, ondernemingen en instellingen moeten erop kunnen vertrouwen dat gemeente Westland zorgvuldig omgaat met (persoons)gegevens. Daarom is het van groot belang dat de organisatie gegevens alleen onder strikte voorwaarden gebruikt. En dat de organisatie ze goed beveiligt tegen onbevoegd gebruik. Het Gegevensbeschermingsbeleid beschrijft de uitgangspunten en doelen hiervoor. Ook waarborgt het beleid dat de gemeente voldoet aan de relevante wet- en regelgeving. De CISO zorgt voor de coördinatie en het toezicht op de naleving van beveiligingsmaatregelen en -procedures. De FG is de interne toezichthouder voor de privacy.
Jaarlijks toetsen we door middel van zelfevaluatie en externe audits de maatregelen voor specifieke onderdelen:

- Basisregistratie Personen (BRP),
- Reisdocumenten,
- Digitale persoonsidentificatie (DigiD),
- Basisregistratie Adressen en Gebouwen (BAG),
- Basisregistratie Grootschalige Topografie (BGT),
- Basisregistratie Ondergrond (BRO),
- Waardering Onroerende Zaken (WOZ) en
- Inkomen (Suwinet).

De organisatie had afgelopen jaren te maken met nieuwe trends en ontwikkelingen. Dit zal ook de komende jaren niet anders zijn. Zo heeft de Coronacrisis nu al een enorme invloed op de toename van digitaal plaats- en tijd onafhankelijk werken. Diverse ontwikkelingen in de nabije toekomst maar ook die afgelopen periode al zijn ingezet mogen niet onderbelicht blijven. Dat vraagt om tijdig anticiperen en middelen beschikbaar stellen om maatregelen te nemen.

De gemeentelijke informatievoorziening is kwetsbaar. We onderscheiden hieronder een aantal categorieën van dreigingen in volgorde van belangrijkheid (*Bron: IBD*).
Dit zijn reminders waar de organisatie nu en de komende jaren rekening mee moet houden.

Intern en onbedoeld
Er zijn dreigingen door onbedoelde neveneffecten van logisch menselijk handelen. Medewerkers doen hun best om het werk snel, efficiënt en kwalitatief goed te doen. Bureaucratie is 'uit' en ondernemerschap is 'in'. De kortste weg naar het resultaat is er vaak één met valkuilen.
Voorbeelden: e-mails met gevoelige gegevens aan de verkeerde geadresseerde sturen, USB-stick verliezen of het per ongeluk wissen van bestanden.

Extern, bedoeld maar ongericht
Het grootste deel van de incidenten vanuit een externe actor komt voort uit geautomatiseerde bulkaanvallen. Kwaadwillenden scannen het internet af op bekende zwakheden in hard- en soft-

ware, proberen veelvoorkomende gebruikersnaam-wachtwoord-combinaties of sturen honderdduizenden phishing berichten aan elk adres dat ze tot hun beschikking hebben.
Gemeenten zijn dan gewoonweg het slachtoffer omdat ze aangesloten zijn op het internet, doorgaans niet omdat ze de Nederlandse overheid zijn. De gevolgen van ongerichte aanvallen kunnen groot zijn: de meeste aanvallen met gijzelsoftware zijn in eerste instantie ongericht. Het komt voor dat buitgemaakte inloggegevens van ongerichte aanvallen worden aangeboden aan de hoogste bieder. In zo'n geval kan een ongerichte aanval het opstapje vormen voor een gerichte aanval.

Extern, bedoeld en gericht
Veel aandacht gaat uit naar gerichte dreigingen van hackers en criminelen. Dit fenomeen levert spannende verhalen op in de media. Dit zijn tevens de gevallen die we maar heel moeilijk kunnen ontdekken en die men ook bij de IBD (dus) relatief weinig tegenkomt.
Een dergelijke gerichte aanval start vaak met onderzoek door de hacker naar informatie die kan worden gebruikt bij een hack. Op sociale media zoals LinkedIn is veel op het oog onschuldige zakelijke informatie te ontdekken waar een kwaadwillende zijn voordeel mee kan doen. De wat meer gesloten bronnen leveren nog meer informatie op. Er circuleren lijsten met miljarden gestolen gebruikersnamen en wachtwoorden van eerdere hacks. De IBD krijgt meldingen van doelgerichte inlogpogingen op systemen of gerichte phishingmails met een keurige aanhef en een plausibele aanleiding met het doel om geld of (inlog) gegevens buit te maken. Digitaal vandalisme zoals het platleggen van websites scharen we ook onder deze dreigingscategorie.

Intern en bedoeld
De meest riskante dreiging komt van binnen de organisatie.
Medewerkers met kwade bedoelingen kunnen uit hoofde van hun functie bij veel gegevens en systemen. Vooral medewerkers met verhoogde toegangsrechten zoals ICT-beheerders en management kunnen grote schade aanrichten. Deze dreiging is nog moeilijker te ontdekken. Interne medewerkers kennen de interne processen en controlemechanismen en kunnen die daarom beter omzeilen dan iemand van buiten.

We weten niet wat we niet weten
Het feit dat er in een gemeente weinig of geen incidenten lijken te zijn, hoeft niet te betekenen dat er niets gebeurt. Besef dat er in elke organisatie incidenten zijn. Als de directie en het management die niet kennen, dan is dat zorgelijk. Het boven tafel krijgen van incidenten vereist een open cultuur waarin medewerkers zich vrij voelen om situaties te melden.
Daarnaast is er ook een technische component: systematisch in de gaten houden wat er gebeurt in de gemeentelijke systemen, afwijkingen herkennen en hier vervolgens adequaat op reageren.

8.1. Risico's voor de ambtelijke organisatie

De meest prominente risico's manifesteren zich in de ambtelijke organisatie; bij de medewerkers die iedere dag gebruikmaken van informatie- en communicatiesystemen om hun werk te doen. Menselijk gedrag vormt één van de grootste risico's in gegevensbescherming. Een onbewuste fout is zo gemaakt. Op een verdacht linkje klikken kan ook in de zakelijke omgeving voorkomen.
In 2021 werd er voor het overgrote deel thuisgewerkt. Medewerkers maakten daardoor misschien meer gebruik van privé computers. Of hadden geen aparte werkruimte en werden zakelijke documenten mogelijk niet voldoende beschermd.
In 2022 zetten we in samenwerking met taakveld POO, met behulp van E-learning, een opleidingstraject voor medewerkers op. Hiermee kunnen alle medewerkers op een voor hun geschikt moment de informatie tot zich nemen. We hopen hiermee de bewustwording te vergroten. We me-

ten in een managementportaal de voortgang hiervan. Dit laatste is van belang in verband met aantoonbaarheid bij audits.

Bedrijfscontinuïteit in het geding
Of het nu door een technische oorzaak komt (fouten in hard- en software) of door een niet technische oorzaak (een faillissement van een dienstverlener, een pandemie, een brand, een vlooienplaag, een overstroming, enzovoort). Het kan voorkomen dat het werk niet kan doorgaan zoals dat normaal gaat. Deze risico's vinden een oorzaak in de digitale wereld of ze manifesteren zich uiteindelijk in het feit dat een computersysteem niet werkt.

Per proces hoort bekend te zijn wat de kernfunctie is en hoe die door middel van een informatiesysteem wordt ondersteund. Gemeenten moeten bij uitval of onbeschikbaarheid van een informatiesysteem een plan hebben.
Risico's met betrekking tot de bedrijfscontinuïteit nemen toe. Omdat online processen steeds meer de standaard worden en de offline alternatieven verdwijnen. Waarbij vroeger voor een aanvraag een papieren formulier met handtekening nog werd overgenomen in een computersysteem, is nu de online aanvraag de directe start van een aanvraagproces. Wanneer een systeem uitvalt kan niet worden teruggevallen op papieren processen.
In 2021 startte de organisatie met de opzet van een business continuïteitsplan. De verwachting is dat dit plan in 2022 opgeleverd wordt. Een continuïteitsplan biedt handvatten om de organisatie weer naar een werkende situatie terug te brengen na een calamiteit.
Ook moet een crisisplan opgesteld worden wat zich specifiek richt op cybercrises. Een hack van de gemeentelijke systemen heeft immers een andere impact dan een grote brand of andere ramp binnen de gemeente. De organisatie heeft voor het opzetten van een cybercrisisplan op dit moment nog geen plannen. Dit is naar onze mening wel noodzakelijk.

Integriteit van gegevens is niet gewaarborgd
We vertrouwen erop dat de persoon die inlogt in een systeem ook degene is aan wie we toestemming geven om dat te doen. En dat deze persoon op dat moment ook een gegronde reden heeft om in te loggen. Om technische (een hack) en niet-technische (een medewerker met kwade bedoelingen) redenen kan het zijn dat iemand werk uitvoert dat niet de bedoeling is. Een kwaadwillende kan in zo'n geval gegevens wijzigen, wissen of toevoegen. Een onterechte factuur indienen of goedkeuren, een vergunning verstrekken, een uitkering toewijzen, de hoogte van een vergoeding bepalen of een paspoort verstrekken. Dat begint allemaal met het invoeren van gegevens in informatiesystemen.

Vertrouwelijke gegevens in verkeerde handen
Een e-mail aan een verkeerd mailadres, een foutje in de toegangsrechten van een gedeelde map (menselijke fouten), een onontdekt lek in een systeem (technische fouten) of een niet gedicht lek in een systeem (een combinatie van menselijke en technische fouten) kunnen ertoe leiden dat vertrouwelijke informatie onbedoeld onder ogen van ongeautoriseerde personen komt. De gemeente werkt met legio vertrouwelijke gegevens over inwoners. Maar ook over de eigen bedrijfsvoering: denk aan aanbestedingen, plannen, memo's, salarissen.

8.2. Risico's voor het openbaar bestuur en de politiek

Imagoschade
Fouten van medewerkers worden het bestuur aangerekend.
Daarnaast krijgen bestuurders en politieke ambtsdragers veel gevoelige en vertrouwelijke informatie onder ogen. Een zorgvuldige omgang is vereist. Het vertrouwen in de gemeente en de ambtsdragers kan ernstig worden aangetast als (vertrouwelijke) informatie wordt gebruikt om er zichzelf of anderen mee te bevoordelen. Belangrijk is ook om (digitale) stukken goed op te bergen. En de interne beveiligingsinstructies op te volgen die gelden voor gebruik van smartphones, tablets en pc's, et cetera. Het vertrouwen in de overheid hangt onder meer samen met de wijze waarop men omgaat met gegevens. Dat wil zeggen: inwoners van de gemeente moeten er op kunnen vertrouwen dat de gemeente gegevens op een passende manier beschermt en plannen uitvoert zoals ze zijn afgesproken.

Financiële schade
Op meerdere manieren kan een gemeente geconfronteerd worden met financiële schade als gevolg van ontbrekende informatiebeveiliging. Denk aan de hack bij gemeente Hof van Twente.
Een ambtenaar, bestuurder of raadslid kan bedoeld of onbedoeld informatie verschaffen waar een kwaadwillende zijn voordeel mee kan doen (en de gemeente gedupeerd achterblijft). Informatie rond bestemmingsplannen, aanbestedingen of veranderende regels kan zeer waardevol zijn.
Onzorgvuldige omgang met persoonsgegevens en overtredingen van de AVG kunnen leiden tot aansprakelijkheidsstellingen van getroffenen of boetes van de privacy toezichthouder.
Een boete wegens onzorgvuldig handelen met de privacy van inwoners zou bovendien leiden tot grote imagoschade.

Schade aan democratische processen
Inbreuken op de beschikbaarheid, integriteit en vertrouwelijkheid van informatiesystemen kunnen het democratische proces aantasten. Dit geldt voor zowel verkiezingen als stemprocessen van volksvertegenwoordigers. Raadsleden moeten ervan op aan kunnen dat hun stem op de juiste wijze wordt verwerkt en dat ze hun stem kunnen baseren op de juiste informatie. Bovendien is bij verkiezingen het stemgeheim een groot goed.

8.3. Risico's voor de inwoners en de ondernemers

Gegevens in verkeerde handen
Gemeenten worden geacht als goed huisvader om te gaan met de gegevens die ze onder hun hoede hebben. Als de informatie van de overheid in verkeerde handen komt zijn de mogelijke gevolgen voor inwoners en ondernemers bijna niet te overzien. Inwoners zijn voor veel gevoelige zaken afhankelijk van de overheid: zorg, werk, inkomen en andere voorzieningen. Tijdens de coronacrisis is een derde van de Nederlandse werkenden afhankelijk van regelingen die geheel of gedeeltelijk worden uitgevoerd door gemeenten. Bijna één op de tien kinderen en jongeren maken gebruik van jeugdzorg. Als over individuele gevallen informatie uitlekt, zijn de betrokkenen daar direct de dupe van.

Dienstverlening van de gemeente niet beschikbaar
Als de dienstverlening van de gemeente niet of verminderd beschikbaar is, dan kunnen inwoners en ondernemers daar hinder van ondervinden. In sommige gevallen zal er sprake zijn van licht ongemak wanneer een inwoner diensten of producten een paar dagen later geleverd krijgt. Uitval van meerdere dagen of zelfs langer kan serieuze maatschappelijke, economische en sociale gevolgen hebben.

Ontwrichting van alledaagse processen

Veel van de systemen die ervoor zorgen dat alledaagse processen goed verlopen worden aangestuurd door computersystemen. Procesautomatisering gaat onder andere over doorstroming van het verkeer, regulering van de waterstand of de toegangsverlening tot gebouwen of faciliteiten. Ook hier kunnen menselijk handelen (bedoeld of onbedoeld) of de techniek leiden tot verstoringen van de beschikbaarheid (uitval van systemen) en integriteit (groen licht in plaats van rood licht, brug open in plaats van brug dicht of ontregeling van rioleringspompen).

Wake-up call: Gijzelhackers Hof van Twente

Aan het eind van 2020 volgde het meest ingrijpende gemeentelijke cybervelligheidsongeluk. Medio december legden gijzelhackers de systemen van Hof van Twente plat. De gemeentelijke dienstverlening kwam abrupt tot stilstand. De Overijsselse gemeente moest op de blaren zitten en zag al haar systemen onbruikbaar worden, omdat de hackers alle data hadden afgegrendeld of vernietigd. Op de eis van losgeld werd niet ingegaan.

Burgemeester Ellen Nauta kon haar inwoners vertellen dat de naweeën van de cyberaanval groot zijn. Het zal nog zeker twee jaar duren voor de gemeente haar ICT-infrastructuur weer op orde heeft. De dienstverlening moet nog grotendeels handmatig verlopen. Volgens Nauta zijn er vooralsnog geen aanwijzingen dat er persoonsgegevens zijn buitgemaakt. Over de kosten van de hack kan ze nog niets zeggen. Wat er precies mis ging, moet eind februari duidelijk worden. Dat onderzoek loopt. Overigens was de gemeente niet tegen cyberinbraak verzekerd.

Hoewel we er alles aan doen om het risico zo klein mogelijk te maken is dit scenario ook voor gemeente Westland niet uit te sluiten.