PBLQ

Invulling van de Digitale Veiligheidsagenda in de gemeente Alkmaar

Versie t.b.v. bestuurlijk wederhoor
november 2023

PBLQ
verbinders in de informatiesamenleving

Inhoudsopgave

1. Inleiding

1.1 Aanleiding en opdracht

In de 21ste eeuw nemen het gebruik en daarmee ook het belang van digitale middelen toe. Met behulp van een steeds omvangrijker digitale infrastructuur beheren en benutten overheden meer en meer data en informatie. Dat betreft onder meer privacygevoelige informatie van hun inwoners. Het belang van een goede bescherming van de digitale infrastructuur en de daarin aanwezige data en informatie neemt daarmee eveneens toe.
Doordat overheden steeds meer gebruik maken van Informatie- en CommunicatieTechnologie worden zij ook steeds kwetsbaarder als de ICT zou falen. Dat kan gebeuren door bijzondere omstandigheden zoals, stroomuitval of andere calamiteiten, maar ook wanneer de digitale infrastructuur overgenomen (‘gehackt’) wordt door kwaadwillende derden. Daarom is het van belang dat overheden hun ICT-infrastructuur goed beschermen, zich voorbereiden op calamiteiten en ook, in het geval van inbreuken, in staat zijn om het functioneren van de digitale infrastructuur snel en adequaat te herstellen.

Digitalisering heeft niet alleen een grote impact op het functioneren van overheden, maar ook op het leven van alle burgers. Ook zij zijn afhankelijk van digitale middelen en lopen risico’s als privacygevoelige informatie in handen valt van derden. Het is daarmee ook een verantwoordelijkheid van overheden om hun inwoners te beschermen en die te ondersteunen in het bevorderen van een veilig gebruik van digitale middelen.

Het realiseren van digitale veiligheid wordt binnen gemeenten vaak als een juridisch en ICT-onderwerp gezien, en dus als het domein van voornamelijk de afdelingen Juridische Zaken en de afdeling ICT (of I&A; Informatie en Automatisering). Dit is echter niet genoeg om te zorgen voor het realiseren van digitale veiligheid, zowel binnen de eigen organisatie als in de lokale gemeenschap. Digitale risico’s beperken zich niet tot de eigen gemeentelijke organisatie. De gemeente werkt geregeld samen met andere overheden of organisaties waarin informatie wordt gedeeld en uitgewisseld. Ook dan dient de gemeente er aandacht voor te hebben dat deze gegevens in veilige handen zijn.
Het risicobewustzijn in de organisatie behoeft permanente aandacht, onder meer door dit te trainen en te oefenen. Is duidelijk hoe de gemeente zal reageren in het geval er inbreuken zijn op de digitale veiligheid? Zijn ieders rollen en verantwoordelijkheden bekend? Vinden er met enige regelmaat simulaties of oefeningen plaats?

Het borgen van digitale veiligheid moet idealiter een kernwaarde zijn van elke medewerker in een overheidsorganisatie. Daarmee is de menselijke factor en de dagelijkse uitvoeringspraktijk voor elke gemeente een belangrijk aandachtspunt. Digitale Veiligheid is daarmee het resultaat van zowel goede technische randvoorwaarden, de wijze waarop de veiligheid is geborgd is in processen en procedures als van de aandacht voor het bewustzijn met betrekking tot digitale veiligheid in de organisatie.

De Vereniging van Nederlandse Gemeenten stimuleert sinds enige tijd dat gemeenten aandacht besteden aan het bewaken en bevorderen van de digitale veiligheid. In dit verband heeft de VNG de Agenda Digitale Veiligheid opgesteld. Deze agenda bevat tien actielijnen om de digitale veiligheid te versterken. Deze tien actielijnen kunnen worden geclusterd in vier aandachtsgebieden. Deze zijn

‘awareness’, ‘governance’, ‘risicogericht handelen’ en ‘één overheid / samen organiseren’. Dit leidt tot de volgende ordening van deze Digitale Agenda:

Agenda Digitale Veiligheid 2020 – 2024	
Awareness	
1.	Digitale Veiligheid vergroten
2.	Weerbare organisatie
3.	De digitale Brandoefening
Governance	
4.	Decentrale verantwoording waar kan, centraal toezicht waar moet
5.	OOV-bevoegdheden en rollen voor de lokale bestuurders
Risicogericht handelen	
6.	Lokale Vitale processen bepalen vanuit maatschappelijke taken
7.	Krachtige partner in de keten
8.	Risicomanagement geeft focus
Eén overheid / Samen organiseren	
9.	Informatiebeveiligingsdienst gemeenten verbreden en versterken
10.	Eén overheid

Een uitwerking van deze agenda vindt plaats in hoofdstuk 2.

De rekenkamercommissie van Alkmaar heeft eind 2022 het initiatief genomen om te verkennen in hoeverre en op welke wijze de gemeente invulling en opvolging geeft aan deze digitale agenda. Dit heeft geleid tot de volgende onderzoeksvraag:

Centrale onderzoeksvraag
Hoe wordt binnen de gemeente Alkmaar invulling gegeven aan de Digitale Veiligheidsagenda?

Deze centrale onderzoeksvraag is uitgewerkt in de volgende deelvragen.

Deelvragen

1. Welke van de 10 actielijnen uit de VNG-agenda digitale veiligheid zijn reeds opgepakt? Hoe zijn deze uitgewerkt en uitgevoerd? Welke resultaten/ effecten zijn bekend?
2. Welke rollen hebben Raad, College en Burgemeester bij het verder ontwikkelen en in uitvoering brengen van de digitale veiligheidsagenda? Hoe zijn deze beschreven en geïmplementeerd?
3. Op welke manier zijn bestuurders (Raad, College, Burgemeester) op het moment van het onderzoek betrokken bij het tot uitvoering brengen van de digitale veiligheidsagenda? In hoeverre zijn ze geïnformeerd? Welk belang hechten zij eraan? Op welke wijze implementeren zij onderdelen van de agenda in beleid en sturing?
4. Op welke manier zijn ambtenaren op dit moment betrokken bij de digitale veiligheidsagenda? In hoeverre zijn ze geïnformeerd? Welk belang hechten zij eraan? Is hun werkwijze ervan doordrongen?

Met de resultaten van het onderzoek wil de rekenkamer de gedachtewisseling in de raad over de sturing op en de controle van digitale veiligheid in de gemeente ondersteunen en stimuleren.

1.2 Referentiekader

Het onderzoek heeft primair een beschrijvend en inventariserend karakter. De beoordeling van de inspanningen en activiteiten van de gemeente staat minder centraal. Om die reden is in dit onderzoek niet gewerkt met een normenkader maar met een referentiekader. Dit kader heeft een ondersteunende functie bij het beschrijven van de staat van digitale veiligheid, zoals daar aandacht aan wordt besteed door de gemeente Alkmaar. De actielijnen van de Agenda Digitale Veiligheid verschaffen het uitgangspunt voor dit kader. Door de bevindingen voor de gemeente Alkmaar in verband te brengen met de actielijnen ontstaat een beter inzicht in de structurering van het gemeentelijk beleid. Dit betekent dat wordt bekeken:

- Of elke actielijn in het beleid van de gemeente Alkmaar en in het dagelijks handelen van de medewerkers een duidelijk herkenbare positie heeft;
- Of het beleid (zowel de voorbereiding als de uitvoering daarvan) recht doet aan hetgeen bij elk van die actielijnen van gemeenten wordt verlangd;
- Of en tot welke resultaten dit leidt.

1.3 Werkwijze

Het onderzoek is begonnen met een startbijeenkomst waaraan de rekenkamercommissie, de onderzoekers van PBLQ en verschillende vertegenwoordigers van de gemeentelijke organisatie, waaronder de portefeuillehouder veiligheid en de portefeuillehouder digitale zaken, hebben deelgenomen. Vervolgens is kennisgenomen van beschikbare relevante documenten. Aansluitend is in tien individuele gesprekken met ambtenaren en portefeuillehouders ingegaan op het gemeentelijk beleid. In twee verdiepingsbijeenkomsten met bij de dagelijkse uitvoering van beleid betrokken ambtenaren is ingegaan op de wijze waarop zij invulling geven aan de digitale veiligheid. Op die manier is getoetst of bij de uitvoering van beleid betrokken ambtenaren de uitgangspunten met betrekking tot digitale veiligheid kennen en naleven.
In het kader van het onderzoek is tevens een gedachtewisseling met raadsleden belegd. Tijdens deze bijeenkomsten is ingegaan op de wijze waarop raadsleden hun kaderstellende, controlerende en volksvertegenwoordigende verantwoordelijkheden met betrekking tot het bevorderen van digitale veiligheid in Alkmaar ervaren.

Het veldwerk voor dit rekenkameronderzoek is kort na de zomer van 2023 afgesloten. Van eventuele ontwikkelingen en aanpassingen in het geldende beleid die na de zomer van 2023 hebben plaatsgevonden, kan in deze rapportage geen melding worden gemaakt.

1.4 Indeling rapport

Dit rapport is als volgt ingedeeld. In hoofdstuk 2 worden de tien actielijnen van de Digitale Veiligheidsagenda elk kort nader beschreven. Vervolgens worden in dit hoofdstuk bij elke actielijn de bevindingen met betrekking tot Alkmaar, verkregen uit diverse documenten, interviews en de praktijkverkenning, gepresenteerd. Hoofdstuk 3 is gericht op de positie en verantwoordelijkheden van de diverse bestuursorganen in Alkmaar, het College van B&W en de gemeenteraad.
De aldus verkregen inzichten leiden in hoofdstuk 4 tot de beantwoording van de onderzoeksvragen en een toetsing aan het referentiekader. Daaraan worden verschillende aanbevelingen verbonden.

2. Invulling kaders digitale veiligheid

2.1 Inleiding

Dit hoofdstuk bevat de verkregen inzichten met betrekking tot de opvolging door de gemeente Alkmaar van de actielijnen in de Agenda Digitale Veiligheid van de VNG. Deze informatie is relevant voor de beantwoording van de volgende twee deelvragen:

Deelvragen

1. *Welke van de 10 actielijnen uit de VNG-agenda digitale veiligheid zijn reeds opgepakt? Hoe zijn deze uitgewerkt en uitgevoerd? Welke resultaten/ effecten zijn bekend?*
4. *Op welke manier zijn ambtenaren op dit moment betrokken bij de digitale veiligheidsagenda? In hoeverre zijn ze geïnformeerd? Welk belang hechten zij eraan? Is hun werkwijze ervan doordrongen?*

De verkregen informatie is ontleend aan drie bronnen. De eerste daarvan zijn de beschikbare beleidsdocumenten van de gemeente. Deze zijn vermeld in bijlage A. De tweede bron betreft de gesprekken die hebben plaatsgevonden met medewerkers van de gemeente die een rol of verantwoordelijkheid hebben in de inrichting van het beleid met betrekking tot digitale veiligheid. In dit verband is ook gesproken met de portefeuillehouder.[1] Een overzicht van de gesproken functionarissen is opgenomen in bijlage B.
In het kader van het onderzoek hebben twee verdiepingssessies plaatsgevonden met ambtenaren die in twee verschillende domeinen betrokken zijn bij de uitvoering van het beleid. Deze sessies vormen de derde informatiebron. De functies van de deelnemers zijn vermeld in bijlage C.

2.2 Awareness

In veel beschouwingen over digitale veiligheid wordt de menselijke factor van groot belang geacht. Vanuit die optiek besteedt de Agenda Digitale Veiligheid van de VNG allereerst aandacht aan het bevorderen van het bewustzijn van medewerkers van gemeenten over de relevante risico's en opgaven. De agenda stelt hierover (pagina 8): "Het is van essentieel belang dat lokale overheden interne bewustwording creëren over het belang van privacybescherming van privacygevoelige data van inwoners en de impact als deze data op straat komen te liggen."
De nagestreefde 'awareness' gaat verder dan louter aandacht voor privacybescherming. Het betreft tevens de aandacht voor pogingen van derden om toegang te krijgen tot de ICT-infrastructuur van de gemeente (hacken). Weliswaar kunnen er vele technische waarborgen tegen hackpogingen of andere inbreuken op de cyberveiligheid worden genomen, de ervaring leert dat de menselijke factor een groot risico vormt. In dat verband wordt in de Digitale Agenda (pagina 8) genoemd: "Het begint echter wel met menselijk falen en kwetsbaarheden; slechte wachtwoorden, een ondoordachte klik of onvoldoende controle op de eigen veiligheid."

Het bevorderen van de Awareness wordt in de digitale agenda uitgewerkt in drie actielijnen. De eerste richt zich op het bewustzijn van de medewerkers en de inwoners, de tweede op voorbereiding op en

[1] Bij aanvang van het onderzoek waren dat twee portefeuillehouders; één voor openbare orde en veiligheid en de andere voor de digitale aangelegenheden van Alkmaar. Echter, direct na aanvang van het onderzoek bestond het college louter nog uit één persoon, die daarmee portefeuillehouder 'van alles' was. Met deze bestuurder, de burgemeester, heeft het gesprek plaatsgevonden. Na aantreden van het huidige college is ICT belegd bij wethouder Epskamp, binnen de brede portefeuille van Personeel en Organisatie. Met deze wethouder heeft geen gesprek plaatsgevonden.

alertheid van de organisatie als het gaat om digitale verstoringen en de derde op het oefenen met digitale noodscenario's ter voorbereiding op daadwerkelijke incidenten.

2.2.1 Actielijn 1: Bewustzijn vergroten

In 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Deze verordening betreft een uitwerking van Europese regelgeving die bedoeld is om de privacy van alle inwoners (beter) te beschermen. In het kader van de AVG zijn organisaties, waaronder ook overheden, verplicht om specifieke functionarissen aan te stellen en allerlei procedures in te regelen. Deze zijn beschreven in het navolgende kader.

Korte Inleiding op de Algemene Verordening Gegevensbescherming (AVG)[2]

De ***AVG*** heeft tot doel om de privacy van burgers te beschermen. Om ervoor te zorgen dat dit inderdaad het geval is, zijn er voor organisaties als gemeenten verschillende waarborgen, procedures en functionarissen van belang. Deze zijn:
Functionaris Gegevensbescherming: Gemeenten zijn verplicht een Functionaris Gegevensbescherming (FG) aan te stellen. Deze functionaris houdt toezicht op de toepassing en naleving van de AVG.
Data protection Impact assessment: De AVG verplicht gemeenten om een data protection impact assessment (**DPIA**) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen, mede om vervolgens maatregelen te kunnen nemen ter verkleining en beheersing van de risico's.
Verwerkingsregisters: Gemeenten zijn verplicht om een verwerkingsregister bij te houden. Dit register bevat informatie over de persoonsgegevens die door de organisatie worden verwerkt.
Een veilige omgang met gegevens is ook zeer gediend met het inrichten en naleven van een gedegen ***informatiebeveiligingsbeleid***. Gemeenten stellen daartoe een ***Chief Information Security Officer (CISO***) aan, die verantwoordelijk is voor dit informatiebeveiligingsbeleid. Dit betreft zowel het implementeren van beleid als het toezicht houden op de uitvoering ervan. Ook het definiëren en ontwerpen van de strategie op het gebied van informatiebeveiliging behoort tot het takenpakket.
Gemeenten stellen tevens een ***Privacy Officer (PO)*** aan. Een Privacy Officer zorgt ervoor dat de AVG wordt nageleefd binnen een organisatie en ziet erop toe dat de privacy en dataverwerking bij elke medewerker die persoonsgegevens verzamelt, in veilige handen is. Een PO geeft advies en biedt ondersteuning, geeft interne trainingen en heeft een rol bij het melden van datalekken.
Een gemeente werkt vaak samen met andere organisaties voor het uitvoeren of ondersteunen van taken. Dit kan een bedrijf zijn, een andere gemeente of bijvoorbeeld een gemeenschappelijke regeling. Zo'n andere organisatie heet een ***verwerker*** van persoonsgegevens. De gemeente blijft zelf eindverantwoordelijk voor de privacy van de persoonsgegevens van zijn inwoners. In AVG termen is de gemeente de ***verwerkingsverantwoordelijke***. Wanneer een andere organisatie persoonsgegevens verwerkt moet er altijd een ***verwerkersovereenkomst*** worden afgesloten tussen beide partijen. Hierin worden afspraken gemaakt over onder andere het doel van de verwerking, geheimhoudingsplicht, beveiliging, verwijderingstermijnen en auditverplichtingen.

Mede vanwege de verplichtingen die voortvloeien uit de AVG en het daarmee sterk verbonden belang van goede informatiebeveiliging heeft de Nederlandse overheid de Baseline Informatiebeveiliging Overheid ontwikkeld.

[2] Zie voor een uitgebreide uitleg voor diverse begrippen en procedures: notendop_avg.pdf (autoriteitpersoonsgegevens.nl)

Baseline Informatiebeveiliging Overheid (BIO)

De Vereniging van Nederlandse Gemeenten heeft in samenwerking met andere (belangenorganisaties van) overheden de **Baseline Informatiebeveiliging Overheid (BIO)** ingericht. In de BIO is het basisniveau voor informatiebeveiliging beschreven. Informatiebeveiliging is het proces van het nemen en beheren van passende technische en organisatorische maatregelen om dit te garanderen. Omdat de AVG stelt dat er technische en organisatorische maatregelen moeten worden ondernomen ten aanzien van de verwerking van persoonsgegevens, is er overlap tussen privacy en informatiebeveiliging. Het op deze wijze ontwikkelde voor Nederlandse overheden ontwikkelde normenkader is de Baseline Informatiebeveiliging Overheid (BIO). In de BIO zijn (verplichte) beheersmaatregelen opgenomen. Verder gaat de BIO uit van risicomanagement op basis van een Plan-Do-Check-Act cyclus om de beveiliging continue bij te stellen en te verbeteren. Voor de verantwoording over informatiebeveiliging gebruiken gemeenten de ENSIA-systematiek (Eenduidige Normatiek Single Information Audit). Via deze systematiek legt de gemeente verantwoording af over de informatieveiligheid van een aantal basisregistraties en informatiestelsels (waaronder de Basisregistratie Personen, DigiD en Suwinet).

Elke gemeente heeft moeten anticiperen op de inwerkingtreding van de AVG. Onder meer hebben gemeenten hun privacybeleid in lijn gebracht met de AVG, de vanwege de AVG verplichte functionarissen aangesteld, verwerkersregisters ingericht en de verschillende instrumenten toegepast.

- *De situatie in Alkmaar*

In februari 2019 heeft het college van B&W van Alkmaar de Nota ‘Afspraken op het beleidsterrein van Informatiebeveiliging informatievoorziening en privacy’ vastgesteld. Dit is een nota ten behoeve van het College van B&W. De nota is niet gedeeld met de gemeenteraad.
De nota betreft in essentie een bevestiging van de vereisten uit de AVG voor Alkmaar, zoals het benoemen van een FG, een CISO en een Privacy Officer. Ook worden de taken en verantwoordelijkheden van diverse functionarissen en afdelingen (B&W, Directie, afdeling I&A) en Juridische Zaken, verder ingevuld.

Over het bevorderen van het bewustzijn van medewerkers stelt deze nota (pagina 3):

> *“De gemeente Alkmaar heeft zich in het projectplan ‘Het Nieuwe Veilig Werken’ tot doel gesteld de bewustwording van medewerkers te vergroten en zich aan geldende wet- en regelgeving te houden. Dat betekent dat de komende drie jaren wordt gewerkt aan het optimaliseren van de opzet, het bestaan en de werking van processen. Daarnaast acht de gemeente Alkmaar het van belang dat alle medewerkers in 2021 weten wat informatiebeveiliging is en wat zij eraan moeten doen om veilig met de informatie om te gaan. Daarbij is het belangrijk dat alle medewerkers beseffen dat zij zelf een verantwoordelijkheid hierin hebben.”*

Op pagina 4 van de nota wordt genoemd:

> *“Het Nieuwe Veilig Werken’ houdt in dat de verantwoordelijkheid om verantwoord met gegevens om te gaan bij de medewerker ligt. Denk hierbij aan papierloos werken, voorkomen datalekken, veilig mailen, veilig omgaan met WiFi, clean screen & desk en zo voort. Medewerkers mogen zowel in de kantooromgeving als elders werken, op beide zijn dezelfde beveiligingseisen van toepassing.”*

Met betrekking tot nieuwe medewerkers is in de nota (pagina 5) vastgelegd:

> *"Bij het aannemen of inhuren van nieuw personeel en het laten verrichten van werkzaamheden door externe medewerkers wordt bewerkstelligd dat zij hun verantwoordelijkheden begrijpen ten aanzien van informatieveiligheid. Deze verantwoordelijkheden zijn vóór het dienstverband vastgelegd in een passende functiebeschrijvingen/opdracht en in de arbeidsvoorwaarden/inhuurovereenkomst."*

In december 2022 is een Nota ten behoeve van de medewerkers over het privacy en informatiebeveiligingsbeleid van Alkmaar opgesteld.[3] Deze is in januari 2023 door het college vastgesteld. In deze Nota worden onder meer de taken en verantwoordelijkheden van allerlei organisatieonderdelen en functionarissen beschreven. In dit verband wordt ook een rol voor de 'ambassadeurs informatiebeveiliging en privacy' genoemd. Hierover wordt gesteld (pagina 16):

> "*Dit is een decentrale rol die belegd is bij medewerkers die met extra training ondersteund worden om de awareness op het gebied van informatiebeveiliging en privacy bij collega's op de werkvloer te stimuleren. De ambassadeurs ondersteunen hun collega's, geven voorlichting en kunnen richting CISO signaleren indien er aandachts- of verbeterpunten zijn. De ambassadeurs ondersteunen de unitmanagers bij het uitvoering geven aan hun verantwoordelijkheid op het vlak van informatievoorziening en privacy.*
> *De CISO organiseert periodieke meetings en ondersteunt de ambassadeurs met specifieke trainingen. Elke unit dient minimaal één medewerker in deze rol te hebben en de ambassadeur de tijd te geven om de taak adequaat in te kunnen vullen.*

Op de pagina's 13 en 14 van deze nota wordt met betrekking tot de medewerkers gesteld:

> *"De medewerkers:*
> - *Zijn bekend met het informatiebeveiligings- en privacy beleid en handelen daarnaar;*
> - *Houden zich aan gedragsafspraken voor het veilig omgaan met persoonsgegevens, informatie en bedrijfsmiddelen;*
> - *Doen periodiek kennis en bewustwording op afgestemd op hun werkzaamheden en verwerkingen die ze binnen hun unit uitvoeren;*
> - *Melden datalekken beveiligingsincidenten en volgen daarbij de mitigerende adviezen van de PO of de CISO op;*
> - *Indien gebruik wordt gemaakt van geleende devices, worden de devices bij beëindiging van het dienstverband teruggegeven aan de gemeente;*
> - *Zijn bekend mee en werken volgens het "Beleid Mobiele Devices en locatieonafhankelijk werken."*

Voor het overige wordt in deze nota uitgebreid ingegaan op procedures rond gegevensbeveiliging, het delen van informatie met andere organisaties (verwerkersovereenkomsten en -registers) en het voldoen aan de BIO waaronder het regelmatig uitvoeren van een ***Data Protection Impact assessment*** (DPIA).

In de interviews die in het kader van dit rekenkameronderzoek met direct betrokken functionarissen hebben plaatsgevonden is dit 'papieren beleid' in algemene zin bevestigd, maar ook op onderdelen

[3] Nota Privacy- en informatiebeveiligingsbeleid gemeente Alkmaar

genuanceerd. Zo is genoemd dat zeker kort na de inwerkingtreding van de AVG in 2018 er veel aandacht is geweest voor het bevorderen van het privacybewustzijn in de organisatie, door middel van trainingen en bewustzijnsacties.
Als uitwerking van de nota heeft de gemeente Alkmaar zich in het projectplan 'Het Nieuwe Veilig Werken' als doel gesteld dat alle medewerkers moeten weten wat informatiebeveiliging is en wat zij eraan moeten doen om veilig met de informatie om te gaan. Medewerkers moeten er zich van bewust zijn dat zij ook zelf de verantwoordelijkheid hiervoor dragen.
In alle in het kader van het onderzoek gevoerde gesprekken is genoemd dat er ook vandaag aan de dag met enige regelmaat acties plaatsvinden om het bewustzijn van medewerkers te bevorderen. Ook is er steeds de gelegenheid om deel te nemen aan daarvoor relevante trainingen. Voor nieuwe medewerkers is het verplicht om een training met betrekking tot privacy en informatieveiligheid te volgen. Ter afsluiting daarvan dienen zij enkele vragen te beantwoorden en daar een voldoende resultaat op te behalen.

Sommige functionarissen noemen dat de aandacht voor het bevorderen van het bewustzijn van de medewerkers voor het belang van een veilige omgang met data en informatie gaandeweg is verminderd.
Dat geldt ook andere aspecten van het privacybeleid. Voor zowel het afsluiten van verwerkingsovereenkomsten als het uitvoeren van DPIA's geldt dat hier ook vandaag aan de dag invulling aan wordt gegeven, maar dat de opvolging van DPIA's en het actualiseren van het verwerkingsregister niet altijd plaatsvinden. Als oorzaken hiervoor worden de bijzondere omstandigheden tijdens de Coronaperiode genoemd en het vertrek van -enkel voor dit beleid cruciale - functionarissen. Voor sommige van hun functies geldt dat zij momenteel op interimbasis en/of gecombineerd met andere verantwoordelijkheden worden ingevuld. De stapeling van verantwoordelijkheden bij een beperkt aantal functionarissen maakt het lastig om aan alle verantwoordelijkheden goede invulling en opvolging te geven. Voor een deel is geprobeerd hierin te voorzien door naast, of in combinatie met, de functie van ambassadeurs informatieveiligheid en privacy specifieke taken en verantwoordelijkheden (zoals die van de Functionaris Gegevensbescherming) lager in de organisatie te beleggen. Sommige medewerkers van de organisatie zijn van mening dat taken en verantwoordelijkheden daarmee minder duidelijk zichtbaar zijn geworden.

In de sessies met uitvoerende medewerkers is gebleken dat zij zich in het algemeen goed bekend tonen met het belang van het bevorderen en bewaken van informatieveiligheid, privacy en cybersecurity. Zij zijn bekend met diverse acties om hun bewustzijn over deze onderwerpen te bevorderen. Tegelijkertijd geven ze aan dat als ze zich willen onttrekken aan deze acties, dit eenvoudig kan plaatsvinden. Zij verwachten niet dat ze daar dan op zullen worden aangesproken. Deze medewerkers geven aan dat ze weten hoe ze moeten handelen indien zij het vermoeden hebben van een datalek of als zij behoefte hebben aan adviezen over privacy en de bescherming van informatie. Ook als zij problemen ervaren met ICT-systemen en -devices weten ze waar ze terecht kunnen. In deze sessies is niet gebleken dat het de deelnemers bekend is dat collega's in hun naaste omgeving invulling geven aan verantwoordelijkheden van de FG. Evenmin is gebleken dat zij goed bekend zijn met de 'ambassadeurs informatiebeveiliging en privacy'. Overigens geldt voor dat laatste dat zij zich wel ervan bewust zijn welke van hun collega's over goede kennis met betrekking tot informatiebeveiliging en privacy beschikken. Hun is dan vooral niet bekend of dit ook collega's zijn die 'ambassadeur' zijn.

- Het beleid voor de lokale gemeenschap

Het streven om het kennisniveau rondom digitale veiligheid te vergroten, geldt niet alleen voor bestuurders en het ambtelijk apparaat, maar ook voor inwoners. Bij de behandeling van de kadernota veiligheid 2019-2022 is er door de raad van Alkmaar unaniem een amendement aangenomen waarin is vastgelegd:

> *"Het college komt in Q4 2019 met concrete voorstellen en een plan van aanpak om het bewustzijn onder haar inwoners op het gebied van cybercrime te vergroten en informatie te geven over hoe dit voorkomen kan worden."*

Door middel van dit amendement is digitale veiligheid een belangrijk onderdeel van het veiligheidsbeleid geworden. In de programmabegroting 2020 van de gemeente Alkmaar wordt hier opvolging aan gegeven. In programma vier, veiligheid, is als doel opgenomen dat inwoners en ondernemers zich bewust moeten zijn van hun digitale kwetsbaarheid en daardoor weerbaarder tegen cybercriminaliteit zijn. In de rapportage 'stand van zaken veiligheid', een tweejaarlijks verslag over de uitvoering van het veiligheidsbeleid staat dat er in 2021 en 2022 campagnes en activiteiten, ten aanzien van (het beschermen tegen) online gevaren zijn opgezet voor ondernemers, jongeren, ouderen en laaggeletterden. Voorbeelden zijn;

- Zelf in hand; een campagne over online oplichting.
- Online boeven de baas; een informatiemarkt om inwoners bewuster te maken over digitale kwetsbaarheid en hen weerbaarder te maken tegen de risico's van online criminaliteit.
- Hackshield; een online spel voor kinderen tussen 8 en 12 jaar over de gevaren op het internet.
- Digitaal wijkambassadeurs; acht digitaal wijkambassadeurs ten behoeve van het voorkomen van cybercrime in hun wijk door hen te informeren en adviseren.

2.2.2 Actielijn 2: Weerbare organisatie

Uitgangspunt van deze actielijn is dat de gemeente is voorbereid op inbreuken op de informatieveiligheid. In dat verband is het niet alleen belangrijk om weerbaar te zijn en veiligheidsmaatregelen te nemen tegen risico's, maar ook veerkrachtig op te kunnen treden wanneer een incident zich daadwerkelijk voordoet. Zo is het belangrijk dat onderbrekingen in de bedrijfsvoering, bijvoorbeeld ten gevolge van een hack maar ook vanwege een calamiteit, snel opgelost kunnen worden.

- *Alkmaar als weerbare organisatie*

In enkele van de in paragraaf 2.2.1 aangehaalde nota's wordt ook ingegaan op de maatregelen die Alkmaar heeft genomen om een weerbare organisatie te kunnen zijn. Zo is binnen de organisatie de functie van CISO gecreëerd en ingevuld; een Chief Information Security Officer. Een CISO heeft een toezichthoudende en controlerende rol op het gebied van informatiebeveiliging. Meestal coördineert de CISO ook de rapportageverplichtingen over de ontwikkelingen rondom informatiebeveiliging. Eind 2022 is de toenmalige CISO met pensioen gegaan. Sindsdien vervult de concerncontroller, naast de rol van de FG, op ad interimbasis ook de rol van CISO. De Autoriteit Persoonsgegevens (AP) geeft aan dat de functie CISO niet verenigbaar is met het vervullen van de functie van de FG, omdat de FG dan niet onafhankelijk kan opereren.[4]

Er zijn ook de nodige maatregelen geïmplementeerd met betrekking tot het beveiligen van de ICT-infrastructuur. Tot voor enkele jaren terug had Alkmaar wat ICT er een voorkeur voor om zowel hardware als softwareapplicaties in eigen beheer te hebben. Sinds enige tijd is dit veranderd. Veel

[4] Verschillende medewerkers hebben daarnaast aangegeven niet tot nauwelijks bekend te zijn met de CISO. De functie van FG en de functionaris in kwestie bleken tijdens de raadsbijeenkomst onbekend voor alle deelnemers.

diensten en processen zijn in ‘in the cloud’ geplaatst. Voor de basis ICT-infrastructuur maakt de gemeente Alkmaar gebruik van de diensten van Microsoft. Verantwoordelijken voor de ICT-infrastructuur geven aan dat Alkmaar hiermee in plaats van zelf de beveiliging van hard- en software te realiseren, gebruik kan maken van de wereldwijde kennis en ervaring van dit bedrijf. Een illustratie daarvan is de wijze waarop de gemeente Alkmaar een zogeheten *Security Operations Centre* (SOC) heeft ingericht.

Een Security Operations Centre

Een SOC werkt als een crisisteam bij incidenten in de informatiebeveiliging. Dit team monitort 24 uur per dag, zeven dagen in de week de systemen van de gemeente op incidenten en verbeteringen. Bij ieder incident wordt binnen vier uur een impact analyse uitgevoerd met behulp van de *Microsoft Cloud Defender*. Het beheer van het SOC vindt plaats onder verantwoordelijkheid van de ‘Chief Information Officer’ van de gemeente. Die bepaalt in eerste instantie de urgentie en de impact van incidenten en heeft ook de bevoegdheid om zo nodig te escaleren. Bij escalatie wordt de gemeentesecretaris op de hoogte gebracht als er keuzes moeten worden gemaakt die consequenties hebben voor de bedrijfscontinuïteit problemen

Het SOC van de gemeente Alkmaar maakt eveneens gebruik van de diensten en ondersteuning vanuit Microsoft.
Voor andere softwareapplicaties – en hun leveranciers - is het gebruikelijk geworden dat de leveranciers zelf de verantwoordelijkheid nemen voor het beheer, de beveiliging en de doorontwikkeling (“Software as a Service’).

De gemeente Alkmaar beschikt over een bedrijfscontinuïteitsplan. Doordat Alkmaar veel diensten ‘in the cloud’ heeft staan, zijn gegevens en applicaties plaats- en tijdonafhankelijk beschikbaar. Dit zijn enkele waarborgen waardoor mogelijke inbreuken op de continuïteit van de bedrijfsvoering betrekkelijk snel opgelost kunnen worden.

Om de kwaliteit van de informatiebeveiliging periodiek te toetsen is de gemeente door de rijksoverheid verplicht om periodiek een ENSIA[5] uit te voeren. Deze audit is gebaseerd op de Baseline Informatievoorziening Overheid (BIO). De gemeente Alkmaar voert de ENSIA inderdaad elke twee jaar uit. In interviews is genoemd dat bij de laatste meting er sprake bleek van slechts geringe vooruitgang. Naar mening van de respondenten was de reden hiervoor dat weliswaar uit eerdere metingen verbeteracties waren afgeleid, maar dat de naleving daarvan te weinig aandacht had gekregen. Daarvoor genoemde redenen zijn personele wisselingen en een gebrek aan personele capaciteit.

Bij het bestendigen en bevorderen van de informatieveiligheid maakt de gemeente Alkmaar ook gebruik van de kennis en informatie die verkregen wordt in regionale samenwerkingsverbanden. Dat betreft om te beginnen de Veiligheidsregio. Elke gemeente is verplicht aangesloten bij een Veiligheidsregio, in het geval van Alkmaar de veiligheidsregio Noord-Holland-Noord. Blijkens het Beleidsplan 2020-2023 richt deze Veiligheidsregio:

> *“zich op het verkleinen van risico’s en het beperken van leed en schade bij incidenten. We doen dit door adequate hulp te bieden en samen te werken met partners, inwoners en ondernemers. Om dit ook in de toekomst kunnen blijven doen, moeten we vooruit blijven kijken.”*

[5] Zie ook het kader aan het begin van dit hoofdstuk. ENSIA staat voor Eenduidige Normatiek Single Information Audit

De veiligheidsregio kent een breed aandachtsgebied, waarvan informatieveiligheid slechts een beperkt onderdeel uitmaakt. In het beleidsplan 2020-2023 wordt kort aan informatieveiligheid en cybersecurity gerefereerd. Louter een mogelijke uitval van vitale voorzieningen (elektriciteit, water) wordt genoemd als een 'waarschijnlijk risico met grote maatschappelijke impact'. Verder wordt 'cyber' genoemd (pagina 21-23) als een nieuw crisistype waar de Veiligheidsregio zich beter op wil voorbereiden.

In de Kadernota veiligheid 2023-2026 van de gemeente Alkmaar worden ook de zogenaamde online aangejaagde ordeverstoringen genoemd:

> "*Online uitingen leiden ook steeds vaker tot maatschappelijke onrust offline. Bijvoorbeeld door het online verspreiden van desinformatie, polariserende berichten en door online op te roepen tot (illegale) evenementen en demonstraties*".

Potentiële verstoringen kunnen mogelijk al eerder gesignaleerd worden, als er ook meer aandacht is voor wat er online gebeurt. De gemeente geeft in deze context aan te willen onderzoeken hoe, binnen de mogelijkheden van de wet, het beste bijgedragen kan worden aan het beheersen van online aangejaagde ordeverstoringen. De concrete uitwerking van dit voornemen is niet bekend.

In de interviews is genoemd dat na vaststelling van het Beleidsplan 2020-2023 binnen de Veiligheidsregio de aandacht voor ICT-gerelateerde risico's is toegenomen. Een duidelijke uiting daarvan is dat in het voorjaar van 2023 in de regio een crisisoefening heeft plaatsgevonden die geconcentreerd was rond een uitval van ICT-voorzieningen. Ten tijde van het onderzoek was de evaluatie van deze oefening nog niet beschikbaar. Genoemd is al wel dat de aandacht voor cyberaanvallen binnenkort wordt toegevoegd aan het rampendraaiboek.

In de kadernota Veiligheid 2023-2026 van de gemeente Alkmaar wordt melding gemaakt van de ontwikkeling van een gemeentelijk veiligheidsinformatieknooppunt (GVIK). Hierover wordt gesteld: "in het gemeentelijk veiligheidsinformatieknooppunt (GVIK) brengen we verschillende informatiestromen samen. Een veiligheidsinformatieknooppunt ondersteunt gemeenten in de uitvoering van de regierol en de wettelijke taken binnen de keten veiligheid, toezicht, handhaving, preventie, en vergunningen. Cijfers van onder andere politie en handhaving worden hier aangevuld met informatie uit de veiligheidsmonitor, gebiedsteams, inwoners, ondernemers en professionals. Met dit actuele veiligheidsoverzicht kunnen we problemen nog eerder signaleren. Dit helpt de burgemeester en het college om op tijd de juiste interventies in te zetten."

Een tweede belangrijke samenwerkingspartner is Noord-Holland-Samen-Veilig (NHSV). Dit is een samenwerkingsverband van 32 gemeenten. Omdat criminaliteit niet stopt bij de gemeentegrenzen wordt samenwerking gezien als een effectieve manier om lokale problemen samen met politie, OM en andere partners in een regionale context te bekijken en aan te pakken. Dit samenwerkingsverband richt zich op vijf thema's, waaronder 'Cybercrime en gedigitaliseerde criminaliteit'. Op hun website staat dat NHSV adviseert en ondersteunt NHSV-gemeenten, politie en OM bij het lokaal aanpakken van cybercrime. Dit gebeurt door het opzetten van projecten waar gemeenten aan deel kunnen nemen, het ontwikkelen van rapportages die zicht geven op de problematiek en het geven van trainingen. NHSV is aangesloten bij landelijke cybercrime initiatieven. De medewerker Openbare Orde en Veiligheid van de gemeente Alkmaar, die in het bijzonder aangesteld is om de aandacht voor en weerbaarheid tegen cybercrime in de lokale gemeenschap te bevorderen noemt dat zij vaak gebruik maakt van de kennis en netwerken van NHSV.
Binnen NHSV worden ook kennis en informatie gedeeld met politie en Openbaar Ministerie. Dit gebeurt ook in rechtstreekse contacten tussen deze organisaties en de gemeente.

In mei 2020 verscheen de gemeentelijke ‘Notitie Cyberveiligheid; Achtergrondinformatie en uitvoeringsplan’. In deze notitie zijn allerlei relevante bedreigingen in de context van cyberveiligheid geïnventariseerd en beschreven. Daaraan is een plan verbonden om deze bedreigingen te beheersen en te verminderen. Voor de uitvoering van deze initiatieven heeft de gemeente op projectbasis een medewerker aangesteld om de aandacht voor, en weerbaarheid tegen cybercrime in de lokale gemeenschap te bevorderen. Ook is daarvoor een projectplan opgesteld. Voor de uitvoering wordt samengewerkt met wijkagenten en bibliotheken, scholen, cybersecuritybedrijven, het MKB en seniorweb, In eerste instantie richt dit project zich daarmee niet op het versterken van de lokale gemeenschap. Tegelijkertijd signaleert de betrokken medewerker dat sommige van de in dit project ontwikkelde activiteiten ook relevantie hebben voor de eigen organisatie.
Dit project naderde ten tijde van dit onderzoek het einde van de vastgelegde periode. Een evaluatie was ten tijde van het onderzoek nog niet beschikbaar. Wel waren de indrukken positief, In verschillende gesprekken is melding gemaakt van het voornemen om dit beleid op vaste basis voort te zetten. In de Kadernota Veiligheid 2023-2026 van de gemeente wordt Cybercriminaliteit als een expliciet aandachtspunt genoemd.

Periodiek vindt er onderzoek[6] plaats naar inbreuken op de veiligheid en de beleving van veiligheid onder de inwoners van Alkmaar. Daarbij wordt ook geïnformeerd naar incidenten waarbij inwoners slachtoffer zijn geworden van hacks, phishing of andere inbreuken op hun informatieveiligheid.

Tenminste sinds 2019 zijn geen risico-analyses uitgevoerd waarbij bijzondere aandacht was voor risico’s die voortkomen uit of samenhangen met cybercriminaliteit. In interviews is genoemd dat hier in de toekomst meer aandacht voor zal zijn.

2.2.3 Actielijn 3: De digitale brandoefening

Gemeenten worden steeds afhankelijker van digitale netwerken. Hoewel de impact van digitale incidenten en –crisis in veel gevallen beperkt blijft tot de eigen bedrijfsvoering, kunnen deze ook gevolgen hebben voor de fysieke omgeving. In het algemeen weten bestuurders vaak wel waar de verantwoordelijkheden van diverse partijen (zoals OM, politie en brandweer) liggen als het gaat om fysieke veiligheid. Dat zou ook moeten gelden voor digitale veiligheidsincidenten met bijvoorbeeld een fysiek element. Dit is juist belangrijk omdat hier zowel ambtenaren bij betrokken zijn vanuit de reguliere informatieveiligheid als ambtenaren vanuit de fysieke veiligheidsketen.

De gemeente Alkmaar heeft in het voorjaar van 2023, geïnitieerd door de veiligheidsregio, een cyberoefening uitgevoerd. Ten tijde van dit rekenkameronderzoek was een evaluatie nog niet beschikbaar. Functionarissen van de gemeente die betrokken waren bij de oefening noemen dat gemeente Alkmaar naar hun mening voldoende heeft gepresteerd.
In interviews met bij de oefening betrokken functionarissen is naar voren gekomen dat er geen plan /voornemen is om de oefeningen met betrekking tot digitale weerbaarheid voortaan periodiek te laten plaatsvinden. Hierboven is al wel genoemd dat de omgang met cyberaanvallen zal worden toegevoegd aan het rampendraaiboek.

[6] Dit betreft de Veiligheidsmonitor, waarvan verslag wordt gedaan in de ‘Rapportage Stand van Zaken Veiligheid Alkmaar 2021’.

2.3 Governance

Elke gemeente kan op enig moment geconfronteerd worden met bijvoorbeeld datalekken, digitale verstoringen, incidenten en digitale criminaliteit. Dergelijke incidenten beperken zich niet tot één plaats maar kunnen ook elders ontwrichtende gevolgen hebben. Bestuurders worden daarom niet alleen geconfronteerd met de eigen bedrijfsvoering, maar óók met (digitale) incidenten in de samenleving. Het maakt dat het thema ‘digitale veiligheid’ ook aan de orde komt op de (regionale) bestuurstafel.

De governance, ten aanzien van het thema ‘digitale veiligheid’, wordt in de digitale agenda uitgewerkt in twee actielijnen. Deze richten zich op de verantwoordelijkheden die bij de gemeente Alkmaar belegd zijn.

2.3.1 Actielijn 4: Decentrale verantwoording waar kan, centraal toezicht waar moet

De rijksoverheid hanteert het basisprincipe dat gemeenten zelf verantwoordelijk zijn en blijven voor hun informatieveiligheid. Via de planning en control-cyclus leggen gemeenten zelf verantwoording af aan de gemeenteraad.

Er vindt in de gemeente Alkmaar bestuurlijke afstemming met college en de raad plaats. In de interviews is door verschillende functionarissen gesteld dat de ambtelijke organisatie op basis van wederzijds vertrouwen een hoge mate van eigen zelfstandigheid en verantwoordelijkheid heeft bij de invulling van de doelstellingen die betrekking hebben op informatieveiligheid. Verantwoording vindt plaats in de jaarrekening en de ENSIA-rapportage. De gemeente voert een zelfevaluatie ENSIA uit. Op basis van deze inventarisatie van de stand van zaken en gebleken tekortkomingen worden in de rapportage ook verbeteracties onderscheiden. De rapportage wordt vastgesteld door het college van B&W en ter kennisname gedeeld met de raad. In 2022 was de ENSIA-rapportage een hamerstuk. In enkele interviews zijn zorgen geuit over het gegeven dat in de periodieke ENSIA-rapportages weinig vooruitgang met betrekking tot de informatieveiligheid van Alkmaar blijkt. Onder meer wordt genoemd dat eerder vastgelegde verbeteracties te weinig aandacht en prioriteit hebben gekregen, mede ten gevolge van personele wisselingen.
De toets op de veiligheid van DIGID en Suwinet vindt plaats door een onafhankelijke auditor.

In de interviews is genoemd dat als er geen grote incidenten zijn, er doorgaans in college of de raad niet over informatieveiligheid wordt gesproken. Behoudens het amendement uit 2019, op basis waarvan een project ter bevordering van de cyberveiligheid in de lokale gemeenschap is ingericht, wordt door betrokkenen melding gemaakt van weinig specifieke aandacht vanuit de raad voor het thema cyber- en informatieveiligheid.

De ENSIA-rapportage, met de daarin opgenomen conclusies en verbeteracties, wordt gedeeld met het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

2.3.2 Actielijn 5: OOV bevoegdheden en rollen voor de lokale bestuurders

Voor elke gemeente geldt dat zowel de burgemeester als het college van B&W een belangrijke rol hebben in het integraal veiligheidsbeleid. In diverse nota’s en plannen van Alkmaar, die in de eerdere paragrafen van dit hoofdstuk al de revue zijn gepasseerd, zijn deze rollen ook specifiek onderscheiden en ingevuld. Ten tijde van het onderzoek bestond het College louter uit de burgemeester. Hierdoor was het lastig om een onderscheid te maken tussen de rollen en bevoegdheden van de

burgemeester, die een zelfstandige verantwoordelijkheid heeft voor de openbare orde en veiligheid, en die van het College als geheel. In het in 2023 aangetreden College is er een wethouder portefeuillehouder voor het onderwerp ‘‘innovatie, kennis en Smartcity’. Deze portefeuille heeft directe raakvlakken met een veilige omgang met data en informatie. Een andere wethouder is portefeuillehouder P&O. Tot deze portefeuille behoort ook de bedrijfsvoering, waaronder ICT en juridische zaken (en daarmee informatiebeveiliging en privacybescherming).

2.4 Risicogericht handelen

Elke gemeente kan geconfronteerd worden met datalekken, digitale verstoringen, incidenten en digitale criminaliteit. Daar waar het aandachtsgebied ‘governance’ zich concentreerde op de gemeente zelf, is in de paragraaf ‘risicogericht handelen’ een bovenlokaal perspectief gekozen. Dit aandachtsgebied kent de actielijnen ‘lokale vitale processen bepalen vanuit maatschappelijke taken’, ‘krachtige partner in de keten’ en ‘risicomanagement geeft focus’. Deze richten zich op het belang van het collectief (h)erkennen van lokale vitale processen, de impact van digitale ontwrichting en het netwerkmanagement bij het thema ‘digitale veiligheid’.

2.4.1 Actielijn 6: Lokale vitale processen bepalen vanuit maatschappelijke taken

Vanuit de agenda digitale veiligheid van de VNG wordt gemeentebestuurders op het hart gedrukt om binnen de eigen gemeente met stakeholders een gesprek te voeren over lokale vitale processen en wat de impact is bij digitale ontwrichting. Vanuit de BIO is het al verplicht om een risicoanalyse uit te voeren en te bedenken hoe de continuïteit gewaarborgd kan worden bij cyberincidenten en -crises. Die principes kunnen gemeentelijke bestuurders ook inzetten voor het gesprek m.b.t. lokale vitale processen, zoals besturingssystemen voor verkeersveiligheid.

De burgemeester van Alkmaar, ten tijde van het onderzoek portefeuillehouder ‘van alles’, noemt daarover regelmatig in gesprek te zijn met politie, OM en de Veiligheidsregio.

2.4.2 Actielijn 7: Krachtige partner in de keten

Steeds meer gemeenten dragen uitvoerende taken over aan andere organisaties, waardoor data meer verspreid raken over ketens. Elke organisatie is zelf verantwoordelijk voor haar informatiebeveiliging en bedrijfscontinuïteit, maar VNG raadt aan raakvlakken en wederzijdse afhankelijkheden en risico’s te verkennen. In de praktijk zijn verwerkersovereenkomsten met organisaties waarmee informatie wordt gedeeld daarvoor een belangrijk instrument. In interviews is genoemd dat als in de praktijk informatie met derden wordt gewisseld, er inderdaad verwerkersovereenkomsten worden afgesloten. Tegelijkertijd is ter sprake gekomen dat de daarvoor noodzakelijke juridische expertise momenteel beperkt beschikbaar is in de organisatie. Ook is genoemd dat het register waarin de verwerkersovereenkomsten, zoals gesteld in de AVG, worden opgenomen niet actueel meer is,

Daarnaast vraagt risicomanagement ook dat informatie over incidenten (regionaal én landelijk) gedeeld moet worden, zodat de gemeente juiste beslissingen kan nemen. Informatie vanuit de Informatiebeveiligingsdienst van de VNG speelt hierin een belangrijke rol.

De Informatiebeveiligingsdienst

De IBD is de sectorale CERT / CSIRT[7] voor alle Nederlandse gemeenten en onderdeel van de Vereniging van Nederlandse Gemeenten. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD draagt namens gemeenten bij aan de Baseline Informatiebeveiliging Overheid (BIO) en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruik maken van de producten en de generieke dienstverlening van de IBD.

De gemeente Alkmaar maakt gebruik van de diensten van de IBD. Eerder is al ter sprake gekomen dat de gemeente Alkmaar kennis en informatie deelt binnen de Veiligheidsregio en binnen Noord-Holland-Samen-Veilig. Ook wordt er informatie gedeeld met politie en Openbaar Ministerie.

2.4.3 Actielijn 8: Risicomanagement geeft focus

VNG benadrukt in de Agenda Digitale Veiligheid het belang van een ‘digitale risicokaart’ ten aanzien van de bedrijfscontinuïteit van lokale vitale processen. Dit biedt houvast voor het prioriteren en plannen van maatregelen met ketenpartners.

Als het gaat om de veiligheid in de lokale gemeenschap maakt de gemeente Alkmaar jaarlijks risicoanalyses. Hiervan wordt verslag gedaan in de ‘Nota Stand van Zaken veiligheid’. De informatie voor deze risicoanalyses wordt ontleend aan verschillende bronnen waaronder de veiligheidsmonitor en aangiftecijfers bij de politie. Cybercriminaliteit krijgen in de voor dit onderzoek bekende nota (de meest actuele dateert uit 2021) beperkte aandacht. Het bestaan van een digitale risicokaart is in het onderzoek niet genoemd.

2.5 Eén overheid/ samen organiseren

2.5.1 Actielijn 9: Versterken gemeentelijke weerbaarheid

Om de digitale weerbaarheid van gemeenten zelf te vergroten raadt de VNG gemeenten aan om:

- Informatiebeveiliging op de agenda van het college te zetten en te zorgen dat lijnmanagers verantwoordelijkheid kunnen nemen. Op deze manier hoopt de VNG dat de top van de organisatie doordrongen is van het belang van informatiebeveiliging en zelf het goede voorbeeld geeft.
- De basis op orde te brengen met de basale beveiligingsprocessen en maatregelen.
- De menselijke schakel te versterken.
- De positie van de CISO te versterken, zodat deze ruimte en middelen heeft en kan investeren in kennis en kunde.
- Het inzicht in risico’s van nieuwe technologieën te verbeteren door de juiste mensen verantwoordelijk te maken en al in het beginstadium de CISO en verantwoordelijke lijnmanagers te betrekken.

Naast deze concrete raadgevingen wordt in de Agenda Digitale Veiligheid gewezen op aandacht voor netwerk monitoring, het bewaken van dataverkeer van de eigen organisatie en respons op eventuele aanvallen.

[7] CERT staat voor ‘Computer Emergency Response Teams’. CSIRT staat voor ‘Computer Security Incident Response Teams’.

- *De situatie in Alkmaar*

In bovenstaande paragrafen is al het nodige aan de orde geweest met betrekking tot de opstelling van de gemeente Alkmaar bij al deze aandachtspunten. Zo is genoemd dat de inrichting van de informatiebeveiliging binnen het college heeft plaatsgevonden en vastgesteld. Daarbij zijn bevoegdheden van het college en van lijnmanagers gespecificeerd. Ook is beschreven dat gemeente Alkmaar de basale beveiligingsprocessen heeft ingericht. Er is gerapporteerd over de activiteiten om het bewustzijn van de medewerkers te versterken, om daarmee de aandacht voor de menselijke factor te versterken. De functie van CISO bestaat binnen de organisatie. Er is aandacht voor de risico's van nieuwe technologieën. Wel zijn er in interviews zorgen geuit over de inrichting en toerusting van de positie van de CISO. Ten tijde van het onderzoek werd deze functie op ad interimbasis ingevuld door een functionaris die ook andere verantwoordelijkheden heeft. In het verlengde daarvan is in enkele interviews de vraag gesteld of de CISO in deze context voldoende expertise en mogelijkheden heeft om gedegen inzicht te verwerven in de risico's van nieuwe technologieën.

2.5.2 Actielijn 10: Eén overheid

VNG en de Rijksoverheid bieden een breed palet aan (ICT)voorzieningen en -diensten aan die gemeenten digitaal veiliger moeten maken. Vanuit de Agenda Digitale Veiligheid wordt gemeenten opgeroepen hier zoveel mogelijk gebruik van te maken. Een van de instrumenten is de Baseline Informatiebeveiliging Overheid (BIO).

- *De situatie in Alkmaar*

Op de thema´s die de fysieke veiligheid van de gemeente raken, namelijk cybercrime & gedigitaliseerde criminaliteit en online aangejaagde ordeverstoring, sluit gemeente Alkmaar aan bij wat er landelijk en regionaal wordt aangeboden aan informatie en producten. Hierboven is al melding gemaakt van de samenwerking met de Veiligheidsregio en Noord-Holland Samen Veilig. Daarnaast volgt Alkmaar wat er landelijk op deze thema's wordt geboden via bijvoorbeeld de Vereniging Nederlandse Gemeenten en door de City Deal Cybercrime en het Centrum voor Criminaliteitspreventie en veiligheid. De gemeente Alkmaar zet actief in op de preventie van cybercrime.

3. De rol van bestuurders

In dit hoofdstuk zijn de rollen van raad, college en burgemeester (als zelfstandig bestuursorgaan) aan de orde. Daarnaast is aandacht besteed aan de wijze waarop aan die rollen in de praktijk invulling wordt gegeven. Richtinggevend zijn de volgende onderzoeksvragen:

Deelvragen	
2.	*Welke rollen hebben Raad, College en Burgemeester bij het verder ontwikkelen en in uitvoering brengen van de digitale veiligheidsagenda? Hoe zijn deze beschreven en geïmplementeerd?*
3.	*Op welke manier zijn bestuurders (Raad, College, Burgemeester) op het moment van het onderzoek betrokken bij het tot uitvoering brengen van de digitale veiligheidsagenda? In hoeverre zijn ze geïnformeerd? Welk belang hechten zij eraan? Op welke wijze implementeren zij onderdelen van de agenda in beleid en sturing?*

In de nota ‘Afspraken op het beleidsterrein van Informatiebeveiliging informatievoorziening en privacy’ uit februari 2019 zijn de rollen van College, burgemeester, directie en diverse voor dit beleid belangrijke functionarissen, zoals de FG, CISO, privacy officer en afdeling I&A, beschreven. Over de voor dit onderwerp specifieke rollen en verantwoordelijkheden van de raad is niets vastgelegd. Dat is overigens niet noodzakelijk, aangezien de verantwoordelijkheid voor het beleid berust bij het college van B&W.

De bewaking van de privacy van inwoners, het voorbereiden op en voorkomen van cybercriminaliteit en het garanderen van informatieveiligheid worden binnen de gemeentelijke organisatie vooral benaderd als uitvoeringskwesties. Al eerder in deze rapportage is genoemd dat bij uitvoeringskwesties de ambtelijke organisatie van Alkmaar veel ruimte wordt gegund om dit naar eigen inzicht in te vullen. Eventuele besluiten worden (niet structureel) ter kennisname gedeeld met de raad.
Informatie over de ambities van de gemeente met betrekking tot privacy en digitale veiligheid maakt deel uit van de P&C-cyclus. In de programmabegroting voor 2023 wordt cyberveiligheid genoemd als één van de thema’s onder het brede thema veiligheid. De daadwerkelijke uitvoering en resultaten vormt een onderdeel van de P&C-documenten. Daarover wordt gemeld: “Tenslotte vraagt de toename van cybercriminaliteit onze onverminderde aandacht.”[8] Deze ambitie wordt uitgewerkt in de volgende ‘subdoelstelling: “Inwoners en ondernemers zijn zich bewuster van hun digitale veiligheid en daardoor weerbaarder voor de risico’s van cybercriminaliteit.” Deze doelstelling wordt in de programmabegroting verder niet uitgewerkt of geconcretiseerd.
In de Programmabegroting is onder de paragraaf bedrijfsvoering ook het een en ander vermeld over privacy. Onder meer wordt genoemd: “De invoering van de Algemene verordening gegevensbescherming (AVG) levert de organisatie veel werk op én vraagt een hoge mate van bewustzijn. We bieden daarom gemeentebrede (verplichte) trainingen[9] en doen regelmatig tests om de effectiviteit van de trainingen op awareness te meten.”[10]

De gemeenteraad wordt zo slechts incidenteel geïnformeerd over het beleid en de uitvoering daarvan. Tijdens een sessie met raads- en commissieleden die in het kader van het onderzoek is belegd kwam naar voren dat aan de deelnemers geen relevante documenten bekend waren. In de documenten die

[8] Gemeente Alkmaar, Programmabegroting 2023, pagina 68.
[9] In de in het kader van dit onderzoek uitgevoerde verdiepingssessies met medewerkers kwam naar voren dat zij niet ervaren dat deze trainingen een verplicht karakter hebben.
[10] Gemeente Alkmaar, Programmabegroting 2023, pagina 130.

in de documentatie die in het kader van het onderzoek aan de rekenkamer ter beschikking is gesteld is geen jaarverslag van de FG aangetroffen. In veel gemeenten is gebruikelijk dat zo'n jaarverslag wordt gedeeld met de raad. In veel gevallen geeft de FG dan ook een toelichting op het verslag aan de raad of raadscommissie. Hiervan is in de gemeente Alkmaar geen sprake.

De rapportage 'Stand van zaken veiligheid' wordt wel gedeeld met de raad. Deze rapportage heeft betrekking op de volle breedte van de veiligheid in de gemeente Alkmaar. Digitale veiligheid vormt hiervan slechts een klein onderdeel. De rapportage is in een technische sessie met raadsleden besproken.

De raad informeert uit eigen initiatief zelden naar uitgangspunten en ontwikkelingen met betrekking tot digitale veiligheid.

Tijdens de speciaal voor dit onderzoek belegde bijeenkomst met raads- en commissieleden gaven de deelnemers aan dat het hen aan kennis en informatie ontbreekt om hun kaderstellende en controlerende verantwoordelijkheden rond dit thema goed in te vullen. Zij herkenden dat zij hierin verantwoordelijkheden dragen, al zijn zij van mening dat zij die ook louter op een algemeen niveau dienen in te vullen.

Hun kaderstellende verantwoordelijkheden hebben dan betrekking op het formuleren van algemene uitgangspunten over het gewenste niveau van veiligheid en het toekennen van de daarvoor noodzakelijke middelen. Voorts gaven enkele deelnemers aan dat de raad scenario's zou willen bespreken over hoe te handelen bij mogelijke inbreuken op de veiligheid en daar voorkeuren in aan te geven.

De aanwezige raads- en commissieleden hadden de ambitie meer werk te willen maken van hun controlerende verantwoordelijkheden. Zo willen ze kunnen vaststellen of de gemeente voldoende voorbereid is om mogelijke inbreuken op de veiligheid. Ook toonden ze de belangstelling voor de uitkomsten van de BIO, om zo een indruk te krijgen waar de gemeente Alkmaar staat op deze baseline en hoe dat zich verhoudt tot andere gemeenten. Een enkele deelnemer deed de suggestie om een raadscommissie 'digitale zaken' in te richten.

Alle deelnemers aan de raadsbijeenkomst benadrukten behoefte te hebben aan meer informatie over de inrichting en uitvoering van het beleid met betrekking tot digitale veiligheid. Zoals al eerder opgemerkt was geen van deelnemers bekend of, en hoe ze over dit thema werden geïnformeerd. Zij gaven ook aan dat het hun aan kennis ontbreekt om het beleid te beoordelen. In dat licht noemden ze behoefte te hebben aan kennisbevordering, bijvoorbeeld door middel van een training of deelname aan studiedagen.

4. Conclusies en aanbevelingen

In het onderzoek hebben vier deelvragen centraal gestaan. Na presentatie van de bevindingen in de vorige twee hoofdstukken, kunnen de deelvragen nu als volgt worden beantwoord:

Deelvragen	
1.	Welke van de tien actielijnen uit de VNG-agenda digitale veiligheid zijn reeds opgepakt? Hoe zijn deze uitgewerkt en uitgevoerd? Welke resultaten/ effecten zijn bekend?
Antw.	Alle tien actielijnen uit de VNG-agenda worden in het beleid van Alkmaar geadresseerd.
2.	Welke rollen hebben Raad, College en Burgemeester bij het verder ontwikkelen en in uitvoering brengen van de digitale veiligheidsagenda? Hoe zijn deze beschreven en geïmplementeerd?
Antw.	De ‘governance’ van het beleid met betrekking tot digitale veiligheid in de gemeente Alkmaar is tot in detail uitgewerkt. In dat verband zijn de rollen van het college en de burgemeester beschreven. De rol van de raad komt slechts in algemene termen aan de orde, maar het beleid vraagt op zichzelf niet om een uitgebreide uitwerking van de rol van de raad.
3.	Op welke manier zijn bestuurders (Raad, College, Burgemeester) op het moment van het onderzoek betrokken bij het tot uitvoering brengen van de digitale veiligheidsagenda? In hoeverre zijn ze geïnformeerd? Welk belang hechten zij eraan? Op welke wijze implementeren zij onderdelen van de agenda in beleid en sturing
Antw.	College en burgemeester geven conform de uitgangspunten van het beleid invulling aan hun verantwoordelijkheden. Zij worden daarover voldoende geïnformeerd. Zij erkennen het belang van het beleid en geven sturing aan de implementatie.
4.	Op welke manier zijn ambtenaren op dit moment betrokken bij de digitale veiligheidsagenda? In hoeverre zijn ze geïnformeerd? Welk belang hechten zij eraan? Is hun werkwijze ervan doordrongen?
Antw.	In lijn met de uitgangspunten en de sturing op de implementatie van het beleid vanuit het college zijn ambtenaren actief met het versterken van de digitale veiligheid van de gemeente Alkmaar. Voor het gros van de betrokken ambtenaren geldt dat zij in algemene zin invulling geven aan de digitale veiligheid, zonder daarbij expliciet de actielijnen van de digitale veiligheidsagenda als uitgangspunt te nemen. Niet in alle situaties in de praktijk zijn ambtenaren ‘doordrongen’ van het belang van digitale veiligheid.

De beantwoording van deze vragen geeft een overwegend positieve indruk van het beleid van de gemeente Alkmaar. De nuance daarbij is wel dat in de uitvoeringspraktijk verschillende tekortkomingen zijn gebleken zoals de stapeling van verantwoordelijkheden bij een beperkt aantal functionarissen.

Zoals aangegeven in het eerste hoofdstuk is bij aanvang van het onderzoek een referentiekader opgesteld om zo meer gestructureerd zicht te krijgen op de bevindingen. Toepassing van dit referentiekader leidt tot het volgende resultaat:

- Heeft elke actielijn in het beleid van de gemeente Alkmaar en in het dagelijks handelen van de medewerkers een duidelijk herkenbare positie?
Zoals uit het antwoord op deelvraag 1 blijkt, geeft Alkmaar invulling aan elke actielijn uit de Digitale Veiligheidsagenda. Tegelijkertijd is naar voren gekomen dat niet elke actielijn een duidelijk herkenbare

positie heeft, noch in het beleid noch in het dagelijks handelen van de medewerkers. Deze algemene constatering resulteert in het volgende beeld van de geformuleerde normen:

	Actielijn	Algemeen beeld[11]	Toelichting / nuancering
1	Digitale Veiligheid vergroten	+	Sommige functionarissen stellen dat de aandacht voor het bevorderen van de 'awareness' de laatste tijd is afgenomen
2	Weerbare organisatie	+	Sommige essentiële functies worden op ad interimbasis ingevuld
3	Digitale Brandoefening	0	Er heeft een oefening plaatsgevonden. Het is in de organisatie nog onbekend of oefeningen een structureel karakter krijgen.
4	Decentrale verantwoording waar kan, centraal toezicht waar moet	+	Er bestaan twijfels over de opvolging van acties uit ENSIA-rapportages
5	OOV-bevoegdheden en rollen voor de lokale bestuurders	+	Onbekend is hoe dit in het nieuwe College is / wordt vastgelegd
6	Lokale vitale processen bepalen vanuit maatschappelijke taken	0	Op het niveau van de Veiligheidsregio is hier weliswaar meer, maar toch nog steeds beperkte aandacht voor.
7	Krachtige partner in de keten	++	Alkmaar werkt enthousiast samen met andere relevante organisaties.
8	Risicomanagement geeft focus	0	In verschillende documenten worden wel risico's benoemd, maar een algemeen beeld en gerichte sturing ontbreken
9	Informatiebeveiligingsdienst gemeenten verbreden en versterken	++	Alkmaar maakt gebruikt van de ondersteuning van Microsoft en de IBD
10	Eén overheid	+	Alkmaar werkt samen met andere overheden

- Het beleid (zowel de voorbereiding als de uitvoering daarvan) doet recht aan hetgeen bij elk van die actielijnen van gemeenten wordt verlangd.
Aan de hand van de nuances in bovenstaand overzicht wordt al duidelijk dat niet bij alle actielijnen volledig recht wordt gedaan aan wat van gemeenten wordt verlangd.

- Leidt dit tot resultaten
Zoals in de inleiding van deze rapportage is aangegeven heeft dit onderzoek een overwegend beschrijvend en inventariserend karakter. De beoordeling van de inspanningen en activiteiten van de

[11] De beoordeling loopt van 'heel positief'(++) naar 'positief' (+), 'neutraal' (0), 'negatief' (-) tot uiteindelijk 'sterk negatief'(--).

gemeente staat daarmee minder centraal. Binnen deze context wordt kort ingegaan op de opbrengsten van het beleid. Gezien de inspanningen en activiteiten die sinds enkele jaren worden ontwikkeld, lijdt het geen twijfel dat er resultaten worden behaald. Zeer aannemelijk is dat de 'awareness' ten aanzien van informatieveiligheid en cybersecurity hoger ligt dan vijf jaar terug. Ook is er binnen de organisatie sprake van meer beleid, voorschriften en werkwijzen die bijdragen aan de weerbaarheid. Er is geoefend, er wordt verantwoording afgelegd, zowel intern als aan de centrale overheid.
Er ontbreken echter 'harde gegevens' om de indruk dat er resultaten worden geboekt te staven. Evenmin kan inzichtelijk worden gemaakt of inbreuken op de veiligheid, zowel binnen de organisatie als in de lokale gemeenschap, nu minder voorkomen dan enkele jaren terug.

De bij dit onderzoek geformuleerde centrale onderzoeksvraag luidt als volgt:

Hoe wordt binnen de gemeente Alkmaar invulling gegeven aan de Digitale Veiligheidsagenda?

Hier kan geen eenduidig en volmondig positief antwoord op worden gegeven. Er zijn immers verschillende nuances en tekortkomingen geconstateerd. In het algemeen zijn het benodigde beleid en daarop gebaseerde richtlijnen en werkwijzen in gemeente Alkmaar in voldoende mate beschikbaar. Vanwege Corona (o.m. wat het inwerken van nieuwe medewerkers betreft) en personele wisselingen op cruciale managementfuncties is de uitvoering onder druk komen te staan. In de praktijk handelen veel medewerkers vanuit zelf bepaalde standaarden en waarborgen, die zij ontlenen aan eerder verkregen informatie over het gewenste beleid. Deze werkwijzen worden mede geschraagd worden door hun persoonlijke professionaliteit. Daarbij is niet altijd gegarandeerd dat de medewerkers volledig voldoen aan het vastgelegde beleid.
Verder is het de vraag of er sprake is van een gestage positieve ontwikkeling. Zo lijkt de opvolging van relevante activiteiten, zoals awarenessbevordering en acties die voortkomen uit ENSIA-rapportages, niet goed belegd.

Alkmaar heeft op het brede thema van de Digitale Veiligheidsagenda zeker ambities, die in de samenwerking met onder meer de Veiligheidsregio en Noord-Holland-Samen-Veilig, ook goede invulling krijgen. Het aanstellen van een OOV-medewerker die zich specifiek richt op het bevorderen van de digitale veiligheid getuigt eveneens van ambitie. De vraag is wel of deze functie en de middelen die bij deze functie beschikbaar zijn gesteld toereikend zijn.

Al met al gebeurt veel, maar de structuur en samenhang in het beleid zijn niet evident. Tevens valt op dat de raad dusdanig ver op afstand staat van dit beleid dat de raad zijn sturende en controlerende verantwoordelijkheden niet kan waarmaken.

Dit leidt tot de volgende aanbevelingen:

	Aanbevelingen aan het college van B&W
1	Maak meer expliciet en concreet hoe invulling wordt gegeven aan elk van de actielijnen uit de digitale agenda van de VNG
2	Heb meer aandacht voor de uitvoeringspraktijk; op papier is veel geregeld, maar niet al het beleid wordt in de praktijk opgevolgd.
3	Beleg de verantwoordelijkheden van de FG weer bij één zelfstandig opererende functionaris
4	Beleg de verantwoordelijkheden van de CISO als enige taak bij één functionaris,
5	Zorg voor een gerichte sturing van het risicomanagement met betrekking tot digitale veiligheid.
6	Zorg voor een meer regelmatige en uitgebreidere informatievoorziening aan de gemeenteraad.
7	Schep voorwaarden voor kennisbevordering over dit thema bij raadsleden.

	Aanbevelingen aan de gemeenteraad
8	Investeer in de eigen kennisbevordering met betrekking tot het thema digitale veiligheid
9	Wees actief in het bewaken en bevorderen van een regelmatige informatievoorziening over dit thema aan de raad.

Bijlage A Bestudeerde Documentatie

Documentnaam	Jaar van vaststelling
BIO Versie 1	2017
Gemeente Alkmaar Programmabegroting 2020 Meerjarenbegroting 2021-2023	2019
Nota aan burgemeester en wethouders – afspraken op het beleidsterrein van informatiebeveiliging informatievoorziening en privacy	2019
Amendement: De digitale deur op slot	2019
Samen hulpvaardig. Beleidsplan Veiligheidsregio Noord-Holland Noord 2020-2023	2020
Notitie Cyberveiligheid – Achtergrondinformatie en uitvoeringsplan	2020
Agenda Digitale Veiligheid 2020-2024 – Een veilige (digitale) gemeente	2020
Rapportage ‘Stand van zaken veiligheid’ 1e helft 2021	2021
Rapportage ‘Stand van zaken veiligheid’ juli ’21 – oktober 2021	2021
Rapport ‘Hoe Veilig is Alkmaar’?	2021
Plan van Aanpak Cyberveilig Alkmaar	2021
Notitie Monitor Veiligheidsbeeld Alkmaar 2021	2021
Gemeentefactsheet Alkmaar	2021
Uitkomsten Ensia 2021	2021
Collegevoorstel Zelfevaluatie ENSIA 2021	2021
Gemeente Alkmaar Programmabegroting 2023 Meerjarenraming 2024-206	2022
Rapportage ‘Stand van zaken veiligheid’ 1e helft 2022	2022
Agenda Digitale Veiligheid 2022-2026	2022
Focusblad Digitale Veiligheid VNG	2022
Cyberwegenkaart CCV	2022
Privacy- en informatiebeveiligingsbeleid gemeente Alkmaar	2022
Kadernota Veiligheid 2023-2026	2023
Security Operations Centrum Alkmaar	2023

Bijlage B Geïnterviewde personen

Functie
Burgemeester
Directeur Bedrijfsvoering,
Concern-controller / Chief Information Security Officer(a.i.)/ FG (a.i.)
Chief Information Officer
Unitmanager ICT,
Unitmanager bestuur,
Unitmanager veiligheid
Information Security Officer
Beleidsmedewerker Openbare orde en veiligheid
Concernjurist en Privacy Officer

Bijlage C Deelnemers aan de verdiepingssessies

Medewerkers Sociaal Domein
Kwaliteitsmedewerker sociaal domein I
Kwaliteitsmedewerker sociaal domein II
Kwaliteitsmedewerker sociaal domein III
Kwaliteitsmedewerker sociaal domein IV
Beleidsmedewerker WMO
Medewerker beleidsafdeling sociaal domein
Vakcoördinator jeugd.

Medewerkers Fysiek Domein
Medewerker Openbare Orde en Veiligheid I
Medewerker Openbare Orde en Veiligheid II
Medewerker Openbare Orde en Veiligheid III
Medewerker Openbare Orde en Veiligheid IV
Medewerker vergunningen I
Medewerker vergunningen II

Bijeenkomst met raads- en commissieleden
Commissielid CDA
Commissielid D66
Raadslid D66
Commissielid PvdA
Commissielid Leefbaar Alkmaar
Commissielid GroenLinks
Raadslid Belangen Alkmaarse Samenleving
Commissielid SP
Commissielid SP
Raadslid Senioren Partij Alkmaar
Commissielid VVD
Raadslid CDA

Bijlage D Afkortingslijst

Afkorting	Betekenis
BIO	Baseline Informatiebeveiliging
CCV	Centrum voor Criminaliteitspreventie en Veiligheid
CISO	Chief Information en Security Officer
DPIA	Data Protection Impact Assessment
ENSIA	Eenduidige Normatiek Single Information Audit
FG	Functionaris Gegevensbescherming
VNG	Vereniging Nederlandse Gemeenten