Onderzoeksrapport
Digitale Veiligheid in Katwijk

Rekenkamercommissie

Katwijk

Onderzoek Digitale veiligheid in Katwijk

Rekenkamercommissie Katwijk

INHOUDSOPGAVE

VOORWOORD

Voor u ligt het rapport over informatiebeveiliging bij de gemeente Katwijk, een onderzoek van de Rekenkamercommissie Katwijk dat is uitgevoerd in de tweede helft van 2018. Het betreft dan ook een momentopname van die periode. Juist in deze periode werd er volop gewerkt aan de verbetering van de informatievoorziening van de gemeente, o.a. door de uitrol van de nieuwe mobiele werkplek en de nieuwe ICT-infrastructuur.

De onderzoekers hebben ten behoeve van dit onderzoek uitvoerig gesproken met medewerkers van de ambtelijke organisatie van de gemeente Katwijk. Daarnaast hebben ze documenten bestudeerd.

De samenwerking met de medewerkers van de gemeente was prettig en de documentatie werd in bijna alle gevallen snel en zorgvuldig aangeleverd. Dit heeft een goede en prettige uitvoering van het onderzoek bevorderd.

We hebben ervaren dat de medewerkers van de gemeente Katwijk zich open en constructief hebben opgesteld en het rekenkameronderzoek zien als een steun in de rug en niet als een afrekenende controle. Wij danken daarom de medewerkers van de gemeente voor de medewerking.

1 INLEIDING

1.1 AANLEIDING

In de afgelopen jaren is de aandacht voor de beveiliging van informatie sterk toegenomen. Dat heeft verschillende oorzaken. Allerlei organisaties, waaronder natuurlijk ook gemeenten, werken steeds 'digitaler' en wisselen in dat verband intern, met andere organisaties in een keten en met burgers en ondernemingen gegevens uit. In de laatste jaren is het besef toegenomen dat gemeenten aan burgers moeten kunnen garanderen dat hun gegevens in veilige handen zijn. Gemeenten beheren uiterst gevoelige gegevens van hun inwoners. Gemeenten moeten het vertrouwen van burgers dat zij zorgvuldig omgaan met hun gegevens verdienen, zowel in de directe contacten met de burger als in verantwoordingen achteraf.

Bovendien is de regelgeving met betrekking tot de bescherming en beveiliging van persoonsgegevens aangescherpt. Dit blijkt in het bijzonder door de Algemene verordening Gegevensbescherming (AVG) die per 25 mei 2018 van toepassing is. Desalniettemin is die regelgeving nog lang niet bij alle gemeenten in het eigen beleid verwerkt, of wordt er op de werkvloer naar gehandeld. Daarmee lopen gemeenten het risico op hoge boetes in het geval zij niet conform de geldende normen de beveiliging van persoonsgegevens op orde hebben.

Er zijn meer redenen dat de aandacht voor informatieveiligheid is toegenomen. Nadat digitalisering, en de daarmee gepaard gaande opkomst van het internet aanvankelijk louter positief werden ervaren, is de laatste jaren het besef toegenomen dat deze ontwikkelingen ook hun schaduwkanten hebben. Gegevens kunnen worden gehackt en misbruikt. In sommige situaties zijn essentiële persoonsgegevens misbruikt om identiteitsfraude mogelijk te maken.

In dit licht heeft de rekenkamercommissie van de gemeente Katwijk besloten een onderzoek te verrichten naar de wijze waarop de gemeente Katwijk invulling geeft aan digitale veiligheid.

1.2 Opdrachtformulering

Ten behoeve van het onderzoek is de volgende onderzoeksvraag geformuleerd:

> *In hoeverre heeft de gemeente Katwijk de informatiebeveiliging van de informatiesystemen in de organisatie doeltreffend ingericht, waarmee risico's worden afgedicht, waardoor geen oneigenlijke toegang tot de gevoelige informatie (zoals persoonsgegevens) kan worden verkregen, informatie in verkeerde handen kan vallen en/of vitale systemen in werking of uit kunnen worden gezet?*

Wij hebben deze onderzoeksvraag geoperationaliseerd door middel van het formuleren van een aantal deelvragen. Hieronder volgen de deelvragen.

1.3 Deelvragen

1. Welke beleidskaders[1], regels en richtlijnen hanteert de gemeente voor de borging van de informatiebeveiliging?
2. Voldoet het beleid en de uitwerking in processen binnen de gemeente aan de bepalingen van het basisnormkader Baseline Informatiebeveiliging Gemeenten (BIG) en aan de Algemene verordening gegevensbescherming (AVG[2], die per 25 mei 2018 van toepassing is)?
3. Welke functionarissen zijn verantwoordelijk gesteld voor de informatiebeveiliging binnen de gemeente?
4. Welke Mobile Device Management (MDM) oplossing heeft de gemeente Katwijk gekozen en op welke wijze wordt met behulp van de MDM een optimale beveiliging van de mobiele devices ingericht?
5. Hoe is de operationalisatie en implementatie van de BIG tot nu toe verlopen?
6. Hoe is dit beleid uitgewerkt en geborgd in processen op de werkvloer?
7. Hoe worden medewerkers betrokken bij en getraind in het borgen van het informatiebeveiligingsbeleid en het privacy beleid?
8. Hoe geeft de gemeente Katwijk invulling aan het testbeleid en de auditing op de digitale veiligheid?
9. Op welke wijze worden de ICT-voorzieningen (waaronder de infrastructuur, de wifi, de volledige werkplek, de website en digitale dienstverlening) van de gemeente Katwijk getest op informatiebeveiliging, met welke frequentie en met welke resultaten?

[1] Naast het vastgestelde en onlangs geactualiseerde privacybeleid en informatiebeveiligingsplan van de gemeente Katwijk.
[2] Omdat de AVG per 25 mei 2018 van kracht is geworden en de WBP per die datum niet meer van kracht is, zullen wij in dit rekenkameronderzoek de AVG als wettelijk kader hanteren.

10. Welke mogelijke risico's zijn te onderkennen in de huidige wijze waarop het privacy- en informatiebeveiligingsbeleid is ingericht en functioneert?
11. Hoe ziet de gemeente erop toe dat het informatiebeveiligingsbeleid van een voldoende niveau is en blijft en wordt er geanticipeerd op toekomstige opgaven?
12. Welke beveiligingsincidenten heeft de gemeente Katwijk de afgelopen twee jaren ondervonden en hoe zijn deze afgewikkeld?

De door ons toegevoegde aandacht voor de positie van de raad heeft geleid tot de volgende twee onderzoeksvragen:

1.4 Deelvragen positie gemeenteraad

13. Op welke wijze is de raad tot nu toe bij de ontwikkeling van de informatieveiligheid betrokken geweest?
14. Op welke manier kan de gemeenteraad het beleid rondom informatieveiligheid controleren en sturen?

Om deze deelvragen, en daarmee ook de onderzoeksvraag te kunnen beantwoorden hebben wij een aantal thema's belicht. Dit zijn de volgende thema's:

1.5 Onderzoeksthema's

Governance

Dit aspect betreft het toetsen van de opzet, het bestaan en de werking van de governance van de gemeente Katwijk omtrent informatiebeveiliging. Het betreft hier minimaal de volgende wettelijke bepalingen:

- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
- Algemene verordening persoonsgegevens (AVG) [3] en/of gemaakte afspraken, bijvoorbeeld in VNG-verband.

Techniek

Dit aspect betreft het testen van de ICT-infrastructuur van de gemeente Katwijk. Deze dient te worden getest op kwetsbaarheden waarmee kwaadwillenden onrechtmatig over bedrijfsgevoelige gegevens, gegevens van burgers zouden kunnen beschikken en/of infrastructuur in werking kunnen stellen of afzetten waardoor maatschappelijke en/ of

[3] Omdat de AVG per 25 mei 2018 van kracht is geworden en de WBP per die datum niet meer van kracht is, zullen wij in dit rekenkameronderzoek de AVG als wettelijk kader hanteren. In de opdracht van de rekenkamercommissie werd de Wet Bescherming Persoonsgegevens uiteraard ook nog genoemd als relevante wettelijke bepaling. De onderzoeksopdracht is voor 25 mei 2018 verstrekt.

financiële schade kan ontstaan. Hierbij dient te worden gedacht aan: black box test, grey box test, monitoring en signalering, forensic readiness[4].

Mens

Bewustwording is een belangrijk onderdeel bij informatiebeveiliging. Onderzocht dient te worden in hoeverre medewerkers van de gemeente zich bewust zijn van informatiebeveiliging en dan met name wat er op dat gebied van hen verwacht moet worden. Te denken valt hierbij aan Phishing e-mails, inlooptests, achterlaten USB-sticks.

In het kader van het onderzoek is eveneens een normenkader opgesteld. Dit normenkader is opgenomen in bijlage B.

Werkwijze

- Na een gezamenlijke kick-off met de leden van de Rekenkamercommissie hebben de onderzoekers van PBLQ het onderzoek in uitvoering genomen.
- De eerste stap was het bestuderen van de opzet van het informatiebeveiligingsbeleid. Dit hebben de onderzoekers gedaan aan de hand van een documentstudie.
- Vervolgens hebben de onderzoekers met tweeëntwintig medewerkers van de gemeente Katwijk gesproken om vast te kunnen stellen of het beleid zoals het op papier bestaat en de maatregelen, die zijn getroffen ook in de praktijk bekend zijn en ook werken.
- Vervolgens hebben de onderzoekers de eerste bevindingen geformuleerd en deze in een convergentiebijeenkomst met een deel van de geïnterviewde medewerkers van de gemeente doorgenomen.
- Tenslotte hebben de onderzoekers hun bevindingen geanalyseerd en verwerkt in voorliggende rapportage.

1.6 LEESWIJZER

In het tweede hoofdstuk is de aandacht geconcentreerd op de opzet van het gemeentelijk informatiebeveiligingsbeleid en de informatiebeveiligingsmaatregelen. Eveneens komt in het tweede hoofdstuk aan de orde de wijze waarop de raad over het beleid wordt geïnformeerd.
De volgende deelvragen worden in hoofdstuk twee beantwoord:

1. Welke beleidskaders, regels en richtlijnen hanteert de gemeente voor de borging

[4] Forensic readiness betreft de mogelijkheid van een organisatie om optimaal gebruik te maken van digitale middelen (email, informatie uit het zaaksysteem, etc) als valide bewijsmateriaal in juridische kwesties.

van de informatiebeveiliging?
2. Voldoet het beleid en de uitwerking in processen binnen de gemeente aan de bepalingen van het basisnormkader (BIG) en aan de Algemene verordening gegevensbescherming (AVG, die per 25 mei van toepassing is)?
3. Welke functionarissen zijn verantwoordelijk gesteld voor de informatiebeveiliging binnen de gemeente?
4. Welke Mobile Device Management (MDM) oplossing heeft de gemeente Katwijk gekozen en op welke wijze wordt met behulp van de MDM een optimale beveiliging van de mobiele devices ingericht?

In het derde hoofdstuk staat centraal in welke mate het beleid en de informatiebeveiligingsmaatregelen ook in de praktijk aanwezig zijn en werken. In hoofdstuk drie worden de volgende deelvragen beantwoord:

5. Hoe is de operationalisatie en implementatie van de BIG tot nu toe verlopen?
6. Hoe is dit beleid uitgewerkt en geborgd in processen op de werkvloer?
7. Hoe worden medewerkers betrokken bij en getraind in het borgen van het informatiebeveiligingsbeleid en het privacy beleid?
8. Hoe geeft de gemeente Katwijk invulling aan het testbeleid en de auditing op de digitale veiligheid?
9. Op welke wijze worden de ICT-voorzieningen (waaronder de infrastructuur, de wifi, de volledige werkplek, de website en digitale dienstverlening) van de gemeente Katwijk getest op informatiebeveiliging, met welke frequentie en met welke resultaten?
10. Welke mogelijke risico's zijn te onderkennen in de huidige wijze waarop het privacy- en informatiebeveiligingsbeleid is ingericht en functioneert?
11. Hoe ziet de gemeente erop toe dat het informatiebeveiligingsbeleid van een voldoende niveau is en blijft en wordt er geanticipeerd op toekomstige opgaven?
12. Welke beveiligingsincidenten heeft de gemeente Katwijk de afgelopen twee jaren ondervonden en hoe zijn deze afgewikkeld?

Het vierde hoofdstuk bevat de beantwoording van de onderzoeksvragen met betrekking tot de positie van de gemeenteraad. Dat betreft de volgende twee deelvragen:

13. Op welke wijze is de raad tot nu toe bij de ontwikkeling van de informatieveiligheid betrokken geweest?
14. Op welke manier kan de gemeenteraad het beleid rondom informatieveiligheid controleren en sturen?

Aansluitend worden in hoofdstuk 5 de conclusies en aanbevelingen weergegeven.

2 OPZET EN BESTAAN VAN INFORMATIEBEVEILIGINGSBELEID

2.1 INLEIDING

In dit hoofdstuk beschrijven wij de wijze waarop de gemeente Katwijk haar beleid op het gebied van informatiebeveiliging en privacy heeft vormgegeven. Tevens gaan wij in op de ambities om verbeteringen aan te brengen. De mate waarin het beleid ook werkt en of die ambities ook worden waargemaakt, komen in het volgende hoofdstuk aan de orde. Daarmee zijn de volgende deelvragen in dit hoofdstuk aan de orde.

1. Welke beleidskaders, regels en richtlijnen hanteert de gemeente voor de borging van de informatiebeveiliging?

2. Voldoet het beleid en de uitwerking in processen binnen de gemeente aan de bepalingen van het basisnormkader BIG en aan de Algemene verordening gegevensbescherming (AVG, die per 25 mei van toepassing is)?

2.2 AANWEZIGHEID VAN INFORMATIEBEVEILIGINGSBELEID

De gemeente Katwijk heeft een strategisch informatiebeveiligingsbeleid dat op 9 mei 2017 door het College B&W is vastgesteld[5]. Het strategisch beleid betreft een beleidskader waarin wordt beschreven waarom informatiebeveiliging van belang is. Het bevat negen regels die specifieke handvatten voor een veilige omgang met informatie bieden.

In het tactisch informatiebeveiligingsbeleid staat beschreven wat er precies aan maatregelen dient te worden genomen[6]. Dit beleidsstuk is op 17 mei 2017 door het College B&W vastgesteld. De maatregelen die staan beschreven in het tactisch

[5] Strategisch informatiebeveiligingsbeleid, gemeente Katwijk, versie DEFINITIEF. d.d. 9 mei 2017.
[6] Tactisch informatiebeveiligingsbeleid, gemeente Katwijk, versie DEFINITIEF. d.d. 17 mei 2017.

informatiebeveiligingsbeleid zijn ontleend aan de BIG[7] en toegespitst op de organisatorische situatie van de gemeente Katwijk.

In januari 2018 is het informatiebeveiligingsplan voor 2018 door het College B&W vastgesteld[8]. Dit plan beschrijft welke informatiebeveiligingsactiviteiten in 2018 zullen worden opgepakt. Het betreft activiteiten die eraan moeten bijdragen dat de gemeente Katwijk voldoet aan de BIG, aangevuld met maatregelen die uit een langetermijnplanning komen; de GAP-analyse. Ook dient als input voor het informatiebeveiligingsplan:

- Verbeteracties die volgen uit incidenten (Datalekken, beveiligingsincident);
- Verbeteracties die volgen uit audits (ENSIA);
- Verbeteracties die volgen uit anderszins gesignaleerde risico's.

De Chief Information Security Officer (CISO) rapporteert over de voortgang van het informatiebeveiligingsplan aan de directie. Daarnaast is in 2017 een Information Security Management System (ISMS) geïmplementeerd waarmee de status van de informatiebeveiligingsactiviteiten kan worden bepaald en gevolgd. De controle op de voortgang van de implementatie van de BIG-maatregelen en de kwaliteit van de informatiebeveiliging wordt met behulp van het ISMS ondersteund. De gemeenteraad wordt eveneens geïnformeerd over de voortgang van informatiebeveiliging en privacy. Dat gebeurt door middel van alinea's in de jaarrapportages en de gemeentelijke begroting.

2.3 Organisatie van informatiebeveiliging

3. Welke functionarissen zijn verantwoordelijk gesteld voor de informatiebeveiliging binnen de gemeente?

2.3.1 Functionarissen op het gebied van informatiebeveiliging en privacy

Centrale dragende functionarissen zoals de CISO, TISO (Technical Information Security Officer) en de Functionaris Gegevensbescherming (FG) zijn benoemd. De CISO en FG zijn, net als de Chief Information Officer (CIO) strategische functionarissen waarbij de

[7] De BIG is sinds 2012 in ontwikkeling in opdracht van de Minister van BZK en heeft als doel om: 1. Gemeenten op een vergelijkbare manier efficiënt te laten werken met informatiebeveiliging. 2. Gemeenten een hulpmiddel te geven om aan alle eisen op het gebied van Informatiebeveiliging te kunnen voldoen. 3. De auditlast bij gemeenten te verminderen. 4. Gemeenten een aantoonbaar betrouwbare partner te laten zijn.
[8] Informatiebeveiligingsplan 2018, gemeente Katwijk, versie DEFINITIEF. d.d. januari 2018.

onafhankelijkheid ten opzichte van de ambtelijke organisatie belangrijk is. De verantwoordelijkheidsverdeling voor de informatiebeveiliging is vormgegeven conform de BIG en de AVG. Uit gesprekken is naar voren gekomen dat deze functionarissen daarom binnen de concernstaf zijn gepositioneerd. Deze functionarissen en de wijze waarop zij organisatorisch zijn opgehangen worden wel beschreven in de aanstellingsbesluiten van de FG en CISO, maar vooralsnog niet in het informatiebeveiligingsbeleid. . Dat wordt wel voorgeschreven in de strategische BIG. De taken en verantwoordelijkheden van de CISO en FG zijn omschreven in hun afzonderlijke functieomschrijvingen. De CISO en FG rapporteren direct aan het College en de gemeenteraad van de gemeente Katwijk middels tertaalrapportages, de ENSIA en de jaarlijkse verklaring privacy en informatiebeveiliging – de *declaration of accountability* Wij hebben deze rapportages aan het College en MT niet ingezien. Wel hebben wij enkele rapportages ingezien over de voortgang BIG-implementatie van 2017.[9]

De FG en CISO zijn in positie. Dat wil zeggen, veel ambtenaren weten wat de verantwoordelijkheden van de FG en CISO zijn en weten hen te vinden bij informatiebeveiligingsincidenten of privacyvraagstukken. De TISO is per 1 april 2018 benoemd en maakt onderdeel uit van het team ICT. De introductie van de nieuwe rol van TISO heeft als doel om de verbinding te maken tussen het beleid en de kaders van de informatiebeveiliging en de techniek van ICT. De TISO staat tussen de CISO en de IT-specialisten van team ICT in. De TISO stuurt op de tactische en operationele invulling van het informatiebeveiligingsbeleid. Omdat de huidige TISO tevens changemanager is, is met het combineren van deze twee rollen door één persoon tevens geborgd dat de informatiebeveiligingsaspecten bij alle voorgestelde wijzigingen in het Change Advisory Board (CAB) besproken worden. De TISO is nog kort in zijn nieuwe rol en is zijn positie aan het verkennen en opbouwen.

Bij veel uitvoerende teams van de afdelingen Samenleving en Ruimte & Veiligheid wordt informatiebeveiliging en gegevensbescherming, meer dan bij andere uitvoerende afdelingen, nog gezien als iets extra´s dat zij naast al hun reguliere werk nog moeten doen. Binnen deze afdelingen is het nog geen gemeengoed dat gegevensbescherming en informatiebeveiliging onderdeel uitmaken van het reguliere werk: hier is het nog niet volledig geaccepteerd. Informatiebeveiliging en privacy zijn daarmee nog onvoldoende geborgd binnen deze twee afdelingen van de gemeentelijke organisatie. Bij de andere afdelingen is dat wel het geval en wordt informatiebeveiliging en privacy wél meer gezien als onderdeel van het reguliere werk.

[9] Dit betreffen drie tertaalrapportages die gericht zijn aan de concerncontroller.

2.3.2 Overleg over informatiebeveiliging en privacy

Er zijn drie verschillende overleggen voor informatiebeveiliging en privacy, de werkgroep informatiebeveiliging, het incidentele kernteam datalekken en de recent gestarte Security Board.

Bij alle overleggen op het gebied van informatiebeveiliging, wordt de FG eveneens betrokken. Hiermee wordt de afstemming tussen informatiebeveiliging en gegevensbescherming ingevuld. Er is een werkgroep informatiebeveiliging. Hierin nemen de TISO, CISO , concernadviseur informatiehuishouding, de externe projectleiders implementatie BIG, en één van de informatiespecialisten deel. Elke woensdag vindt prioriteitenstelling plaats en schuift ook de CIO aan bij deze werkgroep. Wat vervolgens met die prioritering gebeurt hebben wij in dit onderzoek niet vastgesteld.

Ook heeft de gemeente Katwijk plannen om een Security Board in te stellen. Het doel van de Security Board is om naast de lopende zaken ook meer strategische vragen met betrekking tot informatiebeveiliging te bespreken met alle directbetrokkenen. Een eerste security board heeft in september 2018 plaatsgevonden.

Op het gebied van datalekken heeft de gemeente Katwijk een kernteam datalekken dat bestaat uit het Hoofd Concernstaf, de FG, de melder van het datalek, het afdelingshoofd/manager van de melder van het datalek, de Concerncontroller en de CIO. Op het moment dat er een datalek is geconstateerd wordt in het kernteam besproken óf het een datalek is, of het een meldingswaardig datalek betreft en dan kan vervolgens het protocol in werking treden.

2.4 Vormgeving van beleid en maatregelen

2.4.1 Privacy beleid

De gemeente heeft zich goed voorbereid op de AVG. Dit leidde er toe dat de gemeente in mei 2018 bij het van kracht worden van de AVG grotendeels voldeed aan de eisen die de AVG stelt. Zo was het verwerkingenregister grotendeels gereed en gevuld maar was er nog geen sprake van een 100% dekking. Wel waren per 25 mei de baselinetoetsen op alle afdelingen afgerond. Op 11 juli 2017 heeft het College B&W het algemeen privacy beleid Katwijk 2.0 vastgesteld. In dat beleid is opgenomen dat ter voorbereiding op de AVG het privacy beleid elk jaar geaudit zal worden. Wij hebben niet kunnen vaststellen dat er al een eerste volledige afzonderlijke audit op het privacy beleid heeft plaatsgevonden. Wel hebben op verschillende momenten evaluaties van delen van het privacy beleid

plaatsgevonden. Bijvoorbeeld bij de evaluatie van de privacy governance en bij het opstellen van de verklaring van accountability (september 2018). Ook in de ENSIA is privacy geëvalueerd.

Het privacy beleid beschrijft ook een aantal volwassenheidsniveaus voor de omgang met persoonsgegevens. Op 22 september 2018 heeft het College voor de gemeente vastgesteld op welk volwassenheidsniveau de verschillende diensten van de gemeente zich bevinden. Het College heeft zich tevens voorgenomen om per eind 2018 gemeentebreed op het volwassenheidsniveau 3 of 4 te zitten en per eind 2019 op niveau 5. De betreffende volwassenheidsniveaus luiden als volgt:

Niveau 0: De verantwoordelijke heeft erkend dat hij maatregelen wil gaan nemen en daartoe de eerste initiatieven ontplooid.

Niveau 1: Er is een besef omtrent gegevensbescherming. Op hoofdlijnen zijn de grenzen van verantwoordelijkheid en aansprakelijkheid in kaart gebracht en er is een FG aangesteld. Het proces van verinnerlijken is gaande.

Niveau 2: Op systematische wijze zijn de verwerkingen van persoonsgegevens in kaart gebracht. Wijzigingen worden adequaat beheerd. Onderzoeken worden gepland en uitgevoerd. De uitkomsten worden gerelateerd aan het overzicht en inzicht in de verwerkingen.

Niveau 3: Inzicht en overzicht in de verantwoordelijkheden en aansprakelijkheden alsmede in de verwerkingen en de compliance wordt uitgebreid naar de bewerkers. Er zijn duidelijke en transparante afspraken tussen verantwoordelijke en bewerkers en tussen bewerkers onderling gemaakt. Er is een basis gelegd voor het voorkomen van bestuurlijke en civielrechtelijke procedures.

Niveau 4: Actieve en passieve rechten van de betrokkene worden gefaciliteerd. De organisatie (verantwoordelijke of bewerker) kan zich hierover maatschappelijk verantwoorden.

Niveau 5: De betrokkene (klant, medewerker of individu) is “in control” over zijn/ haar persoonsgegevens. De organisatie (verantwoordelijke of bewerker) heeft de voorwaarden voor eerlijk zaken doen gecreëerd en houdt die ook in stand.

Niveau 6: Gegevensbeschermingen privacy zijn “ingebouwd” in de organisatie. Niet alleen in de informatiesystemen maar ook in de administratieve organisatie en het handelen van medewerkers, leveranciers en klanten. De werking van de getroffen maatregelen en mechanismen kan getoond worden. De organisatie is “accountable”. De organisatie heeft gegevensbescherming zodanig verankerd in de bedrijfsvoering dat

gegevensbescherming onderdeel is geworden van het risicomanagement dat een verplicht onderdeel is van de jaarrekening.

Niveau 7: Er is sprake van een heldere beslissingsstructuur voor beleid en aanpak voor gegevensbescherming en privacy als onderdeel van het in standhouden van een verantwoorde bedrijfshuishouding.

Op dit moment zit de gemeente Katwijk tussen niveau 1 en niveau 2 in. Het meest realistische scenario is dat per eind 2018 niveau 2 overal van toepassing is, waarbij enkele afdelingen zoals bijvoorbeeld Burgerzaken stijgt hier vanwege de al jarenlange ervaring met het zorgvuldig omgaan met persoonsgegevens in kwartaal 3 van 2018 al bovenuit. Daarna kan een begin met niveau 3 is gemaakt[10].

2.4.2 Plaats onafhankelijk werken en Mobile Device Management

4. Welke Mobile Device Management (MDM) oplossing heeft de gemeente Katwijk gekozen en op welke wijze wordt met behulp van de MDM een optimale beveiliging van de mobiele devices ingericht?

De gemeente Katwijk werkt ten tijde van het onderzoek aan de overgang richting een nieuwe werkplekomgeving die de medewerkers van de gemeente in staat stelt om plaats onafhankelijk te werken. Ten behoeve van dit plaats onafhankelijk werken heeft de gemeente een beleid[11] opgesteld waarin verschillende informatiebeveiligingsaspecten worden voorgeschreven. Dit beleid is op 24 januari 2018 geagendeerd voor besluitvorming binnen het Management Team van de gemeente Katwijk.

Voor plaats onafhankelijk werken maakt de gemeente Katwijk gebruik van devices, die eigendom zijn van de gemeente (Corporate owned Devices: COD) maar ook kunnen medewerkers eigen devices gebruiken voor hun werk (Bring your own device: BYOD) mits deze voldoen aan de eisen, die de gemeente daaraan stelt. Zo dienen alle devices, dus laptops, smartphones en tablets te zijn voorzien van de door Katwijk gekozen Mobile Device Management (MDM) software Airwatch. Door het in gebruik nemen van het nieuwe Mobile Device Management worden de o.a. (de informatiebeveiligings-)eisen, die gesteld worden aan zowel de COD als de BYOD ingeregeld. Ook voor MDM heeft de gemeente Katwijk beleid[12] geformuleerd dat op 24 januari 2018 binnen het Management Team van Katwijk is geagendeerd voor besluitvorming.

Binnen dit onderzoek hebben we alleen kunnen vaststellen dat de beleidsstukken aanwezig zijn en dat deze relevante inhoud bevatten. Of het beleid daadwerkelijk ook

[10] Totaaloverzicht acties privacy, versie 11 juni 2018
[11] Beleid plaats onafhankelijk werken, versie 2018.03
[12] Mobile Device Management, gemeente Katwijk, versie 1.2. d.d. 19-3-2018

werkt in de praktijk hebben wij niet kunnen vaststellen aangezien de implementatie van de nieuwe netwerkomgeving en het in gebruiknemen van het Mobile Device Management in september 2018 van start is gegaan. Het evalueren van het Mobile Device Beleid in de praktijk is op zijn vroegst een half jaar tot een jaar na de implementatie zinvol. Oorspronkelijk was deze implementatie gepland in het tweede kwartaal 2018.

3 INFORMATIEBEVEILIGINGSBELEID IN DE PRAKTIJK

3.1 INLEIDING

De gemeente Katwijk heeft een duidelijk en actueel informatiebeveiligingsbeleid en een separaat privacy beleid, zoals in het vorige hoofdstuk beschreven. In dit hoofdstuk wordt naast het beleid ook beschreven hoe dit beleid in de praktijk van alledag invulling krijgt. Geeft het beleid ook handelingsperspectief aan de praktijk of is het beleid eerder een theoretische exercitie, die mogelijk ver af staat van het dagelijkse werk van de gemiddelde ambtenaar van de gemeente Katwijk. In dit hoofdstuk ligt de focus op deze dagelijkse praktijk. In dit hoofdstuk staan dan de volgende vragen centraal:

5. Hoe is de operationalisatie en implementatie van de BIG tot nu toe verlopen?
6. Hoe is dit beleid uitgewerkt en geborgd in processen op de werkvloer?

3.2 IMPLEMENTATIE VAN DE BIG

De uitvoering van de BIG vindt in 2018 nog volop plaats onder regie van de CISO en met behulp van twee externe projectleiders. De uitvoering van de BIG is in 2015 gestart met een inventarisatie van de situatie op dat moment in vergelijking met de toekomstig gewenste situatie. De verschillen tussen de aangetroffen situatie en de gewenste, toekomstige situatie worden in deze inventarisatie inzichtelijk gemaakt, dit betreft een zogenaamde GAP-analyse. Op basis van deze inventariserende analyse is door de adviseur informatieveiligheid[13] en de concernadviseur informatie een aanpak gemaakt om de BIG binnen de gemeente Katwijk te implementeren.

In september 2017 zijn voor de implementatie van de BIG twee externe projectleiders aangesteld om versneld acht tot tien maatregelen in te voeren, zoals bijv. het wachtwoordenbeleid of het sneller op slot gaan van het beeldscherm. De reden hiertoe is

[13] De CISO was op het moment van de GAP-analyse nog niet benoemd als CISO, maar was op dat moment nog adviseur informatieveiligheid. De CISO is formeel benoemd per 1 februari 2018. Voor de leesbaarheid van dit rapport en omdat het dezelfde persoon betreft gebruiken we in deze rapportage verder uitsluitend de titel CISO.

dat het werkplekproject op dat moment veel capaciteit vroeg van team ICT en met extra externe capaciteit de BIG implementatie versneld kon worden.

Een vervolgopdracht voor de twee externe projectleiders volgde begin 2018. Deze opdracht luidt dat 75% van de BIG-maatregelen voor eind 2018 geïmplementeerd moeten zijn. Wij hebben kennis genomen van deze vervolgopdracht en we hebben daarin niet kunnen vaststellen in hoeverre de in de opdracht omschreven aanpak aansluit op de uitgevoerde GAP-analyse.
Per januari 2018 was 38% van de maatregelen al ingevoerd. De gemeente Katwijk, had, ook in vergelijking met andere gemeenten, begin 2018 hiermee nog een forse implementatieopgave. Dat betekende dat nu met deze nieuwe opdracht en aanpak in 2018 aanvullend nog 37% van de BIG-maatregelen uitgevoerd moest worden. Inmiddels is de huidige stand van zaken (per 19/9/2018) dat 76% van de BIG-maatregelen is doorgevoerd.

Vervolgens heeft een korte inventarisatie plaatsgevonden en is in afstemming met de CISO een selectie van te nemen maatregelen gemaakt. Bij deze selectie is rekening gehouden met de uitrol van de nieuwe werkplek en ICT-infrastructuur in 2018 en de daardoor beperkte mogelijkheden om nog naast het werkplekproject aanvullende andere maatregelen door te voeren. Binnen de gemeentelijke organisatie is gedurende het vernieuwingsproject voor de werkplek en infrastructuur een zogenaamde “freeze” afgekondigd. Dat is een maatregel, die getroffen wordt om niet teveel technische maatregelen tegelijk uit te voeren. Dat betekent dat alleen wettelijk noodzakelijke en hoog prioritaire technische maatregelen doorgang kunnen vinden gedurende de “freeze” periode. Dat betekent dat een aantal maatregelen ingevoerd kon worden met de uitrol van de nieuwe werkplek en ICT-omgeving. Het vernieuwingsproject leidt tot een verbetering van het gebruikersgemak, door o.a. de invoering van single sign on, dat betreft het eenmalig inloggen op je pc op meerdere applicaties, en tevens tot een verbetering van de informatiebeveiliging. De uitrol van het vernieuwingsproject is twee keer uitgesteld. Inmiddels is de gefaseerde uitrol van de nieuwe werkplek eind september van start te gaan. Hiermee stond per september 2018 de weg open om in relatief korte periode een aantal al enige tijd voorbereide BIG-maatregelen, zoals het gewijzigde autorisatiebeleid, daadwerkelijk in te vullen en uit te rollen.

De selectie BIG-maatregelen voor 2018 betreft een aantal maatregelen met hoge prioriteit, zoals o.a. de back-up & recovery procedure en het Mobile Device Management. De back-up & recovery procedure betreft een procedure waarbij meestal de ICT-specialisten van een organisatie ervoor zorgen dat de data extra opgeslagen worden, zodat in geval van een verstoring in een applicatie, de ICT-specialisten deze data kunnen

terughalen en de medewerkers van de organisatie verder kunnen werken met deze extra opgeslagen data.

Mobile Device Management betreft een oplossing waarbij de IT-specialisten alle bij een organisatie in gebruik zijnde mobiele apparaten op afstand kan instellen en beheren. Mobile Device Management biedt veel extra mogelijkheden om de mobiele apparaten beter te beveiligen. Zo kan een laptop in geval van diefstal met Mobil Device Management bijvoorbeeld op afstand volledig leeggemaakt worden op het moment dat die verbonden is met het internet. Op die manier is het mobiele apparaat weliswaar verdwenen, maar kunnen geen (mogelijk) gevoelige data of informatie buit worden gemaakt. Doordat het Mobile Device Management ingezet wordt op alle mobiele devices, die medewerkers van de gemeente gebruiken voor hun werk, (zowel de COD als de BYOD), worden hiermee de informatiebeveiligingseisen op mobiele devices uitgerold.

Aanvullende informatiebeveiligingsmaatregelen

Vanuit de Suwinet, de BAG, BRP zijn specifieke wettelijke eisen (buiten de AVG) met betrekking tot de bescherming van persoonsgegevens ingesteld. Bij de gemeente Katwijk zijn deze eisen conform bepalingen in de specifieke wetgeving in de praktijk ook ingevuld. Dat blijkt onder andere uit de inrichting van de processen rondom Suwinet. De applicatiebeheerder, die verantwoordelijk is voor bijv. Suwinet, is tevens verantwoordelijk voor het doorvoeren van de informatiebeveiligingsmaatregelen op Suwinet. De informatiebeveiligingsmaatregelen voor specifieke applicaties maken onderdeel uit van de ENSIA-verantwoordingssystematiek en maken tevens onderdeel uit van het informatiebeveiligingsbeleid van de gemeente Katwijk. De CISO is tevens security-officer en eindverantwoordelijk voor de informatiebeveiliging op Suwinet. De applicatiebeheerder Suwinet geeft hier in de dagelijkse praktijk invulling aan. De CISO en de applicatiebeheerder Suwinet hebben minimaal tweejaarlijks (o.a. aan de hand van de ENSIA) contact over de te nemen aanvullende maatregelen en welke aanpassingen dit behoeft in het integrale informatiebeveiligingsplan.

In de praktijk betekenen de informatiebeveiligingsmaatregelen bijvoorbeeld dat medewerkers alleen die gegevens kunnen inzien, waartoe zij gemachtigd oftewel geautoriseerd zijn. Voorheen was dit minder stringent ingesteld, maar ook de specifieke wetgeving en eisen omtrent Suwinet, BAG, BRP en BRO worden strenger.
Indien een medewerker van bijvoorbeeld Samenleven nu een client wil opzoeken op basis van een burgerservicenummer (BSN) en dat buiten zijn of haar reguliere autorisatie valt, wordt dit eerst voorgelegd aan de interne controleur, d.w.z. of er voldoende noodzaak is om deze gegevens in te zien en gebruiken. Pas daarna krijgt de medewerker mogelijk toegang. Dat wordt door verschillende medewerkers als

vertragend in het helpen van de desbetreffende cliënten ervaren. Hiermee wordt wel voldaan aan de informatiebeveiligingsmaatregelen.

3.3 BEWUSTWORDING BINNEN DE ORGANISATIE

7. Hoe worden medewerkers betrokken bij en getraind in het borgen van het informatiebeveiligingsbeleid en het privacy beleid?

De bewustwording op het gebied van informatiebeveiliging en privacy is gestart met een presentatie in de gemeenteraad van juni 2016. Hierbij werden de adviseur concernstaf en de CISO ondersteund door een externe expert. De gemeenteraad is zich door deze sessie bewust geworden van de grote verantwoordelijkheid die de gemeente heeft en heeft vervolgens budget vrijgemaakt voor het opstellen van het informatiebeveiligings- en privacy beleid en het aanstellen van een FG en een CISO.

Deze eerste bewustwordingssessie leidde tot een beleid en een vervolgaanpak. De bewustwordingscampagne bestond uit een presentatie per afdeling (in totaal 31 presentaties) over informatiebeveiliging (o.a. de BIG, ENSIA) en privacy. De CISO en FG hebben deze presentaties samen gegeven. De presentatie werd afgestemd op de specifieke afdeling. Dat wil zeggen dat er een aantal voorbeelden van processen werden opgenomen die relevant zijn voor de betreffende afdeling. Daarnaast zijn er posters en flyers over informatiebeveiliging en gegevensbescherming verspreid in het gemeentehuis.
Naast de bewustwordingscampagne is door de gemeente eveneens een e-learning module aangeschaft. Deze e-learning module (van twee maal zes modules) biedt een online opleiding aan alle medewerkers van de gemeente. Na het volgen van de opleiding wordt elke module afgesloten met een examen. Alle vaste medewerkers van de gemeente Katwijk worden geacht dit examen voor het einde van het jaar gehaald te hebben. In september 2018 zijn er inmiddels al voor vierhonderdzestig medewerkers accounts aangemaakt, terwijl het aantal vaste fte driehonderd bedraagt. Hieruit blijkt dat er ook veel tijdelijke medewerkers door managers worden aangemeld om de e-learning te volgen en het examen af te leggen. De CISO monitort de voortgang op de e-learning examens en informeert de verantwoordelijke managers over de voortgang.
Per 1 november 2018 zijn 56 van de examens voor informatiebeveiliging afgelegd en 47% van de examens voor de gegevensbescherming succesvol afgerond. Vooralsnog zijn geen dwingende sancties bepaald voor het niet-halen van het examen voor eind 2018.

In november 2017 heeft in het kader van de bewustwordingscampagne eveneens een Katwijkse privacy week plaatsgevonden. Het programma bestond o.a. uit een algemene presentatie, een film, een lezing van Maria Genova, een quiz en een inloopspreekuur.

Deze bewustzijnscampagne en de e-learning hebben voor een brede bewustwording gezorgd. Het proces om dit bewustzijn in de dagelijkse werkzaamheden en processen per team vorm te geven vindt nu plaats. Er is vanaf 20 september 2018 een informatiebeveiliging- en privacy spreekuur gestart elke 3e donderdag van de maand. Hier kunnen medewerkers van de gemeente terecht met hun vragen op het gebied van informatiebeveiliging en privacy. Op de kennisbank (intranet) staat alle relevante informatie over zorgvuldig omgaan met gegevensbescherming en informatiebeveiliging voor de medewerkers van de gemeente.

Uit de interviews komt naar voren dat vrijwel alle medewerkers weten wie de ambtelijke verantwoordelijkheid hebben binnen de gemeente voor informatiebeveiliging en privacy, nl. de CISO en FG. De rol van de TISO is nog minder goed bekend bij de verschillende medewerkers. Uit de gesprekken komt eveneens naar voren dat de medewerkers weten dat er een procedure is voor datalekken binnen de gemeente. En dat ze een melding kunnen doen via een e-mail aan een specifiek mailadres. Veel medewerkers weten niet hoe het proces na de melding van het datalek verloopt. Dat hoeft echter geen belemmering te zijn om een datalek te herkennen en hierna adequaat te handelen. De direct betrokkenen bij het datalek-proces hebben wel helder voor ogen wie hierbij betrokken dienen te zijn en welke verschillende stappen doorlopen worden voor de afhandeling conform het proces.

Het proces is als volgt: vervolgens komt de CISO in actie en zoekt direct contact met de onlangs aangestelde TISO. De CISO en TISO nemen soms direct een actie om verdere verspreiding te voorkomen en de CISO roept zo snel mogelijk het kernteam Datalekken bijeen. In het kernteam Datalekken hebben zitting: Hoofd Concernstaf, de FG, de melder van het datalek, het afdelingshoofd/manager van de melder van het datalek, de Concerncontroller en de concernadviseur Informatievoorziening. In het kernteam wordt besproken of het een datalek is, of het een bij de Autoriteit Persoonsgegevens meldingswaardig datalek betreft en dan treedt het protocol in werking.
Er zijn inmiddels meerdere datalekken succesvol aan de hand van het protocol afgewikkeld. Het protocol werkt in de praktijk. Inmiddels is het proces aan de hand van een evaluatie van het gebruik aangepast. Bij de afwikkeling van de eerste datalekken werd de manager van de melder niet genodigd bij de bespreking van het datalek. Inmiddels is het proces hierop aangepast, omdat het voor veel medewerkers, die een datalek melden prettiger is indien zijn/haar leidinggevende bij de bespreking aanwezig is

en dit ook beter is, vanwege de verantwoordelijkheid die de manager draagt voor de gegevensbescherming.
Het proces datalekken is onderdeel van de IT audit. Wij hebben ten behoeve van dit onderzoek een overzicht kunnen inzien met daarin het aantal datalekken en de aard van de datalekken.[14]

3.4 TESTEN VAN INFORMATIEBEVEILIGING

8. Hoe geeft de gemeente Katwijk invulling aan het testbeleid en de auditing op de digitale veiligheid? 9. Op welke wijze worden de ICT-voorzieningen (waaronder de infrastructuur, de wifi, de volledige werkplek, de website en digitale dienstverlening) van de gemeente Katwijk getest op informatiebeveiliging, met welke frequentie en met welke resultaten?

De afgelopen ca. zes jaren heeft het team ICT minimaal een keer per jaar verschillende (pen-)testen[15] laten uitvoeren op haar basis ICT voorzieningen door externe bureaus. De afgelopen drie jaren zijn daar eveneens op initiatief van de CISO testen op het gebruik van de ICT, of het gedrag van de gebruikers bijgekomen. Zo hebben inmiddels phishing testen plaatsgevonden en zijn er meerdere malen mystery guests bij de gemeente langs geweest.
Het testbeleid is geen expliciet onderdeel in het strategisch of tactisch informatiebeveiligingsbeleid, maar de jaarlijkse pentesten zijn wel opgenomen als maatregel in het informatiebeveiligingsplan 2018.

De CISO coördineert de pentesten en rapporteert hierover in zijn reguliere rapportages aan het College en directie. In de praktijk stemt de CISO met het team ICT af over op welke systemen en onderwerpen de pentesten van dat jaar ingezet worden. Indien uit de bevindingen van de pentesten aanvullende maatregelen nodig zijn, worden deze door het team ICT zo snel mogelijk gerealiseerd.
Hierbij ervaren de technisch specialisten geen belemmeringen in het uitvoeren van de verbetermaatregelen. Uiteraard wordt door het management kritisch gekeken naar de kosten van een maatregel in verhouding tot het af te dekken risico. Echter hierbij is het budget in de praktijk niet leidend.
De afgelopen maanden heeft de freeze wel geleid tot een vertraging in het doorvoeren van alle ICT-technische maatregelen, dus ook de te nemen maatregelen na de pentesten.

[14] Document: 2017 Overzicht aantallen en kosten incidenten incl. datalekken (december 2017).xlsx
[15] Een penetratietest of pentest is een toets op kwetsbaarheden in één of meerdere computersystemen (zowel applicaties als server, databases, internet, etc). Bij deze toets worden de gevonden kwetsbaarheden ook gebruikt om in het systeem te komen, feitelijk inbreken in de systemen.

In het voorjaar van 2018 heeft een test plaatsgevonden om na te gaan welke systemen en informatie vanaf het internet bij de gemeente Katwijk of onder verantwoordelijkheid van de gemeente Katwijk zonder meer bereikbaar zijn. De bevindingen die hieruit naar voren gekomen zijn, zijn omgezet in te nemen maatregelen. Ondanks de freeze zijn de maatregelen met de hoogste prioriteit (zogenaamde prio 1-maatregelen) inmiddels voor de zomervakantie al uitgevoerd.

De gemeente Katwijk maakt gebruik van het ENSIA kader dat ontwikkeld is vanuit o.a. de VNG en het Ministerie van BZK. De ENSIA staat voor Eenduidige Normatiek Single Information Audit. Deze methodiek biedt een kader om op basis van een deel zelfevaluatie en een deel externe controle tegelijkertijd verantwoording af te leggen over de informatiebeveiliging aan het gemeentebestuur en de toezichthoudende departementen. Een externe accountant controleert de zelfevaluatie van de gemeente en brengt een verklaring hierover uit.

3.5 Risico's op het gebied van informatiebeveiliging en privacy

10. Welke mogelijke risico's zijn te onderkennen in de huidige wijze waarop het privacy en informatiebeveiligingsbeleid is ingericht en functioneert?

Het huidige privacy- en informatiebeveiligingsbeleid van de gemeente Katwijk heeft zorgvuldig vorm gekregen in zowel een strategisch en tactisch informatiebeveiligingsplan en een jaarplan Informatiebeveiliging. Voor privacy is eveneens sprake van een actueel vastgesteld privacybeleid. Er zijn drie verantwoordelijke functionarissen aangesteld, nl. een FG, een CISO en een TISO. Er zijn overleg- en kennisgremia voor de informatiebeveiliging zijn tevens processen voor het melden van datalekken. De BIG implementatie krijgt op structurele wijze verder invulling, evenals het verder brengen van een hoger volwassenheidsniveau van de privacy binnen de gemeente. De informatiebeveiliging wordt structureel gemonitord, o.a. met behulp van een ISMS. De verantwoording vindt plaats conform de ENSIA-methodiek. Het proces voor inzageverzoeken krijgt nu werkenderweg vorm. Er vinden regelmatig testen van zowel de applicaties en ICT-infrastructuur plaats en er worden gebruikers getest.

Kortom: het beleid is actueel en op orde, de maatregelen die de gemeente moest treffen hebben vorm gekregen en het bewustzijn is aanwezig. De basis is op orde. Aandachtspunt in het verder brengen van het niveau van de informatiebeveiliging en privacy binnen de gemeente Katwijk betreft het breder trekken van de verantwoordelijkheden dan de CISO, FG en TISO en het aanpassen van specifieke

processen binnen de verschillende afdelingen en teams. Hierbij is het van belang dat naast het benoemen van de verantwoordelijken binnen de uitvoerende afdelingen, de personen binnen die uitvoerende afdelingen naast het hebben van een handelingsperspectief ook de verantwoordelijkheid voelen voor informatiebeveiliging.

Een ander aandachtspunt op het gebied van privacy betreft het uitvoeren van privacy impact assessments (PIA's). Deze worden weliswaar op enkele processen van de gemeente Katwijk uitgevoerd, nadat uit de baselinetoetsen naar voren is gekomen dat dit risicovolle processen betreft en een PIA voor deze processen noodzakelijk is. Deze PIA´s zijn echter uitgevoerd aan de hand van verouderde formats. Wij hebben dit voor twee PIA's vastgesteld.[16] Deze formats zijn gebaseerd op niet meer geldende wetgeving (Wet bescherming persoonsgegevens). Deze is per 25 mei vervangen door de AVG waarin een aantal strengere regels zijn opgenomen. Bovendien zijn de PIA's minimaal ingevuld. Zo zijn enkel de vragen beantwoord met 'Ja' of 'Nee' maar ontbreekt de toelichtende beschrijving.

3.6 BORGING VAN INFORMATIEBEVEILIGING

11. Hoe ziet de gemeente erop toe dat het informatiebeveiligingsbeleid van een voldoende niveau is en blijft en er wordt geanticipeerd op toekomstige opgaven?

Het college en de directie worden minimaal in kwartaalrapportages geïnformeerd over de voortgang op het informatiebeveiligingsplan en het projectplan privacy. Beide plannen worden voorafgaand aan de uitvoering voorgelegd ter besluitvorming aan zowel het College als de directie. Hiermee worden het College en de directie geïnformeerd. Het Hoofd Concernstaf en de plaatsvervangend gemeentesecretaris maken onderdeel uit van zowel het maandelijkse informatiebeveiligingsoverleg als het team Datalekken en wordt daarmee naast de kwartaalrapportages eveneens snel geïnformeerd over de stand van zaken, mogelijke datalekken of andere incidenten. Zij draagt tevens zorg om het College en mogelijk de gemeenteraad adequaat te informeren.

De dragende functionarissen (CISO, FG en TISO) zijn benoemd en als vaste medewerkers opgenomen in de formatie. De BIG en de AVG zijn grotendeels geïmplementeerd, er worden plannen gemaakt voor de verdere implementatie en versterking van de informatiebeveiliging en gegevensbescherming vanaf 2019.
Er is tevens meerjarig budget gealloceerd voor informatiebeveiliging en gegevensbescherming. De basis is op orde, maar daarmee is het werk voor de

[16] Wij hebben kennis genomen van de PIA Basis Registratie Personen (BRP) en de PIA Leerlingenvervoer.

informatiebeveiliging en de gegevensbescherming nog zeker niet klaar. Bovendien is het werk van gemeenten ter versterking van de digitale weerbaarheid nooit gereed. In de verdere digitalisering van de samenleving en de dienstverlening van de gemeenten zelf, begeven gemeenten zich op het digitale pad. Om misbruik van het digitale pad te voorkomen, is het versterken van de informatiebeveiliging een structurele opgave om de digitale veiligheid op orde te houden. Digitale veiligheid is daarmee een structurele opgave oftewel een never ending story.

Ook de kaders voor digitale veiligheid zijn ontwikkeling. Er is inmiddels een Baseline Informatiebeveiliging Overheid (BIO) als opvolger van de BIG. De BIO is nog niet van kracht, maar zal mogelijk vanaf 2020 een nieuw kader voor alle overheidsorganisaties op het gebied van digitale veiligheid bieden. Hierop wordt de huidige ENSIA verantwoordingssystematiek uiteraard ook aangepast.

3.7 MONITORING VAN INFORMATIEBEVEILIGINGSBELEID

12. Welke beveiligingsincidenten heeft de gemeente Katwijk de afgelopen twee jaren ondervonden en hoe zijn deze afgewikkeld?

Sinds september 2017 is er een systeem voor de monitoring van de informatiebeveiliging in werking (een ISMS). Het ISMS wordt met name gebruikt om de voortgang van de BIG-implementatie te monitoren.
Het aantal datalekken, beveiligingsincidenten en virussen binnen de gemeente wordt vanaf 2016 gemonitord door het team ICT en de CISO.
In 2016 kende de gemeente 5 meldenswaardige datalekken, in 2017 zes en in 2018 vooralsnog (t/m eind september) twee.
In 2016 waren er 37 beveiligingsincidenten, in 2017 17 en in 2018 (t/m eind september) 6. Het aantal virussen betrof in 2016 7, in 2017 2 en in 2018 t/m eind september nog geen.
Alle gemelde informatiebeveiligingsincidenten worden geregistreerd in Planon[17]. Alle datalekken worden geregistreerd in een Excel spreadsheet. De CISO rapporteert in zijn reguliere (kwartaal-) rapportages over de voortgang van de BIG implementatie, de privacy en de in de achterliggende periode gemelde informatiebeveiligingsincidenten en datalekken aan het MT en de portefeuillehouders.

[17] Planon is een applicatie ter ondersteuning van de bedrijfsvoering van organisaties. In deze applicatie vindt o.a. gebouw- en zaalbeheer, maar tevens veelal de registratie van verschillende (soms) gebouwgebonden meldingen vanuit de organisatie plaats.

Beveiligingsincidenten worden, afhankelijk welk type incident het betreft, afgewikkeld in samenwerking tussen de CISO en het team ICT. Deze incidenten worden eveneens besproken en veelal geëvalueerd in het wekelijkse (operationele) informatiebeveiligingsoverleg.

4 BETROKKENHEID VAN HET COLLEGE EN DE GEMEENTERAAD

4.1 INLEIDING

Een belangrijk aandachtspunt in het onderzoek is de rol van het College van B&W en de gemeenteraad. Is de raad in de positie om kaders voor het informatiebeveiligingsbeleid te formuleren, is de raad in staat dit te controleren en wordt de raad goed geïnformeerd over de ontwikkelingen rond informatiebeveiliging? In dit korte hoofdstuk wordt weergeven welke rol zowel het College van B&W en in het bijzonder de portefeuillehouder en de gemeenteraad volgens het beleid heeft en hoe deze in de praktijk van alledag de afgelopen jaren invulling heeft gekregen.

4.2 BETROKKENHEID VAN HET COLLEGE VAN B&W

Het college heeft volgens het strategisch informatiebeveiligingsplan de integrale verantwoordelijkheid voor de informatieveiligheid, zoals zij ook integraal verantwoordelijk is voor al het beleid en uitvoering van de gemeente Katwijk. In het tactisch informatiebeveiligingsbeleid wordt het als volgt omschreven:

"*Het college van Burgemeester en Wethouders is integraal verantwoordelijk voor de beveiliging (beslissende rol) van informatie binnen de werkprocessen van de gemeente.*

Het college stelt kaders voor informatiebeveiliging (IB) op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders."

In de praktijk wordt aan deze verantwoordelijkheid vooral door de portefeuillehouder digitalisering, privacy en informatisering binnen het College van B&W vormgegeven. In het nieuwe college van B&W, dat voor de zomer van 2018 is aangetreden, is burgemeester Visser verantwoordelijk voor deze portefeuille. In het portefeuillehouders overleg is informatiebeveiliging een vast agendapunt.

4.3 VERANTWOORDING AAN DE RAAD

13. Op welke wijze is de raad tot nu toe bij de ontwikkeling van de informatieveiligheid betrokken geweest?
14. Op welke manier kan de gemeenteraad het beleid rondom informatieveiligheid controleren en sturen?

Uit de gevoerde gesprekken komt naar voren dat de gemeenteraad louter via de gebruikelijke P&C-cyclus en bijbehorende documenten is en wordt geïnformeerd over de inrichting en de verdere ontwikkeling van het beleid. Uiteraard na de initiële, informatieve bijeenkomst over informatiebeveiliging en privacy in de gemeenteraad in 2016.

In 2017 en 2018 is een enkele maal het initiatief genomen om de raad door middel van een aparte informatieavond over dit beleid te informeren. Om allerlei praktische redenen heeft dat geen doorgang kunnen vinden. Voor zover bekend hebben raadsleden ook niet zelf geïnformeerd naar dit beleid, en aanverwante zaken zoals privacybescherming.

Vanuit de gemeenteraad is de auditcommissie werkzaam. De portefeuillehouder en de CISO zijn voornemens met enige regelmaat met deze commissie ook over informatiebeveiliging te zullen overleggen.

Vanuit de organisatie wordt actieve betrokkenheid door de raad op prijs gesteld, omdat het immers aan de raad is om de kaders te stellen en om vervolgens te controleren of aan de ambities op de afgesproken wijze invulling wordt gegeven. Juist in de afweging tussen snelle en adequate dienstverlening en sociale hulp en ondersteuning aan burgers en de hierbij soms ´vertragende´ regels met betrekking tot gegevensbescherming is een afwegingskader of principe-uitspraak vanuit de gemeenteraad wenselijk voor de verantwoordelijke ambtenaren.

5 CONCLUSIES EN AANBEVELINGEN

5.1 BEANTWOORDING VAN DE DEELVRAGEN

In de voorgaande hoofdstukken zijn zowel het beleid als de praktijk van informatiebeveiliging en privacy bij de gemeente Katwijk omschreven. In deze paragraaf worden allereerst de deelvragen uit de voorgaande hoofdstukken in een beknopt overzicht beantwoord. Daarna volgt in paragraaf 5.2 Conclusie en aanbevelingen de overall conclusie en een aantal aanbevelingen ter verdere versterking van de digitale veiligheid bij de gemeente.

De beknopte beantwoording van de deelvragen is opgenomen in onderstaand overzicht.

1. Welke beleidskaders[18], regels en richtlijnen hanteert de gemeente voor de borging van de informatiebeveiliging?
2. Voldoet het beleid en de uitwerking in processen binnen de gemeente aan de bepalingen van het basisnormkader Baseline Informatiebeveiliging Gemeenten (BIG) en aan de Algemene verordening gegevensbescherming (AVG[19], die per 25 mei van toepassing is)?

De gemeente Katwijk heeft conform de AVG en de BIG haar informatiebeveiligingsbeleid en processen vormgegeven en omschreven in een strategisch en tactisch beleid en een jaarplan. Het privacy beleid is eveneens vastgesteld en voldoet aan de wettelijke bepalingen uit de AVG. Het informatiebeveiligingsbeleid voldoet aan de bepalingen, zoals vastgelegd in de BIG. Op zowel het IB-beleid als het privacy beleid zijn nog enkele aanpassingen te doen; zoals het vanuit het privacy beleid verwijzen naar het IB-beleid (vice versa is al gerealiseerd), het opnemen van de rol en verantwoordelijkheid van de in 2018 gestarte nieuwe technische informatiebeveiligingsadviseur (TISO). Dit betreft actualisering en finetuning van het beleid.

3. Welke functionarissen zijn verantwoordelijk gesteld voor de informatiebeveiliging binnen de gemeente?

Binnen de gemeente Katwijk zijn de vereiste verantwoordelijke functionarissen, zoals de FG en de CISO conform de BIG en AVG aangesteld. In het IB- en privacy beleid zijn naast de kernfunctionarissen eveneens de verantwoordelijkheden van anderen binnen de gemeente (zoals het College, de managers, etc.) geschetst. Echter de positionering van de kernfunctionarissen binnen de gemeente (onder welke afdeling en eindverantwoordelijke zij vallen) is niet vastgelegd in het beleid.

[18] Naast het vastgestelde en onlangs geactualiseerde privacybeleid en informatiebeveiligingsplan van de gemeente Katwijk.
[19] Omdat de AVG per 25 mei 2018 van kracht is geworden en de WBP per die datum niet meer van kracht is, zullen wij in dit rekenkameronderzoek de AVG als wettelijk kader hanteren.

4. Welke MDM oplossing heeft de gemeente Katwijk gekozen en op welke wijze wordt met behulp van de MDM een optimale beveiliging van de mobiele devices ingericht?
Bij de gemeente Katwijk is met de uitrol van de nieuwe, mobiele werkplek en een vernieuwing van de ICT-infrastructuur eveneens Mobile Device Management (MDM) uitgerold en het opgestelde beleid voor plaats onafhankelijk werken in werking getreden. Met het in gebruik nemen en zorgvuldig inrichten van de MDM-oplossing die Airwatch biedt kan de informatiebeveiliging van mobiele devices op een hoger niveau gebracht worden, zoals is voorzien. Of het beleid daadwerkelijk geëffectueerd is in de praktijk en hierin de IB op een hoger niveau brengt hebben wij niet kunnen vaststellen in dit onderzoek aangezien de implementatie van de nieuwe netwerkomgeving en het in gebruik nemen van het MDM pas in september 2018 is gestart.

5. Hoe is de operationalisatie en implementatie van de BIG tot nu toe verlopen?

De operationalisatie en implementatie van de BIG is in 2015 bij de gemeente gestart met een GAP-analyse. Vervolgens is in 2017 en 2018 onder andere met behulp van externe projectleiding de BIG gestructureerd geïmplementeerd. Per eind september 2018 is 76% van de BIG-maatregelen geïmplementeerd, maar of daarmee de grootste risico's zijn afgedekt hebben wij niet kunnen vaststellen. De implementatie van de BIG is gemonitord door de CISO en hierover is gestructureerd gerapporteerd.

6. Hoe is dit beleid uitgewerkt en geborgd in processen op de werkvloer?

Het informatiebeveiligingsbeleid en het privacy beleid zijn vastgesteld. De gedragsregels en werkwijzen zijn breder binnen de gemeente aan alle medewerkers kenbaar gemaakt door o.a. bewustwordingsworkshops, e-learning en informatie op het intranet. Het beleid is bekend bij de meeste collega´s, maar de dagelijkse invulling in de diverse werkprocessen van de verschillende afdelingen is nog geen gemeengoed.

7. Hoe worden medewerkers betrokken bij en getraind in het borgen van het informatiebeveiligingsbeleid en het privacy beleid?

De gedragsregels en werkwijzen zijn breder binnen de gemeente aan alle medewerkers kenbaar gemaakt door o.a. bewustwordingsworkshops, e-learning en informatie op het intranet.

8. Hoe geeft de gemeente Katwijk invulling aan het testbeleid en de auditing op de digitale veiligheid?
9. Op welke wijze worden de ICT-voorzieningen (waaronder de infrastructuur, de wifi, de volledige werkplek, de website en digitale dienstverlening) van de gemeente Katwijk getest op informatiebeveiliging, met welke frequentie en met welke resultaten?

De gemeente Katwijk heeft haar beleid met betrekking tot pentesten niet vastgelegd, maar zorgt wel voor regelmatige en gestructureerd testen (2 x per jaar) op de diverse ICT voorzieningen en het beveiligingsbeleid in den brede. Met betrekking tot de auditing van de informatiebeveiliging maakt de gemeente gebruik van de ENSIA. Ook op het privacy beleid heeft inmiddels een (zelf-)audit plaatsgevonden.

10. Welke mogelijke risico's zijn te onderkennen in de huidige wijze waarop het privacy- en informatiebeveiligingsbeleid is ingericht en functioneert?

Het breder borgen van kennis en een gevoel van verantwoordelijkheid binnen de gemeentelijke organisatie en bij de gemeenteraad is een risico. Op dit moment dragen voornamelijk de kernfunctionarissen zoals de FG, CISO en TISO deze

verantwoordelijkheid in de praktijk. In het beleid is de verantwoordelijkheid breder belegd bij o.a. het management van de gemeente. Het vraagt nog enkele jaren extra aandacht om deze verantwoordelijkheid breder binnen de organisatie bij meerdere verantwoordelijken te borgen.
Daarnaast zijn risico-afwegingen op de privacy tot op heden niet conform de AVG-kaders uitgevoerd maar op basis van tot op dat moment geldende kaders. De huidige kaders, en de daarbij te hanteren formats, gaan dieper op de risico's in.

11. Hoe ziet de gemeente erop toe dat het informatiebeveiligingsbeleid van een voldoende niveau is en blijft en wordt er geanticipeerd op toekomstige opgaven?

De directie, het College en de gemeenteraad worden gestructureerd geïnformeerd over de voortgang op de jaarlijkse uitvoering van het beleid (jaarplan). De concretisering van het beleid in een jaarplan wordt door de kernfunctionarissen opgesteld en vastgesteld door de directie en het College.

12. Welke beveiligingsincidenten heeft de gemeente Katwijk de afgelopen twee jaren ondervonden en hoe zijn deze afgewikkeld?

De gemeente kent vaste werkwijzen voor het melden van IB-incidenten en datalekken. Deze procedures vinden plaats onder verantwoordelijkheid van de kernfunctionarissen en zijn binnen de gemeente breed bekend gemaakt.

13. Op welke wijze is de raad tot nu toe bij de ontwikkeling van de informatieveiligheid betrokken geweest?
14. Op welke manier kan de gemeenteraad het beleid rondom informatieveiligheid controleren en sturen?

Uit de gevoerde gesprekken komt naar voren dat de gemeenteraad met name via de gebruikelijke P&C-cyclus en bijbehorende documenten is geïnformeerd over de inrichting en de verdere ontwikkeling van het beleid.
De gemeenteraad kan en moet kaders stellen en om vervolgens te controleren of aan de ambities op de afgesproken wijze invulling wordt gegeven. Bijvoorbeeld in de afweging tussen snelle en adequate dienstverlening en sociale hulp en ondersteuning aan burgers en de hierbij soms ´vertragende´ regels met betrekking tot gegevensbescherming.

5.2 Overall conclusie

Het informatiebeveiligingsbeleid en de basisinrichting van de processen en organisatie voor informatiebeveiliging en privacy zijn grotendeels op orde; er is voldoende aandacht, er is beleid en er zijn plannen (in ontwikkeling, zoals voor privacy) die recht doen aan de ambitie om de huidige situatie verder te verbeteren. Het werk is echter nog niet klaar en behoeft de komende jaren minimaal een even grote inspanning op het bewustzijn en het verder uitwerken van de invulling van informatiebeveiliging en privacy in de processen en dagelijkse casuïstiek.

In het opgestelde informatiebeveiligingsbeleid zijn de verantwoordelijken (bijv. portefeuillehouder, College, managers, etc.) duidelijk omschreven. In de dagelijkse praktijk wordt het grootste deel van de uitvoering van het beleid ingevuld door de CISO,

de FG en sinds kort de TISO. Dat maakt de informatiebeveiligingsorganisatie nog kwetsbaar en afhankelijk van enkele sleutelfunctionarissen. Juist een groot deel van de organisatorische informatiebeveiligings- en privacy maatregelen ligt bij de afdelingen.

5.3 AANBEVELINGEN

Deze paragraaf beschrijft de aanbevelingen die volgen uit bovenstaande conclusie. We maken het onderscheid tussen meer algemene aanbevelingen en aanbevelingen die direct kunnen worden toegepast in de praktijk.

5.3.1 ALGEMENE AANBEVELINGEN

Aanbeveling 1.1: Wij bevelen aan om de informatiebeveiliging en gegevensbescherming binnen de gehele organisatie breder bij de verschillende verantwoordelijken voor informatiebeveiliging en privacy te borgen.

Aanbeveling 1.2: De gemeenteraad moet kaders kunnen stellen, juist bij de veelal lastige weging in het Sociaal Domein, waar snel handelen om cliënten adequaat te kunnen helpen, niet altijd mogelijk is vanwege stringente eisen aan de bescherming van persoonsgegevens. Mogelijk zou de auditcommissie een initiërende rol kunnen hebben bij het discussiëren en opstellen van een dergelijk kader in de gemeenteraad.

5.3.2 TOEPASSING IN DE PRAKTIJK

Volgend uit de meer algemene aanbevelingen én om ook een meer praktisch handelingsperspectief te bieden volgt hier een aantal aanbevelingen die direct in de praktijk kunnen worden toegepast:

Aanbeveling 2.1: Ten behoeve van een betere en bredere borging van informatiebeveiliging en privacy in de organisatie, bevelen wij aan om aan te sluiten op de P&C-cyclus. Zo kan elke afdeling zich jaarlijks via een ‘in control statement’ verantwoorden over de IB- en privacy-maatregelen, die ze hebben getroffen.

Aanbeveling 2.2: Stel per afdeling een verantwoordelijk medewerker aan voor de informatiebeveiliging en privacy (contactpersoon IB & privacy).

Aanbeveling 2.3: Laat de contactpersonen IB & privacy jaarlijks een interne evaluatie per afdeling van de informatiebeveiligings- en privacy maatregelen en -praktijk opstellen onder coördinatie van de interne controleurs.

Aanbeveling 2.4: Evalueer het MDM in beheer en gebruik na een jaar.

Aanbeveling 2.5: Hanteer de meest recente kaders voor de risico-afweging voor gegevensbescherming (gebaseerd op de AVG).

Aanbeveling 2.6: Neem bij een volgende actualisatie van het informatiebeveiligingsbeleid een omschrijving op van het in de praktijk al gerealiseerde testbeleid.

Aanbeveling 2.7: Continueer de gestructureerde en uitgebreide bewustzijnsacties, zoals in 2017 en 2018 ingezet binnen de gemeente in de jaarplannen IB en privacy voor 2019.

REACTIE COLLEGE IN HET KADER VAN HET BESTUURLIJK WEDERHOOR

Postbus 589 - 2220 AN Katwijk

Rekenkamercommissie Katwijk
de Voorzitter
t.a.v. de heer C de Graaf

Contactpersoon:
Mevrouw B. Engelberts

Afdeling:
Bedrijfsvoering

Te bereiken op:
071 – 406 5190

Ons kenmerk: 1346629

Bijlage(n):

Verzenddatum:

Uw kenmerk:
Onderwerp: Bestuurlijke reactie op het rapport Digitale Veiligheid in Katwijk

21 JAN 2019

Katwijk, 15 januari 2019

Geachte heer De Graaf,

Met interesse hebben wij kennis genomen van uw rapport over de digitale veiligheid in de gemeente Katwijk.

Wij zijn verheugd over uw hoofdconclusie dat het informatiebeveiligingsbeleid en de basisinrichting van de processen en organisatie voor informatiebeveiliging en privacy grotendeels op orde zijn; er is voldoende aandacht, er is beleid en er zijn plannen in ontwikkeling (zoals voor privacy) die recht doen aan de ambitie om de huidige situatie verder te verbeteren. Wij zijn ons terdege van bewust dat het werk nog niet klaar is en de komende jaren eveneens een grote inspanning op het bewustzijn en het verder invullen van informatiebeveiliging en privacy in de processen.

Wij zijn u erkentelijk voor het aangereikte praktische handelingsperspectief op de aanbevelingen.
In deze brief geven wij u graag een reactie op de conclusies en aanbevelingen uit uw rapport.

Ten aanzien van de algemene aanbevelingen

1. *Wij bevelen aan om de informatiebeveiliging en gegevensbescherming binnen de gehele organisatie breder bij de verschillende verantwoordelijken voor informatiebeveiliging en privacy te borgen.*

   Reactie: Deze aanbeveling hangt samen met de praktische aanbevelingen onder 1,2 3 en 5.
   Het breder borgen kan op twee wijzen ingevuld worden:
   a. Bij elke afdeling capaciteit vrijmaken, wat ten koste zal gaan van andere taken;
   b. Extra capaciteit organiseren.

   Wij gaan met de gemeenteraad in gesprek over het te bereiken ambitieniveau en in te zetten capaciteit.

2. *De gemeenteraad moet kaders kunnen stellen, juist bij de veelal lastige weging in het Sociaal Domein, waar snel handelen om cliënten adequaat te kunnen helpen, niet altijd mogelijk is vanwege stringente eisen aan de bescherming van persoonsgegevens. Mogelijk zou de auditcommissie een initiërende rol kunnen hebben bij het discussiëren en opstellen van een dergelijk kader in de gemeenteraad.*

   Reactie: Met u zijn wij van mening dat hier een rol zou kunnen liggen voor de auditcommissie. De FG en CISO zouden de auditcommissie hierin kunnen ondersteunen.

Ten aanzien van de praktische toepassing

1. *Ten behoeve van een betere en bredere borging van informatiebeveiliging en privacy in de organisatie, bevelen wij aan om aan te sluiten op de P&C-cyclus. Zo kan elke afdeling zich jaarlijks via een 'in control statement' verantwoorden over de IB- en privacy-maatregelen, die ze hebben getroffen.*

   Reactie: In Q1 zal hiertoe een controlelijst gemaakt worden. De verdere uitvoering hangt samen met de algemene aanbeveling onder 1 .

2. *Stel per afdeling een verantwoordelijk medewerker aan voor de informatiebeveiliging en privacy (contactpersoon IB & privacy).*

   Reactie: Zie ook de reactie bij de eerste algemene aanbeveling.

3. *Laat de contactpersonen IB & privacy jaarlijks een interne evaluatie per afdeling van de informatiebeveiligings- en privacy maatregelen en -praktijk opstellen onder coördinatie van de interne controleurs.*

   Reactie: Deze aanbeveling nemen we ter harte. In Q1 zal hiertoe een controlelijst gemaakt worden. De verdere uitvoering hangt samen met de algemene aanbeveling onder 1.

4. *Evalueer het MDM, in beheer en gebruik na een jaar.*

   Reactie: Het MDM gebruiken wij inmiddels en we nemen de aanbeveling over om dit in 2020 te evalueren.

5. *Hanteer de meest recente kaders voor de risico-afweging voor gegevensbescherming (gebaseerd op de AVG).*

   Reactie: De eerste risico-afwegingen hebben plaatsgevonden op de toen beschikbare modellen. De VNG komt in het eerste kwartaal 2019 met een vragenlijst voor DPIA's die voldoet aan de AVG. Inmiddels zijn wij in het bezit van de ruwe versie. Het tweede kwartaal van 2019 zullen we voor de processen die thans een hoog privacyrisico hebben de DPIA's opnieuw uitvoeren. Vervolgens zullen we in het derde kwartaal van 2019 aan de hand van de nieuwe criteria beoordelen voor welke verwerkingen er alsnog een DPIA moet worden uitgevoerd. Deze zullen in het vierde kwartaal van 2019 en het eerste en tweede kwartaal van 2020 afgerond worden. Deze planning is echter onder voorbehoud dat in het eerste kwartaal van 2019 extra middelen beschikbaar worden gesteld. Daarover gaan wij met de gemeenteraad in gesprek.

6. *Neem bij een volgende actualisatie van het informatiebeveiligingsbeleid een omschrijving op van het in de praktijk al gerealiseerde testbeleid.*

   Reactie: Binnen onze gemeente kennen we informatieseringsbeleid en jaarlijkse informatiebeveiligingsplannen. In het informatiebeveilingsplan voor 2019 is de planning van de in dat jaar uit te voeren testen opgenomen. De actualisatie van het informatiseringsbeleid is gepland in het vierde kwartaal van 2019. De in gang gezette organisatieontwikkeling zou deze planning nog kunnen beïnvloeden.

7. *Continueer de gestructureerde en uitgebreide bewustzijnsacties, zoals in 2017 en 2018 ingezet binnen de gemeente in de jaarplannen IB en privacy voor 2019.*

   Reactie: In het jaarplan IB 2019 is hier al rekening mee gehouden.

Tot slot
De aanbevelingen in het rapport steunen ons in de ontwikkeling die we in gang hebben gezet en we bedanken de onderzoekers daarvoor.

NAWOORD REKENKAMERCOMMISSIE

De rekenkamercommissie is verheugd dat het college de hoofdconclusie deelt, en zich er van bewust is dat het werk nog niet is gedaan. Het is goed te constateren dat het college het onderzoek als nuttig heeft ervaren en de aanbevelingen ziet als steun in de in gang gezette ontwikkelingen.

In grote lijnen neemt het college onze aanbevelingen over, of wordt geconstateerd dat de aanbevelingen al onderdeel van het beleid zijn. Het college merkt op dat de in te zetten capaciteit afhankelijk is van het gewenste ambitieniveau (aanbeveling 1.1, 2.2 en 2.3), en dat de planning afhankelijk is van nog ter beschikking te stellen middelen (aanbeveling 2.5). Hierover gaat het college met de raad in gesprek.

Het rapport – en de reactie van het college – legt nadrukkelijk een rol bij de raad, met een initiërende rol voor uw auditcommissie. Zie paragraaf 4.3 en aanbeveling 1.2. Deze aanbeveling vraagt om een concretere uitwerking dan nu door het college wordt gedaan. De rekenkamercommissie adviseert de raad om de door het college aangeboden ondersteuning door FG en CISO te vragen en samen met hen hier invulling aan te geven. Concrete invulling zal ook kunnen leiden tot betere controle door de raad op de uitvoering van het beleid.

De overall conclusie blijft dat de lijn die door de organisatie is ingezet moet worden voortgezet. De basis is goed, maar het werk is nog niet klaar. En eigenlijk is het nooit af. Digitale veiligheid moet in de haarvaten van de organisatie gaan zitten, en dat vraagt om voortdurende actie. De rekenkamercommissie beseft dat haar aanbevelingen mogelijk gevolgen kunnen hebben voor uw begroting.

Tot slot maakt de rekenkamercommissie graag een compliment aan de organisatie en het college voor wat al is bereikt en voor de energie die daarin is gaan zitten.

BIJLAGE A BRONNEN

DE IN DIT RAPPORT GECITEERDE BRONNEN

Documentnaam	Versie	Datum
Informatiebeveiligingsplan 2018	Definitief	Januari 2018
Strategisch informatiebeveiligingsbeleid	Definitief	9 mei 2017
Tactisch informatiebeveiligingsbeleid	Definitief	16 mei 2018
Algemeen privacybeleid gemeente Katwijk	2.0	Juni 2017
Beleid Plaats Onafhankelijk Werken	2018.03	
Mobile Device Management	1.2	19 maart 2018
Governance voor de privacy		januari 2018
Bewustwording cyber crime, IB en AVG		
Totaaloverzicht acties privacy		11 juni 2018
Verklaring van accountability (privacy en informatiebeveiliging)		18 september 2018

AFGENOMEN INTERVIEWS

	Naam	Functie	Datum
1	Koos van Bekkum	Chief Information Security Officer	2-7-2018
2	Robert van Egmond	Informatiespecialist	2-7-2018
3	Jan Willem Spaargaren	Chief Information Officer, Concernadviseur informatiehuishouding	2-7-2018
4	Mark Koelewijn	Technical Information Security Officer	2-7-2018
5	Bianca Engelberts	Hoofd Concernstaf	4-7-2018
6	John Bol	Concern controller	4-7-2018
7	Vincent Dilengite	Netwerk- en systeembeheerder	5-7-2018
8	Rene Visser	Netwerk- en systeembeheerder	5-7-2018
9	Sebastiaan Verkade	Applicatiebeheerder	5-7-2018
10	Annerine Blufpand	Functionaris Gegevensbescherming	5-7-2018
11	Liesbeth Hoek, Arjan Eendebak	Team Vergunningen	12-7-2018
12	Philip van der Ploeg, Martine Hes,	Team Samenleving	12-7-2018

	Stephanie van Duin, Arthur van Galen		
13	Ingrid Kortland	Teamleider ICT	19-7-2018
14	Richard Harteveld, Christine Gillissen	Team Klantcontact	20-8-2018
15	Wouter Le Febre, John Vloemans	Projectleider implementatie BIG	21-8-2018
16	Koos van Bekkum	Chief Information Security Officer	23-8-2018
17	Arno van de Waesberge	Projectleider inrichting ICT-werkplekken	28-8-2018
18	Cornelis Visser	Burgemeester	30-8-2018

BIJLAGE B NORMENKADER

In het uitgevoerde onderzoek hebben wij gebruik gemaakt van een normenkader. Enkele onderzoeksvragen hebben een beschrijvend karakter. Aan dergelijke vragen is geen norm verbonden.
Voor de onderzoeksvragen die normatief van aard zijn, volgt hieronder het gehanteerde normenkader.

Gemeentelijk beleid (onderzoeksvragen 1, 2, 3, 4 en 5)
Het gemeentelijk informatiebeveiligingsbeleid voldoet tenminste aan de eisen, die in wet- en regelgeving worden gesteld, zoals vastgelegd in BIG en de AVG. In het gemeentelijk beleid wordt ingegaan op: – Juridische aspecten op basis van de AVG en de BIG. – Vertaling naar de beleidskaders informatiebeveiliging. – Organisatie, taken en verantwoordelijkheden voor de informatie- en gegevensveiligheid. – Inrichting reprocessing. – De toepassing van informatiesystemen en ICT. – De gegevens- en informatiestromen. – De positie van en communicatie met de burger. De gemeente hanteert landelijke standaarden, zoals de BIG, routering via gemeentelijke gegevensknoppunten, zoals het GGk e.d. De gemeente is bekend met de AVG, de impact daarvan en heeft een plan van aanpak voor de noodzakelijke aanpassingen, die ten behoeve van de AVG gerealiseerd moeten zijn. In de procesbeschrijvingen en instructies voor de informatiebeveiliging- en privacyprocessen is duidelijk welke functionaris welke gegevens in welke processtap mag verwerken, en onder welke condities dat mag.
Leren en verbeteren (Onderzoeksvragen 6, 7, 8, 9 en 10)
Er bestaat een controleplan voor de informatieveiligheid, waarin onder meer staat: hoe dit proces verloopt, de periodiciteit van de controles, wie daarbij betrokken zijn (functienamen, bijv. FG, CISO, etc. en persoonsnamen), wie controles uitvoert, aan wie wordt gerapporteerd, hoe de resultaten worden vastgelegd, wat de criteria zijn voor vervolgstappen, welke de vervolgstappen kunnen zijn en wie die neemt. Het controleplan sluit aan op het gemeentelijk beveiligingsplan, het privacy beleid en het Integriteitsbeleid. De medewerkers zijn bekend met het informatiebeveiligingsplan. De gemeente heeft vastgelegd hoe en wanneer medewerkers worden getraind in/er

aandacht besteed wordt aan het onderwerp digitale veiligheid. In de praktijk wordt gehandeld conform de wijze waarop de informatieveiligheid is geregeld in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties, de afspraken voor de verwerking van gegevens en de afspraken over het informeren van burgers en het vragen van toestemming. De gemeente heeft een leer- en verbetercyclus waar informatiebeveiliging een apart onderdeel van uitmaakt. De gemeente heeft een routine voor het meten en verbeteren van de informatieveiligheid en legt vast wat de bevindingen en maatregelen zijn. Deze routine is al tenminste één keer uitgevoerd.
Kaderstellende en controlerende rol van de raad (onderzoeksvragen 13 en 14)
In de bestuursrapportages, programmabegroting en programmarekening wordt expliciet aandacht besteed aan de wijze waarop de digitale veiligheid is gewaarborgd. Daaraan worden conclusies en maatregelen verbonden op basis van uitgevoerde controles. Bij de ontwikkeling van beleid heeft informatiebeveiliging en privacybeleid als punt op de agenda van de Raad gestaan.

BIJLAGE C AFKORTINGEN EN VERKLARENDE WOORDENLIJST

AFKORTINGEN

Afkorting	Betekenis
AVG	Algemene Verordening Gegevensbescherming
B&W	Burgemeester en Wethouders
BAG	Basisregistratie adressen en gebouwen
BIG	Baseline Informatiebeveiliging Nederlandse Gemeenten
BRO	Basisregistratie ondergronds
BRP	Basisregistratie personen
BSN	Burgerservicenummer
BYOD	Bring your own device
BZK	Binnenlandse Zaken en Koninkrijksrelaties
CAB	Change Advisory Board
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COD	Corporate owned Devices
ENSIA	Eenduidige Normatiek Singe Information Audit
FG	Functionaris Gegevensbescherming
GGk	Gemeentelijk Gegevensknooppunt
IB	Informatiebeveiliging
ISMS	Information Security Management System
ICT	Informatie- en Communicatietechnologie
MDM	Mobile Device Management
MT	Managementteam
P&C-cyclus	Planning en controlcyclus
PIA	Privacy Impact Assessment
TISO	Technical Information Security Officer
VNG	Vereniging Nederlandse Gemeenten

VERKLARENDE WOORDENLIJST

Technische term	Betekenis
Airwatch	Software die de gemeente Katwijk heeft gekozen voor Mobile Device management (zie onder).
Back-up & recovery	Het proces van het veilig stellen van gegevens (back-up) en herstellen van die gegevens (recovery) in het geval van een incident waarbij gegevens verloren zijn gegaan.
Black-box testing	Dit is een vorm van testen waarbij de tester geen kennis heeft van de structuur van de betrokken ICT-systemen.
e-learning	e-learing is een verzamelterm voor leermiddelen waarbij interactief gebruik wordt gemaakt van digitale middelen.
forensic readiness	Forensic readiness betreft de mogelijkheid van een organisatie om optimaal gebruik te maken van digitale middelen (email, informatie uit het zaaksysteem, etc) als valide bewijsmateriaal in juridische kwesties
Gap-analyse	Een analyse waarbij de gewenste situatie wordt afgezet tegen de huidige situatie. Het verschil is het gat (de 'gap').
Grey-box testing	Dit is een vorm van testen waarbij de tester beperkte kennis heeft van de structuur van de betrokken ICT-systemen.
Freeze	Een periode waarin geen of nauwelijks technische wijzigingen worden doorgevoerd op een informatiesysteem.
Mobile Device Management	Met behulp van MDM kan een IT-afdeling op een veilige manier apparaten toevoegen aan een bedrijfsnetwerk, zelf de instellingen verzorgen voor de draadloze verbinding en het ophalen van updates, toezien op naleving van bedrijfsregels en apparaten op afstand vergrendelen of wissen.[20]
Mystery guest	Een mystery guest is een voor de organisatie externe persoon die opzettelijk probeert (beveiligings-)maatregelen te omzeilen en die daarvoor is ingehuurd door de beveiligingsorganisatie van die organisatie.
Phishing	Een vorm van internetfraude waarbij, vaak per e-mail, een ontvanger verleid wordt op een malafide verwijzing te klikken waardoor schade kan worden toegebracht.
Planon	Software ter ondersteuning van de bedrijfsvoering van organisaties. In deze applicatie vindt o.a. gebouw- en zaalbeheer, maar tevens veelal de registratie van verschillende (soms) gebouwgebonden meldingen vanuit de organisatie

[20] Bron: www.computerworld.nl

	plaats.
single sign on	Dit is het dusdanig inrichten van de autorisatiestructuur van de ICT-omgeving zodat een gebruiker maar één keer zijn of haar inloggegevens hoeft in te voeren om toegang te krijgen tot de applicaties.
Suwinet	Suwinet is een digitale infrastructuur die is ontwikkeld door de Suwipartijen (UWV, SVB en gemeenten) om ervoor te zorgen dat zij gegevens met elkaar kunnen uitwisselen voor de uitoefening van hun wettelijke taak.[21]

[21] Bron: www.bkwi.nl

COLOFON

De rekenkamercommissie is ondersteund door:

PBLQ
Muzenstraat 120
2511 WB Den Haag

Auteurs: Peter Castenmiller
Matthijs Kerkvliet
Marieke van der Putten

T: 070 – 376 36 36

E: info@pblq.nl
I: www.pblq.nl

Onderzoeksrapport
Digitale Veiligheid in Katwijk

Rekenkamercommissie

Katwijk

Onderzoek Digitale veiligheid in Katwijk

Rekenkamercommissie Katwijk

INHOUDSOPGAVE

VOORWOORD

Voor u ligt het rapport over informatiebeveiliging bij de gemeente Katwijk, een onderzoek van de Rekenkamercommissie Katwijk dat is uitgevoerd in de tweede helft van 2018. Het betreft dan ook een momentopname van die periode. Juist in deze periode werd er volop gewerkt aan de verbetering van de informatievoorziening van de gemeente, o.a. door de uitrol van de nieuwe mobiele werkplek en de nieuwe ICT-infrastructuur.

De onderzoekers hebben ten behoeve van dit onderzoek uitvoerig gesproken met medewerkers van de ambtelijke organisatie van de gemeente Katwijk. Daarnaast hebben ze documenten bestudeerd.

De samenwerking met de medewerkers van de gemeente was prettig en de documentatie werd in bijna alle gevallen snel en zorgvuldig aangeleverd. Dit heeft een goede en prettige uitvoering van het onderzoek bevorderd.

We hebben ervaren dat de medewerkers van de gemeente Katwijk zich open en constructief hebben opgesteld en het rekenkameronderzoek zien als een steun in de rug en niet als een afrekenende controle. Wij danken daarom de medewerkers van de gemeente voor de medewerking.

1 INLEIDING

1.1 AANLEIDING

In de afgelopen jaren is de aandacht voor de beveiliging van informatie sterk toegenomen. Dat heeft verschillende oorzaken. Allerlei organisaties, waaronder natuurlijk ook gemeenten, werken steeds 'digitaler' en wisselen in dat verband intern, met andere organisaties in een keten en met burgers en ondernemingen gegevens uit. In de laatste jaren is het besef toegenomen dat gemeenten aan burgers moeten kunnen garanderen dat hun gegevens in veilige handen zijn. Gemeenten beheren uiterst gevoelige gegevens van hun inwoners. Gemeenten moeten het vertrouwen van burgers dat zij zorgvuldig omgaan met hun gegevens verdienen, zowel in de directe contacten met de burger als in verantwoordingen achteraf.

Bovendien is de regelgeving met betrekking tot de bescherming en beveiliging van persoonsgegevens aangescherpt. Dit blijkt in het bijzonder door de Algemene verordening Gegevensbescherming (AVG) die per 25 mei 2018 van toepassing is. Desalniettemin is die regelgeving nog lang niet bij alle gemeenten in het eigen beleid verwerkt, of wordt er op de werkvloer naar gehandeld. Daarmee lopen gemeenten het risico op hoge boetes in het geval zij niet conform de geldende normen de beveiliging van persoonsgegevens op orde hebben.

Er zijn meer redenen dat de aandacht voor informatieveiligheid is toegenomen. Nadat digitalisering, en de daarmee gepaard gaande opkomst van het internet aanvankelijk louter positief werden ervaren, is de laatste jaren het besef toegenomen dat deze ontwikkelingen ook hun schaduwkanten hebben. Gegevens kunnen worden gehackt en misbruikt. In sommige situaties zijn essentiële persoonsgegevens misbruikt om identiteitsfraude mogelijk te maken.

In dit licht heeft de rekenkamercommissie van de gemeente Katwijk besloten een onderzoek te verrichten naar de wijze waarop de gemeente Katwijk invulling geeft aan digitale veiligheid.

1.2 Opdrachtformulering

Ten behoeve van het onderzoek is de volgende onderzoeksvraag geformuleerd:

> *In hoeverre heeft de gemeente Katwijk de informatiebeveiliging van de informatiesystemen in de organisatie doeltreffend ingericht, waarmee risico's worden afgedicht, waardoor geen oneigenlijke toegang tot de gevoelige informatie (zoals persoonsgegevens) kan worden verkregen, informatie in verkeerde handen kan vallen en/of vitale systemen in werking of uit kunnen worden gezet?*

Wij hebben deze onderzoeksvraag geoperationaliseerd door middel van het formuleren van een aantal deelvragen. Hieronder volgen de deelvragen.

1.3 Deelvragen

1. Welke beleidskaders[1], regels en richtlijnen hanteert de gemeente voor de borging van de informatiebeveiliging?
2. Voldoet het beleid en de uitwerking in processen binnen de gemeente aan de bepalingen van het basisnormkader Baseline Informatiebeveiliging Gemeenten (BIG) en aan de Algemene verordening gegevensbescherming (AVG[2], die per 25 mei 2018 van toepassing is)?
3. Welke functionarissen zijn verantwoordelijk gesteld voor de informatiebeveiliging binnen de gemeente?
4. Welke Mobile Device Management (MDM) oplossing heeft de gemeente Katwijk gekozen en op welke wijze wordt met behulp van de MDM een optimale beveiliging van de mobiele devices ingericht?
5. Hoe is de operationalisatie en implementatie van de BIG tot nu toe verlopen?
6. Hoe is dit beleid uitgewerkt en geborgd in processen op de werkvloer?
7. Hoe worden medewerkers betrokken bij en getraind in het borgen van het informatiebeveiligingsbeleid en het privacy beleid?
8. Hoe geeft de gemeente Katwijk invulling aan het testbeleid en de auditing op de digitale veiligheid?
9. Op welke wijze worden de ICT-voorzieningen (waaronder de infrastructuur, de wifi, de volledige werkplek, de website en digitale dienstverlening) van de gemeente Katwijk getest op informatiebeveiliging, met welke frequentie en met welke resultaten?

[1] Naast het vastgestelde en onlangs geactualiseerde privacybeleid en informatiebeveiligingsplan van de gemeente Katwijk.
[2] Omdat de AVG per 25 mei 2018 van kracht is geworden en de WBP per die datum niet meer van kracht is, zullen wij in dit rekenkameronderzoek de AVG als wettelijk kader hanteren.

10. Welke mogelijke risico's zijn te onderkennen in de huidige wijze waarop het privacy- en informatiebeveiligingsbeleid is ingericht en functioneert?
11. Hoe ziet de gemeente erop toe dat het informatiebeveiligingsbeleid van een voldoende niveau is en blijft en wordt er geanticipeerd op toekomstige opgaven?
12. Welke beveiligingsincidenten heeft de gemeente Katwijk de afgelopen twee jaren ondervonden en hoe zijn deze afgewikkeld?

De door ons toegevoegde aandacht voor de positie van de raad heeft geleid tot de volgende twee onderzoeksvragen:

1.4 Deelvragen positie gemeenteraad

13. Op welke wijze is de raad tot nu toe bij de ontwikkeling van de informatieveiligheid betrokken geweest?
14. Op welke manier kan de gemeenteraad het beleid rondom informatieveiligheid controleren en sturen?

Om deze deelvragen, en daarmee ook de onderzoeksvraag te kunnen beantwoorden hebben wij een aantal thema's belicht. Dit zijn de volgende thema's:

1.5 Onderzoeksthema's

Governance

Dit aspect betreft het toetsen van de opzet, het bestaan en de werking van de governance van de gemeente Katwijk omtrent informatiebeveiliging. Het betreft hier minimaal de volgende wettelijke bepalingen:

- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
- Algemene verordening persoonsgegevens (AVG) [3] en/of gemaakte afspraken, bijvoorbeeld in VNG-verband.

Techniek

Dit aspect betreft het testen van de ICT-infrastructuur van de gemeente Katwijk. Deze dient te worden getest op kwetsbaarheden waarmee kwaadwillenden onrechtmatig over bedrijfsgevoelige gegevens, gegevens van burgers zouden kunnen beschikken en/of infrastructuur in werking kunnen stellen of afzetten waardoor maatschappelijke en/ of

[3] Omdat de AVG per 25 mei 2018 van kracht is geworden en de WBP per die datum niet meer van kracht is, zullen wij in dit rekenkameronderzoek de AVG als wettelijk kader hanteren. In de opdracht van de rekenkamercommissie werd de Wet Bescherming Persoonsgegevens uiteraard ook nog genoemd als relevante wettelijke bepaling. De onderzoeksopdracht is voor 25 mei 2018 verstrekt.

financiële schade kan ontstaan. Hierbij dient te worden gedacht aan: black box test, grey box test, monitoring en signalering, forensic readiness[4].

Mens

Bewustwording is een belangrijk onderdeel bij informatiebeveiliging. Onderzocht dient te worden in hoeverre medewerkers van de gemeente zich bewust zijn van informatiebeveiliging en dan met name wat er op dat gebied van hen verwacht moet worden. Te denken valt hierbij aan Phishing e-mails, inlooptests, achterlaten USB-sticks.

In het kader van het onderzoek is eveneens een normenkader opgesteld. Dit normenkader is opgenomen in bijlage B.

Werkwijze

- Na een gezamenlijke kick-off met de leden van de Rekenkamercommissie hebben de onderzoekers van PBLQ het onderzoek in uitvoering genomen.
- De eerste stap was het bestuderen van de opzet van het informatiebeveiligingsbeleid. Dit hebben de onderzoekers gedaan aan de hand van een documentstudie.
- Vervolgens hebben de onderzoekers met tweeëntwintig medewerkers van de gemeente Katwijk gesproken om vast te kunnen stellen of het beleid zoals het op papier bestaat en de maatregelen, die zijn getroffen ook in de praktijk bekend zijn en ook werken.
- Vervolgens hebben de onderzoekers de eerste bevindingen geformuleerd en deze in een convergentiebijeenkomst met een deel van de geïnterviewde medewerkers van de gemeente doorgenomen.
- Tenslotte hebben de onderzoekers hun bevindingen geanalyseerd en verwerkt in voorliggende rapportage.

1.6 LEESWIJZER

In het tweede hoofdstuk is de aandacht geconcentreerd op de opzet van het gemeentelijk informatiebeveiligingsbeleid en de informatiebeveiligingsmaatregelen. Eveneens komt in het tweede hoofdstuk aan de orde de wijze waarop de raad over het beleid wordt geïnformeerd.
De volgende deelvragen worden in hoofdstuk twee beantwoord:

1. Welke beleidskaders, regels en richtlijnen hanteert de gemeente voor de borging

[4] Forensic readiness betreft de mogelijkheid van een organisatie om optimaal gebruik te maken van digitale middelen (email, informatie uit het zaaksysteem, etc) als valide bewijsmateriaal in juridische kwesties.

van de informatiebeveiliging?
2. Voldoet het beleid en de uitwerking in processen binnen de gemeente aan de bepalingen van het basisnormkader (BIG) en aan de Algemene verordening gegevensbescherming (AVG, die per 25 mei van toepassing is)?
3. Welke functionarissen zijn verantwoordelijk gesteld voor de informatiebeveiliging binnen de gemeente?
4. Welke Mobile Device Management (MDM) oplossing heeft de gemeente Katwijk gekozen en op welke wijze wordt met behulp van de MDM een optimale beveiliging van de mobiele devices ingericht?

In het derde hoofdstuk staat centraal in welke mate het beleid en de informatiebeveiligingsmaatregelen ook in de praktijk aanwezig zijn en werken. In hoofdstuk drie worden de volgende deelvragen beantwoord:

5. Hoe is de operationalisatie en implementatie van de BIG tot nu toe verlopen?
6. Hoe is dit beleid uitgewerkt en geborgd in processen op de werkvloer?
7. Hoe worden medewerkers betrokken bij en getraind in het borgen van het informatiebeveiligingsbeleid en het privacy beleid?
8. Hoe geeft de gemeente Katwijk invulling aan het testbeleid en de auditing op de digitale veiligheid?
9. Op welke wijze worden de ICT-voorzieningen (waaronder de infrastructuur, de wifi, de volledige werkplek, de website en digitale dienstverlening) van de gemeente Katwijk getest op informatiebeveiliging, met welke frequentie en met welke resultaten?
10. Welke mogelijke risico's zijn te onderkennen in de huidige wijze waarop het privacy- en informatiebeveiligingsbeleid is ingericht en functioneert?
11. Hoe ziet de gemeente erop toe dat het informatiebeveiligingsbeleid van een voldoende niveau is en blijft en wordt er geanticipeerd op toekomstige opgaven?
12. Welke beveiligingsincidenten heeft de gemeente Katwijk de afgelopen twee jaren ondervonden en hoe zijn deze afgewikkeld?

Het vierde hoofdstuk bevat de beantwoording van de onderzoeksvragen met betrekking tot de positie van de gemeenteraad. Dat betreft de volgende twee deelvragen:

13. Op welke wijze is de raad tot nu toe bij de ontwikkeling van de informatieveiligheid betrokken geweest?
14. Op welke manier kan de gemeenteraad het beleid rondom informatieveiligheid controleren en sturen?

Aansluitend worden in hoofdstuk 5 de conclusies en aanbevelingen weergegeven.

2 OPZET EN BESTAAN VAN INFORMATIEBEVEILIGINGSBELEID

2.1 INLEIDING

In dit hoofdstuk beschrijven wij de wijze waarop de gemeente Katwijk haar beleid op het gebied van informatiebeveiliging en privacy heeft vormgegeven. Tevens gaan wij in op de ambities om verbeteringen aan te brengen. De mate waarin het beleid ook werkt en of die ambities ook worden waargemaakt, komen in het volgende hoofdstuk aan de orde. Daarmee zijn de volgende deelvragen in dit hoofdstuk aan de orde.

1. Welke beleidskaders, regels en richtlijnen hanteert de gemeente voor de borging van de informatiebeveiliging?

2. Voldoet het beleid en de uitwerking in processen binnen de gemeente aan de bepalingen van het basisnormkader BIG en aan de Algemene verordening gegevensbescherming (AVG, die per 25 mei van toepassing is)?

2.2 AANWEZIGHEID VAN INFORMATIEBEVEILIGINGSBELEID

De gemeente Katwijk heeft een strategisch informatiebeveiligingsbeleid dat op 9 mei 2017 door het College B&W is vastgesteld[5]. Het strategisch beleid betreft een beleidskader waarin wordt beschreven waarom informatiebeveiliging van belang is. Het bevat negen regels die specifieke handvatten voor een veilige omgang met informatie bieden.

In het tactisch informatiebeveiligingsbeleid staat beschreven wat er precies aan maatregelen dient te worden genomen[6]. Dit beleidsstuk is op 17 mei 2017 door het College B&W vastgesteld. De maatregelen die staan beschreven in het tactisch

[5] Strategisch informatiebeveiligingsbeleid, gemeente Katwijk, versie DEFINITIEF. d.d. 9 mei 2017.
[6] Tactisch informatiebeveiligingsbeleid, gemeente Katwijk, versie DEFINITIEF. d.d. 17 mei 2017.

informatiebeveiligingsbeleid zijn ontleend aan de BIG[7] en toegespitst op de organisatorische situatie van de gemeente Katwijk.

In januari 2018 is het informatiebeveiligingsplan voor 2018 door het College B&W vastgesteld[8]. Dit plan beschrijft welke informatiebeveiligingsactiviteiten in 2018 zullen worden opgepakt. Het betreft activiteiten die eraan moeten bijdragen dat de gemeente Katwijk voldoet aan de BIG, aangevuld met maatregelen die uit een langetermijnplanning komen; de GAP-analyse. Ook dient als input voor het informatiebeveiligingsplan:

- Verbeteracties die volgen uit incidenten (Datalekken, beveiligingsincident);
- Verbeteracties die volgen uit audits (ENSIA);
- Verbeteracties die volgen uit anderszins gesignaleerde risico's.

De Chief Information Security Officer (CISO) rapporteert over de voortgang van het informatiebeveiligingsplan aan de directie. Daarnaast is in 2017 een Information Security Management System (ISMS) geïmplementeerd waarmee de status van de informatiebeveiligingsactiviteiten kan worden bepaald en gevolgd. De controle op de voortgang van de implementatie van de BIG-maatregelen en de kwaliteit van de informatiebeveiliging wordt met behulp van het ISMS ondersteund. De gemeenteraad wordt eveneens geïnformeerd over de voortgang van informatiebeveiliging en privacy. Dat gebeurt door middel van alinea's in de jaarrapportages en de gemeentelijke begroting.

2.3 Organisatie van informatiebeveiliging

3. Welke functionarissen zijn verantwoordelijk gesteld voor de informatiebeveiliging binnen de gemeente?

2.3.1 Functionarissen op het gebied van informatiebeveiliging en privacy

Centrale dragende functionarissen zoals de CISO, TISO (Technical Information Security Officer) en de Functionaris Gegevensbescherming (FG) zijn benoemd. De CISO en FG zijn, net als de Chief Information Officer (CIO) strategische functionarissen waarbij de

[7] De BIG is sinds 2012 in ontwikkeling in opdracht van de Minister van BZK en heeft als doel om: 1. Gemeenten op een vergelijkbare manier efficiënt te laten werken met informatiebeveiliging. 2. Gemeenten een hulpmiddel te geven om aan alle eisen op het gebied van Informatiebeveiliging te kunnen voldoen. 3. De auditlast bij gemeenten te verminderen. 4. Gemeenten een aantoonbaar betrouwbare partner te laten zijn.
[8] Informatiebeveiligingsplan 2018, gemeente Katwijk, versie DEFINITIEF. d.d. januari 2018.

onafhankelijkheid ten opzichte van de ambtelijke organisatie belangrijk is. De verantwoordelijkheidsverdeling voor de informatiebeveiliging is vormgegeven conform de BIG en de AVG. Uit gesprekken is naar voren gekomen dat deze functionarissen daarom binnen de concernstaf zijn gepositioneerd. Deze functionarissen en de wijze waarop zij organisatorisch zijn opgehangen worden wel beschreven in de aanstellingsbesluiten van de FG en CISO, maar vooralsnog niet in het informatiebeveiligingsbeleid. . Dat wordt wel voorgeschreven in de strategische BIG. De taken en verantwoordelijkheden van de CISO en FG zijn omschreven in hun afzonderlijke functieomschrijvingen. De CISO en FG rapporteren direct aan het College en de gemeenteraad van de gemeente Katwijk middels tertaalrapportages, de ENSIA en de jaarlijkse verklaring privacy en informatiebeveiliging – de *declaration of accountability* Wij hebben deze rapportages aan het College en MT niet ingezien. Wel hebben wij enkele rapportages ingezien over de voortgang BIG-implementatie van 2017.[9]

De FG en CISO zijn in positie. Dat wil zeggen, veel ambtenaren weten wat de verantwoordelijkheden van de FG en CISO zijn en weten hen te vinden bij informatiebeveiligingsincidenten of privacyvraagstukken. De TISO is per 1 april 2018 benoemd en maakt onderdeel uit van het team ICT. De introductie van de nieuwe rol van TISO heeft als doel om de verbinding te maken tussen het beleid en de kaders van de informatiebeveiliging en de techniek van ICT. De TISO staat tussen de CISO en de IT-specialisten van team ICT in. De TISO stuurt op de tactische en operationele invulling van het informatiebeveiligingsbeleid. Omdat de huidige TISO tevens changemanager is, is met het combineren van deze twee rollen door één persoon tevens geborgd dat de informatiebeveiligingsaspecten bij alle voorgestelde wijzigingen in het Change Advisory Board (CAB) besproken worden. De TISO is nog kort in zijn nieuwe rol en is zijn positie aan het verkennen en opbouwen.

Bij veel uitvoerende teams van de afdelingen Samenleving en Ruimte & Veiligheid wordt informatiebeveiliging en gegevensbescherming, meer dan bij andere uitvoerende afdelingen, nog gezien als iets extra´s dat zij naast al hun reguliere werk nog moeten doen. Binnen deze afdelingen is het nog geen gemeengoed dat gegevensbescherming en informatiebeveiliging onderdeel uitmaken van het reguliere werk: hier is het nog niet volledig geaccepteerd. Informatiebeveiliging en privacy zijn daarmee nog onvoldoende geborgd binnen deze twee afdelingen van de gemeentelijke organisatie. Bij de andere afdelingen is dat wel het geval en wordt informatiebeveiliging en privacy wél meer gezien als onderdeel van het reguliere werk.

[9] Dit betreffen drie tertaalrapportages die gericht zijn aan de concerncontroller.

2.3.2 Overleg over informatiebeveiliging en privacy

Er zijn drie verschillende overleggen voor informatiebeveiliging en privacy, de werkgroep informatiebeveiliging, het incidentele kernteam datalekken en de recent gestarte Security Board.

Bij alle overleggen op het gebied van informatiebeveiliging, wordt de FG eveneens betrokken. Hiermee wordt de afstemming tussen informatiebeveiliging en gegevensbescherming ingevuld. Er is een werkgroep informatiebeveiliging. Hierin nemen de TISO, CISO , concernadviseur informatiehuishouding, de externe projectleiders implementatie BIG, en één van de informatiespecialisten deel. Elke woensdag vindt prioriteitenstelling plaats en schuift ook de CIO aan bij deze werkgroep. Wat vervolgens met die prioritering gebeurt hebben wij in dit onderzoek niet vastgesteld.

Ook heeft de gemeente Katwijk plannen om een Security Board in te stellen. Het doel van de Security Board is om naast de lopende zaken ook meer strategische vragen met betrekking tot informatiebeveiliging te bespreken met alle directbetrokkenen. Een eerste security board heeft in september 2018 plaatsgevonden.

Op het gebied van datalekken heeft de gemeente Katwijk een kernteam datalekken dat bestaat uit het Hoofd Concernstaf, de FG, de melder van het datalek, het afdelingshoofd/manager van de melder van het datalek, de Concerncontroller en de CIO. Op het moment dat er een datalek is geconstateerd wordt in het kernteam besproken óf het een datalek is, of het een meldingswaardig datalek betreft en dan kan vervolgens het protocol in werking treden.

2.4 Vormgeving van beleid en maatregelen

2.4.1 Privacy beleid

De gemeente heeft zich goed voorbereid op de AVG. Dit leidde er toe dat de gemeente in mei 2018 bij het van kracht worden van de AVG grotendeels voldeed aan de eisen die de AVG stelt. Zo was het verwerkingenregister grotendeels gereed en gevuld maar was er nog geen sprake van een 100% dekking. Wel waren per 25 mei de baselinetoetsen op alle afdelingen afgerond. Op 11 juli 2017 heeft het College B&W het algemeen privacy beleid Katwijk 2.0 vastgesteld. In dat beleid is opgenomen dat ter voorbereiding op de AVG het privacy beleid elk jaar geaudit zal worden. Wij hebben niet kunnen vaststellen dat er al een eerste volledige afzonderlijke audit op het privacy beleid heeft plaatsgevonden. Wel hebben op verschillende momenten evaluaties van delen van het privacy beleid

plaatsgevonden. Bijvoorbeeld bij de evaluatie van de privacy governance en bij het opstellen van de verklaring van accountability (september 2018). Ook in de ENSIA is privacy geëvalueerd.

Het privacy beleid beschrijft ook een aantal volwassenheidsniveaus voor de omgang met persoonsgegevens. Op 22 september 2018 heeft het College voor de gemeente vastgesteld op welk volwassenheidsniveau de verschillende diensten van de gemeente zich bevinden. Het College heeft zich tevens voorgenomen om per eind 2018 gemeentebreed op het volwassenheidsniveau 3 of 4 te zitten en per eind 2019 op niveau 5. De betreffende volwassenheidsniveaus luiden als volgt:

Niveau 0: De verantwoordelijke heeft erkend dat hij maatregelen wil gaan nemen en daartoe de eerste initiatieven ontplooid.

Niveau 1: Er is een besef omtrent gegevensbescherming. Op hoofdlijnen zijn de grenzen van verantwoordelijkheid en aansprakelijkheid in kaart gebracht en er is een FG aangesteld. Het proces van verinnerlijken is gaande.

Niveau 2: Op systematische wijze zijn de verwerkingen van persoonsgegevens in kaart gebracht. Wijzigingen worden adequaat beheerd. Onderzoeken worden gepland en uitgevoerd. De uitkomsten worden gerelateerd aan het overzicht en inzicht in de verwerkingen.

Niveau 3: Inzicht en overzicht in de verantwoordelijkheden en aansprakelijkheden alsmede in de verwerkingen en de compliance wordt uitgebreid naar de bewerkers. Er zijn duidelijke en transparante afspraken tussen verantwoordelijke en bewerkers en tussen bewerkers onderling gemaakt. Er is een basis gelegd voor het voorkomen van bestuurlijke en civielrechtelijke procedures.

Niveau 4: Actieve en passieve rechten van de betrokkene worden gefaciliteerd. De organisatie (verantwoordelijke of bewerker) kan zich hierover maatschappelijk verantwoorden.

Niveau 5: De betrokkene (klant, medewerker of individu) is “in control” over zijn/ haar persoonsgegevens. De organisatie (verantwoordelijke of bewerker) heeft de voorwaarden voor eerlijk zaken doen gecreëerd en houdt die ook in stand.

Niveau 6: Gegevensbeschermingen privacy zijn “ingebouwd” in de organisatie. Niet alleen in de informatiesystemen maar ook in de administratieve organisatie en het handelen van medewerkers, leveranciers en klanten. De werking van de getroffen maatregelen en mechanismen kan getoond worden. De organisatie is “accountable”. De organisatie heeft gegevensbescherming zodanig verankerd in de bedrijfsvoering dat

gegevensbescherming onderdeel is geworden van het risicomanagement dat een verplicht onderdeel is van de jaarrekening.

Niveau 7: Er is sprake van een heldere beslissingsstructuur voor beleid en aanpak voor gegevensbescherming en privacy als onderdeel van het in standhouden van een verantwoorde bedrijfshuishouding.

Op dit moment zit de gemeente Katwijk tussen niveau 1 en niveau 2 in. Het meest realistische scenario is dat per eind 2018 niveau 2 overal van toepassing is, waarbij enkele afdelingen zoals bijvoorbeeld Burgerzaken stijgt hier vanwege de al jarenlange ervaring met het zorgvuldig omgaan met persoonsgegevens in kwartaal 3 van 2018 al bovenuit. Daarna kan een begin met niveau 3 is gemaakt[10].

2.4.2 Plaats onafhankelijk werken en Mobile Device Management

4. Welke Mobile Device Management (MDM) oplossing heeft de gemeente Katwijk gekozen en op welke wijze wordt met behulp van de MDM een optimale beveiliging van de mobiele devices ingericht?

De gemeente Katwijk werkt ten tijde van het onderzoek aan de overgang richting een nieuwe werkplekomgeving die de medewerkers van de gemeente in staat stelt om plaats onafhankelijk te werken. Ten behoeve van dit plaats onafhankelijk werken heeft de gemeente een beleid[11] opgesteld waarin verschillende informatiebeveiligingsaspecten worden voorgeschreven. Dit beleid is op 24 januari 2018 geagendeerd voor besluitvorming binnen het Management Team van de gemeente Katwijk.

Voor plaats onafhankelijk werken maakt de gemeente Katwijk gebruik van devices, die eigendom zijn van de gemeente (Corporate owned Devices: COD) maar ook kunnen medewerkers eigen devices gebruiken voor hun werk (Bring your own device: BYOD) mits deze voldoen aan de eisen, die de gemeente daaraan stelt. Zo dienen alle devices, dus laptops, smartphones en tablets te zijn voorzien van de door Katwijk gekozen Mobile Device Management (MDM) software Airwatch. Door het in gebruik nemen van het nieuwe Mobile Device Management worden de o.a. (de informatiebeveiligings-)eisen, die gesteld worden aan zowel de COD als de BYOD ingeregeld. Ook voor MDM heeft de gemeente Katwijk beleid[12] geformuleerd dat op 24 januari 2018 binnen het Management Team van Katwijk is geagendeerd voor besluitvorming.

Binnen dit onderzoek hebben we alleen kunnen vaststellen dat de beleidsstukken aanwezig zijn en dat deze relevante inhoud bevatten. Of het beleid daadwerkelijk ook

[10] Totaaloverzicht acties privacy, versie 11 juni 2018
[11] Beleid plaats onafhankelijk werken, versie 2018.03
[12] Mobile Device Management, gemeente Katwijk, versie 1.2. d.d. 19-3-2018

werkt in de praktijk hebben wij niet kunnen vaststellen aangezien de implementatie van de nieuwe netwerkomgeving en het in gebruiknemen van het Mobile Device Management in september 2018 van start is gegaan. Het evalueren van het Mobile Device Beleid in de praktijk is op zijn vroegst een half jaar tot een jaar na de implementatie zinvol. Oorspronkelijk was deze implementatie gepland in het tweede kwartaal 2018.

3 INFORMATIEBEVEILIGINGSBELEID IN DE PRAKTIJK

3.1 INLEIDING

De gemeente Katwijk heeft een duidelijk en actueel informatiebeveiligingsbeleid en een separaat privacy beleid, zoals in het vorige hoofdstuk beschreven. In dit hoofdstuk wordt naast het beleid ook beschreven hoe dit beleid in de praktijk van alledag invulling krijgt. Geeft het beleid ook handelingsperspectief aan de praktijk of is het beleid eerder een theoretische exercitie, die mogelijk ver af staat van het dagelijkse werk van de gemiddelde ambtenaar van de gemeente Katwijk. In dit hoofdstuk ligt de focus op deze dagelijkse praktijk. In dit hoofdstuk staan dan de volgende vragen centraal:

5. Hoe is de operationalisatie en implementatie van de BIG tot nu toe verlopen?
6. Hoe is dit beleid uitgewerkt en geborgd in processen op de werkvloer?

3.2 IMPLEMENTATIE VAN DE BIG

De uitvoering van de BIG vindt in 2018 nog volop plaats onder regie van de CISO en met behulp van twee externe projectleiders. De uitvoering van de BIG is in 2015 gestart met een inventarisatie van de situatie op dat moment in vergelijking met de toekomstig gewenste situatie. De verschillen tussen de aangetroffen situatie en de gewenste, toekomstige situatie worden in deze inventarisatie inzichtelijk gemaakt, dit betreft een zogenaamde GAP-analyse. Op basis van deze inventariserende analyse is door de adviseur informatieveiligheid[13] en de concernadviseur informatie een aanpak gemaakt om de BIG binnen de gemeente Katwijk te implementeren.

In september 2017 zijn voor de implementatie van de BIG twee externe projectleiders aangesteld om versneld acht tot tien maatregelen in te voeren, zoals bijv. het wachtwoordenbeleid of het sneller op slot gaan van het beeldscherm. De reden hiertoe is

[13] De CISO was op het moment van de GAP-analyse nog niet benoemd als CISO, maar was op dat moment nog adviseur informatieveiligheid. De CISO is formeel benoemd per 1 februari 2018. Voor de leesbaarheid van dit rapport en omdat het dezelfde persoon betreft gebruiken we in deze rapportage verder uitsluitend de titel CISO.

dat het werkplekproject op dat moment veel capaciteit vroeg van team ICT en met extra externe capaciteit de BIG implementatie versneld kon worden.

Een vervolgopdracht voor de twee externe projectleiders volgde begin 2018. Deze opdracht luidt dat 75% van de BIG-maatregelen voor eind 2018 geïmplementeerd moeten zijn. Wij hebben kennis genomen van deze vervolgopdracht en we hebben daarin niet kunnen vaststellen in hoeverre de in de opdracht omschreven aanpak aansluit op de uitgevoerde GAP-analyse.
Per januari 2018 was 38% van de maatregelen al ingevoerd. De gemeente Katwijk, had, ook in vergelijking met andere gemeenten, begin 2018 hiermee nog een forse implementatieopgave. Dat betekende dat nu met deze nieuwe opdracht en aanpak in 2018 aanvullend nog 37% van de BIG-maatregelen uitgevoerd moest worden. Inmiddels is de huidige stand van zaken (per 19/9/2018) dat 76% van de BIG-maatregelen is doorgevoerd.

Vervolgens heeft een korte inventarisatie plaatsgevonden en is in afstemming met de CISO een selectie van te nemen maatregelen gemaakt. Bij deze selectie is rekening gehouden met de uitrol van de nieuwe werkplek en ICT-infrastructuur in 2018 en de daardoor beperkte mogelijkheden om nog naast het werkplekproject aanvullende andere maatregelen door te voeren. Binnen de gemeentelijke organisatie is gedurende het vernieuwingsproject voor de werkplek en infrastructuur een zogenaamde “freeze” afgekondigd. Dat is een maatregel, die getroffen wordt om niet teveel technische maatregelen tegelijk uit te voeren. Dat betekent dat alleen wettelijk noodzakelijke en hoog prioritaire technische maatregelen doorgang kunnen vinden gedurende de “freeze” periode. Dat betekent dat een aantal maatregelen ingevoerd kon worden met de uitrol van de nieuwe werkplek en ICT-omgeving. Het vernieuwingsproject leidt tot een verbetering van het gebruikersgemak, door o.a. de invoering van single sign on, dat betreft het eenmalig inloggen op je pc op meerdere applicaties, en tevens tot een verbetering van de informatiebeveiliging. De uitrol van het vernieuwingsproject is twee keer uitgesteld. Inmiddels is de gefaseerde uitrol van de nieuwe werkplek eind september van start te gaan. Hiermee stond per september 2018 de weg open om in relatief korte periode een aantal al enige tijd voorbereide BIG-maatregelen, zoals het gewijzigde autorisatiebeleid, daadwerkelijk in te vullen en uit te rollen.

De selectie BIG-maatregelen voor 2018 betreft een aantal maatregelen met hoge prioriteit, zoals o.a. de back-up & recovery procedure en het Mobile Device Management. De back-up & recovery procedure betreft een procedure waarbij meestal de ICT-specialisten van een organisatie ervoor zorgen dat de data extra opgeslagen worden, zodat in geval van een verstoring in een applicatie, de ICT-specialisten deze data kunnen

terughalen en de medewerkers van de organisatie verder kunnen werken met deze extra opgeslagen data.

Mobile Device Management betreft een oplossing waarbij de IT-specialisten alle bij een organisatie in gebruik zijnde mobiele apparaten op afstand kan instellen en beheren. Mobile Device Management biedt veel extra mogelijkheden om de mobiele apparaten beter te beveiligen. Zo kan een laptop in geval van diefstal met Mobil Device Management bijvoorbeeld op afstand volledig leeggemaakt worden op het moment dat die verbonden is met het internet. Op die manier is het mobiele apparaat weliswaar verdwenen, maar kunnen geen (mogelijk) gevoelige data of informatie buit worden gemaakt. Doordat het Mobile Device Management ingezet wordt op alle mobiele devices, die medewerkers van de gemeente gebruiken voor hun werk, (zowel de COD als de BYOD), worden hiermee de informatiebeveiligingseisen op mobiele devices uitgerold.

Aanvullende informatiebeveiligingsmaatregelen

Vanuit de Suwinet, de BAG, BRP zijn specifieke wettelijke eisen (buiten de AVG) met betrekking tot de bescherming van persoonsgegevens ingesteld. Bij de gemeente Katwijk zijn deze eisen conform bepalingen in de specifieke wetgeving in de praktijk ook ingevuld. Dat blijkt onder andere uit de inrichting van de processen rondom Suwinet. De applicatiebeheerder, die verantwoordelijk is voor bijv. Suwinet, is tevens verantwoordelijk voor het doorvoeren van de informatiebeveiligingsmaatregelen op Suwinet. De informatiebeveiligingsmaatregelen voor specifieke applicaties maken onderdeel uit van de ENSIA-verantwoordingssystematiek en maken tevens onderdeel uit van het informatiebeveiligingsbeleid van de gemeente Katwijk. De CISO is tevens security-officer en eindverantwoordelijk voor de informatiebeveiliging op Suwinet. De applicatiebeheerder Suwinet geeft hier in de dagelijkse praktijk invulling aan. De CISO en de applicatiebeheerder Suwinet hebben minimaal tweejaarlijks (o.a. aan de hand van de ENSIA) contact over de te nemen aanvullende maatregelen en welke aanpassingen dit behoeft in het integrale informatiebeveiligingsplan.

In de praktijk betekenen de informatiebeveiligingsmaatregelen bijvoorbeeld dat medewerkers alleen die gegevens kunnen inzien, waartoe zij gemachtigd oftewel geautoriseerd zijn. Voorheen was dit minder stringent ingesteld, maar ook de specifieke wetgeving en eisen omtrent Suwinet, BAG, BRP en BRO worden strenger.
Indien een medewerker van bijvoorbeeld Samenleven nu een client wil opzoeken op basis van een burgerservicenummer (BSN) en dat buiten zijn of haar reguliere autorisatie valt, wordt dit eerst voorgelegd aan de interne controleur, d.w.z. of er voldoende noodzaak is om deze gegevens in te zien en gebruiken. Pas daarna krijgt de medewerker mogelijk toegang. Dat wordt door verschillende medewerkers als

vertragend in het helpen van de desbetreffende cliënten ervaren. Hiermee wordt wel voldaan aan de informatiebeveiligingsmaatregelen.

3.3 BEWUSTWORDING BINNEN DE ORGANISATIE

7. Hoe worden medewerkers betrokken bij en getraind in het borgen van het informatiebeveiligingsbeleid en het privacy beleid?

De bewustwording op het gebied van informatiebeveiliging en privacy is gestart met een presentatie in de gemeenteraad van juni 2016. Hierbij werden de adviseur concernstaf en de CISO ondersteund door een externe expert. De gemeenteraad is zich door deze sessie bewust geworden van de grote verantwoordelijkheid die de gemeente heeft en heeft vervolgens budget vrijgemaakt voor het opstellen van het informatiebeveiligings- en privacy beleid en het aanstellen van een FG en een CISO.

Deze eerste bewustwordingssessie leidde tot een beleid en een vervolgaanpak. De bewustwordingscampagne bestond uit een presentatie per afdeling (in totaal 31 presentaties) over informatiebeveiliging (o.a. de BIG, ENSIA) en privacy. De CISO en FG hebben deze presentaties samen gegeven. De presentatie werd afgestemd op de specifieke afdeling. Dat wil zeggen dat er een aantal voorbeelden van processen werden opgenomen die relevant zijn voor de betreffende afdeling. Daarnaast zijn er posters en flyers over informatiebeveiliging en gegevensbescherming verspreid in het gemeentehuis.
Naast de bewustwordingscampagne is door de gemeente eveneens een e-learning module aangeschaft. Deze e-learning module (van twee maal zes modules) biedt een online opleiding aan alle medewerkers van de gemeente. Na het volgen van de opleiding wordt elke module afgesloten met een examen. Alle vaste medewerkers van de gemeente Katwijk worden geacht dit examen voor het einde van het jaar gehaald te hebben. In september 2018 zijn er inmiddels al voor vierhonderdzestig medewerkers accounts aangemaakt, terwijl het aantal vaste fte driehonderd bedraagt. Hieruit blijkt dat er ook veel tijdelijke medewerkers door managers worden aangemeld om de e-learning te volgen en het examen af te leggen. De CISO monitort de voortgang op de e-learning examens en informeert de verantwoordelijke managers over de voortgang.
Per 1 november 2018 zijn 56 van de examens voor informatiebeveiliging afgelegd en 47% van de examens voor de gegevensbescherming succesvol afgerond. Vooralsnog zijn geen dwingende sancties bepaald voor het niet-halen van het examen voor eind 2018.

In november 2017 heeft in het kader van de bewustwordingscampagne eveneens een Katwijkse privacy week plaatsgevonden. Het programma bestond o.a. uit een algemene presentatie, een film, een lezing van Maria Genova, een quiz en een inloopspreekuur.

Deze bewustzijnscampagne en de e-learning hebben voor een brede bewustwording gezorgd. Het proces om dit bewustzijn in de dagelijkse werkzaamheden en processen per team vorm te geven vindt nu plaats. Er is vanaf 20 september 2018 een informatiebeveiliging- en privacy spreekuur gestart elke 3e donderdag van de maand. Hier kunnen medewerkers van de gemeente terecht met hun vragen op het gebied van informatiebeveiliging en privacy. Op de kennisbank (intranet) staat alle relevante informatie over zorgvuldig omgaan met gegevensbescherming en informatiebeveiliging voor de medewerkers van de gemeente.

Uit de interviews komt naar voren dat vrijwel alle medewerkers weten wie de ambtelijke verantwoordelijkheid hebben binnen de gemeente voor informatiebeveiliging en privacy, nl. de CISO en FG. De rol van de TISO is nog minder goed bekend bij de verschillende medewerkers. Uit de gesprekken komt eveneens naar voren dat de medewerkers weten dat er een procedure is voor datalekken binnen de gemeente. En dat ze een melding kunnen doen via een e-mail aan een specifiek mailadres. Veel medewerkers weten niet hoe het proces na de melding van het datalek verloopt. Dat hoeft echter geen belemmering te zijn om een datalek te herkennen en hierna adequaat te handelen. De direct betrokkenen bij het datalek-proces hebben wel helder voor ogen wie hierbij betrokken dienen te zijn en welke verschillende stappen doorlopen worden voor de afhandeling conform het proces.

Het proces is als volgt: vervolgens komt de CISO in actie en zoekt direct contact met de onlangs aangestelde TISO. De CISO en TISO nemen soms direct een actie om verdere verspreiding te voorkomen en de CISO roept zo snel mogelijk het kernteam Datalekken bijeen. In het kernteam Datalekken hebben zitting: Hoofd Concernstaf, de FG, de melder van het datalek, het afdelingshoofd/manager van de melder van het datalek, de Concerncontroller en de concernadviseur Informatievoorziening. In het kernteam wordt besproken of het een datalek is, of het een bij de Autoriteit Persoonsgegevens meldingswaardig datalek betreft en dan treedt het protocol in werking.
Er zijn inmiddels meerdere datalekken succesvol aan de hand van het protocol afgewikkeld. Het protocol werkt in de praktijk. Inmiddels is het proces aan de hand van een evaluatie van het gebruik aangepast. Bij de afwikkeling van de eerste datalekken werd de manager van de melder niet genodigd bij de bespreking van het datalek. Inmiddels is het proces hierop aangepast, omdat het voor veel medewerkers, die een datalek melden prettiger is indien zijn/haar leidinggevende bij de bespreking aanwezig is

en dit ook beter is, vanwege de verantwoordelijkheid die de manager draagt voor de gegevensbescherming.
Het proces datalekken is onderdeel van de IT audit. Wij hebben ten behoeve van dit onderzoek een overzicht kunnen inzien met daarin het aantal datalekken en de aard van de datalekken.[14]

3.4 TESTEN VAN INFORMATIEBEVEILIGING

8. Hoe geeft de gemeente Katwijk invulling aan het testbeleid en de auditing op de digitale veiligheid? 9. Op welke wijze worden de ICT-voorzieningen (waaronder de infrastructuur, de wifi, de volledige werkplek, de website en digitale dienstverlening) van de gemeente Katwijk getest op informatiebeveiliging, met welke frequentie en met welke resultaten?

De afgelopen ca. zes jaren heeft het team ICT minimaal een keer per jaar verschillende (pen-)testen[15] laten uitvoeren op haar basis ICT voorzieningen door externe bureaus. De afgelopen drie jaren zijn daar eveneens op initiatief van de CISO testen op het gebruik van de ICT, of het gedrag van de gebruikers bijgekomen. Zo hebben inmiddels phishing testen plaatsgevonden en zijn er meerdere malen mystery guests bij de gemeente langs geweest.
Het testbeleid is geen expliciet onderdeel in het strategisch of tactisch informatiebeveiligingsbeleid, maar de jaarlijkse pentesten zijn wel opgenomen als maatregel in het informatiebeveiligingsplan 2018.

De CISO coördineert de pentesten en rapporteert hierover in zijn reguliere rapportages aan het College en directie. In de praktijk stemt de CISO met het team ICT af over op welke systemen en onderwerpen de pentesten van dat jaar ingezet worden. Indien uit de bevindingen van de pentesten aanvullende maatregelen nodig zijn, worden deze door het team ICT zo snel mogelijk gerealiseerd.
Hierbij ervaren de technisch specialisten geen belemmeringen in het uitvoeren van de verbetermaatregelen. Uiteraard wordt door het management kritisch gekeken naar de kosten van een maatregel in verhouding tot het af te dekken risico. Echter hierbij is het budget in de praktijk niet leidend.
De afgelopen maanden heeft de freeze wel geleid tot een vertraging in het doorvoeren van alle ICT-technische maatregelen, dus ook de te nemen maatregelen na de pentesten.

[14] Document: 2017 Overzicht aantallen en kosten incidenten incl. datalekken (december 2017).xlsx
[15] Een penetratietest of pentest is een toets op kwetsbaarheden in één of meerdere computersystemen (zowel applicaties als server, databases, internet, etc). Bij deze toets worden de gevonden kwetsbaarheden ook gebruikt om in het systeem te komen, feitelijk inbreken in de systemen.

In het voorjaar van 2018 heeft een test plaatsgevonden om na te gaan welke systemen en informatie vanaf het internet bij de gemeente Katwijk of onder verantwoordelijkheid van de gemeente Katwijk zonder meer bereikbaar zijn. De bevindingen die hieruit naar voren gekomen zijn, zijn omgezet in te nemen maatregelen. Ondanks de freeze zijn de maatregelen met de hoogste prioriteit (zogenaamde prio 1-maatregelen) inmiddels voor de zomervakantie al uitgevoerd.

De gemeente Katwijk maakt gebruik van het ENSIA kader dat ontwikkeld is vanuit o.a. de VNG en het Ministerie van BZK. De ENSIA staat voor Eenduidige Normatiek Single Information Audit. Deze methodiek biedt een kader om op basis van een deel zelfevaluatie en een deel externe controle tegelijkertijd verantwoording af te leggen over de informatiebeveiliging aan het gemeentebestuur en de toezichthoudende departementen. Een externe accountant controleert de zelfevaluatie van de gemeente en brengt een verklaring hierover uit.

3.5 Risico's op het gebied van informatiebeveiliging en privacy

10. Welke mogelijke risico's zijn te onderkennen in de huidige wijze waarop het privacy en informatiebeveiligingsbeleid is ingericht en functioneert?

Het huidige privacy- en informatiebeveiligingsbeleid van de gemeente Katwijk heeft zorgvuldig vorm gekregen in zowel een strategisch en tactisch informatiebeveiligingsplan en een jaarplan Informatiebeveiliging. Voor privacy is eveneens sprake van een actueel vastgesteld privacybeleid. Er zijn drie verantwoordelijke functionarissen aangesteld, nl. een FG, een CISO en een TISO. Er zijn overleg- en kennisgremia voor de informatiebeveiliging zijn tevens processen voor het melden van datalekken. De BIG implementatie krijgt op structurele wijze verder invulling, evenals het verder brengen van een hoger volwassenheidsniveau van de privacy binnen de gemeente. De informatiebeveiliging wordt structureel gemonitord, o.a. met behulp van een ISMS. De verantwoording vindt plaats conform de ENSIA-methodiek. Het proces voor inzageverzoeken krijgt nu werkenderweg vorm. Er vinden regelmatig testen van zowel de applicaties en ICT-infrastructuur plaats en er worden gebruikers getest.

Kortom: het beleid is actueel en op orde, de maatregelen die de gemeente moest treffen hebben vorm gekregen en het bewustzijn is aanwezig. De basis is op orde. Aandachtspunt in het verder brengen van het niveau van de informatiebeveiliging en privacy binnen de gemeente Katwijk betreft het breder trekken van de verantwoordelijkheden dan de CISO, FG en TISO en het aanpassen van specifieke

processen binnen de verschillende afdelingen en teams. Hierbij is het van belang dat naast het benoemen van de verantwoordelijken binnen de uitvoerende afdelingen, de personen binnen die uitvoerende afdelingen naast het hebben van een handelingsperspectief ook de verantwoordelijkheid voelen voor informatiebeveiliging.

Een ander aandachtspunt op het gebied van privacy betreft het uitvoeren van privacy impact assessments (PIA's). Deze worden weliswaar op enkele processen van de gemeente Katwijk uitgevoerd, nadat uit de baselinetoetsen naar voren is gekomen dat dit risicovolle processen betreft en een PIA voor deze processen noodzakelijk is. Deze PIA´s zijn echter uitgevoerd aan de hand van verouderde formats. Wij hebben dit voor twee PIA's vastgesteld.[16] Deze formats zijn gebaseerd op niet meer geldende wetgeving (Wet bescherming persoonsgegevens). Deze is per 25 mei vervangen door de AVG waarin een aantal strengere regels zijn opgenomen. Bovendien zijn de PIA's minimaal ingevuld. Zo zijn enkel de vragen beantwoord met 'Ja' of 'Nee' maar ontbreekt de toelichtende beschrijving.

3.6 BORGING VAN INFORMATIEBEVEILIGING

11. Hoe ziet de gemeente erop toe dat het informatiebeveiligingsbeleid van een voldoende niveau is en blijft en er wordt geanticipeerd op toekomstige opgaven?

Het college en de directie worden minimaal in kwartaalrapportages geïnformeerd over de voortgang op het informatiebeveiligingsplan en het projectplan privacy. Beide plannen worden voorafgaand aan de uitvoering voorgelegd ter besluitvorming aan zowel het College als de directie. Hiermee worden het College en de directie geïnformeerd. Het Hoofd Concernstaf en de plaatsvervangend gemeentesecretaris maken onderdeel uit van zowel het maandelijkse informatiebeveiligingsoverleg als het team Datalekken en wordt daarmee naast de kwartaalrapportages eveneens snel geïnformeerd over de stand van zaken, mogelijke datalekken of andere incidenten. Zij draagt tevens zorg om het College en mogelijk de gemeenteraad adequaat te informeren.

De dragende functionarissen (CISO, FG en TISO) zijn benoemd en als vaste medewerkers opgenomen in de formatie. De BIG en de AVG zijn grotendeels geïmplementeerd, er worden plannen gemaakt voor de verdere implementatie en versterking van de informatiebeveiliging en gegevensbescherming vanaf 2019.
Er is tevens meerjarig budget gealloceerd voor informatiebeveiliging en gegevensbescherming. De basis is op orde, maar daarmee is het werk voor de

[16] Wij hebben kennis genomen van de PIA Basis Registratie Personen (BRP) en de PIA Leerlingenvervoer.

informatiebeveiliging en de gegevensbescherming nog zeker niet klaar. Bovendien is het werk van gemeenten ter versterking van de digitale weerbaarheid nooit gereed. In de verdere digitalisering van de samenleving en de dienstverlening van de gemeenten zelf, begeven gemeenten zich op het digitale pad. Om misbruik van het digitale pad te voorkomen, is het versterken van de informatiebeveiliging een structurele opgave om de digitale veiligheid op orde te houden. Digitale veiligheid is daarmee een structurele opgave oftewel een never ending story.

Ook de kaders voor digitale veiligheid zijn ontwikkeling. Er is inmiddels een Baseline Informatiebeveiliging Overheid (BIO) als opvolger van de BIG. De BIO is nog niet van kracht, maar zal mogelijk vanaf 2020 een nieuw kader voor alle overheidsorganisaties op het gebied van digitale veiligheid bieden. Hierop wordt de huidige ENSIA verantwoordingssystematiek uiteraard ook aangepast.

3.7 MONITORING VAN INFORMATIEBEVEILIGINGSBELEID

12. Welke beveiligingsincidenten heeft de gemeente Katwijk de afgelopen twee jaren ondervonden en hoe zijn deze afgewikkeld?

Sinds september 2017 is er een systeem voor de monitoring van de informatiebeveiliging in werking (een ISMS). Het ISMS wordt met name gebruikt om de voortgang van de BIG-implementatie te monitoren.
Het aantal datalekken, beveiligingsincidenten en virussen binnen de gemeente wordt vanaf 2016 gemonitord door het team ICT en de CISO.
In 2016 kende de gemeente 5 meldenswaardige datalekken, in 2017 zes en in 2018 vooralsnog (t/m eind september) twee.
In 2016 waren er 37 beveiligingsincidenten, in 2017 17 en in 2018 (t/m eind september) 6. Het aantal virussen betrof in 2016 7, in 2017 2 en in 2018 t/m eind september nog geen.
Alle gemelde informatiebeveiligingsincidenten worden geregistreerd in Planon[17]. Alle datalekken worden geregistreerd in een Excel spreadsheet. De CISO rapporteert in zijn reguliere (kwartaal-) rapportages over de voortgang van de BIG implementatie, de privacy en de in de achterliggende periode gemelde informatiebeveiligingsincidenten en datalekken aan het MT en de portefeuillehouders.

[17] Planon is een applicatie ter ondersteuning van de bedrijfsvoering van organisaties. In deze applicatie vindt o.a. gebouw- en zaalbeheer, maar tevens veelal de registratie van verschillende (soms) gebouwgebonden meldingen vanuit de organisatie plaats.

Beveiligingsincidenten worden, afhankelijk welk type incident het betreft, afgewikkeld in samenwerking tussen de CISO en het team ICT. Deze incidenten worden eveneens besproken en veelal geëvalueerd in het wekelijkse (operationele) informatiebeveiligingsoverleg.

4 BETROKKENHEID VAN HET COLLEGE EN DE GEMEENTERAAD

4.1 INLEIDING

Een belangrijk aandachtspunt in het onderzoek is de rol van het College van B&W en de gemeenteraad. Is de raad in de positie om kaders voor het informatiebeveiligingsbeleid te formuleren, is de raad in staat dit te controleren en wordt de raad goed geïnformeerd over de ontwikkelingen rond informatiebeveiliging? In dit korte hoofdstuk wordt weergeven welke rol zowel het College van B&W en in het bijzonder de portefeuillehouder en de gemeenteraad volgens het beleid heeft en hoe deze in de praktijk van alledag de afgelopen jaren invulling heeft gekregen.

4.2 BETROKKENHEID VAN HET COLLEGE VAN B&W

Het college heeft volgens het strategisch informatiebeveiligingsplan de integrale verantwoordelijkheid voor de informatieveiligheid, zoals zij ook integraal verantwoordelijk is voor al het beleid en uitvoering van de gemeente Katwijk. In het tactisch informatiebeveiligingsbeleid wordt het als volgt omschreven:

"*Het college van Burgemeester en Wethouders is integraal verantwoordelijk voor de beveiliging (beslissende rol) van informatie binnen de werkprocessen van de gemeente.*

Het college stelt kaders voor informatiebeveiliging (IB) op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders."

In de praktijk wordt aan deze verantwoordelijkheid vooral door de portefeuillehouder digitalisering, privacy en informatisering binnen het College van B&W vormgegeven. In het nieuwe college van B&W, dat voor de zomer van 2018 is aangetreden, is burgemeester Visser verantwoordelijk voor deze portefeuille. In het portefeuillehouders overleg is informatiebeveiliging een vast agendapunt.

4.3 VERANTWOORDING AAN DE RAAD

13. Op welke wijze is de raad tot nu toe bij de ontwikkeling van de informatieveiligheid betrokken geweest?
14. Op welke manier kan de gemeenteraad het beleid rondom informatieveiligheid controleren en sturen?

Uit de gevoerde gesprekken komt naar voren dat de gemeenteraad louter via de gebruikelijke P&C-cyclus en bijbehorende documenten is en wordt geïnformeerd over de inrichting en de verdere ontwikkeling van het beleid. Uiteraard na de initiële, informatieve bijeenkomst over informatiebeveiliging en privacy in de gemeenteraad in 2016.

In 2017 en 2018 is een enkele maal het initiatief genomen om de raad door middel van een aparte informatieavond over dit beleid te informeren. Om allerlei praktische redenen heeft dat geen doorgang kunnen vinden. Voor zover bekend hebben raadsleden ook niet zelf geïnformeerd naar dit beleid, en aanverwante zaken zoals privacybescherming.

Vanuit de gemeenteraad is de auditcommissie werkzaam. De portefeuillehouder en de CISO zijn voornemens met enige regelmaat met deze commissie ook over informatiebeveiliging te zullen overleggen.

Vanuit de organisatie wordt actieve betrokkenheid door de raad op prijs gesteld, omdat het immers aan de raad is om de kaders te stellen en om vervolgens te controleren of aan de ambities op de afgesproken wijze invulling wordt gegeven. Juist in de afweging tussen snelle en adequate dienstverlening en sociale hulp en ondersteuning aan burgers en de hierbij soms ´vertragende´ regels met betrekking tot gegevensbescherming is een afwegingskader of principe-uitspraak vanuit de gemeenteraad wenselijk voor de verantwoordelijke ambtenaren.

5 CONCLUSIES EN AANBEVELINGEN

5.1 BEANTWOORDING VAN DE DEELVRAGEN

In de voorgaande hoofdstukken zijn zowel het beleid als de praktijk van informatiebeveiliging en privacy bij de gemeente Katwijk omschreven. In deze paragraaf worden allereerst de deelvragen uit de voorgaande hoofdstukken in een beknopt overzicht beantwoord. Daarna volgt in paragraaf 5.2 Conclusie en aanbevelingen de overall conclusie en een aantal aanbevelingen ter verdere versterking van de digitale veiligheid bij de gemeente.

De beknopte beantwoording van de deelvragen is opgenomen in onderstaand overzicht.

1. Welke beleidskaders[18], regels en richtlijnen hanteert de gemeente voor de borging van de informatiebeveiliging?
2. Voldoet het beleid en de uitwerking in processen binnen de gemeente aan de bepalingen van het basisnormkader Baseline Informatiebeveiliging Gemeenten (BIG) en aan de Algemene verordening gegevensbescherming (AVG[19], die per 25 mei van toepassing is)?

De gemeente Katwijk heeft conform de AVG en de BIG haar informatiebeveiligingsbeleid en processen vormgegeven en omschreven in een strategisch en tactisch beleid en een jaarplan. Het privacy beleid is eveneens vastgesteld en voldoet aan de wettelijke bepalingen uit de AVG. Het informatiebeveiligingsbeleid voldoet aan de bepalingen, zoals vastgelegd in de BIG. Op zowel het IB-beleid als het privacy beleid zijn nog enkele aanpassingen te doen; zoals het vanuit het privacy beleid verwijzen naar het IB-beleid (vice versa is al gerealiseerd), het opnemen van de rol en verantwoordelijkheid van de in 2018 gestarte nieuwe technische informatiebeveiligingsadviseur (TISO). Dit betreft actualisering en finetuning van het beleid.

3. Welke functionarissen zijn verantwoordelijk gesteld voor de informatiebeveiliging binnen de gemeente?

Binnen de gemeente Katwijk zijn de vereiste verantwoordelijke functionarissen, zoals de FG en de CISO conform de BIG en AVG aangesteld. In het IB- en privacy beleid zijn naast de kernfunctionarissen eveneens de verantwoordelijkheden van anderen binnen de gemeente (zoals het College, de managers, etc.) geschetst. Echter de positionering van de kernfunctionarissen binnen de gemeente (onder welke afdeling en eindverantwoordelijke zij vallen) is niet vastgelegd in het beleid.

[18] Naast het vastgestelde en onlangs geactualiseerde privacybeleid en informatiebeveiligingsplan van de gemeente Katwijk.
[19] Omdat de AVG per 25 mei 2018 van kracht is geworden en de WBP per die datum niet meer van kracht is, zullen wij in dit rekenkameronderzoek de AVG als wettelijk kader hanteren.

4. Welke MDM oplossing heeft de gemeente Katwijk gekozen en op welke wijze wordt met behulp van de MDM een optimale beveiliging van de mobiele devices ingericht?
Bij de gemeente Katwijk is met de uitrol van de nieuwe, mobiele werkplek en een vernieuwing van de ICT-infrastructuur eveneens Mobile Device Management (MDM) uitgerold en het opgestelde beleid voor plaats onafhankelijk werken in werking getreden. Met het in gebruik nemen en zorgvuldig inrichten van de MDM-oplossing die Airwatch biedt kan de informatiebeveiliging van mobiele devices op een hoger niveau gebracht worden, zoals is voorzien. Of het beleid daadwerkelijk geëffectueerd is in de praktijk en hierin de IB op een hoger niveau brengt hebben wij niet kunnen vaststellen in dit onderzoek aangezien de implementatie van de nieuwe netwerkomgeving en het in gebruik nemen van het MDM pas in september 2018 is gestart.

5. Hoe is de operationalisatie en implementatie van de BIG tot nu toe verlopen?

De operationalisatie en implementatie van de BIG is in 2015 bij de gemeente gestart met een GAP-analyse. Vervolgens is in 2017 en 2018 onder andere met behulp van externe projectleiding de BIG gestructureerd geïmplementeerd. Per eind september 2018 is 76% van de BIG-maatregelen geïmplementeerd, maar of daarmee de grootste risico's zijn afgedekt hebben wij niet kunnen vaststellen. De implementatie van de BIG is gemonitord door de CISO en hierover is gestructureerd gerapporteerd.

6. Hoe is dit beleid uitgewerkt en geborgd in processen op de werkvloer?

Het informatiebeveiligingsbeleid en het privacy beleid zijn vastgesteld. De gedragsregels en werkwijzen zijn breder binnen de gemeente aan alle medewerkers kenbaar gemaakt door o.a. bewustwordingsworkshops, e-learning en informatie op het intranet. Het beleid is bekend bij de meeste collega´s, maar de dagelijkse invulling in de diverse werkprocessen van de verschillende afdelingen is nog geen gemeengoed.

7. Hoe worden medewerkers betrokken bij en getraind in het borgen van het informatiebeveiligingsbeleid en het privacy beleid?

De gedragsregels en werkwijzen zijn breder binnen de gemeente aan alle medewerkers kenbaar gemaakt door o.a. bewustwordingsworkshops, e-learning en informatie op het intranet.

8. Hoe geeft de gemeente Katwijk invulling aan het testbeleid en de auditing op de digitale veiligheid?
9. Op welke wijze worden de ICT-voorzieningen (waaronder de infrastructuur, de wifi, de volledige werkplek, de website en digitale dienstverlening) van de gemeente Katwijk getest op informatiebeveiliging, met welke frequentie en met welke resultaten?

De gemeente Katwijk heeft haar beleid met betrekking tot pentesten niet vastgelegd, maar zorgt wel voor regelmatige en gestructureerd testen (2 x per jaar) op de diverse ICT voorzieningen en het beveiligingsbeleid in den brede. Met betrekking tot de auditing van de informatiebeveiliging maakt de gemeente gebruik van de ENSIA. Ook op het privacy beleid heeft inmiddels een (zelf-)audit plaatsgevonden.

10. Welke mogelijke risico's zijn te onderkennen in de huidige wijze waarop het privacy- en informatiebeveiligingsbeleid is ingericht en functioneert?

Het breder borgen van kennis en een gevoel van verantwoordelijkheid binnen de gemeentelijke organisatie en bij de gemeenteraad is een risico. Op dit moment dragen voornamelijk de kernfunctionarissen zoals de FG, CISO en TISO deze

verantwoordelijkheid in de praktijk. In het beleid is de verantwoordelijkheid breder belegd bij o.a. het management van de gemeente. Het vraagt nog enkele jaren extra aandacht om deze verantwoordelijkheid breder binnen de organisatie bij meerdere verantwoordelijken te borgen.
Daarnaast zijn risico-afwegingen op de privacy tot op heden niet conform de AVG-kaders uitgevoerd maar op basis van tot op dat moment geldende kaders. De huidige kaders, en de daarbij te hanteren formats, gaan dieper op de risico's in.

11. Hoe ziet de gemeente erop toe dat het informatiebeveiligingsbeleid van een voldoende niveau is en blijft en wordt er geanticipeerd op toekomstige opgaven?

De directie, het College en de gemeenteraad worden gestructureerd geïnformeerd over de voortgang op de jaarlijkse uitvoering van het beleid (jaarplan). De concretisering van het beleid in een jaarplan wordt door de kernfunctionarissen opgesteld en vastgesteld door de directie en het College.

12. Welke beveiligingsincidenten heeft de gemeente Katwijk de afgelopen twee jaren ondervonden en hoe zijn deze afgewikkeld?

De gemeente kent vaste werkwijzen voor het melden van IB-incidenten en datalekken. Deze procedures vinden plaats onder verantwoordelijkheid van de kernfunctionarissen en zijn binnen de gemeente breed bekend gemaakt.

13. Op welke wijze is de raad tot nu toe bij de ontwikkeling van de informatieveiligheid betrokken geweest?
14. Op welke manier kan de gemeenteraad het beleid rondom informatieveiligheid controleren en sturen?

Uit de gevoerde gesprekken komt naar voren dat de gemeenteraad met name via de gebruikelijke P&C-cyclus en bijbehorende documenten is geïnformeerd over de inrichting en de verdere ontwikkeling van het beleid.
De gemeenteraad kan en moet kaders stellen en om vervolgens te controleren of aan de ambities op de afgesproken wijze invulling wordt gegeven. Bijvoorbeeld in de afweging tussen snelle en adequate dienstverlening en sociale hulp en ondersteuning aan burgers en de hierbij soms ´vertragende´ regels met betrekking tot gegevensbescherming.

5.2 Overall conclusie

Het informatiebeveiligingsbeleid en de basisinrichting van de processen en organisatie voor informatiebeveiliging en privacy zijn grotendeels op orde; er is voldoende aandacht, er is beleid en er zijn plannen (in ontwikkeling, zoals voor privacy) die recht doen aan de ambitie om de huidige situatie verder te verbeteren. Het werk is echter nog niet klaar en behoeft de komende jaren minimaal een even grote inspanning op het bewustzijn en het verder uitwerken van de invulling van informatiebeveiliging en privacy in de processen en dagelijkse casuïstiek.

In het opgestelde informatiebeveiligingsbeleid zijn de verantwoordelijken (bijv. portefeuillehouder, College, managers, etc.) duidelijk omschreven. In de dagelijkse praktijk wordt het grootste deel van de uitvoering van het beleid ingevuld door de CISO,

de FG en sinds kort de TISO. Dat maakt de informatiebeveiligingsorganisatie nog kwetsbaar en afhankelijk van enkele sleutelfunctionarissen. Juist een groot deel van de organisatorische informatiebeveiligings- en privacy maatregelen ligt bij de afdelingen.

5.3 AANBEVELINGEN

Deze paragraaf beschrijft de aanbevelingen die volgen uit bovenstaande conclusie. We maken het onderscheid tussen meer algemene aanbevelingen en aanbevelingen die direct kunnen worden toegepast in de praktijk.

5.3.1 ALGEMENE AANBEVELINGEN

Aanbeveling 1.1: Wij bevelen aan om de informatiebeveiliging en gegevensbescherming binnen de gehele organisatie breder bij de verschillende verantwoordelijken voor informatiebeveiliging en privacy te borgen.

Aanbeveling 1.2: De gemeenteraad moet kaders kunnen stellen, juist bij de veelal lastige weging in het Sociaal Domein, waar snel handelen om cliënten adequaat te kunnen helpen, niet altijd mogelijk is vanwege stringente eisen aan de bescherming van persoonsgegevens. Mogelijk zou de auditcommissie een initiërende rol kunnen hebben bij het discussiëren en opstellen van een dergelijk kader in de gemeenteraad.

5.3.2 TOEPASSING IN DE PRAKTIJK

Volgend uit de meer algemene aanbevelingen én om ook een meer praktisch handelingsperspectief te bieden volgt hier een aantal aanbevelingen die direct in de praktijk kunnen worden toegepast:

Aanbeveling 2.1: Ten behoeve van een betere en bredere borging van informatiebeveiliging en privacy in de organisatie, bevelen wij aan om aan te sluiten op de P&C-cyclus. Zo kan elke afdeling zich jaarlijks via een ‘in control statement’ verantwoorden over de IB- en privacy-maatregelen, die ze hebben getroffen.

Aanbeveling 2.2: Stel per afdeling een verantwoordelijk medewerker aan voor de informatiebeveiliging en privacy (contactpersoon IB & privacy).

Aanbeveling 2.3: Laat de contactpersonen IB & privacy jaarlijks een interne evaluatie per afdeling van de informatiebeveiligings- en privacy maatregelen en -praktijk opstellen onder coördinatie van de interne controleurs.

Aanbeveling 2.4: Evalueer het MDM in beheer en gebruik na een jaar.

Aanbeveling 2.5: Hanteer de meest recente kaders voor de risico-afweging voor gegevensbescherming (gebaseerd op de AVG).

Aanbeveling 2.6: Neem bij een volgende actualisatie van het informatiebeveiligingsbeleid een omschrijving op van het in de praktijk al gerealiseerde testbeleid.

Aanbeveling 2.7: Continueer de gestructureerde en uitgebreide bewustzijnsacties, zoals in 2017 en 2018 ingezet binnen de gemeente in de jaarplannen IB en privacy voor 2019.

REACTIE COLLEGE IN HET KADER VAN HET BESTUURLIJK WEDERHOOR

Postbus 589 - 2220 AN Katwijk

Rekenkamercommissie Katwijk
de Voorzitter
t.a.v. de heer C de Graaf

Contactpersoon:
Mevrouw B. Engelberts

Afdeling:
Bedrijfsvoering

Te bereiken op:
071 – 406 5190

Ons kenmerk: 1346629

Bijlage(n):

Verzenddatum:

Uw kenmerk:
Onderwerp: Bestuurlijke reactie op het rapport Digitale Veiligheid in Katwijk

21 JAN 2019

Katwijk, 15 januari 2019

Geachte heer De Graaf,

Met interesse hebben wij kennis genomen van uw rapport over de digitale veiligheid in de gemeente Katwijk.

Wij zijn verheugd over uw hoofdconclusie dat het informatiebeveiligingsbeleid en de basisinrichting van de processen en organisatie voor informatiebeveiliging en privacy grotendeels op orde zijn; er is voldoende aandacht, er is beleid en er zijn plannen in ontwikkeling (zoals voor privacy) die recht doen aan de ambitie om de huidige situatie verder te verbeteren. Wij zijn ons terdege van bewust dat het werk nog niet klaar is en de komende jaren eveneens een grote inspanning op het bewustzijn en het verder invullen van informatiebeveiliging en privacy in de processen.

Wij zijn u erkentelijk voor het aangereikte praktische handelingsperspectief op de aanbevelingen.
In deze brief geven wij u graag een reactie op de conclusies en aanbevelingen uit uw rapport.

Ten aanzien van de algemene aanbevelingen

1. *Wij bevelen aan om de informatiebeveiliging en gegevensbescherming binnen de gehele organisatie breder bij de verschillende verantwoordelijken voor informatiebeveiliging en privacy te borgen.*

   Reactie: Deze aanbeveling hangt samen met de praktische aanbevelingen onder 1,2 3 en 5.
   Het breder borgen kan op twee wijzen ingevuld worden:
   a. Bij elke afdeling capaciteit vrijmaken, wat ten koste zal gaan van andere taken;
   b. Extra capaciteit organiseren.

   Wij gaan met de gemeenteraad in gesprek over het te bereiken ambitieniveau en in te zetten capaciteit.

2. *De gemeenteraad moet kaders kunnen stellen, juist bij de veelal lastige weging in het Sociaal Domein, waar snel handelen om cliënten adequaat te kunnen helpen, niet altijd mogelijk is vanwege stringente eisen aan de bescherming van persoonsgegevens. Mogelijk zou de auditcommissie een initiërende rol kunnen hebben bij het discussiëren en opstellen van een dergelijk kader in de gemeenteraad.*

   Reactie: Met u zijn wij van mening dat hier een rol zou kunnen liggen voor de auditcommissie. De FG en CISO zouden de auditcommissie hierin kunnen ondersteunen.

Ten aanzien van de praktische toepassing

1. *Ten behoeve van een betere en bredere borging van informatiebeveiliging en privacy in de organisatie, bevelen wij aan om aan te sluiten op de P&C-cyclus. Zo kan elke afdeling zich jaarlijks via een 'in control statement' verantwoorden over de IB- en privacy-maatregelen, die ze hebben getroffen.*

   Reactie: In Q1 zal hiertoe een controlelijst gemaakt worden. De verdere uitvoering hangt samen met de algemene aanbeveling onder 1 .

2. *Stel per afdeling een verantwoordelijk medewerker aan voor de informatiebeveiliging en privacy (contactpersoon IB & privacy).*

   Reactie: Zie ook de reactie bij de eerste algemene aanbeveling.

3. *Laat de contactpersonen IB & privacy jaarlijks een interne evaluatie per afdeling van de informatiebeveiligings- en privacy maatregelen en -praktijk opstellen onder coördinatie van de interne controleurs.*

   Reactie: Deze aanbeveling nemen we ter harte. In Q1 zal hiertoe een controlelijst gemaakt worden. De verdere uitvoering hangt samen met de algemene aanbeveling onder 1.

4. *Evalueer het MDM, in beheer en gebruik na een jaar.*

   Reactie: Het MDM gebruiken wij inmiddels en we nemen de aanbeveling over om dit in 2020 te evalueren.

5. *Hanteer de meest recente kaders voor de risico-afweging voor gegevensbescherming (gebaseerd op de AVG).*

   Reactie: De eerste risico-afwegingen hebben plaatsgevonden op de toen beschikbare modellen. De VNG komt in het eerste kwartaal 2019 met een vragenlijst voor DPIA's die voldoet aan de AVG. Inmiddels zijn wij in het bezit van de ruwe versie. Het tweede kwartaal van 2019 zullen we voor de processen die thans een hoog privacyrisico hebben de DPIA's opnieuw uitvoeren. Vervolgens zullen we in het derde kwartaal van 2019 aan de hand van de nieuwe criteria beoordelen voor welke verwerkingen er alsnog een DPIA moet worden uitgevoerd. Deze zullen in het vierde kwartaal van 2019 en het eerste en tweede kwartaal van 2020 afgerond worden. Deze planning is echter onder voorbehoud dat in het eerste kwartaal van 2019 extra middelen beschikbaar worden gesteld. Daarover gaan wij met de gemeenteraad in gesprek.

6. *Neem bij een volgende actualisatie van het informatiebeveiligingsbeleid een omschrijving op van het in de praktijk al gerealiseerde testbeleid.*

   Reactie: Binnen onze gemeente kennen we informatieseringsbeleid en jaarlijkse informatiebeveiligingsplannen. In het informatiebeveilingsplan voor 2019 is de planning van de in dat jaar uit te voeren testen opgenomen. De actualisatie van het informatiseringsbeleid is gepland in het vierde kwartaal van 2019. De in gang gezette organisatieontwikkeling zou deze planning nog kunnen beïnvloeden.

7. *Continueer de gestructureerde en uitgebreide bewustzijnsacties, zoals in 2017 en 2018 ingezet binnen de gemeente in de jaarplannen IB en privacy voor 2019.*

   Reactie: In het jaarplan IB 2019 is hier al rekening mee gehouden.

Tot slot
De aanbevelingen in het rapport steunen ons in de ontwikkeling die we in gang hebben gezet en we bedanken de onderzoekers daarvoor.

NAWOORD REKENKAMERCOMMISSIE

De rekenkamercommissie is verheugd dat het college de hoofdconclusie deelt, en zich er van bewust is dat het werk nog niet is gedaan. Het is goed te constateren dat het college het onderzoek als nuttig heeft ervaren en de aanbevelingen ziet als steun in de in gang gezette ontwikkelingen.

In grote lijnen neemt het college onze aanbevelingen over, of wordt geconstateerd dat de aanbevelingen al onderdeel van het beleid zijn. Het college merkt op dat de in te zetten capaciteit afhankelijk is van het gewenste ambitieniveau (aanbeveling 1.1, 2.2 en 2.3), en dat de planning afhankelijk is van nog ter beschikking te stellen middelen (aanbeveling 2.5). Hierover gaat het college met de raad in gesprek.

Het rapport – en de reactie van het college – legt nadrukkelijk een rol bij de raad, met een initiërende rol voor uw auditcommissie. Zie paragraaf 4.3 en aanbeveling 1.2. Deze aanbeveling vraagt om een concretere uitwerking dan nu door het college wordt gedaan. De rekenkamercommissie adviseert de raad om de door het college aangeboden ondersteuning door FG en CISO te vragen en samen met hen hier invulling aan te geven. Concrete invulling zal ook kunnen leiden tot betere controle door de raad op de uitvoering van het beleid.

De overall conclusie blijft dat de lijn die door de organisatie is ingezet moet worden voortgezet. De basis is goed, maar het werk is nog niet klaar. En eigenlijk is het nooit af. Digitale veiligheid moet in de haarvaten van de organisatie gaan zitten, en dat vraagt om voortdurende actie. De rekenkamercommissie beseft dat haar aanbevelingen mogelijk gevolgen kunnen hebben voor uw begroting.

Tot slot maakt de rekenkamercommissie graag een compliment aan de organisatie en het college voor wat al is bereikt en voor de energie die daarin is gaan zitten.

BIJLAGE A BRONNEN

DE IN DIT RAPPORT GECITEERDE BRONNEN

Documentnaam	Versie	Datum
Informatiebeveiligingsplan 2018	Definitief	Januari 2018
Strategisch informatiebeveiligingsbeleid	Definitief	9 mei 2017
Tactisch informatiebeveiligingsbeleid	Definitief	16 mei 2018
Algemeen privacybeleid gemeente Katwijk	2.0	Juni 2017
Beleid Plaats Onafhankelijk Werken	2018.03	
Mobile Device Management	1.2	19 maart 2018
Governance voor de privacy		januari 2018
Bewustwording cyber crime, IB en AVG		
Totaaloverzicht acties privacy		11 juni 2018
Verklaring van accountability (privacy en informatiebeveiliging)		18 september 2018

AFGENOMEN INTERVIEWS

	Naam	Functie	Datum
1	Koos van Bekkum	Chief Information Security Officer	2-7-2018
2	Robert van Egmond	Informatiespecialist	2-7-2018
3	Jan Willem Spaargaren	Chief Information Officer, Concernadviseur informatiehuishouding	2-7-2018
4	Mark Koelewijn	Technical Information Security Officer	2-7-2018
5	Bianca Engelberts	Hoofd Concernstaf	4-7-2018
6	John Bol	Concern controller	4-7-2018
7	Vincent Dilengite	Netwerk- en systeembeheerder	5-7-2018
8	Rene Visser	Netwerk- en systeembeheerder	5-7-2018
9	Sebastiaan Verkade	Applicatiebeheerder	5-7-2018
10	Annerine Blufpand	Functionaris Gegevensbescherming	5-7-2018
11	Liesbeth Hoek, Arjan Eendebak	Team Vergunningen	12-7-2018
12	Philip van der Ploeg, Martine Hes,	Team Samenleving	12-7-2018

	Stephanie van Duin, Arthur van Galen		
13	Ingrid Kortland	Teamleider ICT	19-7-2018
14	Richard Harteveld, Christine Gillissen	Team Klantcontact	20-8-2018
15	Wouter Le Febre, John Vloemans	Projectleider implementatie BIG	21-8-2018
16	Koos van Bekkum	Chief Information Security Officer	23-8-2018
17	Arno van de Waesberge	Projectleider inrichting ICT-werkplekken	28-8-2018
18	Cornelis Visser	Burgemeester	30-8-2018

BIJLAGE B NORMENKADER

In het uitgevoerde onderzoek hebben wij gebruik gemaakt van een normenkader. Enkele onderzoeksvragen hebben een beschrijvend karakter. Aan dergelijke vragen is geen norm verbonden.
Voor de onderzoeksvragen die normatief van aard zijn, volgt hieronder het gehanteerde normenkader.

Gemeentelijk beleid (onderzoeksvragen 1, 2, 3, 4 en 5)
Het gemeentelijk informatiebeveiligingsbeleid voldoet tenminste aan de eisen, die in wet- en regelgeving worden gesteld, zoals vastgelegd in BIG en de AVG. In het gemeentelijk beleid wordt ingegaan op: – Juridische aspecten op basis van de AVG en de BIG. – Vertaling naar de beleidskaders informatiebeveiliging. – Organisatie, taken en verantwoordelijkheden voor de informatie- en gegevensveiligheid. – Inrichting reprocessing. – De toepassing van informatiesystemen en ICT. – De gegevens- en informatiestromen. – De positie van en communicatie met de burger. De gemeente hanteert landelijke standaarden, zoals de BIG, routering via gemeentelijke gegevensknoppunten, zoals het GGk e.d. De gemeente is bekend met de AVG, de impact daarvan en heeft een plan van aanpak voor de noodzakelijke aanpassingen, die ten behoeve van de AVG gerealiseerd moeten zijn. In de procesbeschrijvingen en instructies voor de informatiebeveiliging- en privacyprocessen is duidelijk welke functionaris welke gegevens in welke processtap mag verwerken, en onder welke condities dat mag.
Leren en verbeteren (Onderzoeksvragen 6, 7, 8, 9 en 10)
Er bestaat een controleplan voor de informatieveiligheid, waarin onder meer staat: hoe dit proces verloopt, de periodiciteit van de controles, wie daarbij betrokken zijn (functienamen, bijv. FG, CISO, etc. en persoonsnamen), wie controles uitvoert, aan wie wordt gerapporteerd, hoe de resultaten worden vastgelegd, wat de criteria zijn voor vervolgstappen, welke de vervolgstappen kunnen zijn en wie die neemt. Het controleplan sluit aan op het gemeentelijk beveiligingsplan, het privacy beleid en het Integriteitsbeleid. De medewerkers zijn bekend met het informatiebeveiligingsplan. De gemeente heeft vastgelegd hoe en wanneer medewerkers worden getraind in/er

aandacht besteed wordt aan het onderwerp digitale veiligheid. In de praktijk wordt gehandeld conform de wijze waarop de informatieveiligheid is geregeld in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties, de afspraken voor de verwerking van gegevens en de afspraken over het informeren van burgers en het vragen van toestemming. De gemeente heeft een leer- en verbetercyclus waar informatiebeveiliging een apart onderdeel van uitmaakt. De gemeente heeft een routine voor het meten en verbeteren van de informatieveiligheid en legt vast wat de bevindingen en maatregelen zijn. Deze routine is al tenminste één keer uitgevoerd.
Kaderstellende en controlerende rol van de raad (onderzoeksvragen 13 en 14)
In de bestuursrapportages, programmabegroting en programmarekening wordt expliciet aandacht besteed aan de wijze waarop de digitale veiligheid is gewaarborgd. Daaraan worden conclusies en maatregelen verbonden op basis van uitgevoerde controles. Bij de ontwikkeling van beleid heeft informatiebeveiliging en privacybeleid als punt op de agenda van de Raad gestaan.

BIJLAGE C AFKORTINGEN EN VERKLARENDE WOORDENLIJST

AFKORTINGEN

Afkorting	Betekenis
AVG	Algemene Verordening Gegevensbescherming
B&W	Burgemeester en Wethouders
BAG	Basisregistratie adressen en gebouwen
BIG	Baseline Informatiebeveiliging Nederlandse Gemeenten
BRO	Basisregistratie ondergronds
BRP	Basisregistratie personen
BSN	Burgerservicenummer
BYOD	Bring your own device
BZK	Binnenlandse Zaken en Koninkrijksrelaties
CAB	Change Advisory Board
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COD	Corporate owned Devices
ENSIA	Eenduidige Normatiek Singe Information Audit
FG	Functionaris Gegevensbescherming
GGk	Gemeentelijk Gegevensknooppunt
IB	Informatiebeveiliging
ISMS	Information Security Management System
ICT	Informatie- en Communicatietechnologie
MDM	Mobile Device Management
MT	Managementteam
P&C-cyclus	Planning en controlcyclus
PIA	Privacy Impact Assessment
TISO	Technical Information Security Officer
VNG	Vereniging Nederlandse Gemeenten

VERKLARENDE WOORDENLIJST

Technische term	Betekenis
Airwatch	Software die de gemeente Katwijk heeft gekozen voor Mobile Device management (zie onder).
Back-up & recovery	Het proces van het veilig stellen van gegevens (back-up) en herstellen van die gegevens (recovery) in het geval van een incident waarbij gegevens verloren zijn gegaan.
Black-box testing	Dit is een vorm van testen waarbij de tester geen kennis heeft van de structuur van de betrokken ICT-systemen.
e-learning	e-learing is een verzamelterm voor leermiddelen waarbij interactief gebruik wordt gemaakt van digitale middelen.
forensic readiness	Forensic readiness betreft de mogelijkheid van een organisatie om optimaal gebruik te maken van digitale middelen (email, informatie uit het zaaksysteem, etc) als valide bewijsmateriaal in juridische kwesties
Gap-analyse	Een analyse waarbij de gewenste situatie wordt afgezet tegen de huidige situatie. Het verschil is het gat (de 'gap').
Grey-box testing	Dit is een vorm van testen waarbij de tester beperkte kennis heeft van de structuur van de betrokken ICT-systemen.
Freeze	Een periode waarin geen of nauwelijks technische wijzigingen worden doorgevoerd op een informatiesysteem.
Mobile Device Management	Met behulp van MDM kan een IT-afdeling op een veilige manier apparaten toevoegen aan een bedrijfsnetwerk, zelf de instellingen verzorgen voor de draadloze verbinding en het ophalen van updates, toezien op naleving van bedrijfsregels en apparaten op afstand vergrendelen of wissen.[20]
Mystery guest	Een mystery guest is een voor de organisatie externe persoon die opzettelijk probeert (beveiligings-)maatregelen te omzeilen en die daarvoor is ingehuurd door de beveiligingsorganisatie van die organisatie.
Phishing	Een vorm van internetfraude waarbij, vaak per e-mail, een ontvanger verleid wordt op een malafide verwijzing te klikken waardoor schade kan worden toegebracht.
Planon	Software ter ondersteuning van de bedrijfsvoering van organisaties. In deze applicatie vindt o.a. gebouw- en zaalbeheer, maar tevens veelal de registratie van verschillende (soms) gebouwgebonden meldingen vanuit de organisatie

[20] Bron: www.computerworld.nl

	plaats.
single sign on	Dit is het dusdanig inrichten van de autorisatiestructuur van de ICT-omgeving zodat een gebruiker maar één keer zijn of haar inloggegevens hoeft in te voeren om toegang te krijgen tot de applicaties.
Suwinet	Suwinet is een digitale infrastructuur die is ontwikkeld door de Suwipartijen (UWV, SVB en gemeenten) om ervoor te zorgen dat zij gegevens met elkaar kunnen uitwisselen voor de uitoefening van hun wettelijke taak.[21]

[21] Bron: www.bkwi.nl

COLOFON

De rekenkamercommissie is ondersteund door:

PBLQ
Muzenstraat 120
2511 WB Den Haag

Auteurs: Peter Castenmiller
Matthijs Kerkvliet
Marieke van der Putten

T: 070 – 376 36 36

E: info@pblq.nl
I: www.pblq.nl