Digitaal gedrag: veilig en verantwoordelijk

Rekenkamercommissie Leiden en Leiderdorp

Drs. A.L. (Lauryan) Bakker

E.I.A. (Emilie) Stumphius, MSc. LLM

G.S. (Gideon) van der Hulst, MSc

Rekenkamercommissie Leiden-Leiderdorp

N. (Nike) van Helden
Secretaris Rekenkamercommissie Leiden-Leiderdorp

T. 06 – 15 16 98 34
rekenkamer@leiden.nl

Postbus 292
2300 AG Leiden

Kenmerk: RO 15952
Datum: 8 maart 2019

Necker van Naem

Inhoudsopgave

Onderzoeksverantwoording

Aanleiding

De rekenkamercommissie van de gemeenten Leiden en Leiderdorp ziet een maatschappelijke ontwikkeling richting ICT-intensievere organisaties. Het begin van deze ontwikkeling is grotendeels terug te leiden tot de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente'.[1] Met deze resolutie besloten de leden van de VNG in 2013 met elkaar te werken aan de versterking van informatieveiligheid. De resolutie houdt in dat iedere gemeente een informatieveiligheidsbeleid vaststelt aan de hand van de Baseline Informatiebeveiliging Gemeenten (BIG), waarin tactische en strategische eisen zijn vastgelegd.

In de jaren na 2013 groeide de noodzaak om te werken aan informatieveiligheid. De samenleving vraagt om meer mogelijkheden voor digitaal contact, wetgeving wordt regelmatig aangepast en door de decentralisaties in het sociaal domein hebben gemeenten de beschikking over veel (bijzondere) persoonsgegevens. Het beveiligen hiervan lukt nog niet altijd: 19% van de datalekken die in het laatste kwartaal van 2017 bij de Autoriteit Persoonsgegevens werden gemeld, waren afkomstig uit de sector 'openbaar bestuur'.[2]

Digitale veiligheid en informatieveiligheid bij de overheid gaan hand in hand met het begrip privacy. Het gevolg van een datalek kan een inbreuk op de persoonlijke levenssfeer van een inwoner zijn. Landelijk is hier veel aandacht voor. Grote datalekken kwamen uitgebreid in het nieuws. Informatieveiligheid is dus niet alleen essentieel voor de bescherming van de inwoner, maar ook voor de reputatie van de gemeente.

De hierboven beschreven maatschappelijke ontwikkeling richting ICT-intensievere organisaties vormden voor de rekenkamercommissie Leiden en Leiderdorp een aanleiding voor een onderzoek naar digitale veiligheid in de twee gemeenten. Als onderzoekspartner van de rekenkamercommissie heeft Necker van Naem dit onderzoek uitgevoerd in samenwerking met partner Guardian360.

[1] https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/informatieveiligheid/brieven/resolutie-informatieveiligheid-randvoorwaarde-voor-de-professionele-gemeente

[2] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/cijfers-meldplicht-datalekken-vierde-kwartaal-2017

Doelstelling en vraagstelling

Het onderzoek kende de volgende doelstelling:

> Het onderzoek heeft tot doel meer inzicht te verkrijgen in de informatiebeveiliging van Leiden en Leiderdorp. De nadruk ligt daarmee met name op het beoordelen van de opzet, het bestaan en de werking van het informatiebeveiligingsbeleid.

Om de doelstelling te verwezenlijken is gewerkt met deelvragen. De deelvragen zijn opgesteld op basis van vijf thema's:

1. Beleid (opzet);
2. Organisatie (bestaan);
3. Uitvoering (werking);
4. Rol van de raad (werking);
5. Praktijktoetsing (werking).

Symboo

Beleid

1. Beschikken beide gemeenten over een adequaat informatiebeveiligingsbeleid?
2. Welke elementen komen naar voren in het beleid (wet- en regelgeving, techniek, organisatie, menskant?)

Organisatie

3. Hoe is de informatiebeveiligingsfunctie ingericht?
4. Is er sprake van een goed georganiseerde informatiebeveiligingsfunctie?

PDCA-cyclus

5. Welke (zelf)evaluaties worden er uitgevoerd omtrent informatieveiligheid en wat zijn hier de uitkomsten van?
6. Hoe worden verbeterpunten, uit (zelf)evaluaties en uit de praktijk, opgepakt?
7. Zijn de belangrijkste risico's op het gebied van opslag, uitwisseling en beveiliging van informatie en in het bijzonder van (bijzondere) persoonsgegevens in beeld?

Rol van de raad

8. Welke informatie ontvangt de raad over informatieveiligheid?
9. Welke rol kiest de raad omtrent informatieveiligheid (vragen stellen, moties indienen. etc)?

Praktijktoetsing

10. In hoeverre is een kwaadwillende derde in staat om de informatiesystemen binnen te dringen?
    a. Kan deze derde via oneigenlijke middelen toegang tot specifieke mail- en agendagegevens verkrijgen?
    b. Kan deze derde via oneigenlijke middelen toegang tot beheers en/of back-end systemen van webapplicaties krijgen?
11. Is de rollen- en rechtenstructuur zo ingericht dat een vertrouwde gebruiker alleen toegang heeft tot die systemen waar hij/zij toegang zou moeten krijgen?
12. Voldoen de relevante informatiesystemen aan de technische eisen die gesteld worden binnen de BIG en DIGID 2.0?
13. Zijn de medewerkers zich voldoende bewust van de gevaren van phishing e-mails en alerts wanneer zij een dergelijke e-mail ontvangen?

Onderzoeksuitvoering

Op woensdag 13 juni vond het startgesprek plaats. Hierbij waren leden van de rekenkamercommissie, het onderzoeksteam, beide gemeentesecretarissen, de functionaris gegevensbescherming en de CIO aanwezig. De onderzoekers voerden hun werkzaamheden uit in de periode juni 2018 – oktober 2018. De werkzaamheden richtten zich enerzijds op beleid, organisatie en uitvoering en anderzijds op praktijktoetsing. Wat betreft beleid bestonden de werkzaamheden uit een documentstudie en interviews met vertegenwoordigers van de gemeente Leiden, de gemeente Leiderdorp en Servicepunt71. De interviews vonden op 8 augustus, 10 september en 26 september plaats. Van deze gesprekken zijn verslagen gemaakt. De verslagen zijn ter verificatie aan de respondenten voorgelegd en geaccordeerd. De praktijktoetsing werd uitgevoerd door Guardian360, en bestond onder andere uit een phishingtest. Na de praktijktoetsing verzorgde Guardian360 nazorg aan de gemeenten Leiden en Leiderdorp en gemeenschappelijke regeling Servicepunt71 om de gevonden kwetsbaarheden op een gedegen manier te verhelpen.

Op 24 januari is het Onderzoeksrapport aan de organisatie aangeboden voor een toets op de feitelijke juistheid van de bevindingen in het kader van het ambtelijk wederhoor. Op 20 februari ontvingen de onderzoekers de reactie in het kader van het ambtelijk wederhoor. Op 11 maart 2019 is het eindrapport verstuurd naar de griffie ten behoeve van de gemeenteraad.

Eén rapport, twee gemeenten, drie organisaties

Dit rapport bevat informatie over zowel de gemeente Leiden als de gemeente Leiderdorp. Door de intensieve samenwerkingen tussen beide gemeenten in de Leidse Regio en de gemeenschappelijke regeling Servicepunt71[3] overlapt de informatie voor de gemeenten Leiden en Leiderdorp grotendeels. Toch bestaan er ook verschillen. Bij informatie die specifiek geldt voor de gemeente Leiden of de gemeente Leiderdorp of informatie die afkomstig is van Servicepunt71 wordt door middel van een logo aangegeven voor welke organisatie deze informatie geldt.

Figuur 1 Logo's gemeente Leiderdorp, gemeente Leiden en Servicepunt71.

Technisch onderzoek

De onderzoekers realiseren zich dat een onderzoek naar het thema digitale veiligheid in gemeenten leidt tot een rapportage met een relatief veel jargon en technische termen. In de tekst zijn daarom voorbeelden uit gehouden interviews opgenomen om duiding aan te brengen, en achterin de rapportage is een lijst met verklaringen en begrippen opgenomen.

Leeswijzer

Het onderzoeksrapport bestaat uit vijf hoofdstukken:

- Hoofdstuk 1 behandelt het beleid van de gemeenten Leiden en Leiderdorp op het gebied van digitale veiligheid. In de beleidsstukken staan ook de thema's uit de volgende hoofdstukken uitgewerkt: organisatie, uitvoeringen de rol van de gemeenteraad. Hoofdstuk 2 tot en met 4 bouwen dus voort op hoofdstuk 1.
- Hoofdstuk 2 gaat in op de organisatiestructuur van de gemeenten Leiden en Leiderdorp omtrent digitale veiligheid.
- Hoofdstuk 3 bevat informatie over de uitvoering van digitale veiligheid in de gemeenten ten grondslag liggen.
- Hoofdstuk 4 biedt inzicht in de rol van de gemeenteraden en informatievoorziening aan de gemeenteraden van Leiden en Leiderdorp.
- Hoofdstuk 5 geeft tenslotte informatie over de uitkomsten van de praktijktoetsen. Dit betreft informatie op een dergelijk abstractieniveau dat geen concrete kwetsbaarheden van de gemeenten worden benoemd. Diepgaandere bevindingen zijn met de gemeenten gedeeld via aparte bijlagen.

Achterin dit rapport vindt u een aantal bijlagen met daarin onder andere een bronvermelding in bijlage I, het gebruikte normenkader in bijlage II, een afkortingen- en begrippenlijst in bijlage III en bijlagen volgend uit de praktijktoetsen in bijlage IV.

[3] Binnen de gemeenschappelijke regeling Servicepunt71 wordt samen gewerkt door de vier gemeenten uit de Leidse Regio (gemeente Leiden, gemeente Leiderdorp, gemeente Zoeterwoude, gemeente Oegstgeest). In dit onderzoek wordt alleen gekeken naar de gemeente Leiden en Leiderdorp.

Onderzoeksrapport

1 Beleid

In dit hoofdstuk wordt eerst een algemene beschouwing gegeven op de aard van het beleid rondom digitale veiligheid van de gemeenten Leiden en Leiderdorp. Hierbij wordt uiteengezet welke beleidsstukken gelden, waar deze mogelijk verschillen tussen de gemeente Leiden en de gemeente Leiderdorp, wat de inhoud van deze stukken is en hoe deze geduid zijn in de interviews.

De volgende deelvragen staan centraal in dit hoofdstuk:

Beleid

1. *Beschikken beide gemeenten over een adequaat informatiebeveiligingsbeleid?*
2. *Welke elementen komen naar voren in het beleid (wet- en regelgeving, techniek, organisatie, menskant)?*

1.1 / Samenvatting

De gemeenten Leiden en Leiderdorp hebben overwegend hetzelfde beleid op het gebied van digitale veiligheid. De beleidstukken voor digitale veiligheid gelden namelijk in de meeste gevallen voor alle gemeenten uit de Leidse Regio die samenwerken binnen Servicepunt71, en voor Servicepunt71 zelf.

De beleidsstukken zijn inhoudelijk volledig en bieden uitgangspunten of specifieke regels op de thema's organisatie, beheer van gegevens, werkprocessen, de benodigde techniek voor informatiebeveiliging en het bewustzijn van medewerkers. In het beleid, waaronder het informatiebeveiligingsbeleid, wordt verwezen naar relevante landelijke wet- en regelgeving, zoals bijvoorbeeld de Baseline Informatievoorziening Gemeenten (BIG).

Wel is het zo dat de beleidsstukken toe zijn aan een update. In een beweeglijke context zoals die van het thema digitale veiligheid is dat op zich niet vreemd; het beleid wordt dusdanig opgesteld dat het ook actueel blijft bij nieuwe technologische ontwikkelingen. Inmiddels is het echter wel degelijk tijd voor een update. Het informatiebeveiligingsbeleid stamt uit 2016, en het beleid gegevensbescherming uit 2015. Een belangrijke ontwikkeling sindsdien die een plek moet krijgen in het beleid is de inwerkingtreding van de AVG. Omdat er nog veel onduidelijkheden waren rondom de specifieke consequenties van de AVG heeft de gemeente er voor gekozen om het beleid pas na inwerkingtreding te actualiseren. In de betreffende beleidsstukken wordt al wel gerefereerd aan de komst van de AVG.

Toetsing normenkader - beleid	
1. Er is een informatieveiligheidsbeleid. 2. De beleidsstukken beschrijven onder andere rollen en verantwoordelijkheden, werkprocessen, veiligheidsmaatregelen. 3. Het beleid wordt periodiek up-to-date gebracht. 4. In het beleid wordt verwezen naar de relevante wettelijke kaders. 5. De gemeente hanteert in haar beleid de normen uit de BIG.	1. Voldaan, dit beleid geldt voor de Leidse regio. 2. Voldaan, deze zaken komen terug in het beleid. 3. Deels voldaan. De stukken zijn toe aan een update; er wordt aan gewerkt. 4. Voldaan, dit komt terug in het beleid. 5. Voldaan, de BIG-normen zijn het uitgangspunt in het beleid.

1.2 / Introductie gemeenschappelijk beleid

De relevante beleidsstukken ten aanzien van digitale veiligheid worden in paragraaf 1.3 tot 1.5 inhoudelijk behandeld. In deze paragraaf volgen eerst een aantal overkoepelende beschouwingen ten aanzien van het beleid.

Gezamenlijk beleid voor digitale veiligheid voor de Leidse Regio, overlap tussen de beleidsdocumenten

De gemeenten die samen de Leidse Regio vormen (Leiden, Leiderdorp, Oegstgeest en Zoeterwoude) hebben grotendeels hetzelfde beleid op het gebied van digitale veiligheid.

- Beleid gegevensbescherming (uitgebracht op 20 augustus 2015). Dit stuk geldt ook voor Servicepunt71;
- Informatiebeveiligingsbeleid (uitgebracht in augustus 2016).
- Privacy by design (uitgebracht op 19 juli 2016). Dit is geen officieel beleidsstuk, maar vanwege de strategische aard van het stuk (dit document bevat richtlijnen waaraan een informatiesysteem die persoonsgegevens verwerkt moet voldoen om deze persoonsgegevens te beschermen) wordt dit toch onder 'beleid' beschreven;

De documenten staan los van elkaar, maar er is veel overlap. In de documenten wordt hier de volgende verklaring voor gegeven: bij gegevensbescherming staat wetgeving centraal. Informatieveiligheid maakt de uitvoer en beheersing van deze wetgeving mogelijk.[4] Informatieveiligheid raakt aan en overlapt daarmee met gegevensbescherming (privacy).

Beleid en procedures worden herijkt of zijn aan herijking toe

De actualisering van digitale veiligheidsbeleid is een continu proces; het veld is steeds in beweging. Op dit moment werkt de Nederlandse overheid, en daarmee ook gemeenten, bijvoorbeeld toe naar de Baseline Informatievoorziening Overheid (BIO), die de BIG opvolgt. Het is de verwachting van alle overheidslagen dat de BIO op 1 januari 2020 van kracht wordt. In 2019 kunnen gemeenten zich voorbereiden op de overgang van de BIG naar de BIO. Bovendien ontwikkelt techniek zich snel. Dergelijke ontwikkelingen zorgen ervoor dat gemeenten hun beleid regelmatig moeten actualiseren.

Het huidige informatiebeveiligingsbeleid van de Leidse regio is toe aan herijking, om aan te sluiten bij de AVG en ontwikkelingen in de regionale samenwerking. Het huidige informatiebeveiligingsbeleid is opgesteld in 2016.[5]Er is bewust gekozen om het beleid niet eerder te actualiseren, maar te wachten op de eerste praktijkervaringen na de invoering van de AVG omdat er nog veel vraagtekens bestonden en bestaan omtrent de gevolgen van de AVG. Ook het beleid Gegevensbescherming wordt geactualiseerd. Ook hierbij is gewacht tot na de invoering van de AVG. De actualisatie stond in eerste instantie gepland voor het derde kwartaal van 2018, maar is inmiddels verschoven naar het eerste half jaar van 2019. De afstemming van het nieuwe beleid vergt om meerdere redenen meer tijd dan verwacht: met het oog op de komst van de BIO, de regionalisering van de informatievoorzieningstaken (VRIS) en de daarbij behorende wijzigingen in de governance leiden tot een langer proces.

Naast de beleidsstukken zijn ook enkele procedures aan herijking toe. Een voorbeeld hiervan is de procedure voor het melden van datalekken en beveiligingsincidenten. Een tweede voorbeeld is de procedure voor het al dan niet intrekken van autorisaties van werknemers die langdurig geen gebruik maken van hun autorisatie voor een bepaald account.

[4] Informatiebeveiligingsbeleid gemeente Leiderdorp, p. 9; Informatiebeveiligingsbeleid gemeente Leiden p. 6.; Beleid gegevensbescherming, p.3

[5] Informatiebeveiligingsbeleid gemeente Leiden; Informatiebeveiligingsbeleid gemeente Leiderdorp.

Versterken samenwerking door het project VRIS

In 2016 hebben de gemeenten Leiden en Leiderdorp samen met de andere gemeenten uit de Leidse Regio besloten de samenwerking op het terrein van informatievoorziening, informatiebeleid en informatiemanagement te intensiveren en te versterken. Daarom hebben de besturen van de vier gemeenten en het bestuur van Servicepunt71 opdracht gegeven tot het project *Versterking van de Regionale I-Samenwerking* (VRIS). Één van de gezamenlijke opgaven is ´Versterking informatiebeveiliging en gegevensbescherming'. Voor dit globale doel zijn meerdere subdoelen geformuleerd. Voorbeelden hiervan zijn het stimuleren van bewustzijn, BIG compliancy en het aanstellen van een functionaris gegevensbescherming (FG)' voor de regio.[6,7] Een andere deel van het VRIS project is de wens om meer regionaal te gaan werken. Vanuit deze wens wordt een groep medewerkers, waaronder de informatiemanagers en gegevensbeheerders, onder de verantwoordelijkheid van de Chief Information Officer (CIO) gebracht. Dit wordt de 'I-kolom' genoemd. Op het moment zijn de gemeenten uit de Leidse Regio en Servicepunt71 daarom in een overgangsperiode. Deze transitie wordt uitgebreid besproken in hoofdstuk 2: Governance.

Beleid gegevensbescherming en informatiebeveiligingsbeleid zijn van goede kwaliteit; een aantal verbetermogelijkheden zichtbaar.

De beleidsstukken van de gemeenten Leiden en Leiderdorp zijn kwalitatief goed en volledig. De onderwerpen die in een privacy- of informatiebeveiligingsbeleid behandeld dienen te worden, staan ook daadwerkelijk in het beleid. De beleidsstukken volgen de landelijke richtlijnen. De onderstaande verbetermogelijkheden zijn zichtbaar. Dit zijn allen verbetermogelijkheden die voortvloeien uit de dynamische context van privacy en informatieveiligheid, waar juridische en technologische ontwikkelingen elkaar snel opvolgen.

/ De organisatie van informatieveiligheid in SP71-verband is in ontwikkeling. De beleidsstukken moeten hier op het vlak van organisatiestructuur op worden aangepast.
/ De BIO wordt op 1 januari 2020 van kracht. In 2019 kunnen gemeenten zich voorbereiden op de overgang van de BIG naar de BIO. Het informatiebeveiligingsbeleid houdt daar nu nog geen rekening mee.
/ De beleidsstukken zijn nog niet afgestemd op de AVG.

1.3 / Informatiebeveiligingsbeleid

Addendum vormt verschil tussen Leiden en Leiderdorp

De uitgangspunten van het informatiebeveiligingsbeleid zijn voor de gemeenten Leiden en Leiderdorp gelijk,[8] maar voor wat betreft de organisatievormen hebben de gemeenten het beleid 'op maat gesneden'. Het informatiebeveiligingsbeleid is voor zowel de gemeente Leiden als Leiderdorp vastgesteld door het college en dateert van augustus 2016.[9]

[6] Uitvoeringsprogramma VRIS Leidse Regio, p. 8.

[7] Inmiddels is de FG voor de Leidse Regio aangesteld. Daarnaast zijn er nog twee plaatsvervangend FG's actief in de regio. – Bron: privacy organisatie juli 2018.

[8] Informatiebeveiligingsbeleid gemeente Leiden; Informatiebeveiligingsbeleid gemeente Leiderdorp

[9] Informatiebeveiligingsbeleid gemeente Leiden, voorblad.

Vóór het informatiebeveiligingsbeleid werd vastgesteld had de Leidse regio een statuut ten aanzien van informatiebeveiliging. Leiderdorp voegde daar (net als Zoeterwoude en Oegstgeest) een addendum aan toe: de Governance- en Incidentenprocedure. De relevante punten uit dit addendum zijn als uitbreiding in het huidige informatiebeveiligingsbeleid opgenomen. Het addendum maakt geen deel meer uit van het huidige beleid.

Informatiebeveiligingsbeleid gebaseerd op nationale en internationale kaders

Het informatiebeveiligingsbeleid bevat vooral technische normen, er zijn geen maatschappelijke doelen in omschreven. In het informatiebeveiligingsbeleid wordt verwezen naar relevante wet- en regelgeving.[10] Het Informatiebeveiligingsbeleid is gebaseerd op de Baseline Informatievoorziening Gemeenten (BIG) en de (NEN/ISO) Code voor informatiebeveiliging.[11] Eerstgenoemde is een nationaal kader, de laatstgenoemde is een internationale kwaliteitsstandaard. De BIG is een set normen en maatregelen voor een basis beveiligingsniveau op drie niveaus: strategisch, tactisch en operationeel. Dit wordt weergegeven in figuur 2.

De BIG geldt als basis-normenkader, waarop de gemeente afweegt en prioriteert op basis van het pas toe of leg uit principe.[12] Ook ontleent het beleid uitgangspunten aan de Code en de BIG, zoals bijvoorbeeld:

- Alle informatie en informatiesystemen zijn van kritiek en vitaal belang voor de gemeente. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)-management, met het College van B&W als eindverantwoordelijke. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.[13]
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het management systeem van informatiebeveiliging.[14]

Figuur 2 Overzicht Baseline Informatiebeveiliging Gemeenten[15]

De BIO wordt op 1 januari 2020 van kracht. In 2019 kunnen gemeenten zich voorbereiden op de overgang van de BIG naar de BIO. Geïnterviewden verwachten dat het werken volgens de BIO inzichtelijkere rapportages aan het bestuur oplevert, ter ondersteuning van de PDCA-cyclus. De wens is om hiervoor een Information Security Management Systeem (ISMS) te implementeren. Momenteel (maart 2019) wordt gewerkt aan de aanbesteding.

Aanpak informatiebeveiliging is Risk-Based

De aanpak van informatiebeveiliging in de gemeenten Leiden en Leiderdorp is 'risk based'. Dat betekent dat er beveiligingsmaatregelen worden getroffen op basis van een toets aan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) van VNG/KING (GAP-analyse). Indien een systeem meer maatregelen nodig heeft, wordt een risicoanalyse uitgevoerd. Daartoe inventariseert de proceseigenaar de kwetsbaarheid van zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beschermingseisen van de informatie.[16] Eind 2017 werd bijvoorbeeld een conceptversie van de risicoanalyse uitgevoerd voor een chatfunctie op de website van Erfgoed Leiden en Omstreken. Later werd

[10] Onder meer Informatiebeveiligingsbeleid Gemeente Leiden, p. 35.

[11] Informatiebeveiligingsbeleid Gemeente Leiden, p. 6.

[12] Informatiebeveiligingsbeleid Gemeente Leiden, p. 8.

[13] Informatiebeveiligingsbeleid Gemeente Leiden, p. 5.

[14] Informatiebeveiligingsbeleid Gemeente Leiden, p. 5.

[15] www.informatiebeveiliging-gemeenten.nl

[16] Informatiebeveiligingsbeleid Gemeente Leiden, p. 7.

ook een definitieve risicoanalyse gemaakt van de chatfunctie. Hieruit bleken een aantal risico's die aanleiding geven om het project vooralsnog stil te leggen en de chatfunctie niet te implementeren.

Aandacht voor governance, uitvoering, techniek en bewustzijn in het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid is – naast de aansluiting op wet- en regelgeving - bestudeerd op de aanwezigheid van bepalingen omtrent governance/organisatie, uitvoering/techniek en bewustzijn/menskant. Deze thema's komen terug in het beleid. In de volgende hoofdstukken worden deze thema's verder uitgewerkt. In onderstaande tabel wordt dit met verwijzing naar een aantal voorbeeldbepalingen weergegeven.

Aspect	Opgenomen in beleid?	Voorbeeldbepalingen
Governance/organisatie	Ja	De coördinatie van informatiebeveiliging is belegd bij de CISO. Servicepunt71 heeft een coördinator informatiebeveiliging aangesteld voor dagelijks beheer van de (technische) IB-aspecten.
Werkprocessen/techniek	Ja	Niemand mag geautoriseerd worden om een gehele cyclus van handelingen te verrichten. Bij contractuele overeenkomsten gelden in beginsel altijd de Algemene Inkoopvoorwaarden, waarin onder meer geheimhouding en aansprakelijkheid is geregeld.
Bewustzijn/menskant	Ja	De gemeente/ de directie/ de afdeling bevordert algehele communicatie en bewustwording rondom informatieveiligheid. In werkoverleggen wordt periodiek aandacht geschonken aan informatieveiligheid. Voor zover relevant worden hierover afspraken vastgelegd in planningsgesprekken.

Informatiebeveiliging verbeteren via Regionaal Actieplan Informatieveiligheid

In het uitvoeringprogramma voor het project VRIS is opgenomen dat acties ten behoeve van concrete doelen, bijvoorbeeld compliancy met de BIG, jaarlijks worden uitgewerkt in een regionaal actieplan.[17] Een voorbeeld van een maatregel uit het actieplan 2017 is het implementeren van beveiligde gegevensuitwisseling (veilig mailen). Daarnaast is er in het actieplan aandacht voor Bewustwording en logging (het registreren van handelingen die medewerkers verrichten in applicaties). Tenslotte voorzag het actieplan 2017 in een nieuwe risicoanalyse in het eerste kwartaal van 2018. De resultaten zouden input geven voor het actieplan 2018.[18]

1.4 / Beleid gegevensbescherming

Beleid gegevensbescherming biedt kaders voor werken met persoonsgegevens

Het Beleid Gegevensbescherming geldt voor zowel de gemeente Leiden als Leiderdorp. Het is vastgesteld door de colleges van beide gemeenten en dateert van augustus 2015. Ter voorbereiding op de AVG is besloten dat dit beleid elk jaar wordt geauditeerd.[19]

De visie op gegevensbescherming van de gemeente Leiden is dat de gemeente respect heeft voor de persoonlijke levenssfeer van haar inwoners, ondernemers en medewerkers. Het Beleid Gegevensbescherming geeft kaders voor het verwerken van privacygevoelige informatie (waaronder persoonsgegevens), de bescherming van en omgang met deze gegevens. De kaders gelden voor de gemeenten, samenwerkingsverbanden die zijn of worden aangegaan, waaronder Servicepunt71, en derden die zijn of

[17] Uitvoeringsprogramma VRIS Leidse Regio, p, 33.

[18] Regionaal Actieplan Informatieveiligheid (2017), p.4; Regionaal Actieplan Informatieveiligheid (2017), p.6

[19] Beleid gegevensbescherming, p. 5.

worden ingeschakeld[20]. Het Beleid gegevensbescherming dient als kapstok waaraan voor een specifiek vakgebied een beheerplan of privacyprotocol gehangen kan worden.[21]

Het Beleid Gegevensbescherming bevat onder andere kaders over het volgende: [22]

- Juridisch kader;
- De governance en organisatorische borging van gegevensverwerking (Wbp, verantwoording aan de raad, wijze van inrichten gegevensverwerking, sturing en monitoring, bewerkersovereenkomsten met derden);
- Werkprocessen (omgang met persoonsgegevens, meldplicht datalekken, bewaren van gegevens, toestemming, open communicatie);
- Waarborgen voor gegevensbescherming (Privacy Impact Assessment, dataclassificatie, logging van gegevensgebruik, melding gegevensverwerking CPB);
- Rechten van betrokkene (recht tot inzage en correctie, recht van verzet, indienen bezwaar).

De kaders zijn beknopt en schetsen alleen op hoofdlijnen wat de situatie in de gemeenten is. Ten aanzien van sturing en monitoring wordt bijvoorbeeld alleen het volgende gezegd: 'Elke afdelingshoofd is verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens die binnen zijn of haar afdeling plaatsvindt. Zij zijn daarom ook verantwoordelijk om te monitoren of persoonsgegevens zorgvuldig verwerkt worden, en dit zo nodig bij te sturen.

De functionaris gegevensbescherming en coördinator informatiebeveiliging hebben de verantwoordelijkheid om structureel te toetsen of de wettelijke eisen en de gemeentelijk richtlijnen op het gebied van privacy en informatiebeveiliging zijn geïmplementeerd en worden uitgevoerd. Hoe zij dit doen staat beschreven in hoofdstuk 4 van het beleid gegevensbescherming.

Aandacht voor governance, werkprocessen, techniek en bewustzijn in het Beleid Gegevensbescherming

Ook het Beleid Gegevensbescherming is – naast de aansluiting op wet- en regelgeving - bestudeerd op de aanwezigheid van bepalingen omtrent governance/organisatie, werkprocessen/techniek en bewustzijn/menskant. Deze thema's komen terug in het beleid. In onderstaande tabel wordt dit met verwijzing naar een aantal voorbeeldbepalingen weergegeven.

Aspect	Opgenomen in beleid?	Voorbeeldbepalingen
Governance/organisatie	Ja	Er wordt een Functionaris Gegevensbescherming (FG) aangesteld). Afdelingshoofden dienen te monitoren of persoonsgegevens zorgvuldig verwerkt worden.
Werkprocessen/techniek	Ja	Afspraken met externen over gegevensverwerking worden vastgelegd in een bewerkersovereenkomst. Het gebruik van systemen waarin persoonsgegevens worden verwerkt, wordt gelogd. Ten aanzien van ieder proces en informatiesysteem vindt dataclassificatie plaats.
Bewustzijn/menskant	Ja	Kennisoverdracht is essentieel voor het realiseren van bewustwording Er zijn specifieke functionarissen benoemd die informatiebeveiliging onder de aandacht brengen bij medewerkers.

1.5 / Privacy by Design

Werken aan privacy tijdens ontwikkeling (nieuwe) producten en diensten

[20] Wanneer andere partijen gegevens van de gemeente delen, worden bij het aangaan van de overeenkomst afspraken gemaakt over de wijze waarop met gegevens wordt omgegaan, of er wordt een bewerkersovereenkomst afgesloten.

[21] Beleid gegevensbescherming, p. 3.

[22] Beleid gegevensbescherming, p. 3.

De gemeenten Leiden en Leiderdorp werken via Privacy by Design, een methodiek waarbij al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht wordt besteed aan privacy verhogende maatregelen en dataminimalisatie. Deze methodiek is opgenomen in het beleidsdocument Privacy by Design van 19 juli 2016.[23]Het document 'Privacy by design' betreft een (uitgebreide) checklist voor nieuwe informatiesystemen of grote wijzigingen in systemen.[24] Deze checklist geldt ook als toetsingskader voor bestaande systemen. De check/toets wordt uitgevoerd door de Functionaris Gegevensbescherming en/of privacy beheerder.[25]

[23] Privacy by Design, p. 1.

[24] Privacy by Design, p. 3.

[25] Privacy by Design, p. 3.

2 Organisatie

In dit hoofdstuk wordt ingegaan op hoe de organisatie van de gemeenten Leiden en Leiderdorp op het gebied van digitale veiligheid is ingericht. Welke functies en rollen bestaan er met betrekking tot digitale veiligheid, hoe werkt de samenwerking in Servicepunt71, en functioneert de organisatie goed? Er is daarbij zowel aandacht voor de governance op papier als in de praktijk.

De volgende deelvragen staan centraal in dit hoofdstuk:

Organisatie

3. *Hoe is de informatiebeveiligingsfunctie ingericht?*
4. *Is er sprake van een goed georganiseerde informatiebeveiligingsfunctie?*

2.1 / Samenvatting

In hoofdstuk 1 werd al beschreven dat de algemene verantwoordelijkheden op het gebied van digitale veiligheid zijn opgenomen in beleid van de gemeenten Leiden en Leiderdorp. Aan deze rollen zijn taken uit de beleidscyclus gekoppeld.

De governance van de gemeenten Leiden en Leiderdorp op het gebied van digitale veiligheid is in transitie. De komende jaren zal er ten aanzien van de governance dus nog het een en ander veranderen. Meer medewerkers die betrokken zijn bij digitale veiligheid gaan werken voor de Leidse Regio in plaats van voor afzonderlijke gemeenten. In deze lijn is de uitvoering van informatiebeveiliging regionaal belegd, bij Servicepunt71. Verder zijn medewerkers die verantwoordelijk zijn voor de ondersteuning, advisering en toetsing van privacyvraagstukken georganiseerd in een regionaal team, hoewel zij nog in dienst zijn bij de gemeente Leiden. Niet alle medewerkers die betrokken zijn bij digitale veiligheid gaan werken voor de Leidse Regio; zowel de gemeente Leiden als de gemeente Leiderdorp heeft een eigen Chief Information Security Officer in dienst. De Functionaris Gegevensbescherming en Chief Information Officer zijn wel werkzaam op regioniveau. Op bestuurlijk niveau ligt de verantwoordelijkheid voor digitale veiligheid bij de portefeuillehouder bedrijfsvoering.

In het onderzoek is zichtbaar dat de functionarissen onderling contact hebben, dat ze werken aan verbetertrajecten op het gebied van mens en techniek en dat de FG en CISO een aanspreekpunt zijn voor zowel het bestuur als voor medewerkers uit de organisatie. Er wordt grotendeels gewerkt volgens de ingerichte governance-structuur; deze wordt werkbaar gevonden. In de praktijk zijn er kleine aanpassingen. Dit heeft te maken met de ontwikkeling van de samenwerking in de Leidse regio op het gebied van informatiebeveiliging.

Organisatie	
1. De rollen en verantwoordelijkheden op het gebied van informatieveiligheid/privacy zijn vastgelegd. 2. Er is een CISO, CIO en FG aangesteld. 3. Voor medewerkers binnen de gemeenten is er een duidelijk aanspreekpunt op het gebied van informatieveiligheid.	1. Voldaan, o.a. in de beleidsstukken. 2. Voldaan, deels in regionaal verband. 3. Voldaan, hetzij binnen de afdeling, hetzij centraal in de organisatie.

2.2 / Verantwoordelijkheden digitale veiligheid

Uitvoering Informatiebeveiliging regionaal belegd bij Servicepunt71

Servicepunt71 verzorgt de bedrijfsvoering van de vier gemeenten, waaronder de ICT-infrastructuur. Over het algemeen zijn geïnterviewden van alle organisaties tevreden met de samenwerking op het gebied van digitale veiligheid binnen Servicepunt71.

Servicepunt71 heeft een eigen bestuur, gevormd door bestuurlijke vertegenwoordigers van de vier gemeenten, en de Strategiegroep Gezamenlijke Bedrijfsvoering (SGB), bestaande uit de vier gemeentesecretarissen. Zij krijgen daarbij advies van de Chief Information Officer (CIO). In de interviews werd aangegeven dat veel zaken eerst in het SGB worden besproken, alvorens ze worden doorgeleid naar het bestuur.

Wethouders met portefeuille bedrijfsvoering eindverantwoordelijk, overlap met andere rollen

Samengevat is de (bestuurlijke) verantwoordelijkheid voor digitale veiligheid als volgt ingericht in Leiden en Leiderdorp:

/ burgemeester: integraal verantwoordelijk voor veiligheid
/ portefeuillehouder Bedrijfsvoering: verantwoordelijk voor digitale veiligheid
/ portefeuillehouders: verantwoordelijkheid voor digitale veiligheid binnen de verschillende beleidsdomeinen
/ college: generieke verantwoordelijkheid vanuit collegiaal bestuur
/ gemeentesecretaris: algemene verantwoordelijkheid voor de organisatie.

De verantwoordelijkheden zullen vaak overlappen of samenkomen. De rollen van de burgemeester en wethouder komen samen wanneer binnen de gemeente digitaal iets gebeurt wat uitstraalt op veiligheid buiten de organisatie. In beide gemeenten zijn geen specifieke procedures opgesteld voor een dergelijke (fictieve) situatie, anders dan de reguliere veiligheidsplannen.

Algemene verantwoordelijkheden opgenomen in informatiebeveiligingsbeleid

In het informatiebeveiligingsbeleid van de gemeenten Leiden en Leiderdorp is opgenomen wie welke rollen en verantwoordelijkheid heeft met betrekking tot informatiebeveiliging.[26] De doelstelling van deze organisatiestructuur is het beheren van informatiebeveiliging binnen de ambtelijke organisaties Leiden en Leiderdorp en de gemeenschappelijke regeling Servicepunt71.[27]

/ Het college van Burgemeester en Wethouders is integraal verantwoordelijk voor de beveiliging (beslissende rol) van informatie binnen de werkprocessen van de gemeente.
/ De Directie[28] (in sturende rol) van de gemeente is verantwoordelijk voor kaderstelling en sturing.
/ De clusterdirecties[29] binnen de gemeente (in vragende rol) zijn verantwoordelijk voor de integrale beveiliging van hun organisatieonderdelen.

[26] Informatiebeveiligingsbeleid Gemeente Leiden, p. 9; Informatiebeveiligingsbeleid Gemeente Leiderdorp, p. 12

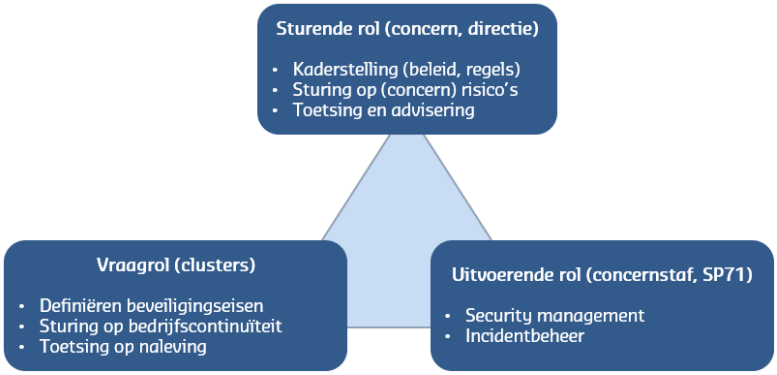
[27] Informatiebeveiligingsbeleid Gemeente Leiden, p. 9; Informatiebeveiligingsbeleid Gemeente Leiderdorp, p. 12

[28] Dit is de term zoals gebruikt door de gemeente Leiden, door de gemeente Leiderdorp wordt dit aangeduid als het programmamanagersteam (PMT). Informatiebeveiligingsbeleid Gemeente Leiderdorp, p. 12

[29] Dit is de term zoals gebruikt door de gemeente Leiden, door de gemeente Leiderdorp wordt dit aangeduid als resultaatteams. Informatiebeveiligingsbeleid Gemeente Leiderdorp, p. 12

/ De Concernstaf[30] en de gemeentelijke Service Organisatie Servicepunt71 (ICT, HR, etc., in uitvoerende rol) is verantwoordelijk voor uitvoering.

Figuur 1 Relaties tussen de verantwoordelijkheden[31]



Rollen in ontwikkeling informatiebeveiliging gekoppeld aan verantwoordelijkheden PDCA cyclus

De taken van de genoemde verantwoordelijken (sturen, vragen, uitvoeren) zijn gekoppeld aan de PDCA-cyclus. In onderstaande tabel is aangegeven wat dat concreet betekent voor het takenpakket.

Tabel 1 Rollen verantwoordelijken in PDCA Cyclus[32]

Wie	**Plan:** **Kaderstelling**	**Do:** **Uitvoering**	**Check:** **Controle**	**Act:** **Verbetering**
Sturen: **Directie dagelijkse uitvoering:** **CIO/CISO**	Ontwikkelen van kaders (beleid en architectuur); reglementen; meerjarenplanning.	Inbedding landelijke en EU-richtlijnen, advisering, handreikingen, crisisbeheersing en incident respons.	Controle, audit, pentesten.	Bijsturen: opdrachtverstrekking voor verbeteracties. Rapportage aan directie/ B&W
Vragen: **Alle afdelingen**	Formuleren van beveiligingseisen (classificatie) en opstellen clusterbeleid en beveiligingsplannen.	Stimuleren van beveiligingsbewustzijn bij medewerkers, risico- en bedrijfscontinuïteit-management.	Interne controle (IC), sturen op naleving van regels door medewerkers (gedrag), compliancy.	Verbeteren bedrijfscontinuïteit. Rapportage aan CIO/CISO.
Uitvoeren: **Concernstaf en SP71 uitvoerende rol)**	Beleidsvoorbereiding, technische onderzoeken (marktverkenningen).	Leveren van security management en services (ICT), incidentbeheer, logging, monitoring en advies.	Vulnerability scanning, evaluatie en rapportage.	Uitvoeren verbeteracties. Advies aan de CIO over aanpassingen aan de informatievoorziening.

[30] Dit is de term zoals gebruikt door de gemeente Leiden, door de gemeente Leiderdorp wordt dit aangeduid als het team informatievoorziening. Informatiebeveiligingsbeleid Gemeente Leiderdorp, p. 12

[31] De term 'clusters' wordt gebruikt om een bepaald deel van de organisatie aan te duiden.

[32] Informatiebeveiligingsbeleid gemeente Leiden, p. 10; Informatiebeveiligingsbeleid gemeente Leiderdorp, p. 13.

In dit schema is de FG niet opgenomen, omdat er nog geen FG was op het moment dat het beleid werd vastgesteld. De FG bevindt zich organisatorisch gezien op hetzelfde niveau als de CISO. Leiderdorp kende voorheen een controller informatieveiligheid. Deze functie is vervallen en de taken zijn belegd bij de CISO.

2.3 / Betrokken functies en rollen digitale veiligheid

Transitie naar werken voor de Leidse Regio

De gemeenten Leiden en Leiderdorp en Servicepunt71 zijn in transitie. De transitie staat in het teken van werken voor de Leidse Regio in plaats van werken voor aparte organisaties (de gemeenten en Servicepunt71). In het project VRIS wordt hier ook aandacht aan besteed.

Tijdens interviews bleek dat de informatiemanagers, informatiebeveiligers en privacybeheerders de eerste teams zijn, die zijn gestart met werken volgens het nieuwe werken: voor de Leidse regio. De privacybeheerders in de Leidse regio zijn allen officieel (nog) in dienst van de gemeente Leiden, maar werken voor de regio. De werkwijze, het beleid en de implementatie zijn regionaal afgestemd en voorbereid.

Volgens de geïnterviewden is de planning om stapsgewijs meer medewerkers die nu nog werken voor de afzonderlijke organisaties, zoals bijvoorbeeld functioneel beheerders en applicatiebeheerders, officieel in dienst te nemen bij de Leidse regio. In januari 2019 wordt hierin naar verwachting weer een stap gezet. Het gehele proces duurt waarschijnlijk tot medio 2020.

Regionaal IB&P-overleg
Vanuit het uitvoeringsprogramma Versterken Regionale I-Samenwerking (VRIS) is er een regio-overleg IB&P. Het gezamenlijk (als regio) werken aan opgaven en gestelde doelen wordt vanuit dat overleg geïnitieerd. Dit overleg heeft een hoge frequentie: het streven is om elkaar tweewekelijks te treffen. Van alle bijeenkomsten wordt een verslag gemaakt. Het overleg buigt zich onder meer over de voortgang van maatregelen en over veiligheidsincidenten, zowel binnen de gemeente als bij externe samenwerkingspartners.

Governance privacy georganiseerd in regionaal privacyteam
De governance omtrent privacy is ingevuld in een regionaal privacyteam, sinds medio 2018. Het regionale privacyteam bestaat uit 5 fulltime privacy officers (voorheen: privacybeheerders), aangevuld met tijdelijke inzet of trainees voor specifieke opdrachten. Het privacyteam vormt samen met de regionale Functionaris Gegevensbescherming en twee deeltijd plaatsvervangende FG's, aangevuld met specifieke expertise van thans 2 juristen van Servicepunt71, de regionale privacy-organisatie.

Iedere organisatie die gekoppeld is aan het regionale team heeft een eigen privacybeheerder als contactpersoon.[33]

Elke organisatie heeft eigen betrokkenen voor digitale veiligheid, FG en CIO aangesteld bij de regio

Hoewel de gemeenten Leiden en Leiderdorp regionaal samenwerken en dienstverlening hebben ondergebracht bij Servicepunt71, hebben beide gemeenten een eigen CISO in dienst. Deze kent de verantwoordelijken bij het Servicepunt71, maar weet ook wat er speelt binnen de gemeente. In het informatiebeveiligingsbeleid is de globale taakomschrijving van de CISO's opgenomen. De CISO bevordert en adviseert gevraagd en ongevraagd over informatiebeveiliging en rapporteert eens per kwartaal aan de directie over de stand van zaken.[34] De CISO heeft het overzicht van de digitale systemen binnen de gemeente en onderneemt actie op het moment dat er technische maatregelen nodig zijn voor de versterking van informatiebeveiliging. Na de reorganisatie in het kader van VRIS zal er regionaal nog één CISO zijn.

De Functionaris Gegevensbescherming (FG) en Chief Information Officer (CIO) zijn aangesteld bij de Leidse regio. Zij dragen vanuit die functie een brede verantwoordelijkheid. In het informatiebeveiligingsbeleid is opgenomen dat de CIO namens de clusterdirectie op dagelijkse basis invulling geeft aan de sturende rol door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering.[35] De rol van de FG wordt met name toegelicht in het beleid Gegevensbescherming, wat meer raakt aan privacy. In het beleid is opgenomen dat de FG toezicht houdt op de naleving van de uit de Wbp en de AVG voortvloeiende eisen, toezicht houdt op de naleving van het beleid en informatie geeft en advies uitbrengt over de verplichtingen op grond van de Wbp en de AVG. Concrete voorbeelden van taken die bij deze functie horen zijn het uitdenken van bewustwordingscampagnes, het

[33] Privacy organisatie juli 2018 (gemeenten Leiden en Leiderdorp).

[34] Informatiebeveiligingsbeleid Gemeente Leiden, p. 10.

[35] Informatiebeveiligingsbeleid Gemeente Leiden, p. 10.

inventariseren van verbetermogelijkheden en zorgdragen voor de implementatie van nieuwe wetgeving. De FG bepaalt in het geval van een datalek ook of het nodig is om een melding bij de AP in te dienen. De FG heeft samen met de coördinator informatiebeveiliging de verantwoordelijkheid om structureel te toetsen of de wettelijke eisen en de gemeentelijk richtlijnen op het gebied van privacy en informatiebeveiliging zijn geïmplementeerd en worden uitgevoerd.[36]

In de verschillende interviews bleek dat medewerkers de bovenstaande verantwoordelijken voor digitale veiligheid goed weten te vinden met hun vragen. Dit betreft zowel vragen naar wat er wel en niet mag als verzoeken om mee te denken over hoe een proces ingericht moet worden.

Precieze invulling governance privacy nog niet rond; governance informatiebeveiliging ligt bij VRIS

Tijdens de interviews werd aangegeven dat, doordat de organisaties in de Leidse regio in transitie zijn, nog niet duidelijk is hoeveel fte er uiteindelijk nodig is voor informatiebeveiliging en privacy. Voor privacy is er op dit moment vijf fte privacybeheerders beschikbaar. Aangevuld met de regionale FG, de plaatsvervangend FG's en juridische capaciteit vanuit Servicepunt71, verwachten geïnterviewden dat dit op basis van de huidige inzichten voldoende is voor de regio.

Het is nog niet duidelijk hoeveel fte er beschikbaar komt voor informatiebeveiliging. Het bepalen van het aantal fte's voor informatiebeveiliging is opgenomen in het programma VRIS en is afhankelijk van de omvang van het regionale takenpakket en de wijze waarop dit wordt georganiseerd.[37]

[36] Beleid gegevensbescherming, p. 6.

[37] Een van de onderdelen van het VRIS project is de versterking van de informatiefunctie. Uitvoeringsprogramma Versterking Regionale I-Samenwerking Leidse Regio – definitief, p.52.

3 Uitvoering

In dit hoofdstuk worden de werkprocessen van de uitvoeringspraktijk in Leiden en Leiderdorp en bijServicepunt71 beschreven. Daarbij is aandacht voor welke (zelf)evaluaties er zijn in de gemeenten, hoe mogelijke verbeterpunten worden opgepakt en of er risico's in beeld zijn ten aanzien van digitale veiligheid.

De volgende deelvragen staan centraal in dit hoofdstuk:

Beheer (werking)

5. Welke (zelf)evaluaties worden er uitgevoerd omtrent informatieveiligheid en wat zijn hier de uitkomsten van?
6. Hoe worden verbeterpunten, uit (zelf)evaluaties en uit de praktijk, opgepakt?
7. Zijn de belangrijkste risico's op het gebied van opslag, uitwisseling en beveiliging van informatie en in het bijzonder van (bijzondere) persoonsgegevens in beeld?

3.1 / Samenvatting

De gemeenten en het servicepunt hebben verschillende zelfaudits die standaard worden uitgevoerd. De verplichte audits worden uitgevoerd. Daarnaast zijn externe partijen ingehuurd voor het uitvoeren van systeemtesten, phishingtesten en mystery guest-bezoeken.

Vanuit de verschillende zelfevaluaties en de dagelijkse praktijk hebben de gemeenten zicht op een aantal digitale risico's. Ook 'offline' kunnen risico's ontstaan voor digitale veiligheid (zoals het op een briefje bewaren van wachtwoorden of onbekenden mee laten lopen in het gemeentehuis). De gemeenten zijn zich hiervan bewust en handelen daarnaar. Toch blijven er ook veel risico's ongezien. Dit bleek in de praktijktoetsing van dit onderzoek (zie hoofdstuk 5). Dit maakt de organisatie op onderdelen kwetsbaar.

Om de risico's waar wel zicht op is te ondervangen leren de gemeenten van de datalekken die zich voordoen, bespreken zij te nemen acties in verschillende overlegstructuren en bouwen zij natuurlijk voort op de ervaringen uit de praktijk en uit de verschillende zelfaudits. Verbeterpunten die uit de evaluaties en audits volgen worden opgepakt op de plek waar dat het meest passend is. Dat kan centraal zijn, of op een afdeling zelf.

Uitvoering	
1. De gemeente voert jaarlijks een audit of controle uit om te beoordelen of de gemeente 'in control' is op het gebied van informatieveiligheid. 2. De gemeente pakt verbeterpunten die blijken uit onderzoeken, audits of controles op. 3. De gemeente heeft een procedure voor de omgang met incidenten. 4. Mogelijke risico's worden gesignaleerd. Hier wordt aantoonbaar actie op ondernomen. 5. Er wordt een systematiek gebruikt bij de beoordeling of bepaalde risico's wel of niet genomen worden.	1. Voldaan; via ENSIA en aanvullende testen. 2. Deels voldaan, zo blijkt uit gesprekken; maar er zijn geen vastgestelde verbeterplannen aangetroffen in het onderzoek. 3. Voldaan, deze procedure is aangetroffen. 4. Deels voldaan. Een voorbeeld is het overzicht van incidenten, waaraan direct acties worden gekoppeld. Tegelijkertijd zijn er ook veel risico's die onzichtbaar blijven. 5. Voldaan; vooraf vindt een risicoanalyse plaats.

3.2 / Zelfevaluaties

Baselinetoets Privacy By Design

De samenwerkende gemeenten en het Servicepunt71 voeren de baselinetoets BIG 'Privacy by Design' voor de processen binnen de organisaties uit. In de toets wordt het proces van A tot Z beschreven, en worden betrokkenen en hun rechten in kaart gebracht. De toets voldoet aan de wettelijke kaders. Vervolgens zijn er vragenlijsten ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid (BIV) om in te vullen. Op basis daarvan kan een advies ten aanzien van de beveiligingsbehoefte worden opgesteld. De onderzoekers hebben een baselinetoets voor de chatfunctie ELO in kunnen zien als voorbeeld.

ENSIA

Gemeenten rapporteren aan de raad over informatiebeveiliging middels de systematiek van ENSIA (Eenduidige Normatiek Single Information Audit). ENSIA is in het leven geroepen om de verantwoordingslasten ten aanzien van informatieveiligheid te verminderen en de informatie toegankelijker te maken. Het totale proces bestaat uit een voorbereiding, zelfevaluatie, horizontale verantwoording, verticale verantwoording en een evaluatie. Ook in Leiden en Leiderdorp wordt de zelfevaluatie gedeeld met de gemeenteraad.

Afdelingsspecifieke audits

Voor sommige werkterreinen van de gemeente geldt dat er verplichte zelf-audits worden uitgevoerd. Dit is bijvoorbeeld het geval bij de Basisregistratie Persoonsgegevens (BRP). Iedere drie jaar wordt een zelfevaluatie uitgevoerd. Dat kost volgens geïnterviewden veel tijd, maar het levert ook wat op: verbeterpunten die uit de zelfevaluatie blijken worden meegenomen in het jaarplan voor het jaar daarop. De geïnterviewden gaven aan dat het meestal lukt om de verbeterpunten in het eerstvolgende jaar op te pakken, maar niet altijd.

GAP-analyse en visitatiecommissie

In het kader van de BIG (zie ook hoofdstuk 1) is in Leiden 2016 een 0-meting uitgevoerd. In deze GAP-analyse wordt afgevinkt of wel of niet aan de normen uit de Baseline Informatiebeveiliging Gemeenten wordt voldaan. Kort daarna, op 5 oktober 2016, heeft de Visitatiecommissie Informatieveiligheid van de VNG een bezoek gebracht aan de gemeente Leiden. In het verslag van dit bezoek is aangegeven wat de visitatiecommissie positief vond (bijvoorbeeld: regionale samenwerking) en waar nog verbetermogelijkheden lagen (bijvoorbeeld: het college en de raad structureel deelgenoot maken van het gesprek over informatieveiligheid, door bij aanpalende thema's als dienstverlening en transparantie duidelijk te maken welke dilemma's spelen). Naar aanleiding van de gap-analyse en deze tips is een actieplan opgesteld. In het jaarverslag 2017 stelt de gemeente dat eind 2017 circa 50% van de beveiligingsmaatregelen geïmplementeerd waren en dat de implementatie in 2018 wordt voortgezet. De manieren waarop de organisatie de raad en het college gespreksgenoot maakt rondom het thema digitale veiligheid zijn beschreven in hoofdstuk 4.

Incidenteel: externe test van de systemen

In het voorjaar van 2017 is een zogenaamde 'Penetratietest en vulnerability assessment' uitgevoerd bij Servicepunt 71. Hier is een externe partij voor ingehuurd die een black-box extern, intern en wifi-assessment op niveau 2 hebben uitgevoerd op de bedrijfsomgeving. Het doel was 'om een overzicht te krijgen van de status van beveiliging van de getoetste omgeving en van de eventuele kwetsbaarheden die aanwezig zijn.'[38]

Uit de toetsing en analyse bleek dat Servicepunt71 een hoog bedrijfsrisico liep, door een aantal makkelijk te misbruiken kritische en hoge kwetsbaarheden op de assets en services in de getoetste omgeving. Het bedrijf dat de toets uitvoerde gaf hierbij aan dat het risico te ondervangen is en met de juiste maatregelen tot een gemiddeld of laag risico kan worden teruggebracht.

Voor de gemeente Leiden is in het voorjaar van 2017 een 'social engineering' onderzoek uitgevoerd. Hierbij werd gebruik gemaakt van phishing, en van een mystery guest om drie locaties van de gemeente binnen te dringen. De phishingmail, verstuurd vanuit het Servicepunt71, leverde 258 unieke accountgegevens van medewerkers op, om mee in te kunnen loggen op de omgeving van de gemeente Leiden. Wel werden ruim 280 meldingen van de mailing door medewerkers gemaakt bij het servicepunt. Het onderzoek op de fysieke beveiliging toonde aan dat gemakkelijk toegang kon worden verkregen tot de onderzochte objecten, en dat er gevoelige informatie eenvoudig bereikbaar was (op papier en via onbeheerde niet-vergrendelde computers). [39] In het jaarverslag 2017 staat vermeld dat op basis van de bevindingen uit dit onderzoek verschillende aanpassingen zijn doorgevoerd.

In de Boardletter van 2016 gaf accountant Ernst & Young aan niet uit te kunnen gaan van een aantal ICT-systemen voor hun controle. Hier zijn door D66 en de VVD ook raadsvragen over gesteld. Het college formuleerde een plan van aanpak voor de benodigde verbeteringen. Dit plan van aanpak werd globaal ook weergegeven in de reactie op de Boardletter 2016. Naar aanleiding van de rapportage van Ernst & Young is er in projectvorm aan de opvolging van de aanbevelingen voor de ICT-systemen gewerkt. Bij dit project is ook een aantal andere applicaties betrokken, waarvoor nog niet eerder een IT audit was afgenomen. Hierbij is gekeken naar de 'opzet' en het 'bestaan' van de beheersmaatregelen aan de hand van de minimale normen voor IT beheersing die toezien op logische toegangsbeveiliging en wijzigingenbeheer. Van het project is een verslag gemaakt, waarin de voortgang op de aanbevelingen werd bijgehouden.[40]

[38] Auditrapportage 'Penetratietest en vulnerability assessment' van SECWATCH, 24 mei 2017, managementsamenvatting.

[39] Rapportage 'Social engineering gemeente Leiden', ESET, voorjaar 2017.

[40] IT audit juni 2017, Opvolging aanbevelingen IT-audits van negen applicaties 2013-2016 & audit vier overige applicaties.

3.3 / Risico's in beeld

Technische risico's

De technische risico's zijn door Guardian 360 in beeld gebracht. Hiervoor verwijzen wij naar hoofdstuk 5.

Risico's t.a.v. menselijk gedrag

Naast de technische risico's zijn de beide gemeenten zich bewust van het feit dat menselijk handelen een risico op kan leveren voor informatieveiligheid. In de interviews werden hiervoor als voorbeelden met name genoemd het niet vergrendelen van computers, het mee laten lopen van een onbekende binnen het gemeentehuis, het bewaren van wachtwoorden op zichtbare plekken of het delen van gegevens met personen die dergelijke gegevens eigenlijk niet in mogen zien. De gemeente werkt op verschillende manieren aan het verhogen van bewustzijn ten aanzien van informatieveiligheid, zodat de risico's die het menselijk handelen vormen voor digitale veiligheid beperkt blijven. Hoe de gemeente dat doet, wordt in paragraaf 3.4 besproken.

3.4 / Risicobeheersing

Er zijn verschillende manieren waarop de gemeente risico's ondervangt. Deels staan een goed informatiebeveiligingsbeleid en een sterk georganiseerde informatiebeveiligingsfunctie ten dienste van risicobeheersing. In 3.2 is al beschreven hoe er wordt omgegaan met de uitkomsten van zelfevaluaties of steekproeven. In deze paragraaf wordt aandacht besteed aan een aantal overlegstructuren die specifiek relevant zijn voor incidenten en daaropvolgende maatregelen. Daarnaast wordt de 'offline' kant van informatiebeveiliging behandeld.

Overlegstructuren incidenten

Daarnaast is er voor interne crises per gemeente een "Kernteam IB", bestaand uit CISO, security functionaris van servicepunt71, relevante experts en de gemeentelijke communicatie-afdeling.[41] Dit team komt uitsluitend bijeen in geval van grote incidenten of calamiteiten. Geïnterviewden geven verder aan dat de burgemeesters betrokken worden op het moment dat de algemene veiligheid in de gemeente in het geding is. Dit geldt zowel voor de gemeente Leiden als Leiderdorp.

De CISO van de gemeente meldt incidenten bij de wethouder met de portefeuille dienstverlening indien hij/zij dit nodig acht. Dit is op basis van eigen inschatting van de CISO, er zijn hiervoor in beide gemeenten geen vaste afspraken gemaakt.

Omgang met incidenten/datalekken

Het beleidsdocument Informatiebeveiligingsbeleid wijdt een hoofdstuk aan beveiligingsincidenten, [42] maar dit onderwerp is verder uitgewerkt in het 'Proces melden datalek en beveiligingsincident', dat per 1 maart 2016 in werking is getreden (versie februari 2016). Dit document geeft voor alle mogelijk te nemen stappen (zoals 'melding ontvangen' of 'Bepalen welke repressieve en correctieve maatregelen worden getroffen') een uitleg/stappenplan, inclusief het benoemen van wie waarvoor verantwoordelijk is. Iedereen is bevoegd een incident te melden.[43] De Chief Information Officer (CIO) is ambtelijk eigenaar van het proces melden datalek.[44]

Bij elke melding wordt in ieder geval de CISO geïnformeerd en de verantwoordelijke manager, en wordt de CIO geraadpleegd en geïnformeerd. Wanneer er persoonsgegevens in het spel zijn, wordt ook de FG betrokken en wordt een 'crisisteam' ingesteld dat 'bestaat uit verantwoordelijken en specialisten'[45]. De specialisten kunnen van Servicepunt71 zijn. De FG bepaalt [46]aan de hand van de richtlijn van de Autoriteit Persoonsgegevens of een melding aan de AP noodzakelijk is.

[41] Informatiebeveiligingsbeleid Gemeente Leiden, p. 12.

[42] Informatiebeveiligingsbeleid Gemeente Leiden, p. 32-33.

[43] Proces melden datalek en beveiligingsincident, versie februari 2016, p. 3.

[44] Proces melden datalek en beveiligingsincident, versie februari 2016, p. 4.

[45] Proces melden datalek en beveiligingsincident, versie februari 2016, p. 11.

[46] Integriteits- en geheimhoudingsverklaring.

Bij Servicepunt71 wordt jaarlijks een overzicht van de beveiligingsincidenten en datalekken gemaakt. Per incident wordt bijgehouden wat er is gebeurd, of er een melding gemaakt moest worden bij de AP, welke vervolgactie is ondernomen en om hoeveel betrokkenen het gaat. In 2017 traden de volgende incidenten op:

	Aantal beveiligingsincidenten	Aantal meldingen bij de AP
Leiden	28	11
Leiderdorp	5	3
Servicepunt71	2	1

De meeste datalekken hebben een menselijke oorzaak. Daarin verschillen de gemeentes niet van andere organisaties. In de interviews werd aangegeven dat de ervaringen en leerpunten rond een opgelopen datalek over het algemeen door de manager binnen het team worden besproken. Daarbij gaat het niet om 'naming and shaming' maar om het leermoment. De geïnterviewden hebben het beeld dat medewerkers zich voldoende veilig voelen om een datalek te melden. Op de afdelingen van de gemeenten liggen flyers over wat te doen bij een datalek. Dat draagt ook bij aan het bewustzijn ten aanzien van het belang van melden en bespreken van datalekken.

'Offline risicopreventie': bewustwording medewerkers

Uit de praktijktoetsing (zie hoofdstuk 5) blijkt dat de mate van bewustzijn bij medewerkers verschilt. De gemeente monitort het bewustzijn van medewerkers omtrent digitale veiligheid niet structureel, maar werkt wel op verschillende manieren aan het bewustzijn van medewerkers: met werkafspraken, afstemmingsmomenten en trainingsmomenten.

Werkafspraken

Er zijn zes gouden regels voor informatiebeveiliging opgesteld die gelden voor de organisaties van de Leidse regio. Om deze te verspreiden zijn er posters opgehangen bij bijvoorbeeld koffiecorners. In het jaar 2018 hebben er verschillende posters gehangen om medewerkers bewust te maken van informatiebeveiliging. Het voornemen is om deze informatie ook op andere manieren te verspreiden, bijvoorbeeld door de posterinformatie als screensavers van medewerkers in te stellen.

Eén van de gouden regels is opletten met het verwerken van persoonsgegevens op papier. Wanneer dit papier niet beveiligd wordt opgeborgen is er strikt genomen sprake van een datalek. Er zijn daarom maatregelen om fouten met werken op papier tegen te gaan. Ten eerste wordt printen ontmoedigd. Daarnaast kunnen de werknemers alleen printen als zij zelf fysiek bij de printer aanwezig zijn. Hierdoor blijven documenten niet te lange tijd onbeheerd in de printer liggen. Daarnaast worden de risico's van werken op papier en menselijk handelen in het algemeen besproken tijdens werkoverleggen.

Daarnaast is nog relevant om te vermelden dat alle medewerkers in de twee gemeenten bij indiensttreding een integriteits- en geheimhoudingsverklaring ondertekenen. Dit biedt ook gedragsregels ten aanzien van geheimhouding, toegang tot gebouwen, omgang met informatie en bedrijfsmiddelen, integriteit, omgangsvormen en inzage in gegevens.

Afstemmingsmomenten

De CISO, FG en/of privacybeheerders schuiven regelmatig aan bij werkoverleggen om informatiebeveiliging te bespreken met medewerkers. Meestal worden dan praktische zaken besproken, bijvoorbeeld het opstellen van het register gegevensverwerking. Om bewustwording te vergroten zijn er in diverse teams presentaties gegeven door de privacybeheerders. Sommige afdelingen hebben de ambitie om meer aandacht te besteden aan informatiebeveiliging, dit wordt dan ondersteund door de CIO, FG en CISO uit de betreffende organisatie. Een voorbeeld hiervan is dat een afdeling een scorebord ophing dat de voortgang of scores van de afdeling bijhield op het gebied van schermvergrendeling.

Trainingsmomenten

In de interviews werd aangegeven dat er geen vaste cursussen of trainingen worden gevolgd door individuele professionals. Wel wordt het bewustzijn ten aanzien van digitale veiligheid op andere manieren getraind.

Ter promotie van informatiebeveiliging maken de organisaties uit de Leidse regio gebruik van producten van de Informatiebeveiligingsdienst (IBD) voor Nederlandse gemeenten. Een voorbeeld hiervan is het spel Crisisgame. Dit is een digitaal spel dat door teams kan worden gespeeld waarbij een datalek wordt gesimuleerd en waarin bewustwording het doel is.

Om enerzijds bewustwording te creëren en anderzijds de kennis van medewerkers te testen zijn incidentenprocedures getest op meerdere afdelingen. Het proces is daarbij vergelijkbaar met een brandtest. De uitkomst was dat de kennis van de procedure vooraf nog niet bij iedereen paraat is. De procedure is vervolgens met de medewerkers doorgesproken.

In de periode januari tot en met mei 2018 zijn er daarnaast ook 1-daagse trainingen ‘Privacy in de Praktijk’ verzorgd die plaatsvonden op de locatie van SP71. De training was op basis van inschrijving beschikbaar voor alle medewerkers van de Leidse regio. De training is door ongeveer 100 medewerkers gevolgd, die deze informatie vervolgens verspreid hebben binnen hun organisatie. Aanvullend op deze training zijn er binnen diverse teams presentaties verzorgd, waarbij aandacht is gegeven aan de basisbeginselen en bewustwording.

4 Rol van de raad

Dit hoofdstuk behandelt de rol van de gemeenteraad. In losse paragrafen wordt besproken welke informatievoorziening plaatsvindt richting de gemeenteraad en hoe de gemeenteraad haar rol kiest of krijgt in het kader van digitale veiligheid.

De volgende deelvragen staan centraal in dit hoofdstuk

Rol van de raad

8. *Welke informatie ontvangt de raad over informatieveiligheid?*
9. *Welke rol kiest de raad omtrent informatieveiligheid (vragen stellen, moties indienen, etc)?*

4.1 / Samenvatting

De gemeenteraden van Leiden en Leiderdorp ontvangen informatie over digitale veiligheid in hun gemeente. Dit gebeurt op vaste momenten (in het kader van ENSIA), en incidenteel. Zo ontving de gemeenteraad van de gemeente Leiden informatie over de visitatiecommissie informatieveiligheid, en ontvingen raadsleden uit de gemeente Leiderdorp informatie over de AVG en de gevolgen hiervan voor de gemeente. Ook op andere momenten en manieren is er in de radenaandacht voor digitale veiligheid, bijvoorbeeld door raadsvragen die zijdelings verband houden met het thema (afvalpassen, sociaal domein). Voor het eigenstandige thema digitale veiligheid is weinig aandacht in de raden. Dit komt vermoedelijk omdat het onderwerp wordt gezien als onderdeel van de bedrijfsvoering.

Raad	
1. De gemeenteraad besteedt aandacht aan het onderwerp informatieveiligheid. 2. De gemeenteraad wordt actief geïnformeerd over de borging van informatieveiligheid binnen de gemeente en bij organisaties waar zij mee werkt. 3. Vragen vanuit de gemeenteraad over dit onderwerp worden adequaat beantwoord. 4. De organisatie weet wat er vanuit ENSIA nodig is om goed te rapporteren aan de gemeenteraad en handelt hiernaar.	1. In Leiden: voldaan, er worden vragen gesteld en er is een bijeenkomst geweest. In Leiderdorp: deels voldaan, er is een bijeenkomst geweest maar de raad stelt zelf weinig vragen. 2. Deels voldaan, het betreft vaak informatie op hoofdlijnen. Bij incidenten wordt de raad wel geïnformeerd. 3. In Leiden: voldaan, de schriftelijke beantwoording van vragen is helder. In Leiderdorp worden geen vragen over het thema zelf gesteld. 4. Voldaan, de ENSIA rapportages voldoen aan de eisen die daar voor gesteld zijn.

4.2 / Informatievoorziening aan de raad

Gemeenteraden Leiden en Leiderdorp ontvangen informatie in het kader van de ENSIA

Zowel de gemeenteraad van Leiden als Leiderdorp ontvangt jaarlijks, in het kader van verticale verantwoording, informatie over de uitkomsten van de ENSIA. Daarbij ontvangen de raden ook de bijbehorende collegeverklaring. In 2017 werd door beide gemeenten de verklaring afgelegd voor SUWI en voor DigiD. [47,48] Onderdeel van de ENSIA waren toetsing aan de Basisregistratie Adressen en Gebouwen (BAG) en Basisregistratie Grootschalige Topografie (BGT). De verantwoordingsrapportages over de BGT en BAG zijn gedeeld met de gemeenteraden van Leiden en Leiderdorp.[49,50]

Gemeenteraden ontvangen met name informatie op belangrijke momenten uit P&C-cyclus

Geïnterviewden geven aan dat de gemeenteraden van Leiden en Leiderdorp voornamelijk op belangrijke momenten uit de P&C-cyclus informatie over digitale veiligheid ontvangen.

Een van de verplichtingen die volgt uit de ENSIA is dat er in het jaarverslag aandacht moet zijn voor informatieveiligheid. Jaarlijks ontvangen de gemeenteraden van de gemeenten Leiden en Leiderdorp het jaarverslag van de ambtelijke organisatie. In het jaarverslag van beide gemeenten is in de paragraaf bedrijfsvoering aandacht voor informatieveiligheid.[51] In Leiden wordt daarnaast ook aandacht besteed aan het thema gegevensbescherming in het jaarverslag.

Indien nodig krijgen de gemeenteraden tussentijds informatie

De gemeenteraden van zowel Leiden als Leiderdorp worden, als dit nodig is, ook buiten de belangrijke momenten uit de P&C cylcus om incidenteel geïnformeerd over digitale veiligheid.

Het college van de gemeente Leiden informeerde de raad bijvoorbeeld via een wethoudersbrief over het verslag van de visitatiecommissie informatieveiligheid.[52] Andere stukken die gedurende de P&C-cyclus binnenkomen, maar niet belangrijk genoeg zijn om direct te delen met de raad, worden volgens geïnterviewden opgespaard tot de rapportage momenten uit de P&C-cyclus.

Het college van de gemeente Leiderdorp verstuurt ook tussentijds informatie naar de raad. Zo verstuurde het college bijvoorbeeld op 14 november 2017 een informatiebrief over de AVG naar de gemeente.[53] In de brief is onder andere uitgelegd wat de AVG is en wat de belangrijkste gevolgen zijn voor de gemeente.

Informatie over datalekken

In de beide gemeenten zijn de raden in het verleden geïnformeerd rondom datalekken of kwetsbaarheden in de informatiebeveiliging. Rondom de gemeenteraadsverkiezingen werd bijvoorbeeld bekend dat dat er een datalek had plaatsgevonden binnen de gemeente Leiderdorp. Daar ontstond de nodige ophef over. De gemeenteraad en het college van de gemeente Leiderdorp hebben toen contact gehad. Ook in Leiden informeerde het college de raad over een kwetsbaarheid, toen de accountant hier opmerkingen over plaatste in de Board Letter 2016 (zie paragraaf 3.3).

---

[47] Assurancerapport ENSIA 2017 DigiD en Suwinet – 27 maart 2018; Collegeverklaring ENSIA 2017 – bijlage; Collegeverklaring ENSIA 2017 – 2 mei 2018; Collegeverklaring ENSIA 2017 – bijlage;

[48] Raad informeren over ENSIA – 14 juni 2018; Assurancerapport ENSIA 2017 DigiD en Suwinet – 15 maart 2018; Assurancerapport ENSIA 2017 DigiD en Suwinet bijlage C1 en C2 – 15 maart 2018.

[49] Verantwoordingsrapportage BAG – gemeente Leiden; Verantwoordingsrapportage BGT – gemeente Leiden.

[50] Verantwoordingsrapportage BAG – gemeente Leiderdorp; Verantwoordingsrapportage BGT – gemeente Leiderdorp.

[51] Tekst uit paragraaf bedrijfsvoering jaarverslag 2017 – gemeente Leiden; Jaarverslag gemeente Leiderdorp 2016.

[52] Wethoudersbrief visitatiecommissie – 18 januari 2017.

[53] Brief van het college over AVG – 14 november 2017

Mogelijkheden voor sessies en workshops over digitale veiligheid voor gemeenteraden

In de inwerkprogramma's van de raden is aandacht besteed aan digitale veiligheid. In de beide gemeentes gebeurde dit als onderdeel van een ander thema. Daarnaast Worden de gemeenteraden uit de Leidse regio in een informatiebijeenkomst geïnformeerd over het VRIS-programma. De bijeenkomsten in Leiden en Oegstgeest hebben al plaatsgevonden, Leiderdorp en Zoeterwoude volgen nog.

"Informatievoorziening richting gemeenteraad Leiden moet beter"

In interviews met collegeleden werd aangegeven dat de informatievoorziening richting de gemeenteraad niet optimaal is. Het college heeft echter zelf niet altijd voldoende of de juiste informatie om de gemeenteraad te informeren. Dit komt omdat digitale veiligheid volgens de geïnterviewden snel wordt geschaard onder techniek en daarom wordt weggeorganiseerd bij de leden van het college. Hierdoor krijgt het college onvoldoende grip op het thema om de raad uitgebreid te informeren.

De informatievoorziening aan de gemeenteraad zou volgens geïnterviewden beter kunnen door op een simpele en inzichtelijke wijze te rapporteren. Rapportages kunnen verbeterd worden door inzicht te bieden in de afzonderlijke aspecten van digitale veiligheid en de voortgang inzichtelijk te maken door, bijvoorbeeld, te werken met het toekennen van kleuren ('stoplichtmodel'). Het verbeteren van de rapportages is een punt waaraan de gemeente Leiden werkt in het kader van de implementatie van de BIO.

De geïnterviewden zien een rol weggelegd voor de CIO voor de informatievoorziening aan de raad. De CIO zou op specifieke momenten, bijvoorbeeld een jaar na de invoering van de AVG of aanstelling van de FG, kunnen rapporteren over de voortgang van digitale veiligheid.

"Gemeenteraad Leiden heeft niet alle informatie nodig"

Volgens geïnterviewden van de gemeente Leiden heeft de gemeenteraad niet alle informatie nodig die binnen de ambtelijke organisatie aanwezig is. Het is vooral belangrijk dat de juiste informatie op een inzichtelijke manier wordt gerapporteerd. De gemeente Leiden heeft nog niet helemaal duidelijk wat zij wel en niet willen rapporteren. Een terugkerend vraagstuk is volgens geïnterviewden bijvoorbeeld waarover er wel en waarover er niet gerapporteerd moet worden aan de raad. In hoeverre geef je je kwetsbaarheden op het gebied van digitale veiligheid weer in een rapport en hoe toegankelijk maak je zo een rapport?

4.3 / Rol van de Raad

Gemeenteraad Leiden stelt actief vragen over digitale veiligheid, college antwoord met regelmaat schriftelijk

Geïnterviewden ervaren de gemeenteraad van de gemeente Leiden als actief op het thema informatiebeveiliging. De gemeenteraad van de gemeente Leiden stelde in de vorige raadsperiode regelmatig vragen over digitale veiligheid. Dit kunnen vragen zijn over incidenten of de status van digitale veiligheid[54], maar ook over de AVG werden veel vragen gesteld door leden van de raad. Het college neemt tijd voor deze vragen. De gemeenteraad stelt volgens geïnterviewden met name vragen over casussen die voortvloeien uit een gebrek aan digitale veiligheid. Het college reageerde in de afgelopen jaren meermaals schriftelijk op vragen van de gemeenteraad over digitale veiligheid. [55]

[54] Antwoord college van B&W op schriftelijke vraag VVD Leiden – 30 januari 2018; Antwoord college van B&W op schriftelijke vagen VVD en D66 Leiden – 12 januari 2017; Antwoord college van B&W op schriftelijke vagen D66 Leiden – 5 juli 2016

[55] Link naar beantwoording raadsvragen over de AVG – 2018.

Gemeenteraad Leiderdorp stelt weinig vragen over digitale veiligheid

Volgens geïnterviewden stelt de gemeenteraad van de gemeente Leiderdorp weinig vragen over informatiebeveiliging. De vragen van de raad gaan meer in op casuïstiek binnen beleidsterreinen (afval, sociaal domein) dan op de bedrijfsvoering omtrent digitale veiligheid. Raadsleden discussiëren volgens geïnterviewden ook over wat zij vinden dat er aan informatie gedeeld mag worden. Al met al gebruikt de gemeenteraad meer zijn controlerende functie dan de kaderstellende functie.

Gemeenteraad Leiden is zich bewust van zijn gebruikersrol, gemeente faciliteert

Geïnterviewden geven aan dat de gemeenteraad zich over het algemeen bewust is van digitale veiligheid, en ook van zijn eigen gebruikersrol. Over het algemeen worden door gemeenteraden openbare stukken besproken, wanneer er toch vertrouwelijke stukken worden besproken gaan de raadsleden van de gemeente Leiden hier bewust mee om volgens geïnterviewden.

De stukken voor de gemeenteraden van de gemeente Leiden en de gemeente Leiderdorp worden gedeeld via raadsinformatiesystemen (RIS). Ter beveiliging van e-mailverkeer hebben raadsleden van de gemeente Leiden een e-mailaccount van de gemeente, zodat raadsleden niet via persoonlijk e-mailadres hoeven te mailen. De gemeente heeft echter geen controle over hoe raadsleden communiceren. Er zijn volgens geïnterviewden plannen om het veilig mailen systeem ZIVVER aan de raad beschikbaar te stellen, zodat zij net als medewerkers van de gemeente veilig documenten kunnen verzenden. Daarnaast werkt een plaatsvervangend FG aan een document waarin onder andere aandacht is voor digitale veiligheid. De plaatsvervangend FG heeft ook een presentatie over privacy (waaronder digitale veiligheid) gegeven op verzoek van de raadscommissie Rekeningen.

Ook gemeenteraad Leiderdorp bewust van gebruikersrol

Ook de raad van Leiderdorp is zich volgens geïnterviewden bewust van zijn gebruikersrol. De raad bespreekt over het algemeen openbare stukken, wanneer er toch vertrouwelijke stukken worden besproken gaan de raadsleden van de gemeente Leiderdorp hier bewust mee om volgens geïnterviewden. Bij het aanbieden van de stukken aan de raad wordt meegegeven of de stukken een vertrouwelijk karakter hebben of openbaar zijn. De gemeenteraad van de gemeente Leiderdorp heeft daarnaast als gebruiker een eigen e-mailsysteem, heeft een eigen website en beheert een gesloten en open informatiesysteem. Vertrouwelijke stukken worden opgeslagen in het besloten informatiesysteem. Geïnterviewden geven op basis van eigen ervaring aan dat raadsleden zich zeer bewust zijn van het feit dat ze deze informatie niet mogen delen of lekken. Ook kunnen leden van de gemeenteraad kunnen documenten opvragen, maar mogen deze alleen inzien op het gemeentehuis, onder controle van een medewerker van de gemeente. Dit voorkomt lekken volgens geïnterviewden.

5 Praktijktoetsing

In dit hoofdstuk staan de resultaten van de praktijktoetsing weergegeven. Hierbij heeft de rekenkamercommissie in afstemming met Guardian360 bepaald welke informatie openbaar gedeeld kon worden en op welk niveau. Dit in verband met de gevoeligheid van de informatie en de mogelijke kwetsbaarheden. De volgende deelvragen staan centraal in dit hoofdstuk:

Praktijktoetsing

10. In hoeverre is een kwaadwillende derde in staat om de informatiesystemen binnen te dringen?
    a. Kan deze derde via oneigenlijke middelen toegang tot specifieke mail- en agendagegevens verkrijgen?
    b. Kan deze derde via oneigenlijke middelen toegang tot beheers en/of back-end systemen van webapplicaties krijgen?
11. Is de rollen- en rechtenstructuur zo ingericht dat een vertrouwde gebruiker alleen toegang heeft tot die systemen waar hij/zij toegang zou moeten krijgen?
12. Voldoen de relevante informatiesystemen aan de technische eisen die gesteld worden binnen de BIG en DIGID 2.0?
13. Zijn de medewerkers zich voldoende bewust van de gevaren van phising e-mails en alerts wanneer zij een dergelijke e-mail ontvangen?

5.1 / Samenvatting

In afstemming met beide gemeenten en Servicepunt 71 hebben ethisch hackers een praktijktoetsing uitgevoerd. Deze bestond uit interne en externe penetratietesten en een phishingtest. Door een praktijktoetsing uit te voeren, worden bestaande risico's in beeld gebracht én kunnen er technische oplossingen worden geboden. Uit de externe penetratietest blijkt dat het risico op de onderzochte systemen laag is. Uit de interne penetratietest blijkt een hoger risico; een kwaadwillende van binnenin – iemand die toegang heeft tot het kantoornetwerk van de gemeente – kan via een aantal wegen toegang krijgen tot informatiesystemen waarvoor specifieke toestemming of autorisatie nodig is. Deze kwetsbaarheden zijn benoemd, evenals de beheersmaatregelen om ze te repareren. Uit de phishingtest komt een middelhoog risico naar voren. De valse e-mail die is verstuurd, is een beperkt aantal keer geopend, maar verschillende medewerkers hebben snel melding gemaakt van de e-mail. Ook zijn er snel preventieve technische maatregelen aanwezig, waardoor de e-mail bij een deel van de medewerkers niet is aangekomen.

5.2 / Inleiding en werkwijze

Korte introductie Guardian360

Bij Guardian360 werken gecertificeerde security engineers met ervaring op het gebied van het beveiligen van complexe IT-infrastructuren. Guardian360 voert regelmatig penetratietesten uit bij bijvoorbeeld gemeenten, ziekenhuizen en zorginstellingen waarmee ethisch hackers van Guardian360 toegang proberen te krijgen tot de IT-infrastructuur van de opdrachtgever. Aan de hand van de bevindingen van Guardian360 kunnen opdrachtgevers de informatiebeveiliging van hun organisatie verbeteren.

Gehanteerde werkwijze

Het doel van de door Guardian360 uitgevoerde testen is het identificeren en verifiëren van kwetsbaarheden in applicaties, beschikbare services en mogelijke manieren om data te verzamelen of binnen te dringen op de (netwerk) infrastructuur van de Gemeente Leiden en Gemeente Leiderdorp. Naast het in kaart brengen van deze kwetsbaarheden zijn oplossingen beschreven om de gevonden kwetsbaarheden te verhelpen.

Om zwakheden in de security van de applicaties en infrastructuur te identificeren, zijn verschillende scans en handmatige controles uitgevoerd. Hierbij is uitgegaan van hoe een aanvaller de infrastructuur zou benaderen.

De uitgevoerde testen zijn onder te verdelen in drie fases;

1. Een externe test waarbij vanaf het internet de veiligheid van twee (web)applicaties en de onderliggende servers is onderzocht.
2. Een interne test waarbij vanuit de kantooromgeving is gezocht naar kwetsbaarheden in het draadloze netwerk, het kantoornetwerk en zes interne (web)applicaties en de onderliggende servers.
3. Een phishingtest waarbij geprobeerd is om de inloggegevens van een specifieke gebruikersgroep te achterhalen via e-mail.

Toelichting op de gekozen infrastructuur, systemen en applicaties

Binnen de beschikbare tijd voor de penetratietest was het niet mogelijk om het gehele netwerk en alle applicaties te onderzoeken op kwetsbaarheden. Daarom is in overleg tussen de Rekenkamercommissie Leiden-Leiderdorp, Gemeente Leiden, Gemeente Leiderdorp, Servicepunt71, Necker van Naem en Guardian360 een scope van de te onderzoeken infrastructuur, systemen en applicaties vooraf vastgesteld. Hierbij is rekening gehouden met de volgende factoren:

- Zowel extern (vanaf het internet) bereikbare systemen en intern (vanaf het kantoornetwerk) bereikbare systemen.
- Zowel systemen die alleen door Gemeente Leiden gebruikt worden, systemen die alleen door Gemeente Leiderdorp gebruikt worden en gedeelde systemen die door beide gemeenten gedeeld worden.
- Systemen die gevoelige informatie bevatten en systemen die minder gevoelige informatie bevatten.

Voor het uitvoeren van de phishingtest is een gebruikersgroep gekozen die bij beide gemeenten aanwezig is en gebruik maken van dezelfde interne applicatie.

5.3 / Resultaten penetratietesten

Inleiding

In verband met de vertrouwelijkheid van de gevonden kwetsbaarheden kunnen niet alle bevindingen en details in dit verslag beschreven worden. Desondanks wordt in dit hoofdstuk getracht met enkele voorbeelden een beeld te schetsen van hoeverre een kwaadwillende in staat is om de informatiesystemen van Gemeente Leiden en Gemeente Leiderdorp binnen te dringen.

Resultaten extern bereikbare netwerk en applicaties

Guardian360 heeft geen ernstige kwetsbaarheden gevonden in de onderzochte extern bereikbare applicaties en systemen. Wel worden door Guardian360 een aantal verbeterpunten beschreven in de opgeleverde rapportages.

Resultaten intern bereikbare netwerk en applicaties

Binnen het onderzochte kantoornetwerk van Gemeente Leiden en Gemeente Leiderdorp zijn enkele ernstige kwetsbaarheden gevonden. Tevens zijn er in de onderzochte intern bereikbare applicaties en onderliggende infrastructuur enkele ernstige kwetsbaarheden gevonden. Deze kwetsbaarheden hadden vooral te maken met ontbrekende updates en configuratiefouten van applicaties en systemen.

Kanttekening is wel dat, om deze interne kwetsbaarheden te misbruiken, een aanvaller al toegang moet hebben tot het kantoornetwerk waardoor de kans op misbruik van deze kwetsbaarheden lager in geschat zou kunnen worden. Een aantal voorbeeldscenario's waarbij een aanvaller toegang tot het kantoornetwerk kan krijgen zijn:

- Een kwaadwillende medewerker.

- Inloggegevens die door een gerichte phishingactie zijn achterhaald en vervolgens gebruikt worden om toegang te krijgen tot het Wi-Fi netwerk.
- Een aanvaller die zijn laptop of een draadloze router weet aan te sluiten op een onbewaakte netwerkpoort binnen een van de kantoorpanden.
- Een aanvaller krijgt toegang tot het netwerk via een met virus besmette werkplek van een medewerker of leverancier.

Rollen- en Rechtenstructuur

Guardian360 heeft geconstateerd dat er gebruik wordt gemaakt van verschillende rollen- en rechtenstructuren om toegang tot systemen en applicaties te regelen. Ondanks de aanwezigheid van de rollen- en rechtenstructuur heeft Guardian360 vanuit het interne netwerk zonder gebruikersaccounts toegang verkregen tot systemen waarvoor zij niet geautoriseerd was.

Afwijkingen Baseline Informatiebeveiliging Nederlandse Gemeenten

Van de gevonden kwetsbaarheden is door Guardian360 onderzocht of deze leiden tot een afwijking van de BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten). Hierbij zijn in de onderzochte systemen enkele afwijkingen geconstateerd.

Een van de afwijkingen heeft bijvoorbeeld betrekking op het ontbreken van security updates op meerdere systemen. Voor deze systemen zijn wel security updates door leveranciers beschikbaar gesteld. Dit betekent een afwijking van hoofdstuk 12.6.1 van de Baseline Informatiebeveiliging Nederlandse Gemeenten welke beschrijft; “Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week.”[56]

Verschillen tussen Gemeente Leiden en Gemeente Leiderdorp

Guardian360 heeft geen onderscheid kunnen maken tussen de twee gemeenten in de aanwezige kwetsbaarheden. De gevonden kwetsbaarheden in de onderzochte systemen lijken van vergelijkbare aard te zijn. Dit is vermoedelijk doordat de netwerken, systemen en applicaties van beide gemeenten door dezelfde partij (Servicepunt71) zijn ingericht en beheerd worden en er veelal gebruik gemaakt wordt van dezelfde of vergelijkbare systemen en applicaties.

5.4 / Resultaten phishingtest

Inleiding

Om het bewustzijn van medewerkers voor de gevaren van een phishing e-mail te toetsen heeft Guardian360 een phishing aanval uitgevoerd op een groep gebruikers van Gemeente Leiden en Gemeente Leiderdorp. Deze gebruikersgroepen maken beide gebruik van eenzelfde interne applicatie. Het inlogscherm van deze interne applicatie is nagebouwd, voorzien van een geldig certificaat (“groen slotje”) en geplaatst op een domein dat lijkt op het echte domein. Vervolgens hebben de medewerkers een e-mail ontvangen die afkomstig leek te zijn van Servicepunt71 met het verzoek om in te loggen om de applicatie.

De uitgevoerde test was van niveau “expert”. Dit betekent dat er geen opzettelijke fouten aanwezig waren waardoor de medewerkers deze e-mail eenvoudig als phishing e-mail konden herkennen.

Resultaten

Een beperkt aantal medewerkers heeft na het ontvangen van de e-mail de nagemaakte website geopend en inloggegevens ingevuld. Aanvallers hadden op deze manier dus mogelijk inloggegevens van medewerkers kunnen achterhalen die vervolgens in verdere aanvallen gebruikt kunnen worden.

Uit terugkoppeling van de contactpersonen die binnen de Gemeente Leiden en Gemeente Leiderdorp op de hoogte waren van de phishingtest, blijkt dat er een aantal van de medewerkers adequaat heeft gereageerd. Deze medewerkers en functioneel beheerders hebben na het ontvangen van de phishing e-mail melding gemaakt bij Servicepunt71.

Servicepunt71 had hierdoor tijdig kunnen reageren op de aanval door bijvoorbeeld medewerkers te informeren en vragen preventief hun wachtwoord te wijzigen, de e-mail te blokkeren etc. In dit geval heeft na het binnenkomen van de eerste meldingen bij Servicepunt71, de medewerker die op de hoogte was van de test zijn collega's gevraagd geen acties te ondernemen zodat het verdere verloop van test afgewacht kon worden.

[56] Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten

Naast het adequaat reageren van de medewerkers hebben preventieve technische maatregelen ervoor gezorgd dat de e-mail niet is aangekomen bij een groep gebruikers. Dit lijkt te komen door aanwezigheid van een zelflerend spamfilter. Doordat de e-mail niet is aangekomen bij een groep gebruikers in Leiderdorp– omdat het systeem inmiddels 'geleerd' had dat spam was - is geen goed onderscheid te maken tussen de resultaten van Gemeente Leiden en Gemeente Leiderdorp.

5.4 Tot slot

Voor het uitvoeren van de testen hebben Gemeente Leiden, Gemeente Leiderdorp en Servicepunt71 uitgebreide medewerking verleend.

De resultaten en bevindingen van de penetratietest en phishingtest zijn door Guardian360 aan Gemeente Leiden, Gemeente Leiderdorp en Servicepunt71 gepresenteerd. Daarnaast hebben deze partijen een uitgebreide rapportage ontvangen waarin Guardian360 de gevonden kwetsbaarheden en oplossingen beschrijft.

Bijlage I - Bronnen en respondenten

Documenten

Op basis van een informatie-uitvraag hebben de gemeenten Leiden en Leiderdorp het volgende bronmateriaal aangeleverd:

Gemeente Leiden	Gemeente Leiderdorp
Beleid	**Beleid**
Beleid Gegevensbescherming versie 1.1 – 20 augustus 2015	Beleid Gegevensbescherming versie 1.1 – 20 augustus 2015
Privacy by Design versie 1.4 – 19 juli 2016	Privacy by Design versie 1.4 – 19 juli 2016
Informatiebeveiligingsbeleid gemeente Leiden versie 1.0 – augustus 2016	Informatiebeveiligingsbeleid gemeente Leiderdorp versie 1.0 – augustus 2016
Regionaal actieplan informatieveiligheid – 22 mei 2017	Regionaal actieplan informatieveiligheid – 22 mei 2017
Uitgebreide Baselinetoets Privacy by Design versie 1.0 – 3 augustus 2017	Uitgebreide Baselinetoets Privacy by Design versie 1.0 – 3 augustus 2017
Privacy Impact Assessment (PIA) versie 1.0 – 4 mei 2017 (concept)	Privacy Impact Assessment (PIA) versie 1.0 – 4 mei 2017 (concept)
Verwerkersovereenkomst Leidse regio Wbp en AVG standaard versie 1.0 – 11 april 2018	Verwerkersovereenkomst Leidse regio Wbp en AVG standaard versie 1.0 – 11 april 2018
Uitvoeringsprogramma Versterken Regionale I-Samenwerking 2017 – 21 maart 2017	Uitvoeringsprogramma Versterken Regionale I-Samenwerking 2017 – 21 maart 2017
Organisatie	**Organisatie**
Wie en wat – Informatiebeveiliging en privacy	Wie en wat – Informatiebeveiliging en privacy
Privacy organisatie - juli 2018	Privacy organisatie - juli 2018
Proces melden datalek/beveiligingsincident versie 1.0 – 23 februari 2016	Proces melden datalek/beveiligingsincident versie 1.0 – 23 februari 2016
Integriteits-en geheimhoudingsverklaring	Integriteits-en geheimhoudingsverklaring
Beleid logische toegangsbeveiliging versie 1.0.1 – juli 2016 (document van de IBD)	
Beheer	**Beheer**
Verslag visitatiecommissie VNG informatieveiligheid gemeente Leiden – 5 oktober 2016	Rapportage social engineering assessment gemeente Leiden
Rapportage social engineering assessment gemeente Leiden	Auditrapportage Servicepunt 71 – 24 mei 2017
Auditrapportage Servicepunt 71 – 24 mei 2017	Uitgebreide Baselinetoets Privacy By Design – e-VOI versie 1.0 – 1 maart 2018 (concept)
Presentatie over informatieveiligheid voor College van B&W Leiden – 13 juni 2017	Uitgebreide Baselinetoets Privacy By Design – Chatfunctie op de website versie 1.0 – 14 december 2017 (concept)
Uitgebreide Baselinetoets Privacy By Design – e-VOI versie 1.0 – 1 maart 2018 (concept)	Regionale GAP analyse
Uitgebreide Baselinetoets Privacy By Design – Chatfunctie op de website versie 1.0 – 14 december 2017 (concept)	Verslag regio overleg informatiebeveiliging en privacy – 28 juni 2018
Regionale GAP analyse	Actiepuntenlijst werkgroep informatiebeveiliging en privacy – 22 februari 2018
Verslag regio overleg informatiebeveiliging en privacy – 28 juni 2018	Highlight report programma VRIS – 19 maart 2018

Actiepuntenlijst werkgroep informatiebeveiliging en privacy – 22 februari 2018	Audit register van verwerkingen gemeente Leiderdorp
Highlight report programma VRIS – 19 maart 2018	Dataclassificatie Leiderdorp
Audit register van verwerkingen gemeente Leiden	
Informatievoorziening aan de gemeenteraad	**Informatievoorziening aan de gemeenteraad**
Tekst uit paragraaf bedrijfsvoering jaarverslag 2017 – gemeente Leiden	Raad informeren over ENSIA – 14 juni 2018
Wethoudersbrief visitatiecommissie – 18 januari 2017	Brief van het college over AVG – 14 november 2017
Antwoord college van B&W op schriftelijke vraag VVD Leiden – 30 januari 2018	Third Party Mededeling DigiD – beveiligingsassessment 2017-2018
Antwoord college van B&W op schriftelijke vagen VVD en D66 Leiden – 12 januari 2017	Third Party Mededeling DigiD – Duijnborgh Audit – 12 oktober 2017
Antwoord college van B&W op schriftelijke vagen D66 Leiden – 5 juli 2016	Assurancerapport ENSIA 2017 DigiD en Suwinet – 15 maart 2018
Link naar beantwoording raadsvragen over de AVG – 2018	Assurancerapport ENSIA 2017 DigiD en Suwinet bijlage C1 en C2 – 15 maart 2018
Collegeverklaring ENSIA 2017 – 2 mei 2018	Verantwoordingsrapportage BAG – gemeente Leiderdorp
Collegeverklaring ENSIA 2017 – bijlage	Verantwoordingsrapportage BGT – gemeente Leiderdorp
Assurancerapport ENSIA 2017 DigiD en Suwinet – 27 maart 2018	Collegeverklaring ENSIA 2017 – 24 april 2018
Assurancerapport ENSIA 2017 DigiD en Suwinet bijlage C – 27 maart 2018	Jaarverslag gemeente Leiderdorp 2016
Third Party Mededeling DigiD 2017	
Verantwoordingsrapportage BAG – Gemeente Leiden	
Verantwoordingsrapportage BGT – gemeente Leiden	
Collegebesluit ENSIA (niet getekend)	
Praktijktoetsing	**Praktijktoetsing**
Incident Q1 2017	Applicatielijst – 27 juni 2018
Incident Q2 2017	Registratie beveiligingsincidenten
Incident Q3 2017	Overzicht meldingen datalek aan AP – 28 december 2017
Incident Q4 2017	Overzicht meldingen datalek aan AP – 29 juni 2018
Incident Q1 2018	
Incident Q2 2018	
Overzicht meldingen datalek aan AP – 28 december 2017	
Overzicht meldingen datalek aan AP – 29 juni 2018	

Open Bronnen

Ter verdieping van het onderzoek zijn er aanvullende gegevens gebruikt uit de volgende open bronnen en documenten:
Website gemeente Leiden (https://gemeente.leiden.nl/)
Website gemeente Leiderdorp (https://www.leiderdorp.nl/)
Website van Nederlandse Gemeenten (https://vng.nl/)
Website IBD (https://www.informatiebeveiligingsdienst.nl/)
Tactische Baseline Informatiebeveiliging Nederlandse gemeenten – V.1.02
Strategische Baseline Informatiebeveiliging Nederlandse gemeenten – V.1.02

Gesprekspartners

Ter verdieping van dit onderzoek zijn twee groepsinterviews gehouden. De gespreksverslagen van deze interviews zijn ter verificatie aan de gesprekspartners voorgelegd en geaccordeerd. De verslagen dienen als achtergrondinformatie voor het Onderzoeksrapport.

Datum	Naam	Functie
08 augustus 2018	De heer Hoekstra	CIO bij Leidse Regio en Servicepunt71
	De heer Haasnoot	FG bij Leidse Regio en Servicepunt71
	De heer van Zuuk	CISO bij de gemeente Leiden
	De heer Errami	CISO bij de gemeente Leiderdorp
10 september 2018	De heer Lenferink	Burgemeester bij de gemeente Leiden
	De heer Nauta	Gemeentesecretaris bij de gemeente Leiden
	De heer Dirkse	Wethouder bij de gemeente Leiden
	De heer Den Hartog	Plaatsvervangend FG bij de gemeente Leiden
	Mevrouw Driessen	Burgemeester bij de gemeente Leiderdorp
	De heer Romeijn	Gemeentesecretaris bij de gemeente Leiderdorp
	De heer Gardenier	Wethouder bij de gemeente Leiderdorp
26 september 2018	De heer Cambier	Senior beleidsmedewerker burgerzaken, applicatiebeheerder BRP - Leiderdorp
	De heer Beugels	Kwaliteitsmedewerker gegevensbeheer, BRP specialist - Leiden
	De heer Buijs	Functioneel beheerder cluster PMO en gebruikersbeheerder SUWI - Leiden
	Mevrouw Tran	Contractbeheerder - Servicepunt71
	Mevrouw Van der Meij	Senior inkoopadviseur - Servicepunt71
	Mevrouw Mulder	Beleidsmedewerker burgerzaken en beveiligingsbeheerder BRP - Leiden
	De heer Rodenburg	Adviseur informatie en control HRM – Servicepunt71

Bijlage II – Normenkader

Voor de twee gemeenten geldt grotendeels dezelfde beoordeling. Om die reden hebben we één normenkader ingevuld. Alleen bij de raden komen we tot verschillende beoordelingen. Dit is hieronder aangegeven.

Beleid	
1. Er is een informatieveiligheidsbeleid. 2. De beleidsstukken beschrijven onder andere rollen en verantwoordelijkheden, werkprocessen, veiligheidsmaatregelen. 3. Het beleid wordt periodiek up-to-date gebracht. 4. In het beleid wordt verwezen naar de relevante wettelijke kaders. 5. De gemeente hanteert in haar beleid de normen uit de BIG.	1. Voldaan, dit beleid geldt voor de Leidse regio. 2. Voldaan, deze zaken komen terug in het beleid. 3. Deels voldaan. De stukken zijn nu toe aan een update; er wordt aan gewerkt. 4. Voldaan, dit komt terug in het beleid. 5. Voldaan, de BIG-normen zijn het uitgangspunt in het beleid.
Organisatie	
1. De rollen en verantwoordelijkheden op het gebied van informatieveiligheid/privacy zijn vastgelegd. 2. Er is een CISO, CIO en FG aangesteld. 3. Voor medewerkers binnen de gemeenten is er een duidelijk aanspreekpunt op het gebied van informatieveiligheid.	1. Voldaan, o.a. in de beleidsstukken. 2. Voldaan, deels in regionaal verband. 3. Voldaan, hetzij binnen de afdeling, hetzij centraal in de organisatie.
Uitvoering	
1. De gemeente voert jaarlijks een audit of controle uit om te beoordelen of de gemeente 'in control' is op het gebied van informatieveiligheid. 2. De gemeente pakt verbeterpunten die blijken uit onderzoeken, audits of controles op. 3. De gemeente heeft een procedure voor de omgang met incidenten. 4. Mogelijke risico's worden gesignaleerd. Hier wordt aantoonbaar actie op ondernomen. 5. Er wordt een systematiek gebruikt bij de beoordeling of bepaalde risico's wel of niet genomen worden.	1. Voldaan; via ENSIA en aanvullende tests 2. Deels voldaan, zo blijkt uit gesprekken; maar er zijn geen vastgestelde verbeterplannen aangetroffen in het onderzoek. 3. Voldaan, deze procedure is aangetroffen. 4. Deels voldaan. Een voorbeeld is het overzicht van incidenten, waaraan direct acties worden gekoppeld. Tegelijkertijd zijn er ook veel risico's die onzichtbaar blijven. 5. Voldaan; vooraf vindt een risicoanalyse plaats
Raad	
1. De gemeenteraad besteedt aandacht aan het onderwerp informatieveiligheid. 2. De gemeenteraad wordt actief geïnformeerd over de borging van informatieveiligheid binnen de gemeente en bij organisaties waar zij mee werkt. 3. Vragen vanuit de gemeenteraad over dit onderwerp worden adequaat beantwoord. 4. De organisatie weet wat er vanuit ENSIA nodig is om goed te rapporteren aan de gemeenteraad en handelt hiernaar.	1. In Leiden: voldaan, er worden vragen gesteld en er is een bijeenkomst geweest. In Leiderdorp: deels voldaan, er is een bijeenkomst geweest maar de raad stelt zelf weinig vragen. 2. Deels voldaan, het betreft vaak informatie op hoofdlijnen. Bij incidenten wordt de raad wel geïnformeerd. 3. In Leiden: voldaan, de schriftelijke beantwoording van vragen is helder. In Leiderdorp worden hier geen vragen over gesteld. 4. Voldaan, de ENSIA rapportages voldoen aan de eisen die daar voor gesteld zijn.

Normen waarop Guardian360 heeft getoetst:

- Open Web Application Security Project (OWASP);
- DigiD Norm 1.0;
- DigiD norm 2.0;
- Nationaal Cyber Security Centrum (NCSC) richtlijnen;
- Baseline Informatiebeveiliging Gemeenten (BIG);
- Baseline Informatiebeveiliging Rijksoverheid (BIR), waar relevant.

Bijlage III - Verklaringen- en begrippenlijst

AP – Autoriteit Persoonsgegevens (tot 1 januari 2016 College bescherming persoonsgegevens). De AP houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

AVG – Algemene Verordening Gegevensbescherming: een Europese verordening (dus met rechtstreekse werking) die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert.

BAG – Basisregistratie Adressen en Gebouwen.

BGT - Basisregistratie Grootschalige Topografie.

BIG – Baseline Informatiebeveiliging Nederlandse Gemeenten; gemeentelijke basisnormenkader voor informatieveiligheid.

BIO – Baseline Informatiebeveiliging Overheid; basisnormenkader voor informatieveiligheid voor de overheid.

BRP – Basisregistratie Persoonsgegevens

CIO – Chief Information Officer: is binnen een organisatie de hoogste verantwoordelijke op het gebied van de ICT.

CISO – Chief Information Security Officer: Specialist op het gebied van de Informatie Beveiligingsfunctie, genoemd in de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

DigiD - Een systeem waarmee Nederlandse overheden op internet iemands identiteit kunnen verifiëren.

ENSIA – Eenduidige Normatiek Single Information Audit: Systematiek voor verantwoording over informatieveiligheid. Het proces bestaat uit een voorbereiding, zelfevaluatie, horizontale verantwoording, verticale verantwoording en een evaluatie.

FG – Functionaris voor de Gegevensbescherming. Functionaris die binnen de organisatie toezicht houdt op de toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG).

GAP Analyse: een methode om een vergelijking te maken tussen een bestaande en een gewenste situatie.

GR - Gemeenschappelijke regeling.

Leidse Regio: De gemeenten Leiden, Leiderdorp, Oegstgeest en Zoeterwoude vormen deze regio

IBD – Informatiebeveiligingsdienst voor gemeenten.

P&C Cyclus - Cyclus van planning en control.

PDCA Cyclus – Plan Do Check Act Cyclus.

PIA – Privacy Impact Assessment: Een instrument waarmee de risico's op het gebied van privacy in kaart kunnen worden gebracht.

Project VRIS - Project *Versterking van de Regionale I-Samenwerking* (VRIS)

PvA – Plan van Aanpak

Register gegevensverwerking - Het register gegevensverwerking bevat informatie over de persoonsgegevens die worden verwerkt. Het vervangt de bestaande verplichting uit de Wet bescherming persoonsgegevens om gegevensverwerkingen bij de Autoriteit Persoonsgegevens te melden.

Servicepunt71 – Gemeenschappelijke regeling van de gemeenten Leiden, Leiderdorp, Oegstgeest en Zoeterwoude waarin onder andere digitale veiligheid is ondergebracht.

SUWInet – Registratiesysteem; systeem van informatie-uitwisseling in de keten van werk en inkomen. Uitvloeisel van de Wet structuur uitvoeringsorganisatie werk en inkomen.

SUWI – Wet Structuur uitvoeringsorganisatie werk en inkomen.

VNG – Vereniging van Nederlandse gemeenten.

Wbp – Wet bescherming persoonsgegevens. Deze wet is na de invoering van de Algemene Verordening Gegevensbescherming op 25 mei 2018 niet meer van toepassing.

Wmo – Wet maatschappelijke ondersteuning; Gemeenten moeten ervoor zorgen dat mensen zo lang mogelijk thuis kunnen blijven wonen. De gemeente geeft ondersteuning thuis via de Wmo. Officieel heet deze wet Wmo 2015.