Oegstgeest
Wassenaar
Voorschoten
Leidschendam-Voorburg
Rekenkamercommissie

Aan: De raadsleden en burgercommissie-leden van Wassenaar, Voorschoten, Oegstgeest, Leidschendam-Voorburg

Datum: 26 april 2021

Betreft: Onderzoek *informatiebeveiliging van gemeenten en verbonden partijen*

Bijlage: Onderzoeksrapportage

Geachte leden,

Hierbij ontvangt u onze onderzoeksrapportage naar de informatiebeveiliging van de gemeenten Wassenaar, Voorschoten, Oegstgeest en Leidschendam-Voorburg en hun verbonden partijen.

Aanleiding onderzoek

De Rekenkamercommissie wilde in kaart brengen wat de gemeenten hebben gedaan na het eerdere onderzoek *Beter sturen op digitale dienstverlening* (2016).

Op basis daarvan namen alle colleges van B&W de aanbevelingen over om:

- risicoanalyses uit te voeren en zo nodig aanvullende maatregelen te nemen voor systemen en processen;
- eventuele risico's op te nemen in de paragraaf Weerstandsvermogen van de programmabegroting;
- expliciet te sturen op het formuleren van concrete kaders op informatiebeveiliging door verbonden partijen.

Het belang van een goede informatiebeveiliging is afgelopen jaren duidelijk naar voren gekomen. Zo ondervonden de gemeenten Lochem en Hof van Twente in 2019 en 2020 de gevolgen van datalekken.

Doel onderzoek

Het doel was om inzicht te bieden en eventueel verbetersuggesties aan te reiken voor:

- het informatiebeveiligingsbeleid en de operationele procedures;
- de mate van kwetsbaarheid van de gemeentelijke IT-netwerken;
- de wijze waarop verantwoording wordt afgelegd over informatiebeveiliging.

Uitvoering onderzoek

Het onderzoeksbureau IB&P heeft in de periode mei tot en met november 2020:

- gemeentelijke documenten bestudeerd over informatiebeveiliging;
- gesprekken gevoerd met de chief information security officer (CISO), de functionaris gegevensbescherming (FG) en de griffier van elke gemeente;
- een digitale vragenlijst verstuurd naar verbonden partijen en met hen gesproken;
- penetratietesten[1] en kwetsbaarhedenscans[2] uitgevoerd;
- per gemeente een vertrouwelijke rapportage opgeleverd over met name de kwetsbaarheden van de gemeentelijke IT-netwerken (hierop is direct actie ondernomen).

Bevindingen

Het onderzoek leverde bevindingen op die *positief* waren, *zorgwekkend*, of *extra aandacht* vragen.

Positief:

Het informatiebeveiligingsbeleid en de organisatie rondom informatiebeveiliging bij de gemeenten zijn op orde. De meeste verbonden partijen hebben een informatiebeveiligingsbeleid opgesteld, dat periodiek wordt bijgesteld.

Daarnaast werken de gemeenten aan bewustwording over informatiebeveiliging en privacy. Betrokkenen worden geïnformeerd bij een datalek. En het aantal datalekken wordt vermeld in de jaarrekeningen.

Zorgwekkend:

- de gemeentelijke IT-netwerken zijn kwetsbaar door de aanwezigheid van verouderde software, cipher suites[3] en protocollen voor encryptie[4], en door het gebruik van foute headers[5]. Dit is aangetoond door de penetratietesten;
- de gemeenten voeren te weinig risicoanalyses, penetratietesten en kwetsbaarhedenscans uit.

---

[1] *Met penetratietesten wordt geprobeerd in te breken in IT-netwerken of websites.*
[2] *Gedurende kwetsbaarhedenscans analyseert een softwareprogramma automatisch naar bekende kwetsbaarheden.*
[3] *Cipher suites bepalen hoe het digitaal verkeer tussen een server en een cliënt wordt versleuteld en verwerkt.*
[4] *Encryptie is het coderen (versleutelen) van digitale gegevens.*
[5] *Headers informeren de webbrowser hoe te handelen tijdens de interactie met de website.*

Extra aandacht:

- de gemeenten beoordelen niet-systematisch de operationele procedures, inventariseren niet-systematisch de risico's met verbonden partijen, en passen het informatiebeveiligingsbeleid niet aan;
- de gemeenten hebben een onvolledig en/of gedateerd verwerkingsregister[6];
- de gemeenten hebben de informatiebeveiligingsrisico's en beheersingsmaatregelen niet opgenomen in de paragraaf Weerstandsvermogen van de programmabegroting (= aangenomen aanbeveling in 2016);
- de gemeenten geven vrijwel geen sturing aan de verbonden partijen op het gebied van informatiebeveiliging (= aangenomen aanbeveling in 2016).

Op bladzijde 35 van de onderzoeksrapportage is een kort overzicht opgenomen van de belangrijkste bevindingen per gemeente.

Aanbevelingen

Verzoek uw college om:

1) de IT-netwerken te versterken door de geconstateerde kwetsbaarheden op te heffen;
2) minimaal jaarlijks risicoanalyses, penetratietesten en kwetsbaarhedenscans uit te voeren;
3) systematisch operationele procedures te beoordelen, systematisch de risico's met verbonden partijen te inventariseren, en het informatiebeveiligingsbeleid zo nodig aan te passen;
4) het verwerkingsregister volledig en/of geactualiseerd te maken;
5) de informatiebeveiligingsrisico's en beheersingsmaatregelen op te nemen in de paragraaf Weerstandsvermogen en in een speciale paragraaf informatiebeveiliging in de gemeentelijke programmabegroting;
6) sluitende afspraken te maken met verbonden partijen op het gebied van informatiebeveiliging;
7) kennisuitwisseling over informatiebeveiliging te stimuleren tussen FG's, CISO's en verbonden partijen;
8) jaarlijks afzonderlijk te rapporteren over informatiebeveiliging en privacybeleid, en de betrokkenheid van de gemeenteraad hierbij te vergroten (bijvoorbeeld door training).

---

[6] *In een verwerkingsregister houdt de gemeente verplicht haar verwerkingsactiviteiten bij van persoonsgegevens.*

Bestuurlijke reacties

De colleges van B&W van Wassenaar en Voorschoten herkennen de '*grote inzet*' van de organisatie om informatiebeveiliging te verbeteren. Zij vinden de aanbevelingen *'waardevol'* en nemen deze grotendeels over.
De aanbeveling voor een jaarlijkse risicoanalyse wordt afgewezen. Want *'een tweejaarlijkse risicoanalyse biedt voldoende zicht op eventuele risico's'*.
Volgens genoemde colleges van B&W zijn de aanbevelingen in de planning opgenomen, of al in uitvoering (zoals de geconstateerde kwetsbaarheden).

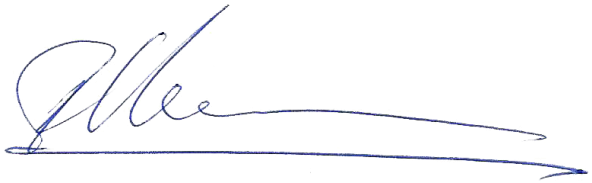
Het college van B&W van Oegstgeest dankt de Rekenkamercommissie voor het onderzoek. Zij stelt dat de gemeente al voldoet aan veel van de aanbevelingen.
De geconstateerde technische tekortkomingen waren volgens het college *'ernstig, maar hadden geen impact op de dienstverlening van de gemeente'*; de tekortkomingen zijn opgelost.
Het college overweegt om een aparte paragraaf informatiebeveiliging op te nemen in de programmabegroting. Zij streeft naar '*meer onderlinge kennisuitwisseling'*.

Het college van B&W van Leidschendam-Voorburg wil de betrokkenen *'complimenteren met het onderzoek en de onderzoeksrapportage*'.
Zij kan zich vinden in de constateringen en aanbevelingen in de onderzoeksrapportage en de aanbiedingsbrief.
Volgens het college waren de geconstateerde onvolkomenheden *'reeds bekend'*; oplossingen ervoor zijn opgenomen in de planning, of al in uitvoering.

Tenslotte

Wij gaan graag met u in gesprek over dit onderwerp. Bijvoorbeeld tijdens een speciale bijeenkomst, ondersteund door het onderzoeksbureau.

Met vriendelijke groet,
Rekenkamercommissie Wassenaar, Voorschoten, Oegstgeest en Leidschendam-Voorburg



Dolf Kamermans, voorzitter

IB&P
Dat gaat je niets aan

Rekenkameronderzoek informatiebeveiliging van gemeenten en verbonden partijen

Colofon

Dit is een uitgave van IB&P B.V.
Versie 2.1

Auteurs
Peter Kluitmans
Renco Schoemaker - CCISO, CISSP, CISM, CIPP/E
Erna Havinga - MBA, CISSP, CISM, CISA
Anouk Tijhuis - CIPP/E

Vormgeving
Yoeri Laros

Technische analyse
Duijnborgh Audit B.V.

8 februari 2021
info@ib-p.nl

IB&P
Postbus 638 | 8000 AP | Zwolle | 038-760 1350

© IB&P BV 2020

Samenvatting

De wereldwijde digitalisering gaat razendsnel en transformeert onze maatschappij in een rap tempo. Dit biedt kansen voor gemeenten, die immers midden in de informatiesamenleving opereren, maar brengt ook nieuwe risico's en uitdagingen met zich mee. Een goede informatiebeveiliging wordt daarom steeds belangrijker. Zonder goede informatiebeveiliging liggen cybercriminaliteit, fraude, oplichting en ondermijning op de loer.

Aanleiding

De Rekenkamercommissie (RKC) Wassenaar, Voorschoten, Oegstgeest en Leidschendam-Voorburg (WVOLV) heeft onderzoek laten uitvoeren naar de informatiebeveiliging binnen de gemeentelijke organisaties en de daaraan verbonden partijen. In een eerder rapport, 'Beter sturen op digitale dienstverlening' (2016), deed de RKC onder meer de aanbeveling: 'College, zorg voor risicoanalyses betreffende informatiebeveiliging en voer de Baseline Informatieveiligheid Gemeenten (BIG) in.'
De RKC is benieuwd op welke wijze de vier gemeenten opvolging hebben gegeven aan deze aanbeveling, namelijk: de zorg voor risicoanalyses betreffende informatiebeveiliging.

Het belang van informatie-beveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie. De ontwikkelingen rondom informatiebeveiliging volgen elkaar snel op. Systemen worden verder doorontwikkeld en onderling gekoppeld, software-updates volgen elkaar snel op en er worden steeds nieuwe aanvalsmethoden door hackers ontwikkeld.

Informatiebeveiliging is sterk afhankelijk van het inzicht dat een gemeente heeft in de bedrijfsprocessen en de risico's die er op hoog, midden en laag niveau worden geconstateerd. Hiervoor dienen dus over de (kritische) bedrijfsprocessen een risico analyse te worden uitgevoerd. Risico's veranderen continu doordat doelstellingen, interne en externe dreigingen, de omgeving en wet- en regelgeving veranderen. Als onvoldoende rekening wordt gehouden met de veranderende risico's, zijn maatregelen op termijn niet meer passend. Informatiebeveiliging vergt daarom een cyclisch, iteratief en terugkerend proces met als doel risico's te mitigeren.

Informatiebeveiliging en privacy gaan hand in hand. Het gevolg van een datalek kan een inbreuk zijn op de persoonlijke levenssfeer van een inwoner. Landelijk is hier veel aandacht voor. Zo komen grote datalekken in het nieuws en is de reputatieschade voor de betreffende organisatie groot. Informatiebeveiliging is dus niet alleen essentieel voor de bescherming van de inwoner, maar ook voor de reputatie van de gemeente ook al zou het datalek bij een verbonden partij plaatsvinden.

Onderzoeksopzet

Het onderzoek is uitgevoerd door onafhankelijk adviesbureau IB&P in de periode mei t/m september 2020 en richt zich niet alleen op de vier gemeenten, maar ook op de verbonden partijen. Op basis van elf onderzoeksvragen is het informatiebeveiligingsbeleid, de verantwoording hierover en de operationele implementatie daarvan getoetst. Informatie is verkregen vanuit documentatie, interviews met CISO's[1], FG's[2] en griffiers, en vanuit online enquêtes. Niet alle geïnterviewde CISO's en FG's hadden formeel deze

[1] De Chief Information Security Officer (CISO) is de informatiebeveiligingsfunctionaris binnen de ambtelijke organisatie

[2] De Functionaris Gegevensbescherming (FG) is de interne toezichthouder op de naleving van de privacywetgeving (Algemene Verordening Gegevensbescherming – AVG)

© IB&P BV 2020

functie of rol, maar voerden wel de werkzaamheden uit. Ook bij een aantal van de verbonden partijen zijn deze functionarissen geïnterviewd, de rest van de verbonden partijen hebben een online enquête ingevuld. Daarnaast is een technische analyse van de IT-infrastructuur uitgevoerd binnen de gemeenten. De onderliggende technische rapporten bij dit onderzoek zijn al eerder vertrouwelijk opgeleverd aan de CISO's van de respectievelijke gemeenten zodat, waar nodig, maatregelen genomen konden worden.

Hieronder zetten we een aantal bevindingen en aanbevelingen op rij, verdeeld over de hoofdthema's Beleid – Verantwoording – Operationele implementatie en Technische analyse Het gekleurde schuifje geeft aan wat de urgentie is van de aanbeveling. Groen = is op orde, oranje = heeft aandacht nodig en rood = is urgent/ zorgwekkend.

Beleid

- **Behoud de aanwezige aandacht en inzet voor informatiebeveiliging en privacy.** De inzet, oplettendheid en bevlogenheid van verantwoordelijke ambtenaren en bestuurders is onmisbaar.

In kader van het onderzoek is met name gekeken naar het informatiebeveiligingsbeleid en privacybeleid van de organisatie. Alle gemeenten hebben een vastgesteld informatiebeveiligings- en privacybeleid, net als de meeste verbonden partijen. Verder valt positief op dat er dagelijks door vele medewerkers met inzet wordt getracht de gemeenten veilig(er) te maken en te houden. Dat wordt onbedoeld vaak gezien als een vanzelfsprekendheid (net als water uit de kraan), maar verdient hier aandacht. Voorts wordt door middel van opleiding, training en voorlichting structureel gewerkt aan bewustwording.

Verantwoording

- **Stuur blijvend op het beleidsterrein informatiebeveiliging (en privacy) bij verbonden partijen door hen hier jaarlijks over te laten rapporteren.** Maak de verantwoording onderdeel van het jaarlijkse Plan-Do-Check-Act proces voor informatiebeveiliging en beleg de coördinatie op de uitvoering van dit proces bij de CISO.

De sturing en controle op de uitvoering van het informatiebeveiligings- en privacybeleid bij samenwerkingsverbanden is onvoldoende. Daarin is geen verbetering gekomen sinds het rekenkamerrapport 'Grip op samenwerking?'[3] (2014). De bestaande verantwoording en controle is te weinig gericht op informatiebeveiliging, terwijl de gemeenten daarvoor wel de eindverantwoordelijkheid dragen. Veelal ontbreken operationele afspraken over de afhandeling en opvolging van datalekken tussen gemeenten en verbonden partijen.

- **Verdiep en verbreed de uitwisseling van kennis, aanpak en ervaringen tussen gemeenten onderling.** Formaliseer een (bestuurlijke) overlegstructuur en schenk aandacht aan het jaarlijkse Plan-Do-Check-Act proces voor informatiebeveiliging zelf. Onderling leren dient plaats te vinden op zowel het beleidsdomein, het uitvoeringsdomein als het controledomein.

Gemeenten voeren dezelfde wettelijke taken uit en werken daarbij in toenemende mate met elkaar samen in uitlopende verbanden. Er wordt goed gebruik gemaakt van wat de Informatiebeveiligingsdienst (onderdeel VNG) aanreikt, maar de WVOLV-gemeenten weten onderling weinig van elkaar over hoe er wordt gewerkt en wat er speelt. Wel wordt er in andere – veelal regionale – verbanden kennis en ervaring uitgewisseld. Dát er onderling geleerd wordt is belangrijker dan in welke constellatie dat gebeurt.

[3] https://www.rekenkamerwvolv.nl/wp-content/uploads/2018/02/Rapport_Grip_op_Samenwerking_iPad.pdf

© IB&P BV 2020

Operationele Implementatie

- **Voer tenminste jaarlijks risicoanalyses uit en integreer hierin zowel informatiebeveiliging als privacy. De uitvoering van taken door verbonden partijen valt hier ook binnen.** Stuur vervolgens op het beheersen van deze risico's en stel indien nodig beleidskaders en operationele uitvoering bij. Neem de risico's plus beheersmaatregelen op in de gemeentelijke programmabegroting.

In 2014 is geconcludeerd dat gemeenten niet systematisch risicoanalyses uitvoeren, waarin de risico's van samenwerkingsverbanden in kaart worden gebracht. Dit is tot op heden niet verbeterd. Voorts lopen zij achter met het maken van dergelijke risicoanalyses op het gebied van informatiebeveiliging terwijl dit een verplichting is vanuit het normenkader Baseline Informatiebeveiliging Overheid (BIO), die per 1 januari 2020 van kracht is. Door gemeenten en de meeste verbonden partijen wordt gewerkt aan de invoering van deze BIO. Voorkom dat sturing op risico's verwordt tot sturing op maatregelen.

- **Inventariseer alle verwerkingen van persoonsgegevens en actualiseer daarmee het verwerkingsregister. Neem in alle verwerkersovereenkomsten concrete afspraken over beveiligingsmaatregelen op.** Vraag vervolgens minimaal jaarlijks om een verantwoordingsrapportage om de naleving vast te stellen. Borg dit richting de toekomst in het inkoopproces. Instrueer de FG hier strikt toezicht op te houden.

Registers van verwerkingen zijn verplichte registraties over het gebruik van persoonsgegevens binnen de gemeente. Bij een gemeente ontbreekt een dergelijk register en bij de overige gemeenten zijn deze onvolledig en/of gedateerd. Een andere verplichting is het afsluiten van overeenkomsten met organisaties die met persoonsgegevens van burgers werken onder de (mede)verantwoordelijkheid van de gemeente. Dit kan een verbonden partij zijn. In een relatief groot aantal van deze overeenkomsten is onduidelijk welke beveiligingsmaatregelen die organisaties (behoren te) nemen.

Technische Analyse

- **Volg de adviezen uit de technische analyse op en voer periodiek kwetsbaarhedenscans uit. Laat minimaal jaarlijks penetratietesten uitvoeren door een daarin gespecialiseerd bureau.** Blijf hackers voor door structureel zelf van buiten naar binnen te (laten) kijken en richt een proces in voor het snel kunnen oplossen van de gevonden kwetsbaarheden.

Informatiebeveiliging is veel breder dan alleen de techniek, maar niettemin is de technische beveiliging van IT een belangrijk onderdeel. De staat hiervan is te toetsen met kwetsbaarhedenscans (nadruk op 'verkennen') en penetratietesten (nadruk op 'binnendringen'). De gemeenten voeren deze niet of te beperkt uit. Het uitgangspunt daarbij is minimaal jaarlijks én bij grote veranderingen. Uit de uitgevoerde toetsen is gebleken dat de gemeentelijke netwerken kwetsbaar zijn door de aanwezigheid van onder meer verouderde software. Dit is door een kwaadwillende vrij eenvoudig te 'verkennen' waardoor 'binnendringen' een reëel risico wordt.

Daarom: informatiebeveiliging

Samenvattend: alle zaken staan wel in de steigers, maar behoeven nog veel aandacht in de systematische uitwerking in de praktijk. De gemeenten zijn op dit moment niet voldoende 'in control' op informatiebeveiliging omdat de risico's en het gebruik van persoonsgegevens onvoldoende in beeld zijn. Dit gecombineerd met de nauwelijks aanwezige verantwoordingsinformatie maakt sturen op dit beleidsterrein erg moeilijk.

© IB&P BV 2020

De digitale weerbaarheid van gemeenten staat onder druk door een toenemende complexiteit en connectiviteit in het IT-landschap, nieuwe ontwikkelingen en door te weinig aandacht voor digitale veiligheid bij nieuwe, innovatieve projecten.
Kortom, vandaag 'voldoen' betekent niet dat dit ook voor morgen geldt. Nul risico lopen bestaat niet, maar 'in control' komen op deze risico's wél. Achteropraken kan desastreuze gevolgen hebben, zo ondervonden bijvoorbeeld de gemeente Lochem (2019) en de gemeente Hof van Twente (2020). Daarom: informatiebeveiliging.

Binnen de gemeenten werd veelal gebruik gemaakt van het template van de Informatiebeveiligingsdienst (IBD) van VNG voor het schrijven van een informatiebeveiligingsbeleid.
De strategische doelen van het informatiebeveiligingsbeleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

Het vaststellen van een informatiebeveiligingsbeleid is procedureel op orde, de verantwoordelijkheden zijn binnen de organisaties belegd. Alleen is het zichtbaar uit de aanvullende conclusies dat de implementatie van dit beleid nog de nodige aandacht vergt.

© IB&P BV 2020

Rekenkameronderzoek informatiebeveiliging van gemeenten en verbonden partijen

© IB&P BV 2020

Inhoudsopgave

© IB&P BV 2020

1 Inleiding en onderzoeksaanpak

© IB&P BV 2020

1. Inleiding en onderzoeksaanpak

De wereldwijde digitalisering gaat razendsnel en transformeert onze maatschappij in een rap tempo. Dit biedt nieuwe kansen, als gemeente sta je immers midden in de informatiesamenleving, maar brengt ook (nieuwe) risico's en uitdagingen met zich mee. Een goede informatiebeveiliging wordt daarom steeds belangrijker. Gemeenten verwerken namelijk grote hoeveelheden gegevens in een veelvoud aan systemen en processen. Veel van deze gegevens betreffen (bijzondere) persoonsgegevens of andere gevoelige gegevens die goed beschermd moeten zijn. Daarnaast wisselen de gemeenten ook gegevens uit met de zogenaamde verbonden partijen. Zonder goede informatiebeveiliging liggen cybercriminaliteit, fraude, oplichting en ondermijning op de loer.

De hierboven beschreven ontwikkeling is voor de Rekenkamercommissie (RKC) Wassenaar, Voorschoten, Oegstgeest en Leidschendam-Voorburg (WVOLV) aanleiding geweest een onderzoek uit te laten voeren naar de informatiebeveiliging binnen de gemeentelijke organisaties en de daaraan verbonden partijen.

De RKC heeft eerder, in 2016, het onderzoek 'Beter sturen op digitale dienstverlening' uitgevoerd. In dit onderzoeksrapport zijn onder meer aanbevelingen gegeven op het gebied van informatiebeveiliging[4]. Deze aanbevelingen zijn destijds door alle vier de colleges van Burgemeesters & Wethouders (B&W) overgenomen. Dit vervolgonderzoek gaat over wat er met de aanbevelingen uit het rapport van 2016 is gedaan.

1.1 De zorg voor risicoanalyses betreffende informatiebeveiliging

De centrale vraag in het onderzoek 'Beter sturen op digitale dienstverlening' luidde:

Wat is de visie en het beleid van de vier gemeenten ten aanzien van digitale dienstverlening, en de sturing en controle daarop - zowel de digitale dienstverlening door de eigen gemeente, als door verbonden partijen en uitvoeringspartijen? En wat is de rolverdeling van de raden en de colleges van burgemeester en wethouders hierin?

In aanbeveling vier van bovengenoemd onderzoek staat: *'College, zorg voor risicoanalyses betreffende informatiebeveiliging en voer de Baseline Informatieveiligheid Gemeenten (BIG) in.'*

De RKC is benieuwd op welke wijze de vier gemeenten opvolging hebben gegeven aan deze aanbeveling uit 2016, namelijk: de zorg voor risicoanalyses betreffende informatiebeveiliging. Hiertoe heeft de RKC laten onderzoeken hoe informatiebeveiliging is geborgd in beleid en beheer en hoe ermee wordt omgegaan in de praktijk. Zowel qua organisatie en processen als in de techniek. De resultaten van dit onderzoek leest u in dit rapport.

1.2 Reikwijdte van dit vervolgonderzoek

Het onderzoek brengt in beeld hoe informatiebeveiliging is geborgd 'op papier' en hoe ermee wordt omgegaan in 'de praktijk', met bijzondere aandacht voor de inrichting van de IT-infrastructuur.

[4] Zie "Conclusie en aanbeveling 4" uit het rapport "Beter sturen op digitale dienstverlening" 13 april 2016

© IB&P BV 2020

In de scope van het onderzoek zijn de vragen die de RKC geformuleerd heeft met betrekking tot informatiebeveiliging opgenomen. Deze vragen zijn ingedeeld in de onderdelen: Beleid, verantwoording, operationele implementatie en technische analyse. In bijlage 2 zijn de 11 onderzoeksvragen weergegeven. Dit vervolgonderzoek richt zich niet alleen op de informatiebeveiliging, maar is ook gericht op datalekken zoals in een aantal onderzoeksvragen is terug te zien. De verwerking van persoonsgegevens valt onder de Algemene Verordening Gegevensbescherming (AVG). Datalekken hebben per definitie betrekking op persoonsgegevens, en derhalve ook de beveiliging daarvan. De periode waarop dit onderzoek zich richt loopt van 2018 tot en met de eerste helft van 2020.

1.3 Onderzoeksaanpak

Het onderzoek richt zich niet alleen op de vier gemeenten, maar ook op de aan de gemeenten verbonden partijen. De informatie is middels interviews, (online) enquêtes en technische analyses verzameld en vervolgens geanalyseerd.

1.3.1 Onderzoek gemeenten WVOLV

Het onderzoek beperkt zich vanzelfsprekend tot de gemeenten Wassenaar, Voorschoten, Oegstgeest en Leidschendam-Voorburg (WVOLV). Tijdens het onderzoek naar de informatiebeveiligingsaspecten zijn de volgende onderwerpen aan bod gekomen.

1.	Beleid	Wat is het informatiebeveiligingsbeleid?
2.	Verantwoording	Op welke wijze wordt over informatiebeveiliging verantwoording afgelegd?
3.	Operationele implementatie	Op welke wijze is het beleid omgezet in operationele procedures en zijn deze (aantoonbaar)geborgd binnen de organisatie?
4.	Technische analyse	Op welke wijze is de IT-infrastructuur ingericht om te kunnen voldoen aan het beleid? (d.m.v. penetratietesten en kwetsbaarheidsanalyses)

Tezamen geeft dit antwoord op de onderzoeksvragen uit bijlage 2. Om de onderzoeksvragen te kunnen beantwoorden zijn bij alle gemeenten de Chief Information Security Officer (CISO), de Functionaris Gegevensbescherming (FG) en de griffier geïnterviewd. Van de interviews zijn gespreksverslagen opgesteld die ter verificatie zijn aangeboden aan de geïnterviewden.

1.3.2 Onderzoek verbonden partijen

Een verbonden partij is een privaatrechtelijke of publiekrechtelijke organisatie waarin de gemeente een bestuurlijk en een financieel belang heeft. Onder een bestuurlijk belang wordt verstaan: zeggenschap, via vertegenwoordiging in het bestuur of via stemrecht. Onder een financieel belang wordt verstaan: een aan de verbonden partij ter beschikking gesteld bedrag, dat niet verhaalbaar is door de gemeente, indien de verbonden partij failliet gaat.

In het eerder aangehaalde rapport ‘Beter sturen op digitale dienstverlening’ uit 2016 is geadviseerd expliciet te sturen op het formuleren van concrete kaders op informatiebeveiliging door verbonden partijen.

Om een goed beeld te krijgen van de informatiebeveiliging binnen de verbonden partijen is ervoor gekozen het onderzoek hier langs twee lijnen uit te voeren.

© IB&P BV 2020

Online vragenlijst

Gezien het opgegeven aantal verbonden partijen was het niet mogelijk deze allemaal in detail mee te nemen in het onderzoek. Daarom is besloten een online enquête uit te zetten onder deze organisaties (zie bijlage 3). In de enquête zijn vragen gesteld over informatiebeveiliging, uitgaande van de Baseline Informatiebeveiliging Overheid (BIO). Op basis van deze vragenlijst kan niet alleen een uitspraak gedaan worden over het voldoen aan de actuele normenkaders, maar ook de organisatorische sturing en verantwoording hierover.

Voorts heeft de focus uitsluitend gelegen op de verbonden partijen die omgaan met 1) bijzondere persoonsgegevens, 2) gevoelige financiële gegevens en/of 3) andere gevoelige gegevens, zoals vertrouwelijke rapporten.

Interviews

Om het onderzoek naar verbonden partijen voldoende diepgang te geven, zijn twee verbonden partijen per gemeente nader onderzocht door middel van interviews. Dit gaat in totaal dus om acht verbonden partijen (zie bijlage 3). De keuze voor deze verbonden partijen is gebaseerd op de mate waarin deze (bijzondere) persoons- of gevoelige financiële gegevens verwerken. Van de interviews zijn verslagen gemaakt die ter goedkeuring zijn aangeboden aan de geïnterviewden.

1.3.3 Indeling onderzoek

Het onderzoek is opgedeeld in zes fasen die elkaar logisch opvolgen, maar in de praktijk met elkaar overlappen. Zo liepen de interviews, enquête en technische analyses parallel na afronding van de inventarisatiefase. In de analysefase is alles samengebracht en vervolgens in rapportagevorm opgeleverd in voorliggend rapport.

1.	Inventarisatie	In deze fase is een inventarisatie gemaakt van degenen die betrokken moeten worden bij het onderzoek. Tevens is bepaald welke verbonden partijen worden uitgenodigd voor een interview. Tot slot zijn bij alle vier de gemeenten algemene documenten, beleidsdocumenten en procedures op basis van de BIO opgevraagd.
2.	Interviews	De interviews bestaan uit een vaste set vragen die vanzelfsprekend verband houden met de onderzoeksvragen, maar ook met de aangeleverde documentatie. Van de interviews is een gespreksverslag opgesteld. Het gespreksverslag is steeds geverifieerd door de geïnterviewde.
3.	Enquête	De niet-geïnterviewde verbonden partijen zijn bevraagd via een online enquête. De enquête resulteert in een algemeen beeld met betrekking tot de status van de informatiebeveiliging bij de verbonden partij.
4.	Technische analyse	Bij elke gemeente is een penetratietest en een kwetsbaarheidsanalyse uitgevoerd. De penetratietest is uitgevoerd als een zogenaamde black box test. De kwetsbaarheden-scan is uitgevoerd met ‘administrator-credentials’ waardoor ingelogd kon worden op de servers. Voor het uitvoeren van de technische analyse is per gemeente een vrijwaringsverklaring vereist.

© IB&P BV 2020

5. Analyseren — Nadat alle informatie is verzameld zijn de gegevens gegroepeerd, in onderlinge samenhang geïnterpreteerd, geanalyseerd en zijn conclusies en aanbevelingen opgesteld. De resultaten van de technische analyse zijn met de betrokken gemeenten gedeeld.

6. Rapportage. — De rapportage is tweeledig: er wordt één rapport aangeboden aan de RKC. Dit rapport staat open voor publicatie. Daarnaast wordt er per gemeente een rapport geschreven. Dit rapport is vertrouwelijk.

1.4 Leeswijzer

Dit rapport bevat de conclusies en aanbevelingen die volgen uit het onderzoek. Het rapport bestaat, buiten deze inleiding, uit nog vier hoofdstukken. In hoofdstuk 2 wordt uiteengezet wat wordt verstaan onder informatiebeveiliging en privacy. Hoofdstuk 3 behandelt de vijf onderwerpen: beleid, verantwoording, operationele implementatie, technische analyse en leren. In hoofdstuk 4 worden op basis van de bevindingen de conclusies van het onderzoek beschreven en tot slot worden in hoofdstuk 5 de conclusies omgezet naar een aantal aanbevelingen. Ook zijn hier een slotbeschouwing en stellingen voor een debat opgenomen. Door dit rapport heen treft u enkele tekstkaders met achtergrondkleur aan; deze kaders maken integraal onderdeel uit van het rapport. Ze zijn toegevoegd om de leesbaarheid van het rapport te vergroten.

In de bijlage van dit rapport is als eerste een Handreiking voor gemeenteraden, een overzicht van de onderzoeksvragen (bijlage 2), de geïnterviewde personen (bijlage 3) en de gebruikte afkortingen (bijlage 4) te vinden.

© IB&P BV 2020

2 Wat verstaan we onder informatiebeveiliging

© IB&P BV 2020

2. Wat verstaan we onder informatiebeveiliging?

Informatiebeveiliging is vandaag de dag een veelbesproken onderwerp. Veel werkprocessen, besluitvorming en procedures zijn in hoge mate afhankelijk van (juiste) informatie, en is de gemeente juist daar erg kwetsbaar. Binnen informatiebeveiliging wordt er gekeken naar de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Met de invoering van de Algemene Verordening Gegevensbescherming (AVG)[5] zijn de regels rondom de bescherming van persoonsgegevens aangescherpt en daarmee ook het belang van informatiebeveiliging benadrukt. In dit hoofdstuk worden de diverse begrippen uitgelegd in hun onderlinge samenhang.

2.1 Terminologie

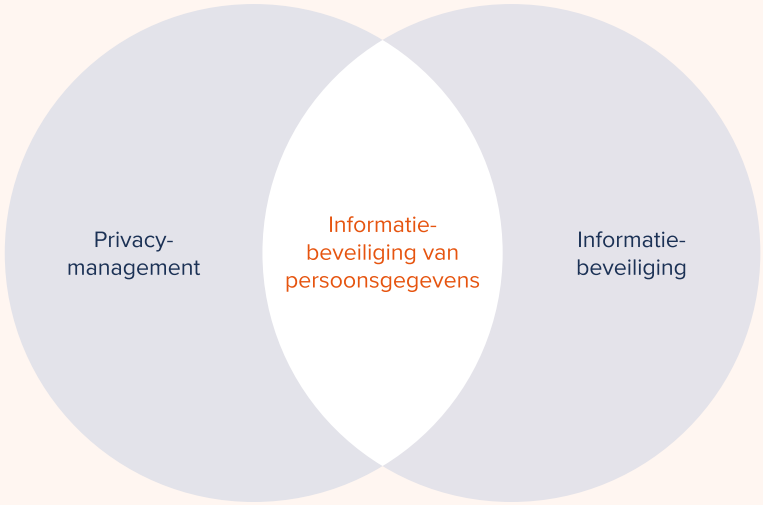
De begrippen informatieveiligheid en informatiebeveiliging worden vaak door elkaar gebruikt, afhankelijk van de context. Maar wat is het verschil? Informatieveiligheid verwijst veelal naar het doel: een informatieveilige gemeente. Informatiebeveiliging verwijst naar de instrumenten en maatregelen om dat doel te bereiken.

De definitie van informatiebeveiliging is het treffen en onderhouden van maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening en informatiesystemen te garanderen.

Gegevensbescherming is het proces waarbij persoonsgegevens worden beschermd tegen beschadiging, verlies en toegang door onbevoegde partijen. Privacy gaat over de afscherming van persoonsgegevens. De verleiding om deze gegevens te gebruiken voor andere doeleinden dan waarvoor ze bedoeld zijn, is groot. Om de privacy te waarborgen, moeten deze gegevens goed worden beveiligd. Waar privacy en informatiebeveiliging elkaar raken, gaat het over de beveiliging van persoonsgegevens.

[5] https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/algemene-verordening-gegevensbescherming-avg

Informatiebeveiliging en privacymanagement



Informatiebeveiliging en privacymanagement zijn nauw verweven, maar zeker niet hetzelfde. Goede privacybescherming bevat informatiebeveiliging van persoonsgegevens, maar daarnaast ook andere onderdelen. Daarbij kun je bijvoorbeeld denken aan het bepalen van de grondslag voor de verwerking van persoonsgegevens: op welke grond mag ik deze gegevens verwerken? Informatiebeveiliging kan prima geregeld zijn voor gegevens die je eigenlijk niet zou mogen hebben. Dan is de informatiebeveiliging op orde maar privacy-management niet.

Een ander onderdeel van privacy-management is het waarborgen van de rechten van betrokkenen: degene over wie persoonsgegevens worden verzameld, heeft onder andere recht op inzage, correctie en verwijdering. Dit heeft weinig te maken met informatiebeveiliging.

Daarnaast zijn er onderdelen van informatiebeveiliging die niet met persoonsgegevens te maken hebben, zoals het beveiligen van financiële of organisatiegegevens.

2.2 Wet- en regelgeving in relatie tot risicomanagement

De aandacht voor informatiebeveiliging en privacy is de afgelopen jaren enorm toegenomen, aangewakkerd door de veranderlijkheid van het thema en nieuwe of geactualiseerde wet- en regelgeving. Door de komst van de meldplicht datalekken zijn issues, die er voorheen ook al waren, zichtbaar geworden. De ontwikkelingen op het vlak van informatiebeveiliging en privacymanagement volgen elkaar snel op en moeten een antwoord bieden op steeds weer nieuwe (digitaliserings)vragen.

2.2.1 Baseline Informatiebeveiliging Overheid (BIO)

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen. Sinds 1 januari 2020 is de BIO van kracht. De BIO vervangt de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). De Informatiebeveiligingsdienst voor gemeenten (IBD) is een initiatief van alle Nederlandse gemeenten en valt onder de Vereniging van Nederlandse Gemeenten – VNG Realisatie. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging (en privacy) met kennisproducten zoals handreikingen en factsheets. De producten bevatten praktische handvatten voor gemeenten en adviezen in lijn met de BIO en de AVG.

2.2.2 Algemene Verordening Gegevensbescherming (AVG)

De Algemene Verordening Gegevensbescherming (AVG) is een Europese verordening die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties standaardiseert. Het doel van de AVG is niet alleen om de bescherming van persoonsgegevens te garanderen, maar ook om het vrije verkeer van gegevens te waarborgen.

Dat gaat in de praktijk niet altijd goed, zo weten we. We spreken dan over een datalek. Onder een **datalek** verstaan we de toegang tot, vernietiging, wijziging of het vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie, of zonder dat dit wettelijk is toegestaan. In de context van privacy spreekt men over het ‘verwerken van persoonsgegevens’ in de ruimste zin des woords.

Onder **gegevensverwerking** verstaan we het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending,

© IB&P BV 2020

verspreiden of op andere wijze ter beschikking stellen, combineren, afschermen, wissen of vernietigen van persoonsgegevens.

De AVG spreekt over risicomanagement. Als een gegevensverwerking mogelijk een hoog privacy-risico oplevert voor de mensen van wie de organisatie gegevens verwerkt, moet volgens de AVG een **Data Protection Impact Assessment (DPIA)** worden uitgevoerd. Dat is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen. Hierbij dienen nadrukkelijk en aantoonbaar de belangen van de betrokkenen waarop de persoonsgegevens betrekking hebben, te worden meegewogen. Vervolgens kunnen passende maatregelen genomen worden die de risico's reduceren of wegnemen.

Informatiebeveiliging en privacy gaan hand in hand. Het gevolg van een datalek kan een inbreuk zijn op de persoonlijke levenssfeer van een inwoner. Landelijk is hier veel aandacht voor. Zo komen grote datalekken in het nieuws en is de reputatieschade voor de betreffende organisatie groot. Informatieveiligheid is dus niet alleen essentieel voor de bescherming van de inwoner, maar ook voor de reputatie van de gemeente ook al zou het datalek bij een verbonden partij plaatsvinden.

Daarnaast moet een inbreuk in verband met persoonsgegevens gemeld worden aan de Autoriteit Persoonsgegevens (AP) als er sprake is van een risico voor de rechten en vrijheden van betrokkene(n). Bij een hoog risico moet de betrokkene zelf ook geïnformeerd worden. Formeel is de drempel om te melden bij de AP laag. Een relatief klein voorval als een geopend retour gestuurde brief met gevoelige persoonsgegevens, is al iets wat gemeld moet worden aan de AP.

Risicomanagement

Binnen dit rapport wordt vaak een verwijzing gemaakt naar risicomanagement. Met name gaat het hier om risicomanagement op het gebied van informatiebeveiliging en/of privacy. Hierbij een korte beschrijving wat hieronder wordt verstaan:

Risicomanagement is een middel om op een gestructureerde manier risico's in kaart te brengen, te evalueren en – door er pro-actief mee om te gaan – beter te beheersen. De gemeente inventariseert risico's en de gevolgen van deze risico's en verbindt er maatregelen aan. Door al in een vroeg stadium na te denken over de mogelijke risico's die de gemeente loopt, wil men deze voorkomen en de eventuele ernstige gevolgen ervan beperken.

Risicomanagement bestaat grofweg uit zes stappen:

1) Identificatie van risico's
2) Analyse en beoordeling van risico's (in bijv. laag, medium, hoog)
3) Analyse van huidige beheersmaatregelen
4) Ontwerpen en uitvoeren aanvullende beheersmaatregelen
5) Controleren, evalueren en rapporteren
6) Resultaten integreren in de besluitvormingsprocessen

Vaak is het lastig voor een proceseigenaar om vanuit het niets bedreigingen en risico's op het gebied van de informatieveiligheid voor de eigen afdeling in kaart te brengen. Maar dit wordt vanuit het informatiebeveiligingsbeleid of het managementsysteem (ISMS) vaak wel vereist. Een veel gebruikte

methode om dit proces van risico-inventarisatie te ondersteunen is de zogenaamde MAPGOOD-methode. MAPGOOD staat voor Mensen, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgeving en Diensten. Dit zijn verschillende invalshoeken die je kunt gebruiken in een gesprek met een afdelingsmanager om naar bedreigingen en risico's te kijken om zo beveiligingsmaatregelen in kaart te brengen.

- Mens, denk aan: directe en indirecte gebruikers, en functioneel en technisch applicatiebeheer.
- Apparatuur, denk aan: webserver, applicatieserver, beheer van werkplekken en werkplekken/ laptops van gebruikers.
- Programmatuur, denk aan: de diverse applicaties die gebruikt worden.
- Gegevens, denk aan: basisregistraties, financiële verantwoording en vergunningen.
- Organisatie, denk aan: beheer-, gebruikers- en ontwikkelorganisatie.
- Omgeving, denk aan: locatie, serverruimte en werkplekken.
- Diensten, denk aan: technisch systeembeheer, IT-infrastructuur en onderhoudscontracten met externe dienstverleners of verbonden partijen.

© IB&P BV 2020

3 Bevindingen

© IB&P BV 2020

3. Bevindingen

Na de inleiding en ook korte theoretische uiteenzetting over informatiebeveiliging en privacy, staan in dit hoofdstuk de bevindingen van het onderzoek centraal. Te starten met enkele algemene bevindingen.

3.1 Algemene bevindingen

De algemene documenten, beleidsdocumenten en procedures die voor het onderzoek van belang waren, zijn deels aangeleverd door de gemeenten. Daarbij valt op dat de meeste beleidsdocumenten zijn aangeleverd en de procedures gebaseerd op de BIO veelal ontbreken. De aangeleverde documenten zijn gebruikt bij de interviews. In enkele gevallen zijn na het interview nog aanvullende documenten aangeleverd. Het is evident dat het niet mogelijk is te rapporteren over de niet aangeleverde documenten.

De antwoorden op de onderzoeksvragen zijn verdeeld over vijf onderwerpen die in de volgende paragrafen achtereenvolgens aan bod komen. Het gaat om de eerder aangehaalde onderwerpen beleid, verantwoording, operationele implementatie en technische analyse. Bij elk onderwerp wordt de volgende structuur gehanteerd:

- Algemeen (definities)
- Bevindingen
- Toelichting

3.2 Beleid

Algemeen

De focus binnen dit onderzoek richt zich voornamelijk op het Informatiebeveiligingsbeleid en Privacy beleid. Onder beleid wordt hierbij verstaan: Het aangeven van de richting en de middelen (cq. Instrumenten) waarmee men de doelen op het gebied van informatiebeveiliging en privacy wil gaan realiseren. Het doel van het informatiebeveiligingsbeleid is de betrouwbaarheid van de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel niveau te beperken.

Organisaties zijn zelf verantwoordelijk voor het voldoen aan de privacyregels van de AVG. Afhankelijk van de soort verwerkingsactiviteiten moet een organisatie een privacybeleid opstellen en implementeren. Een privacybeleid legt de kaders en verantwoordelijkheden vast voor de verwerking van persoonsgegevens.

Informatiebeveiliging is bij uitstek een thema waarop een organisatie risico's neemt. Risico's zijn niet te vermijden, omdat geen risico lopen onbetaalbaar en onwerkbaar is. Maar dit vraagt wel om een bewuste afweging of onderbouwing. Risicomanagement is een middel om op een gestructureerde manier risico's in kaart te brengen, te evalueren en – door er proactief mee om te gaan – beter te beheersen. De organisatie inventariseert risico's en de gevolgen van de risico's en verbindt er beheersmaatregelen aan. Door al in een vroeg stadium na te denken over de mogelijke risico's die de organisatie loopt, wil men de kans dat het gevaar zich voordoet reduceren en de eventuele impact ervan beperken. In de praktijk is het een combinatie van beide. Risicomanagement is een nadrukkelijk onderdeel binnen de BIO.

De dynamiek van de ontwikkelingen in de omgeving van de gemeente is van invloed op het dreigingsbeeld waarop gemeentelijke organisaties zich moeten instellen. Deze dynamiek vereist een cyclische benadering

© IB&P BV 2020

van informatiebeveiliging (Plan, Do, Check, Act) door onder andere het uitvoeren van risicoanalyses. In een risicoanalyse wordt de actualiteit en volledigheid van de aanwezige beveiligingsmaatregelen periodiek vergeleken met de actuele dreigingen.

De Informatiebeveiligingsdienst (IBD) van VNG geeft ondersteuning aan gemeenten voor het opstellen van het informatiebeveiligingsbeleid. Zij geven aan dat de scope van het informatiebeveiligingsbeleid alle gemeentelijke processen omvat, de onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Bevindingen

- Alle gemeenten en verbonden partijen hebben een vastgesteld informatiebeveiligings- en privacybeleid, maar de gemeenten geven niet of nauwelijks sturing of (directe) richtlijnen aan de verbonden partijen op het gebied van informatiebeveiliging. In veel gevallen waren de beleidstukken gebaseerd op het informatibeveiligingsbeleid template van de IBD (VNG).

- In het rekenkamerrapport 'Grip op samenwerking?' uit 2014 is aangegeven dat de sturing en controle op samenwerkingsverbanden – in het bijzonder vanuit de raad – onvoldoende is. Tevens is geconcludeerd dat de gemeenten niet systematisch risicoanalyses opstellen, waarin de risico's van samenwerkingsverbanden voor de gemeente in kaart worden gebracht. Door het ontbreken van deze analyses is de informatievoorziening en aandacht ook niet afgestemd op het risicoprofiel van het samenwerkingsverband.

- De gemeenten zijn gestart met het maken van (informatiebeveiliging) risicoanalyses. Het opstellen van de risicoanalyses gebeurt echter nog niet systematisch. Ook de risico-inventrarisatie rondom de risico's die de gemeenten lopen binnen de samenwerking met de verbonden partijen worden niet geïnventariseerd/uitgevoerd.

- De informatiebeveiligingsrisico's en beheersingsmaatregelen zijn bij de gemeenten niet opgenomen in de gemeentelijke programmabegroting.

- De meeste verbonden partijen hebben een proces voor risicomanagement waarbij de informatiebeveiligingsrisico's en beheersmaatregelen jaarlijks worden geïdentificeerd en beoordeeld.

- In één van de aangeleverde stukken met betrekking tot een risico-inventarisatie is het 'niet voldoen aan de AVG' opgenomen als risico. In de jaarstukken 2019 van Servicepunt 71 (gemeente Oegstgeest) is het niet op orde hebben van informatiebeveiliging en bescherming van persoonsgegevens opgenomen als risico.

- Er is regelmatig overleg tussen de vertegenwoordiger van de gemeente in het algemeen bestuur van de verbonden partij en de verbonden partij. Hierbij staat informatiebeveiliging zelden op de agenda. Daarnaast vindt bij een aantal verbonden partijen ambtelijk overleg plaats. In dit ambtelijk overleg is geen specifieke aandacht voor informatiebeveiliging en/of gegevensbescherming.

- Bij enkele gemeenten is de gemeenteraad genoemd als communicatiedoelgroep in het communicatieplan over de informatiebeveiliging. Echter is er geen invulling gegeven aan deze communicatie richting de gemeenteraad.

© IB&P BV 2020

- Bij enkele verbonden partijen is vastgelegd welke gegevens mogen worden uitgewisseld met partners.

- Elke gemeente neemt deel aan een aantal samenwerkingsverbanden/ gemeenschappelijke regelingen. In daarvoor opgestelde samenwerkingsovereenkomsten is niets vastgelegd over informatiebeveiliging. Ondanks dat er regelmatig overleg is tussen de gemeente en de verbonden partij, komt bij dit overleg informatiebeveiliging onvoldoende aan de orde. Door de gegevensuitwisseling met de verbonden partijen is het belangrijk dat de informatievoorziening betrouwbaar – ofwel in dit geval: veilig – is. Gebreken in de (beveiliging van) informatie bij de ene organisatie kan immers direct gevolgen hebben voor de bedrijfsvoering bij een andere organisatie.

Weerstandsvermogen

Conclusie 4 uit het rekenkamerrapport 'Beter sturen op digitale dienstverlening' (2016) luidt: *Op het gebied van informatieveiligheid lopen de gemeenten risico's. Omdat de gemeenten (nog) geen risicoanalyses hebben uitgevoerd, zijn de risico´s ten aanzien van informatiebeveiliging niet voldoende in beeld.*
Aanbeveling 4 luidt: *Zorg voor risicoanalyses betreffende informatiebeveiliging en voer de Baseline Informatieveiligheid Gemeenten (BIG) in. In 2016 is hier niet aan voldaan. De risico's dienen opgenomen te worden in de paragraaf 'Weerstandsvermogen' van de Programmabegroting.*

In de paragraaf 'Weerstandsvermogen' van de programmabegrotingen van de gemeenten staan wel risico's vermeld. Dit betreft echter geen informatiebeveiligingsrisico's en/of beheersingsmaatregelen. De gemeenschappelijke regeling Duivenvoorde van de gemeenten Wassenaar en Voorschoten heeft in haar jaarrekening 2019 een paragraaf informatieveiligheid en privacy opgenomen. De gemeenten Wassenaar en Voorschoten zijn voornemens om met ingang van volgend jaar een aparte paragraaf over informatiebeveiliging op te nemen in de begroting.

Toelichting
Aanvullende maatregelen die nog nodig zijn om de informatiebeveiligingsrisico's in beeld te brengen zijn het uitvoeren van penetratietesten, kwetsbaarheidsanalyse en steekproeven.

Samenwerkingsverbanden

Regionale sociale diensten, uitvoeringsdiensten, andere overheidsinstanties en verdere ketenpartners (zoals de GGD en de GGZ), krijgen steeds meer aandacht voor informatiebeveiliging en privacy. De verwachting is dan ook dat zij meer eisen gaan stellen op dat gebied, en mogelijk in de toekomst alleen zaken willen en/of mogen doen met gemeenten die hun zaakjes op orde hebben. Het zou toch – op z'n minst – erg teleurstellend zijn als je om deze reden niet kunt samenwerken in een keten? En: bestuurlijk liggen dit soort zaken vaak gevoelig.

Het is op dit moment nog niet zo dat een certificering op de BIO mogelijk of verplicht is, maar het is niet ondenkbaar dat dat in de nabije toekomst wel het geval zal zijn. Maar ook zonder de eis van certificering geldt dat als je in het nieuws bent geweest met datalekken, dit ook zeker doordringt bij ketenpartners. Dat maakt je minder aantrekkelijk en minder betrouwbaar als gemeente.

© IB&P BV 2020

3.3 Verantwoording

Algemeen

Onder verantwoording wordt in dit onderzoek verstaan: op welke wijze wordt over de informatiebeveiliging en privacy gerapporteerd aan een hoger echelon.

Het is de verantwoordelijkheid van de gemeente om ervoor te zorgen dat mensen hun privacy-rechten kunnen uitoefenen. Privacy-rechten zijn het recht op inzage; rectificatie, wissing, beperking van verwerking; overdraagbaarheid en bezwaar[6]. De gemeente is de zogenoemde verwerkersverantwoordelijke. Ook al gaat het over verwerkingen die de gemeente heeft uitbesteed (=verwerker). In de verwerkersovereenkomst worden werkafspraken vastgelegd met deze verwerker(s).

Heeft de gemeente of de verwerker een datalek dat gemeld moet worden aan de Autoriteit Persoonsgegeven (AP), dan moet dit door de gemeente als verwerkingsverantwoordelijke binnen 72 uur gemeld worden aan de AP. Als een verwerker kennis krijgt van een (mogelijk) datalek moet hij dit conform de standaard verwerkersovereenkomst gemeenten binnen 24 uur aan de gemeente melden.

Er is geen wettelijke meldplicht aan de gemeenteraad. Hoe en waarover de gemeenteraad wordt geïnformeerd is niet in privacywetgeving vastgelegd, maar kan wel in het privacy beleid worden beschreven. De gemeenteraad zou wel jaarlijks een jaarverslag gegevensbescherming moeten ontvangen van de Functionaris Gegevensbescherming (FG). In het jaarverslag zit informatie over datalekken.

Bevindingen

- Alleen de gemeente Leidschendam-Voorburg rapporteert over de informatiebeveiligingsrisico's aan het managementteam. De verantwoording en controle is vooral gericht op financiële resultaten.
- Gebleken is dat de gemeenteraad maar weinig vragen over het onderwerp informatiebeveiliging en gegevensbescherming stelt. Dit kan een uitvloeisel van de rolopvatting zijn, maar betekent ook dat de raad weinig zicht heeft op de stand van zaken in de uitvoeringspraktijk.
- Er zijn door de gemeenten geen controles uitgevoerd bij de verbonden partijen op het gebied van informatiebeveiliging en/of privacy.
- De verbonden partijen hebben aangegeven te rapporteren (minimaal jaarlijks) aan het management over informatiebeveiliging en privacy. In het jaarverslag van de verbonden partij is soms een rapportage over informatiebeveiliging en/of privacy opgenomen.
- De verbonden partijen rapporteren alleen intern op het gebied van informatiebeveiliging en privacy en melden nauwelijks zaken aan de gemeente. Daar staat tegenover dat gemeenten helemaal geen meldingen doen aan de verbonden partijen.
- In de onderzoeksperiode is er bij enkele gemeenten voorlichting over informatiebeveiliging en privacy gegeven aan de gemeenteraad.

[6] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten

© IB&P BV 2020

Toelichting
Het vertrekpunt is een complete inventarisatie van de informatiebeveiligingsrisico's, inclusief de risico's die voortvloeien uit het samenwerken met de verbonden partijen. Op basis van deze inventarisatie kan een rapportageformat worden opgesteld en zijn concrete afspraken te maken over de periodiciteit van rapporteren. Zonder structurele rapportage ontbreekt het aan sturingsmogelijkheden.

Datalekken

In de periode 2018 tot met de eerste helft van 2020 hebben drie van de vier gemeenten beveiligingsincidenten geregistreerd in een datalekkenregister, waarvan één datalek is gemeld aan de Autoriteit Persoonsgegevens (AP). De gemeente Oegstgeest gebruikt het incidentenregister ook om de opvolging van maatregelen te monitoren. Eén gemeente heeft geen datalekkenregister, maar geeft wel aan dat er beveiligingsincidenten en datalekken zijn geweest in de periode 2018 tot en met de eerste helft van 2020.

- Er worden niet veel beveiligingsincidenten en datalekken geconstateerd. Dat kan betekenen dat ze er ook daadwerkelijk niet zijn geweest. Waarschijnlijk ligt hier echter een kans voor meer bewustwording wat betreft het herkennen van (potentiële) datalekken. Een datalek is een kans om te leren. Er is merkbaar dat in sommige gevallen een bepaalde 'meldingsangst' overheerst. Men is bang om slapende honden wakker te maken en medewerkers kunnen zich persoonlijk aangevallen voelen. Politieke gevoeligheid en onderlinge verhoudingen kunnen een rol spelen bij de beoordeling om een beveiligingsincident niet als 'te melden datalek' aan te merken, terwijl dat wel had gemoeten.

Elke gemeenteraad is via de jaarrekening geïnformeerd over het aantal datalekken in het betreffende jaar. De gemeenten communiceren niet in algemene zin over datalekken met hun inwoners. Op de websites van de gemeenten is geen informatie te vinden over datalekken. Betrokkenen bij een datalek worden telefonisch en/of per brief geïnformeerd. Er zijn gevallen waarbij geen melding van een datalek is gedaan aan de AP, maar waarbij betrokkenen wel zijn geïnformeerd.

- Indien verbonden partijen optreden als verwerker zijn zij doorgaans verplicht datalekken te melden aan de gemeente die optreedt als verwerkersverantwoordelijke. Hier kan echter in goed overleg van worden afgeweken in de verwerkersovereenkomst. Er zijn echter geen afspraken over het melden en de taakverdeling tussen de verbonden partijen en de gemeenten bij datalekken.

Bij datalekken en beveiligingsincidenten wordt wel gekeken naar maatregelen om het incident een volgende keer te voorkomen. Zoals het twee-paar-ogen principe bij het vullen van enveloppen. Niet elke gemeente legt deze maatregelen vast.

De meeste verbonden partijen onderzoeken en leggen datalekken vast. Het aantal datalekken bij de verbonden partijen varieert van enkele datalekken per jaar tot een wekelijkse melding van de datalekken aan de toezichthouder. Veelal betreft het verkeerd geadresseerde of bezorgde post, verzonden mailberichten aan de verkeerde adressant of (privé)mailadressen die in BCC hadden moeten staan. De datalekken worden door de verbonden partij gemeld aan de AP indien nodig.

De verbonden partij meldt een datalek niet altijd aan de betrokkene. Veelal omdat de betrokkene zelf niet op de hoogte is van het datalek (voorbeeld retour gekomen geopende post) of omdat het datalek

© IB&P BV 2020

waarschijnlijk geen ongunstige gevolgen heeft voor de persoonlijke levenssfeer. Het is ook niet altijd verplicht het datalek te melden aan de betrokkene.

Na het onderzoeken van een datalek worden ook vaak verbetervoorstellen voor intern gebruik opgesteld om eenzelfde datalek in de toekomst te voorkomen. Als verbetervoorstellen bij de verbonden partijen zijn genoemd: het verhogen van het bewustzijn als het gaat om privacy en informatiebeveiliging door middel van informatieverstrekking op het intranet en tijdens werkoverleggen, cursussen (e-learning) en posters. Bij een enkele verbonden partij wordt een nieuw beveiligd emailsysteem ingevoerd, dat de gebruiker waarschuwt bij het verzenden van email met gevoelige gegevens, zoals het Burgerservicenummer (BSN).

3.4 Operationele implementatie

Algemeen

Onder operationele implementatie wordt verstaan: de wijze waarop het beleid is omgezet in operationele procedures en hoe deze zijn geborgd binnen de organisatie. Een sprekend voorbeeld is het beheren van accounts en wachtwoorden. Eén van de technieken om informatie te beveiligen is de toepassing van tweefactorauthenticatie. Hierbij moeten twee stappen succesvol worden doorlopen om toegang te krijgen tot een account. De eerste stap is vaak het invoeren van een gebruikersnaam en wachtwoord. De tweede stap is iets dat je hebt (authenticator op de mobiele telefoon of speciale USB-key) of iets dat je bent (vingerafdruk of andere biometrische eigenschap). Kortom, er zijn twee factoren nodig om je identiteit te bevestigen.

Dit is een voorbeeld van een operationele implementatie van een beleidsrichtlijn. Verhoudingsgewijs is er (bewust) vrij veel tijd gestoken in het onderzoeken in hoeverre operationele implementatie heeft plaatsgevonden. Immers, het geduldige papier heeft alleen zin indien ernaar gehandeld wordt in de praktijk.

Praktijksituatie – herkenbaar?

Bij meerdere gemeenten is gestart met een nulmeting (GAP-analyse) om vast te stellen in hoeverre de BIO al is geïmplementeerd. Het valt op dat het moeilijk blijkt om na die nulmeting tot actie te komen. Regelmatig blijft het onderwerp liggen. Redenen die hiervoor genoemd worden, zijn:

- Er is geen vraag vanuit de organisatie. Dan wordt het een push vanuit IT, wat je niet wilt.
- De organisatie is in transitie waardoor er andere prioriteiten zijn. Of er zijn andere redenen waardoor het onderwerp geen prioriteit heeft.
- Het is nog onvoldoende duidelijk welke risico's zo hoog zijn dat directe actie noodzakelijk is.
- De relatie met de dienstverlening aan de burgers is onduidelijk.
- Het onderwerp wordt niet gedragen door het management.
- De nulmeting is in gang gezet door de bestuurder en niet door degenen die met de resultaten aan de slag moeten.

Bevindingen

- In het kader van de invoering van de BIO brengen de gemeenten de risico's in kaart. Geen enkele gemeente heeft dit voor de primaire processen afgerond. Dit behoeft meer aandacht. De te nemen

© IB&P BV 2020

maatregelen zijn veelal gebaseerd op de prioritering van de geïnventariseerde risico's. De meeste verbonden partijen zijn bezig met de invoering van de BIO.

- Een deel van de aangeleverde procedures is gebaseerd op de BIG en niet op de BIO. Sommige procedures zijn niet aanwezig of aangeleverd.

- Alle gemeenten en de meeste verbonden partijen hebben beheersingsmaatregelen genomen om het hacken van netwerken te voorkomen dan wel om de gevolgen van een hack zoveel mogelijk in te perken. Hier wordt invulling aan gegeven door de invoering van tweefactorauthenticatie, de inrichting van het netwerk, back-up en recovery procedures, een calamiteitenplan en uitwijkmogelijkheden.

- Voor wat betreft de fysieke beveiliging geldt dat er voor de niet publiek toegankelijke ruimten gebruik wordt gemaakt van een toegangscontrolesysteem. Dit om te voorkomen dat onbevoegden binnendringen. Toegang tot bepaalde ruimten is alleen mogelijk met een tag/druppel/pasje. Bezoekers aan de verbonden partij moeten zich melden bij de receptie/balie en worden opgehaald en begeleid.

- De gemeenten en de verbonden partijen hebben een vastgesteld screeningsbeleid. Bij het in diensttreden van medewerkers, zowel bij de gemeente als bij de verbonden partijen, is er aandacht voor de beveiliging. Medewerkers worden gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging.

- Door middel van opleiding, training en voorlichting wordt gewerkt aan de bewustwording over informatiebeveiliging en privacy. Het vrijblijvende karakter daarvan draagt echter niet bij aan een duurzaam effect. Bij de WODV is deelname aan e-learning informatieveiligheid en privacy verplicht.

- Er is op het intranet van de gemeenten informatie beschikbaar over informatiebeveiliging.

- Door het voeren van een 'clear desk' en 'clear screen' beleid, wordt de inzage van informatie door onbevoegden beperkt.

- De meeste verbonden partijen hebben de IT-infrastructuur uitbesteed. De verbonden partijen hebben de informatiesystemen geclassificeerd zodat duidelijk is welke bescherming nodig is en ze hebben maatregelen getroffen om onbedoelde of ongeautoriseerde wijzingen of misbruik van bedrijfsmiddelen waar te nemen dan wel te voorkomen door scheiding van taken. De meeste verbonden partijen verlenen alleen toegang vanuit een onvertrouwde omgeving naar een vertrouwde zone op basis van tweefactor-authenticatie.

- De verbonden partijen hebben richtlijnen opgesteld op het gebied van thuiswerken en gedragsregels voor het gebruik van bedrijfsmiddelen. De meeste verbonden partijen stellen hulpmiddelen beschikbaar voor het beheren van wachtwoorden.

- Alle verbonden partijen verlenen toegang tot een informatiesysteem na autorisatie door een bevoegd persoon. De toegangsrechten worden toegekend op basis van functiescheiding op grond van een risicoafweging. Bij de meeste verbonden partijen worden de toegangsrechten periodiek beoordeeld. Ook beschikken de meeste verbonden partijen over een formele registratie- en afmeldprocedure voor het beheren van gebruikersaccounts.

© IB&P BV 2020

- Bij de verbonden partijen benadrukt en stimuleert het management het belang van deelname aan opleiding en training op het gebied van informatiebeveiliging. Bij de verbonden partijen is iedereen in staat om veilig beveiligingsissues te melden.

- Om een register van verwerkingen actueel te houden is onderhoud nodig. Nieuwe verwerkingen moeten worden toegevoegd en wijzigingen in bestaande verwerkingen kunnen ook gevolgen hebben voor het register. Eén gemeente heeft nog geen register van verwerkingen opgesteld. De overige aangeleverde registers zijn voor het grootste deel goed gevuld, maar zijn nog niet op alle punten volledig. Zo zijn niet overal de categorieën 'betrokkenen' of 'bewaartermijnen' ingevuld en staat de categorie 'bijzondere persoonsgegevens' onder de categorie 'reguliere persoonsgegevens'. Ook is niet duidelijk hoe actueel de registers zijn.

- In en verwerkersovereenkomst worden de te verwerken persoonsgegevens vastgelegd, die een verwerker (bijvoorbeeld een leverancier) in opdracht van de gemeente verwerkt. In een groot aantal verwerkersovereenkomsten van de gemeenten is niet aangegeven hoe een passend niveau van beveiliging wordt aangetoond door de verwerker.

- De verbonden partijen hebben regels opgesteld over het gebruik van de bedrijfsmiddelen en informeren de medewerkers over het belang van informatiebeveiliging.

- De verbonden partijen hebben een register van verwerkingen opgesteld zoals vanuit de AVG vereist wordt. Ook hebben zij verwerkingsovereenkomsten opgesteld met verwerkers volgens de eisen vanuit de AVG. De meeste verbonden partijen beschikken over een procedure die de actualiteit van het verwerkingsregister borgt.

- De gemeenten dan wel werkorganisaties hebben een aantal Data Protection Impact Assessments (DPIA's) uitgevoerd, maar dit is nog onvoldoende om een compleet beeld te hebben van de privacyrisico's bij verwerkingen die een hoog risico opleveren voor betrokkenen. De opvolging van maatregelen verdient nog wel aandacht. Net als het structureler uitvoeren van DPIA's.

Toelichting

Alle gemeenten zijn nog bezig met de invoering van de BIO. De ene gemeente is hier verder mee dan de andere. Met de invoering van de BIO moeten de gemeenten (opnieuw) een risicoanalyse uitvoeren. Een structurele rapportage over de geïnventariseerde risico's ontbreekt. De genomen en te nemen maatregelen zijn uiteenlopend.

Een aantal procedures is nog gebaseerd op de BIG (voorloper van de BIO). De BIO is sinds 2019 het normenkader voor de informatiebeveiliging. Procedures dienen regelmatig te worden gereviewd. Voor de werking van de procedures maakt de overgang van de BIG naar de BIO soms weinig verschil. De implementatie van het beleid in procedures verdient aandacht.

Elke gemeente heeft een breed pakket aan beheersingsmaatregelen genomen om het hacken van het netwerk en het binnendringen van gebouwen te voorkomen. Zo heeft elke gemeente een toegangscontrolesysteem. Door voorlichting en informatieverstrekking via het intranet en de uitvoering van technische maatregelen wordt gepoogd om de gevolgen van een hack, het binnendringen van gebouwen en datalekken te verzachten.

© IB&P BV 2020

Er is een aantal verwerkersovereenkomsten afgesloten. Nergens is gebleken dat er een daadwerkelijke controle wordt uitgevoerd op de wijze waarop externe partijen met persoonsgegevens omgaan. De relaties tussen de gemeenten en de verbonden partijen bestonden al voor de komst van de AVG. De contractuele verhoudingen zijn nadien niet of nauwelijks veranderd. Ook is niet of nauwelijks in kaart gebracht of de verbonden partij verwerker, gezamenlijk verwerkingsverantwoordelijke of zelfstandig verwerkingsverantwoordelijke is.

3.5 Technische analyse

Algemeen

De technische analyse is erop gericht om in kaart te brengen of de IT-omgevingen van de vier gemeenten kwetsbaar zijn voor aanvallen van buitenaf of binnenuit. De kwetsbaarheden zijn onderzocht door het uitvoeren van penetratietesten (black box scans van buitenaf) met een beperkte doorlooptijd op de internet facing (web)pagina's van de gemeenten. Daarnaast zijn interne kwetsbaarhedenscans uitgevoerd op de ITinfrastructuur van de gemeenten.

Een penetratietest (of pentest) is een technisch geavanceerde poging om de beveiliging van een informatiesysteem, website of netwerk te kraken en daarop in te breken. Het doel van een penetratietest is om te bepalen in hoeverre de onderzochte servers en webapplicaties, die de gemeente onderhoudt en beheert, kwetsbaar zijn voor een aanval vanaf het internet. Ook wordt gecontroleerd op robuustheid en beveiliging van deze servers en webapplicaties. Een penetratietest wordt uitgevoerd om inzicht te krijgen in de effectiviteit van het (beveiligings-) systeem en om verbeterpunten te definiëren. Voor dit onderzoek heeft elke gemeente een aantal webapplicaties (URL's = adres van een www-pagina op het internet) opgegeven. Op deze webapplicaties is een penetratietest uitgevoerd.

Bij een kwetsbaarhedenscan wordt, veelal middels geautomatiseerde tools, de IT-infrastructuur onderzocht. Alle servers en netwerkelementen die binnen de scope van het onderzoek vallen, worden onderzocht op zo'n 142.000 bekende kwetsbaarheden. Met een dergelijke scan wordt duidelijk of de organisatie de systemen up-to-date heeft. De kwetsbaarhedenscan geeft weer of de IT-infrastructuur goed is ingericht en geen verkeerde of verouderde configuratie bevat.

In verband met de vertrouwelijkheid van de gevonden kwetsbaarheden zijn niet alle bevindingen en details in dit verslag opgenomen. Een samenvatting van de bevindingen uit de penetratietest en kwetsbaarheden-scan is opgenomen in het vertrouwelijke rapport per gemeente.
De technische analyse is terug te vinden in de reeds separaat aan de gemeentelijke CISO verstrekte penetratietest en kwetsbaarheden-scan rapport (vertrouwelijk).

Bevindingen penetratietest

- De helft van de gemeenten heeft in de onderzoeksperiode penetratietesten laten uitvoeren door andere partijen. Er zijn weinig of geen penetratietesten uitgevoerd bij de verbonden partijen. Bij het uitgangspunt dat minimaal eenmaal per jaar een penetratietest gehouden dient te worden, voeren gemeenten nu te weinig penetratietesten uit.

- Bij de uitgevoerde penetratietesten is een aantal zorgwekkende kwetsbaarheden gevonden, die een veiligheidsrisico opleveren. Bij alle gemeenten zijn op de onderzochte applicaties verouderde softwareversies aangetroffen. Op alle onderzochte webservers zijn verouderde protocollen voor

© IB&P BV 2020

encryptie (versleuteling) ingeschakeld en wordt gebruik gemaakt van verouderde cipher suites. Cipher suites zijn beschrijvingen van rekenprocessen, die helpen bij de beveiliging van een netwerkverbinding.

- De meeste onderzochte websites maken geen gebruik van HSTS-headers. Een HSTS-header is een beveiligingsmechanisme om websites te beschermen tegen aanvallen. Met de HSTS-header kunnen bepaalde man-in-the-middle aanvallen worden voorkomen. Een man-in-the-middle aanval is een aanval waarbij informatie tussen twee communiceren partijen wordt onderschept, zonder dat beide partijen daar weet van hebben.

- Niet alle onderzochte webapplicaties maken gebruik van een anti-caching header. Met een anti-caching header wordt voorkomen dat privacygevoelige informatie wordt opgeslagen. Daarnaast beschikken niet alle webapplicaties over correct geconfigureerde security headers. Met een goed geconfigureerde header kan de webserver de browser instrueren waar bepaalde content vandaan mag komen, zodat de rest kan worden geblokkeerd.

- Bij de penetratietest zijn Cross-Site scripting aanvalsmogelijkheden gevonden. Cross-site scripting is een fout in de beveiliging van een webapplicatie, waarbij een bepaalde invoer niet juist wordt verwerkt en bij een aanvaller terecht kan komen. Daarnaast is bij een aantal websites de firewall zodanig geconfigureerd dat naast de poorten die noodzakelijk zijn voor de correcte werking van de webapplicatie ook poorten voor de mailserver open staan. Het is noodzakelijk spoedig te onderzoeken of deze poorten inderdaad open moeten staan.

- Niet alle domeinen zijn voorzien van een Certificate Authority Authorization (CAA)-record. Een CAA-record is een internetbeveiligingsmechanisme waarmee de domeinnaamhouder het eigendom van de website kan bewijzen. Sommige applicaties geven een te uitgebreide foutmelding weer. Een uitgebreide foutmelding kan een aanvaller informatie verschaffen over kwetsbaarheden. Daarnaast zijn Domain Name System Security Extensions (DNSSEC) niet ingeschakeld voor alle domeinen. DNS is het systeem dat op het internet gebruikt wordt om namen van computers naar numerieke adressen (IP-adressen) te vertalen en omgekeerd. DNSSEC voorziet het DNS-record van een digitale handtekening, zodat gecontroleerd kan worden of het record authentiek is.

- Op de onderzochte applicaties zijn extern ingeladen softwarebibliotheken aangetroffen. Hierdoor kan malware geïmporteerd worden. Het is mogelijk gebleken om in een applicatie een account aan te maken met verhoogde rechten.

- Niet alle cookies van de webapplicatie beschikken over de juiste attributen. Cookies zijn kleine bestandjes met informatie die de browser van de eindgebruiker gebruikt om zich te identificeren. Het is dan ook belangrijk dat de inhoud van deze cookies correct is én niet in verkeerde handen terechtkomt.

- Verdere detaillering wordt in dit (openbare) rapport bewust achterwege gelaten. De uitkomsten van de penetratietests en de kwetsbaarhedenscans zijn gedeeld met de respectievelijke gemeenten en komen uitgebreider aan bod in de vertrouwelijke rapportage per gemeente.

© IB&P BV 2020

Bevindingen kwetsbaarhedenscan

- De interne netwerken van de gemeenten zijn niet afdoende gesegmenteerd, waardoor het risico bestaat dat onbevoegden zich toegang tot het netwerk kunnen verschaffen.
- Het patch-proces is niet effectief ingericht voor de tijdige installatie van alle beveiligings-patches.
- Het beheer van de servers is niet beperkt tot diegenen die het beheer moeten uitvoeren.
- Het draadloze netwerk is niet afdoende afgeschermd van het interne (bedrade) netwerk, waardoor gasten op het wifinetwerk (draadloos) zich mogelijk toegang kunnen verschaffen tot de verschillende interne managementsystemen van de gemeente.
- Het interne netwerk bevat geen beheerzone, wat wel wordt aangeraden om te implementeren zodat de beheeractiviteiten en beheertoegang zijn gescheiden van het reguliere netwerk (waar de medewerkers op werken).
- Het bedrade netwerk van sommige gemeenten beschikt niet over een Network Access Control (NAC)-oplossing. De NAC regelt de toegang tot het netwerk, door te controleren of voldaan wordt aan bepaalde voorwaarden.

Toelichting

Sommige gemeenten zijn in afwachting zijn van de invoering van GGI-Veilig. Bij GGI-Veilig is het mogelijk om producten en diensten voor de operationele informatiebeveiliging (waaronder penetratietesten) centraal af te nemen.

Eén van de methoden om de beveiliging van grote netwerken te beheren is om ze te verdelen in gescheiden netwerkdomeinen. De domeinen kunnen worden gekozen op basis van betrouwbaarheidsniveaus (bijvoorbeeld openbaar toegankelijk domein, bureaubladdomein, serverdomein), organisatieafdelingen (bijvoorbeeld personeelszaken, financiën) of een combinatie hiervan.

Door het indelen van het netwerk in verschillende logische zones naar gelang van de kwetsbaarheid en gevoeligheid van de informatie, wordt de kwetsbaarheid verminderd. Ook het beperken van de onderlinge toegang tussen de zones draagt bij aan het verminderen van de kwetsbaarheid. Om de logische toegang tot het netwerk te beperken kan gebruik gemaakt worden van een NAC-oplossing.

Patches zijn doorgaans kleine programma's die aanpassingen maken om fouten op te lossen, of verbeteringen aan te brengen in bestaande software en/of hardware. Het patchen van kwetsbaarheden is verplicht vanuit de BIO (control 12.6.1). Het patchmanagement behoort te zijn vastgelegd in duidelijke afspraken en procedures.

Aanvallen op systemen kunnen plaatsvinden door het misbruiken van functies van informatiesystemen en hardware die 'aan' staan. Het proces om ervoor te zorgen dat functies die niet nodig zijn worden uitgeschakeld en/of van het systeem worden verwijderd heet 'hardening'. Hardening van de actieve IT-infrastructuur, servers en netwerkcomponenten is een belangrijke stap om persoonlijke gegevens en informatie te beschermen en is nodig om de basis op orde te hebben. Het hardeningsbeleid van de

© IB&P BV 2020

gemeente geeft richting aan de wijze waarop de gemeente maatregelen wenst te treffen voor hardening. Draadloze netwerken vereisen speciale aandacht in verband met de mogelijkheid om toegang te krijgen tot het interne netwerk. Personen die toegang hebben tot het draadloze netwerk behoren alleen toegang te krijgen tot het internet. Toegang tot het interne netwerk via het draadloze netwerk behoort via een VPN-verbinding te lopen. Op deze manier ontstaat een strikte scheiding tussen beveiligd en onbeveiligd verkeer.

3.6 Wat kunnen gemeenten van elkaar leren?

Algemeen

Wat kunnen de vier gemeenten van elkaar leren en van andere gemeenten in het land? Deze vraag staat hier centraal.

Bevindingen

- De WVOLV-gemeenten verschillen onderling veel van elkaar. Daarnaast werken de gemeenten allemaal met andere regio's en verbanden samen. De WVOLV-gemeenten weten weinig van elkaar hoe zij werken en wat er speelt. Dit maakt de informatie-uitwisseling en het leren van elkaar lastig.

- De 'best practices', handreikingen en voorbeelden van de Informatiebeveiligingsdienst voor gemeenten (IBD) kunnen vaker als uitgangspunt gebruikt worden. Zodoende werk je als gemeente al vanuit hetzelfde document of met dezelfde methodiek. Dit vergemakkelijkt het samenwerken en onderling leren.

- De gemeente Leidschendam-Voorburg heeft de verantwoordelijkheid voor informatiebeveiliging en privacy goed in de lijn belegd. De aanpak en producten van Leidschendam-Voorburg worden regelmatig gebruikt als voorbeeld. Deze gemeente kan hiervoor als voorbeeld voor andere gemeenten dienen. De overige gemeenten zijn juist sterker in het voldoen aan de verantwoordingsplicht vanuit de AVG en hebben een completer overzicht van bijvoorbeeld hun verwerkingen en datalekken.

- De CISO's en FG's van de gemeenten hebben periodiek collegiaal overleg met andere gemeenten buiten de WVOLV. Een overleg met de verbonden partijen ontbreekt.

Toelichting

Er is geen overlegstructuur tussen de WVOLV-gemeenten. Door de uitwisseling van informatie tussen de gemeenten en met de verbonden partijen te bevorderen, ontstaat wederzijds begrip en wordt de mogelijkheid om van elkaar te leren, gecreëerd. Voorbeeld: de gemeenten hebben de informatiebeveiligingsrisico's nog niet volledig in beeld, hier kunnen de gemeenten van elkaar leren.

Een regionaal overleg voor CISO's en/of FG's met periodieke bijeenkomsten, waarbij kennis en ervaring worden uitgewisseld, strekt nadrukkelijk tot aanbeveling. Dit hoeft niet expliciet binnen de WVOLV-gemeenten te gebeuren, maar kan ook binnen andere samenwerkingsverbanden plaatsvinden.

© IB&P BV 2020

4 Conclusies

© IB&P BV 2020

4. Conclusies

In dit hoofdstuk staan de te trekken conclusies op basis van het onderzoek centraal. Ze zijn gebaseerd op de opgesomde bevindingen uit het vorige hoofdstuk. In dit (openbare) rapport worden alleen algemeen geldende conclusies getrokken en geen conclusies per gemeente. Samenvattend: alle zaken met betrekking tot informatiebeveiliging staan wel in de steigers, maar behoeven nog veel aandacht in de systematische uitwerking in de praktijk.

4.1 Beleid, verantwoording en operationele implementatie

De centrale vraag van de RKC is hoe de gemeenten opvolging hebben gegeven aan de zorg voor risicoanalyses betreffende informatiebeveiliging. Hierbij is een 'stoplichtmodel' gebruikt waarbij de kleuren de onderstaande betekenis hebben. De aanbevelingen zijn opgenomen in hoofdstuk 5.

Groen betekent op orde.

Oranje heeft aandacht nodig.

Rood is urgent/zorgwekkend.

- Uit het onderzoek blijkt dat het informatiebeveiligingsbeleid en de organisatie rondom informatieveiligheid bij de gemeenten in opzet op orde is. De meeste verbonden partijen hebben een informatiebeveiligingsbeleid opgesteld, dat periodiek wordt bijgesteld.
- De gemeenten stellen niet systematisch informatiebeveiligingsrisicoanalyses op, waarbij ook de informatiebeveiligingsrisico's met de verbonden partijen worden geïnventariseerd. De gemeenten hebben de risico's nog niet volledig in kaart gebracht. De meeste verbonden partijen hebben de informatiebeveiligingsrisico's en beheersmaatregelen wel beschreven.
- De operationele procedures worden zelf niet periodiek beoordeeld en – waar nodig – geactualiseerd. Een deel van de procedures is nog gebaseerd op de BIG in plaats van de BIO terwijl de BIO vanaf 1 januari 2020 van kracht is, met daaraan voorafgaand een overgangsperiode.
- In een groot aantal standaard verwerkersovereenkomsten is het aantonen van een passend niveau van informatiebeveiliging door de verwerkende partij niet ingevuld. Dit maakt sturing en controle op de beveiligingsmaatregelen bij deze verwerkers feitelijk onmogelijk.
- De informatiebeveiligingsrisico's en beheersingsmaatregelen zijn in de onderzoeksperiode niet opgenomen in de gemeentelijke programmabegroting.
- In het rekenkamerrapport 'Beter sturen op digitale dienstverlening' is geadviseerd expliciet te sturen op het formuleren van concrete kaders op informatiebeveiliging door verbonden partijen. Aangezien de gemeenten geen sturing of (directe) richtlijnen aan de verbonden partijen geven op het gebied van informatiebeveiliging, is aan dit advies geen invulling gegeven.

© IB&P BV 2020

In het rekenkamerrapport ‘Grip op samenwerking?’ is aangegeven dat de sturing en controle op samenwerkingsverbanden onvoldoende is. Dit is niet verbeterd. De verantwoording en controle is nog te veel gericht op financiële resultaten.

Gebleken is dat de gemeenteraad maar weinig vragen over het onderwerp informatiebeveiliging en gegevensbescherming stelt. Dit kan een uitvloeisel van de rolopvatting zijn, maar betekent ook dat de raad weinig zicht heeft op de stand van zaken in de uitvoeringspraktijk.

Binnen de gemeenten worden niet veel beveiligingsincidenten en datalekken geconstateerd. Ter informatie: in 2019 ontving de AP 4.624 datalekmeldingen vanuit overheidsorganisaties. Een stijging met 27% ten opzichte van 2018.

Door middel van opleiding, training en voorlichting wordt gewerkt aan de bewustwording over informatiebeveiliging en gegevensbescherming.

4.2 Penetratietesten en kwetsbaarhedenscans

Op basis van de uitgevoerde penetratietesten en kwetsbaarhedenscan is in dit rapport een aantal algemene conclusies te trekken. Meer details zijn te vinden in de deelrapporten per gemeente.

De gemeenten voeren te weinig penetratietesten uit. Uit de in dit onderzoek uitgevoerde penetratietesten is gebleken dat de netwerken binnen de gemeenten kwetsbaar zijn door de aanwezigheid van verouderde software, verouderde cipher suites en protocollen voor encryptie en het niet gebruiken van de juiste headers. Deze kwetsbaarheden behoeven op korte termijn aandacht.

De serverzones, gebruikerszone en beheerzone dienen verder opgesplitst te worden en het verkeer tussen de interne zones beperkt tot het absoluut noodzakelijke.
De procedure voor het patchen dient strikter te worden gehandhaafd om verouderde en kwetsbare software te voorkomen.

4.3 Conclusies per gemeente

De genoemde aanbevelingen in dit rapport zijn in meer en mindere mate voor alle gemeenten van toepassing. De met name technische tekortkomingen en conclusies per gemeente zijn vermeld in de deelrapporten per gemeente.

- Deelrapport Leidschendam-Voorbrug
- Deelrapport Oegstgeest
- Deelrapport Voorschoten
- Deelrapport Wassenaar

De vertrouwelijke rapporten met de resultaten van de penetratietest en de kwetsbaarhedenscan zijn reeds gedeeld met de verantwoordelijke functionaris (CISO) van de respectievelijke gemeenten. In deze rapporten is specifiek aangegeven welke kwetsbaarheden binnen de informatiebeveiliging van de gemeente zijn ontdekt met aanbevelingen om deze zo spoedig mogelijk te verhelpen. Deze rapporten bevatten dus de meeste (technische) detaillering.

© IB&P BV 2020

Summier overzicht van bevindingen:

Gemeente	Op orde	Aandacht nodig	Zorgwekkend
Leidschendam-Voorburg	Privacy en informatiebeveiligings-beleid	Informatiebeveiliging staat op agenda van de gemeenteraad Procedures uitwerken volgens BIO Opstellen verwerkingsregister Registratie van beveiligings-incidenten en datalekken	Geen structurele uitvoering van pentesten – wel noodzakelijk gebleken
Oegstgeest	Privacy en informatiebeveiligings-beleid	Informatiebeveiligings-risico's onvoldoende in kaart Uitvoering DPIA's behoeft aandacht Datalekken worden onvoldoende herkend Informatiebeveiliging staat niet op agenda van de gemeenteraad	Geen structurele uitvoering van pentesten – wel noodzakelijk gebleken
Voorschoten	Privacy en informatiebeveiligings-beleid	Informatiebeveiligings-risico's onvoldoende in kaart Procedures uitwerken volgens BIO Informatiebeveiliging staat niet op agenda van de gemeenteraad Datalekken worden onvoldoende herkend	Geen structurele uitvoering van pentesten – wel noodzakelijk gebleken
Wassenaar	Privacy en informatiebeveiligings-beleid	Informatiebeveiligings-risico's onvoldoende in kaart Procedures uitwerken volgens BIO Datalekken worden onvoldoende herkend Informatiebeveiliging staat niet op agenda van de gemeenteraad	Geen structurele uitvoering van pentesten – wel noodzakelijk gebleken

© IB&P BV 2020

5 Aanbevelingen

© IB&P BV 2020

5. Aanbevelingen

Wat kan er verbeterd worden in het licht van de bevindingen en daaruit getrokken conclusies? Dat staat centraal in dit vijfde en tevens laatste hoofdstuk. De aanbevelingen zijn van uiteenlopende aard en enkele zijn in het bijzonder gericht aan de gemeenteraden. Het rapport wordt afgesloten met een slotbeschouwing en enkele stellingen voor een debat.

5.1 Algemene aanbevelingen

Voer minimaal jaarlijks risicoanalyses uit op het gebied van informatiebeveiliging en pas op basis van de uitkomsten het informatiebeveiligingsbeleid aan.
Maak hierbij gebruik van de ondersteuningsproducten van de IBD om de onderlinge samenwerking tussen gemeenten en verbonden partijen te stimuleren. Dat geldt ook voor technische risico's door nieuwe kwetsbaarheden, die dagelijks ontstaan door de voortschrijdende technologie en de inventiviteit van hackers.

Richt het procesmanagement van de informatiebeveiliging in volgens de Plan-Do-Check-Act (PDCA)-cyclus.
Dit borgt een gezonde verhouding tussen bedrijfsvoering en beveiligingsmaatregelen door het centraal stellen van risicomanagement en het aldus reduceren van informatiebeveiligingsrisico's tot een acceptabel niveau. 'In control' zijn betekent immers niet 'geen risico lopen'.

Neem in de gemeentelijke programmabegroting een paragraaf op over de informatiebeveiligingsrisico's en beheersingsmaatregelen.
Neem in de overleggen met de verbonden partij informatiebeveiliging en privacy op als vast agendapunt. Maak met alle partijen afspraken over de gegevensverstrekking, waaronder de uitwisseling van persoonsgegevens.

Los de kwetsbaarheden op die uit de penetratietesten zijn gebleken en laat vervolgens periodiek audits en penetratietesten uitvoeren door gespecialiseerde bureaus.
Installeer (security) software updates zo snel mogelijk na verschijning. Schakel de verouderde cipher suites uit en schakel moderne veilige cipher suites in. Configureer de security headers op een correcte wijzen en maak gebruik van HSTS-headers en anti-caching headers.

Deel het netwerk in met verschillende logische zones naar gelang de kwetsbaarheid en gevoeligheid van de informatie.
Beperk de onderlinge toegang tussen de zones. Stel een patch- en hardeningsbeleid op (voor zover nog niet aanwezig) en monitor de naleving hiervan.

Richt het toezicht op de naleving van verwerkersovereenkomsten in.
Als verwerkingsverantwoordelijke is de gemeente verantwoordelijk voor de gehele verwerking en keten van (sub)verwerkers. Actief toezicht op het nakomen van de gemaakte afspraken, waaronder de naleving van de beveiligingsmaatregelen, is noodzakelijk. In de regel geschiedt dit door eens per jaar om een verantwoording te vragen bij de verwerker.

Betrek de relevante verbonden partijen bij het (regionaal) overleg voor CISO's en/of FG's ten behoeve van kennis- en ervaring uitwisseling.
De bij dit onderzoek betrokken organisaties zijn op het gebied van informatiebeveiliging en privacy met dezelfde zaken bezig en er valt de nodige winst te behalen door elkaar meer op te zoeken en met elkaar af te stemmen.

© IB&P BV 2020

5.2 Aanbevelingen voor de gemeenteraad

Alle gemeenten zijn nog bezig met de invoering van de BIO. De ene gemeente is hier verder mee dan de andere. Met de invoering van de BIO moeten de gemeenten (opnieuw) een risicoanalyse uitvoeren. De BIO-zelfevaluatie maakt onderdeel uit van de ENSIA-verantwoordingssystematiek, maar is geen verplicht onderdeel in de rapportage naar de raad. ENSIA streeft naar een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatiebeveiliging. Met ENSIA sluit de verantwoording over informatieveiligheid aan op de planning en control-cyclus van de gemeente.

De rol van de raad in het kader van privacy en informatiebeveiliging is niet vastgelegd. Uit het onderzoek blijkt dat er weinig vragen door de raad gesteld zijn over de thema's informatiebeveiliging en gegevensbescherming. Er zijn verschillende mogelijkheden (voorlichting, e-learning, et cetera) om de betrokkenheid van de raad bij het thema te vergroten.

Aanbevelingen

Geef aan het college aan welke informatie nodig is om als effectieve toezichthouder op de informatie-beveiliging en privacybescherming te kunnen functioneren. Laat via de reguliere P&C-producten rapporteren over de voortgang. Agendeer jaarlijks een speciale vergadering gewijd aan informatiebeveiliging.

Vergroot de betrokkenheid van de raad bij informatiebeveiliging en privacy.
Dit door (periodiek) in gesprek te gaan met de uitvoerende medewerkers over deze thema's of door eisen te stellen aan de informatievoorziening op dit vlak.

Volg net als de ambtelijke organisatie als raad tenminste jaarlijks een training in bewustwording over informatiebeveiliging en privacy.
Dit kan bijvoorbeeld door hier jaarlijks een raadsinformatiebijeenkomst voor te reserveren en/of door jaarlijks een actuele e-learning module op het onderwerp te doorlopen.

5.3 Slotbeschouwing

Aan de interviews en het aanleveren van documenten hebben alle gemeenten en verbonden partijen meegewerkt. De gemeenten hebben niet alle gevraagde documenten aangeleverd, met name enige procedures ontbraken.

Het verkrijgen van de vrijwaringsverklaring voor het kunnen uitvoeren van de technische analyse leverde vertraging op. De gemeenten hebben het afgeven van een vrijwaringsverklaring onderzocht en met elkaar afgestemd. Uiteindelijk is de vrijwaringsverklaring door alle gemeenten verstrekt.

Ondanks dat er nog punten voor verbetering van de informatiebeveiliging en privacy zijn, is er in de afgelopen periode door talloze medewerkers hard gewerkt om de gemeentelijke informatiebeveiliging zo goed mogelijk te verbeteren.
IB&P bedankt de geïnterviewden en andere betrokken, die in welke vorm dan ook een bijdrage hebben geleverd aan dit rapport voor hun openheid, inzet en medewerking.

© IB&P BV 2020

Bijlagen

© IB&P BV 2020

IB&P
Dat gaat je niets aan

Handreiking gemeenteraden: Praatplaat Rekenkameronderzoek Informatiebeveiliging

De Rekenkamercommissie Wassenaar, Voorschoten, Oegstgeest en Leidschendam-Voorburg (WVOLV) heeft een onderzoek laten uitvoeren naar de informatiebeveiliging binnen de gemeentelijke organisaties en de daaraan verbonden partijen. Deze handreiking is bedoeld om binnen de gemeenteraden de dialoog te starten over informatiebeveiliging aan de hand van diverse denkrichtingen over acht vragen.

1 Wie is verantwoordelijk voor informatiebeveiliging?

- Informatiebeveiliging heeft een sterk technisch karakter en hoort derhalve bij de ICT-afdeling.
- Bedrijfsvoering dekt ook informatiebeveiliging en dus hoort dit onderwerp niet thuis op de bestuurstafel.
- Omdat het college vanuit de privacywet (AVG) eindverantwoordelijk is voor persoonsgegevens verwerken, is zij dat ook voor het beveiligen daarvan.

2 Welke rol heeft de gemeenteraad in het veilig houden van de gemeente?

- Informatiebeveiliging is te technisch van aard voor raadsleden en dus vooral iets voor het college om op te sturen.
- De gemeenteraad dient toe te zien op de (wettelijke) ondergrens. Dat is al moeilijk genoeg, zo leert de praktijk.
- Een sleutelrol is weggelegd voor de gemeenteraad vanwege de grote informatiebeveiligingsrisico's die er zijn.

3 Is informatiebeveiliging nu vooral risico's beheren of verplichte maatregelen invoeren?

- De invoering van het normenkader 'Baseline Informatiebeveiliging Overheid' staat gelijk aan informatiebeveiliging.
- Wát er moet gebeuren is wel duidelijk; het is vooral een kwestie van (samen) organiseren en invoeren.
- Beveiligingsmaatregelen zijn grotendeels bekend, maar dienen verband te houden met risico's die de gemeente loopt.

4 Hoe verhoudt de digitaliseringopgave zich tot de privacy van burgers en medewerkers?

- Een excellente dienstverlening aan burgers en bedrijven is altijd de hoogste prioriteit.
- De Europese privacywet (AVG) is nóg een wet waaraan voldaan moet worden. Er zijn er zoveel.
- Privacywaarborgen zijn randvoorwaardelijk bij het digitaliseren van de dienstverlening aan burgers en bedrijven.

5 Hoeveel verantwoordelijkheid dragen de verbonden partijen op het gebied van informatiebeveiliging?

- Verbonden partijen zijn gehouden aan de privacywet (AVG) en dragen derhalve zelf eindverantwoordelijkheid.
- Over de verantwoordelijkheid van de gemeente in relatie tot verbonden partijen zijn schriftelijke afspraken vereist.
- Verbonden partijen zijn zélf verantwoordelijk, maar de gemeenten zien daar wel structureel op toe.

6 Hoe ver dient de jaarlijkse controle op de naleving van beveiligingsmaatregelen bij verbonden partijen te gaan?

- Het maken van schriftelijke afspraken tussen gemeenten en verbonden partijen is voldoende. Geen controle nodig.
- Gemeenten zouden de verantwoording vanuit verbonden partijen moeten stimuleren, maar het blijft optioneel.
- De gemeente is eindverantwoordelijk voor veel taken die verbonden partijen uitvoeren dus de controle dient substantieel te zijn.

https://ib-p.nl

Bijlage 2: Onderzoeksvragen

1. In hoeverre is de sturing van de gemeenten aan verbonden partijen toereikend op het gebied van informatiebeveiliging?

2. In hoeverre zijn de risico's en beheersingsmaatregelen in kaart gebracht in de paragraaf Weerstandsvermogen van de gemeentelijke programmabegrotingen?

3. In hoeverre zijn de gemeenteraden en de Informatiebeveiligingsdienst (IBD) geïnformeerd over het aantal datalekken, de resultaten van de penetratietests en de verbetervoorstellen bij gemeenten en verbonden partijen?

4. Op welke wijze communiceren de gemeenten met hun bevolking over ontstane datalekken?

5. Wat kunnen de vier gemeenten van elkaar leren en van andere gemeenten in het land?

6. Welke beheersingsmaatregelen hebben de gemeenten en verbonden partijen genomen om hacken van computernetwerken, binnendringen van gebouwen en andere datalekken te voorkomen, respectievelijk de gevolgen ervan te verzachten?

7. In hoeverre hebben de gemeenten en verbonden partijen de risico's volledig in kaart gebracht en welke maatregelen zijn er eventueel aanvullend nodig?

8. Wat was het aantal datalekken en de aard en omvang ervan?

9. Wat was het aantal uitgevoerde penetratietests en de resultaten ervan?

10. Hoe eenvoudig is het om gevoelige informatie te krijgen via hacken van het gemeentelijk computernetwerk?

11. Tot welke verbetervoorstellen hebben de datalekken en penetratietests geleid?

© IB&P BV 2020

Bijlage 3: lijst met geïnterviewde personen

Gemeente Wassenaar

	Datum	Naam	Organisatie
1.	21/8/2020	Edwin Ykema	Werkorganisatie Duivenvoorde
2.	2/9/2020	FG	Werkorganisatie Duivenvoorde
3.	24/8/2020	Nina Keltjens	Gemeente Wassenaar
4.	24/8/2020	Jaap Kleinhesselink	Gemeente Wassenaar

Gemeente Voorschoten

	Datum	Naam	Organisatie
1.	21/8/2020	Edwin Ykema	Werkorganisatie Duivenvoorde
2.	2/9/2020	FG	Werkorganisatie Duivenvoorde
3.	17/8/2020	Minke Elkerbout	Gemeente Voorschoten

Gemeente Oegstgeest

	Datum	Naam	Organisatie
1.	17/7/2020	Suzanne de Wilde	Servicepunt 71
2.	19/8/2020	Robert Haasnoot	Servicepunt 71
3.	3/9/2020	Fred Kromhout	Gemeente Oegstgeest

Gemeente Leidschendam-Voorburg

	Datum	Naam	Organisatie
1.	21/8/2020	Edwin Ykema	Werkorganisatie Duivenvoorde
2.	2/9/2020	FG	Werkorganisatie Duivenvoorde
3.	24/8/2020	Nina Keltjens	Gemeente Wassenaar
4.	24/8/2020	Jaap Kleinhesselink	Gemeente Wassenaar

© IB&P BV 2020

Geïnterviewde verbonden partijen

	Datum	Naam	Organisatie
1.	21/8/2020	Edwin Ykema	Werkorganisatie Duivenvoorde
2.	2/9/2020	FG	Werkorganisatie Duivenvoorde
3.	17/7/2020	Suzanne de Wilde	Servicepunt 71
4.	19/8/2020	Robert Haasnoot	Servicepunt 71
5.	3/8/2020	Rob Vroonland	Belastingsamenwerking Gouwe Rijnland
6.	3/8/2020	Joop Kempers	Belastingsamenwerking Gouwe Rijnland
7.	3/8/2020	Lidy van Kesteren	Belastingsamenwerking Gouwe Rijnland
8.	31/7/2020	Helen Kortekaas	Gemeenschappelijk Regeling Kust, Duin en Bollenstreek
9.	23/7/2020	Lizette Ploos van Amstel	Werkorganisatie Duivenvoorde/Inkoopbureau H10
10.	27/7/2020	Matthijs van der Vorm	Regionale Dienst Openbare Gezondheidszorg
11.	27/7/2020	Nourddine Chaara	Regionale Dienst Openbare Gezondheidszorg
12.	25/8/2020	Stef van Putten	Omgevingsdienst West Holland
13.	25/8/2020	Ilona Nusteen	Omgevingsdienst West Holland
14.	25/8/2020	Frank Heijmerberg	Omgevingsdienst West Holland
15.	25/8/2020	Saskia Boer	Omgevingsdienst West Holland
16.	24/7/2020	Desirée Bolsius	Veiligheidsregio Haaglanden
17.	19/8/2020	Marcel Solleveld	Werkorganisatie Duivenvoorde/ Avalex
18.	2/9/2020	Marcel Caljouw	Avalex

© IB&P BV 2020

Verbonden partijen

	Werkzaam voor				Onderzoek	
Naam	Wassenaar	Voorschoten	Oegstgeest	Leidschendam	Interview	Enquête
Werkorganisatie Duivenvoorde	●	●			●	
Servicepunt 71			●		●	●
Belastingsamenwerking Gouwe Rijnland	●	●	●		●	
Gemeenschappelijke Regeling Kust, Duin en Bollenstreek	●		●		●	
Inkoopbureau H10	●	●		●	●	●
Regionale Dienst Openbare Gezondheidszorg		●	●		●	
Omgevingsdienst West Holland		●	●		●	
Veiligheidsregio Haaglanden	●			●	●	
Gemeenschappelijke Regeling Avalex	●			●	●	
GGD en VT Haaglanden	●			●		●
Metropoolregio Rotterdam Den Haag	●			●		●
Omgevingsdienst Haaglanden	●			●		●
Gemeenschappelijke Regeling Holland Rijnland		●	●			●
Veiligheidsregio Holland Midden		●	●			●

Opmerking: De Werkvoorziening Rijswijk e.o. is niet opgenomen in het overzicht, omdat deze organisatie in liquidatie is en over enkele maanden niet meer zal bestaan.

© IB&P BV 2020

Bijlage 4: Gebruikte afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BCC	Black Carbon Copy
BIG	Baseline Informatiebeveiliging Nederlandse Gemeenten
BIO	Baseline Informatiebeveiliging Overheid
BSN	Burgerservicenummer
CAA	Certification Authority Authorization
CISO	Chief Information Security Officer
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DPIA	Data Protection Impact Assessment
ENSIA	Eenduidige Normatiek Single Information Audit
FG	Functionaris Gegevensbescherming
GGD	Gemeentelijke Gezondheidsdienst
GGI	Gemeentelijke Gemeenschappelijke Infrastructuur
HTTP	Hypertext Transfer Protocol
HSTS	HTTP Strict Transport Security
IBD	Informatiebeveiligingsdienst voor gemeenten
IP	Internet Protocol
NAC	Netwerk Access Control
PDCA	Plan, Do, Check, Act
RKC	Rekenkamercommissie
URL	Uniform Resource Locator
VPN	Virtueel Particulier Netwerk
VR	Veiligheidsregio
WODV	Werkorganisatie Duivenvoorde
WVOLV	Wassenaar, Voorschoten, Oegstgeest, Leidschendam-Voorburg

© IB&P BV 2020