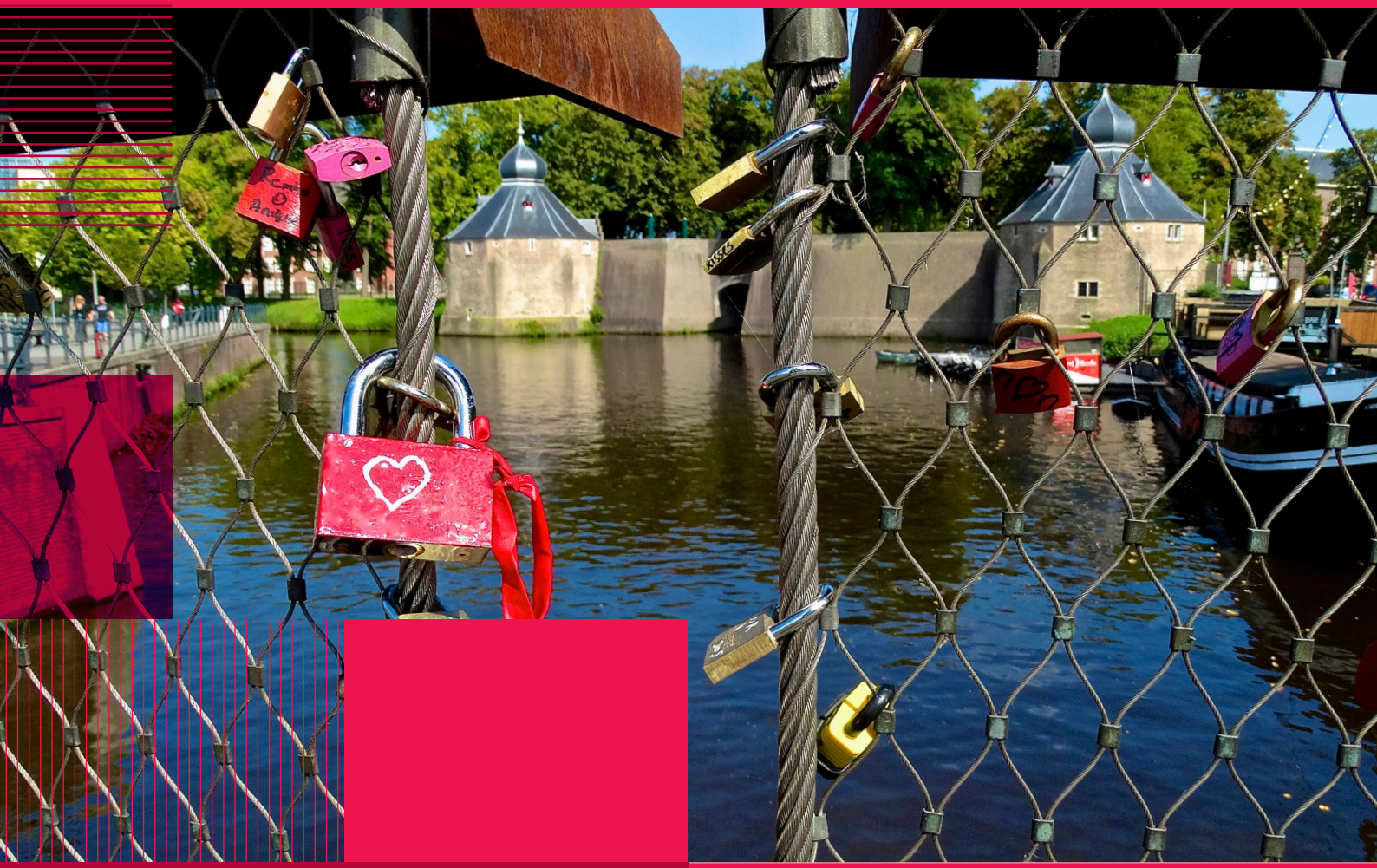
Rekenkamer Breda

Informatiebeveiliging bij de Gemeente Breda



Gemeente Breda

REKENKAMER BREDA

Informatiebeveiliging bij de gemeente Breda

Nov. 2016

‘Informatiebeveiliging bij de gemeente Breda’

Rekenkamer Breda
Contact: secretaris Dr. Juliët Wiggers 076-5294686 of ja.wiggers@breda.nl
Voorzitter: Dr. Joop Roebroek
Leden: mr. Karel Tercic en drs. Lex van Eijndhoven RA
Foto kaft: Wessel Keizer©

Nov. 2016

INHOUDSOPGAVE Pagina

BESTUURLIJK RAPPORT 'INFORMATIEBEVEILIGING BIJ DE GEMEENTE BREDA'

1. Inleiding

Informatiebeveiliging is een onderwerp dat steeds belangrijker wordt voor overheden/gemeenten. Het toenemende aantal cyberaanvallen, de grote hoeveelheid persoonsgegevens waar gemeenten verantwoordelijk voor zijn (en de privacykwesties hieromtrent) en de steeds uitgebreidere wetgeving omtrent informatiebeveiliging en privacy, nopen gemeenten om zich steeds beter te beveiligen en om steeds bewuster om te gaan met (vertrouwelijke) informatie.

Verlies van gegevens(dragers), onzorgvuldig of oneigenlijk gebruik, het manipuleren van informatie en/of inbraak in informatiesystemen kan grote schade opleveren voor overheden, burgers en bedrijven. Burgers, bedrijven en organisaties moeten erop kunnen vertrouwen, dat gegevens in goede handen zijn bij de overheid. Het is belangrijk om ook als gemeenteraad goed bij dergelijke belangrijke strategische kwesties betrokken te zijn.

De Rekenkamer heeft in de periode dec. 2015-juli 2016 onderzoek verricht naar de stand van zaken van de informatiebeveiliging binnen de gemeente Breda. Over de onderzoeksopzet (zie Rapport van bevindingen hoofdstuk 1 - 2) is vooraf overleg gevoerd met de raadsfracties en de ambtelijke organisatie. Het onderzoek richt zich enerzijds op hoe goed de gemeente Breda digitaal beveiligd is, anderzijds op het gemeentelijke informatiebeveiligingsbeleid en hoe het staat met de uitvoering hiervan (voldoet Breda aan de gestelde normen?). Het onderzoek naar de digitale beveiliging is door een extern bureau (Hoffmann Bedrijfsrecherche BV) uitgevoerd. In verband met de vertrouwelijkheid van de uitkomsten rapporteert het rekenkamerrapport hier slechts op hoofdlijnen over dit deel van het onderzoek[1]. De Rekenkamer heeft zelf het onderzoek naar het informatiebeveiligingsbeleid gedaan (zie Rapport van bevindingen hoofdstuk 3 en 4).

2. Samenvatting bevindingen uit het digitale beveiligingsonderzoek

Het bureau heeft diverse kwetsbaarhedentests en hacktests gedaan om te onderzoeken hoe goed de toegang tot het externe en het interne netwerk en de WIFI beveiligd is. Daarnaast heeft het bureau een forensic readiness scan verricht om te onderzoeken of de gemeente Breda goed voorbereid is op het opsporen en aanpakken van aanvallen/lekken. Overall blijkt uit het onderzoek dat de gemeente Breda op sommige punten (redelijk) goed beveiligd is, maar dat op andere punten nog extra maatregelen nodig zijn. Uit de forensic readyness test blijkt dat de gemeente Breda nog niet voldoende forensic ready is. Alle bevindingen uit het onderzoek zijn meteen aan de ambtelijke organisatie doorgegeven en op alle punten zijn inmiddels acties ingezet en/of gepland. In dit rapport volgt uitsluitend een rapportage op hoofdlijnen.

Externe netwerk

De externe website van de gemeente Breda is over het geheel genomen redelijk goed beveiligd, zo constateert Hoffmann. Er zijn 12 kwetsbaarheden ten aanzien van het externe netwerk geconstateerd, die geen van allen zeer kritiek zijn of een hoog risico vormen. Dat betekent dat het externe netwerk niet gemakkelijk van buitenaf te hacken is. De gevonden kwetsbaarheden hebben vooral te maken met verouderde[2] software, te weinig versleutelde verbindingen en interne gebruikersnamen die op te sporen zijn. De constatering is dat een kwaadwillende niet zomaar binnen kan komen, maar dat de kwetsbaarheden wel eventueel gebruikt kunnen worden voor een gerichtere aanval.

[1] Een uitgebreidere samenvatting is als geheim document ter inzage neergelegd voor raadsleden.

[2] Verouderde software ondersteunt de beveiliging niet meer (optimaal) en biedt geen beveiligingsupdates meer. Daardoor levert dit beveiligingsrisico's op.

Interne netwerk
Het interne netwerk is veel minder goed beveiligd. In totaal trof het bureau 8 kwetsbaarheden in het interne netwerk aan: 4 kritieke kwetsbaarheden, 2 hoog risico kwetsbaarheden, 1 medium en 1 laag risico kwetsbaarheid. Eenmaal binnen blijkt het mogelijk te zijn om toegang te krijgen tot alle gegevens en systemen van de gemeente Breda en zelfs beheerder en 'eigenaar' van de systemen te worden (domain administrator en domain controller met alle rechten om zaken te wijzigen, te verwijderen of toe te voegen). Dat lukte de onderzoekers op meerdere manieren en via meerdere toegangen. Ook hier hebben de kwetsbaarheden vooral te maken met verouderde software en onbeveiligde c.q. te weinig gelimiteerde verbindingen/toegangen. Daarnaast o.a. met een serie zwakke wachtwoorden en met oude accounts en installatiebestanden (die nog wel toegang bieden). Zoals gezegd, heeft de gemeente Breda de kwetsbaarheden inmiddels zoveel mogelijk aangepakt en opgeruimd naar aanleiding van de rapportage van Hoffmann.

De WIFI
De interne (medewerkers-)WIFI is goed beveiligd, zo blijkt uit het onderzoek: het is de onderzoekers niet gelukt om binnen te komen. De openbare (gast)WIFI is minder goed beveiligd. Door in de buurt van andere gebruikers in te loggen, bleek het mogelijk om contact te leggen met andere ingelogde apparaten, deze te scannen op kwetsbaarheden en mogelijke toegangen te forceren.

De Forensic readiness scan
Daarnaast heeft het bureau een forensic readiness scan uitgevoerd. Om goed voorbereid te zijn, is het belangrijk om:

1. Een uitgewerkt en actief incidentenmanagement te hebben;
2. De loggegevens voor langere tijd te bewaren, zodat achterhaald kan worden wat er gebeurd is en waar de aanval/het lek vandaan komt;
3. Goede recente backups van alle bestanden en systemen te hebben, zodat snel een recente schone backup teruggezet kan worden.

1. Incidentenmanagement
De gemeente Breda heeft in het Informatiebeveiligingsplan 2014 (gemeente Breda, 2014) kort beschreven hoe om te gaan met incidenten. Er is nog geen uitgebreider concreet incidentenprotocol opgesteld, noch een uitgebreid meldingssysteem voor datalekken, zo constateert het bureau.
Het externe netwerk van de gemeente Breda bevat een zogeheten honeypot-systeem[3], dat bedoeld is om gegevens over aanvallen te verzamelen. Dat systeem is momenteel verouderd en de gemeente Breda doet tot op heden niets met de verzamelde gegevens. Op advies van het bureau is nu een nieuwe versie gevraagd, waar de gemeente zelf toegang toe krijgt om aanvallen te kunnen analyseren.

2. Bewaren loggegevens
Het bureau constateert dat over het geheel genomen de voor forensisch onderzoek relevante loggegevens te beperkt bewaard worden bij de gemeente Breda. De gemeente heeft geen centraal logsysteem van alle loggegevens, er worden te weinig (relevante) gegevens bewaard en de bewaartermijnen zijn veelal te beperkt om goed te kunnen onderzoeken waar een aanval of een lek vandaan komt. Ook heeft nog geen risicoclassificatie van gegevens plaatsgevonden en kunnen de bedrijfskritische informatie en processen beter geborgd worden. De gemeente Breda is wat dit betreft nog niet voldoende forensic ready, zo is de conclusie.

3. Backups
De gemeente Breda heeft een uitgewerkte backup procedure en er worden voldoende backups bewaard, waardoor snel vrij recente schone backups kunnen worden teruggezet. Dit heeft zich in de afgelopen twee jaar twee keer voorgedaan bij grote incidenten/aanvallen, waarbij de

[3] Dit systeem is geïnstalleerd door het Nationale Cybersecurity Centrum (NCSC) en heeft als doel om aanvallers aan te trekken en gegevens over hun activiteiten vast te leggen.

gemeente snel heeft ingegrepen. Het bureau constateert wel dat beter gecheckt moet worden of de wettelijke bewaartermijnen aangehouden worden voor alle backups.

Conclusies en aanbevelingen uit het digitale beveiligingsonderzoek
Het bureau heeft een hele serie technische aanbevelingen opgesteld op basis van de bevindingen. Deze zijn, zoals gezegd, meteen doorgestuurd naar en opgepakt door de ambtelijke organisatie. Gaande het onderzoek zijn al enkele acties ondernomen, zoals het ingewikkelder maken van de benodigde wachtwoorden en het opruimen van verouderde accounts. Ook heeft de gemeente Breda de aanschaf van enkele nieuwe (software)systemen voor 2016 en 2017 op de rol staan, o.a. een nieuwe gemeentelijke website [4] (www.breda.nl) in 2017.

3. Samenvatting van het informatiebeveiligingsbeleid van de gemeente Breda

Informatiebeveiliging is echter niet uitsluitend een ict-kwestie, maar heeft vooral ook te maken met hoe omgegaan wordt met informatie, met menselijk gedrag, het uitvoeren van verantwoordelijkheden, een integraal informatieveiligheidsbeleid op alle (beleids)terreinen en met een ruime bekendheid hiermee bij iedereen. Daartoe is een strategisch gemeentebrede informatiebeveiligingsaanpak nodig, die alle beleidsterreinen, afdelingen en informatiestromen bestrijkt. Zoals de Visitatiecommissie Informatieveiligheid het formuleert: ‘Informatieveiligheid zou eigenlijk aan de basis van alle bedrijfsprocessen en alle belangrijke bestuurlijke vraagstukken moeten staan’ en ‘als voorwaarde voor succes moeten gaan voelen’.

Sinds 2013 stimuleert het Rijk gemeenten om de informatiebeveiliging te professionaliseren, uit te breiden en te verbeteren. De gemeente Breda heeft dit actief opgepakt en in 2014 een informatiebeveiligingsbeleidsplan vastgesteld, waarin de landelijke BIG-normen[5] als uitgangspunt genomen zijn (zie Rapport van bevindingen hoofdstuk 3). In de afgelopen twee jaar heeft de gemeente Breda daartoe stappen gezet in de vormgeving en uitvoering van de informatiebeveiliging (o.a. via het Uitvoeringsplan 2015). In 2015 heeft de gemeente samen met een groot aantal gemeenten een convenant met het Rijk gesloten en zich gecommitteerd om per 1 januari 2017 te gaan voldoen aan de landelijke BIG-normen. Vóór 2017 dient de gemeente via een GAP-analyse te onderzoeken in hoeverre zij voldoet aan de BIG-normen. Een landelijke Visitatiecommissie Informatieveiligheid voert in 2015-2016 gesprekken in 120 gemeenten om de stand van zaken te toetsen. De visitatiecommissie is in januari 2016 bij de gemeente Breda langs geweest (zie bijlage 3 voor Visitatierapport Breda).

De Rekenkamer heeft het informatiebeveiligingsbeleid onderzocht aan de hand van documentanalyses, gesprekken en een korte enquête onder alle afdelingshoofden van de gemeente Breda.
Overall blijkt uit het rekenkameronderzoek dat de gemeente Breda nog niet geheel aan alle BIG-normen voldoet en dat nog diverse aspecten nader uitgewerkt en uitgevoerd moeten worden (zie Rapport van bevindingen hoofdstuk 4).

De Rekenkamer constateert dat de gemeente Breda in de afgelopen twee jaar al belangrijke stappen heeft gezet op een aantal terreinen, maar dat andere terreinen nog zijn blijven liggen. De ondernomen werkzaamheden zijn tot op heden vooral gericht geweest op het opdoen van kennis door de eigen informatiemedewerkers, het verbeteren van de digitale veiligheid en het verrichten van audits en tests in deze, het inrichten van interne gemeentelijke verantwoordelijkheden en van de werkprocessen binnen de afdeling ‘Proces en Informatie’, en het verbeteren van het fysieke veiligheidsbeheer. Ook op het gebied van privacybescherming op het sociaal domein zijn enkele

[4] Dit ondanks dat de website van de gemeente Breda slechts 3 jaar oud is. De beveiliging van verouderde software wordt niet (goed) meer ondersteund en geüpdatet door het softwarebedrijf. Dat geeft aan hoe snel digitale systemen tegenwoordig verouderd zijn. Overigens bestaat ook onvrede met de huidige website: deze zou rommelig, onoverzichtelijk en te weinig praktisch zijn en te veel ruimte op de voorpagina geven aan twitter, shout- en allerlei andere berichten.

[5] BIG= Baseline Informatiebeveiliging Nederlandse Gemeenten, waarin basisnormen en richtlijnen staan.

stappen gezet, zoals een Privacy Impact Assessment bij de start van de decentralisaties in 2015, al zal die assessment periodiek opnieuw uitgevoerd moeten worden.

Aan een aantal zaken, die voorgenomen waren in het Uitvoeringsplan 2015, is de gemeente Breda niet of veel minder toegekomen, zo komt uit het onderzoek naar voren. Dit betreft met name het vergroten van de kennis en het bewustzijn binnen de gehele organisatie ten aanzien van informatieveiligheid, het gedrag van alle medewerkers ten aanzien van informatieveiligheid, acties om de uitkomsten van de verrichte audits, tests e.d. op te pakken, het verder uitwerken en oppakken van het incidentenmanagement (t.a.v. aanvallen en datalekken), het opzetten van een meldingssysteem naar de organisatie toe (en protocollen) bij incidenten als virusaanvallen, phishing mails, uitval van systemen en datalekken, en informatiebeveiligingsafspraken in contracten/overeenkomsten met leveranciers, partners en derden.

Ten aanzien van de BIG-normen constateert de Rekenkamer:

1. *Informatiebeveiligingsbeleidsplan*

De gemeente Breda heeft een informatiebeveiligingsplan (2014) en uitvoeringsplannen (2015 en 2016-2017), waarin benodigde maatregelen staan uitgewerkt om te gaan voldoen aan de BIG. Gaande het onderzoek van de Rekenkamer (dec. 2015-sept. 2016) heeft de gemeente Breda al diverse zaken aangepast, uitgevoerd en nieuwe acties voorgenomen in het in juni 2016 verschenen Informatieveiligheidsplan 2016-2017. Het Informatieveiligheidsplan en de uitvoeringsplannen zijn overigens niet in de raad besproken en niet door de raad vastgesteld. De gemeente Breda heeft geen separaat privacybeleidsplan.

2. *Organisatie en verantwoordelijkheden*

Binnen de gemeente Breda zijn inmiddels verschillende verantwoordelijkheden en gespecialiseerde beveiligings- en privacyfunctionarissen benoemd in de organisatie, i.c. binnen het College en het Servicebedrijf. Daarnaast is in principe iedere afdeling zelf verantwoordelijk voor de eigen informatiestromen en systemen, waardoor een versnippering in de verantwoordelijkheden en uitvoering bestaat. Uit de gesprekken en de rekenkamerenquête blijkt dat nog niet iedere afdeling precies weet wat alle aspecten van het informatiebeveiligingsbeleid behelzen en welke acties benodigd zijn. De Rekenkamer constateert derhalve dat de verantwoordelijkheden in de bredere gemeentelijke organisatie nog verder moeten worden versterkt, evenals de inbedding en uitvoering van een gemeentebreed strategisch informatieveiligheidsbeleid op iedere afdeling. Om dit te bewerkstelligen, zou de informatiebeveiliging meer centraal aangestuurd kunnen worden, onder meer door de benoeming van een Centrale Informatie Security Officer (CISO), zoals in de BIG-normen staat. De gemeente Breda heeft nog geen Centrale Informatie Security Officer (CISO) benoemd, die de centrale sturing vormgeeft, onafhankelijk opereert en zelfstandig rapporteert aan MT en gemeentesecretaris. Ook de VNG Visitatiecommissie Informatieveiligheid constateert dat in Breda nog geen CISO benoemd is en dat meer centrale sturing gegeven kan worden (zie bijlage 2 Visitatierapport Informatieveiligheid).

3. *Fysieke toegangsbeveiliging*

De fysieke toegangsbeveiliging en autorisaties ten aanzien van ruimtes en systemen zou nog verder moeten worden aangescherpt, zo komt uit de gesprekken naar voren. Het gaat hierbij onder meer om de beveiliging van het stadhuis en de beveiliging van het stadskantoor (i.c. van bepaalde (archief-, burgerzaken- en ICT-)ruimtes).

4. *Digitale beveiliging en tests*

De gemeente Breda heeft met name ten aanzien van de digitale beveiliging redelijk wat audits, tests en onderzoeken verricht, laten verrichten en meegewerkt aan landelijke onderzoeken. De gemeente Breda stelt zich daarin actief op. Het verbeteren van de digitale beveiliging is in de afgelopen 2 jaar ook een speerpunt geweest. Bij de gemeentelijke basisadministratie (GBA), het gemeentelijke uitkeringensysteem (SUWI) en DigiD toetst de gemeente Breda al langer actief op de bescherming van persoonlijke gegevens. Breda blijkt i.c. bij SUWinet aan alle getoetste normen te voldoen.

Bij de gedecentraliseerde taken op het sociaal domein is de uitwerking van privacyregels/protocollen in de uitvoeringspraktijk en de toetsing hiervan pas recent van de grond gekomen, zoals overigens bij de meeste gemeenten. Daar kunnen autorisaties (wie mag gegevens inzien en verwerken?), privacyprotocollen en beschermingsniveaus ten aanzien van alle werkprocessen (wat mag wel en wat mag niet in het verzamelen, doorsturen en gebruik van gegevens?) nog verder worden uitgewerkt. Strenge privacynormen en integrale hulp/zorg blijken in de praktijk vaak lastig te combineren te zijn, zo komt naar voren. De gemeente Breda heeft nog geen uitgewerkt Privacyhandvest met richtlijnen hoe om te gaan met gegevens van burgers die op allerlei terreinen verzameld worden. Een dergelijk uitgeschreven Privacyhandvest zou ook als leidraad kunnen fungeren voor de privacytoetsing.
De VNG adviseert, mede met het oog op de verscherpte privacynormen in het kader van de onlangs vastgestelde Europese Verordening Gegevensbescherming (EVG), om vóór 2018 alle werkprocessen en data te gaan inventariseren en te classificeren wat betreft beschermingsniveaus, privacyregels en protocollen. In het Bredase Informatieveiligheidsplan 2016-2017 (juni 2016) staat dataclassificatie en het inventariseren van beschermingsniveaus nu als voorgenomen actie vermeld.

5. *Het informatiebeveiligingsbudget*

In de gemeentelijke begroting-Jaarverslag staat geen budget voor informatieveiligheid vermeld, wel zijn bedragen gereserveerd voor de aanschaf van nieuwe software. In het Uitvoeringsplan Informatieveiligheid 2016-2017 staat voor maatregelen op het informatiebeveiligingsgebied een budget van €167.000,- begroot. Het is aan de raad om te beoordelen of dat voldoende is.

6. *Bewustwording, gedrag ten aanzien van informatieveiligheid*

Het menselijk gedrag blijkt één van de grootste risicofactoren te zijn in het veilig omgaan met informatie. Op dat vlak heeft de gemeente Breda pas zeer recent enkele acties[6] ondernomen. Uit het onderzoek blijkt dat het informatiebeveiligingsbeleid, de richtlijnen en de benodigde acties nog niet overal in de gemeentelijke organisatie bekend zijn. De gemeente Breda heeft ook nog niet veel ondernomen op het gebied van de bewustwording van medewerkers ten aanzien van de risico's en benodigde acties in het kader van informatiebeveiliging. De gemeente Breda heeft nog geen uitgewerkte gedragsrichtlijnen en/of 'nettiquette' [7] opgesteld en nog geen leertrajecten richting de medewerkers georganiseerd hoe veilig om te gaan met gegevens, bestanden en systemen. Ook bestaat nog geen standaard meldsysteem bij aanvallen, lekken e.d.. Op deze vlakken zijn zeker nog maatregelen nodig, zo komt uit de gesprekken naar voren en uit de enquête die de Rekenkamer in de organisatie gehouden heeft. Iedere afdeling is immers wel zelf verantwoordelijk voor de eigen data/systemen en ook het melden van datalekken moet door de afdelingen zelf plaatsvinden. Ook de Visitatiecommissie Informatieveiligheid constateert dat de bewustwording van medewerkers ten aanzien van informatieveiligheid en een bredere inbedding in de organisatie, nog belangrijke aandachtspunten zijn voor de gemeente Breda. Inmiddels (juni 2016) heeft de gemeente Breda een mystery guest onderzoek laten uitvoeren (o.a. om de clean deskpolicy te checken) en staat bewustwording als speerpunt benoemd in het recent verschenen Informatieveiligheidsplan 2016-2017 (juni 2016), met in de bijlage een Actieplan Ibewustzijn & risicodenken.

7. *Contracten, overeenkomsten en afspraken met leveranciers, partners e.d.*

Pas recent besteedt de gemeente Breda extra aandacht aan informatiebeveiliging en privacybescherming in de (nieuwe) contracten en overeenkomsten met leveranciers, partners en andere externe partijen. In de oudere contracten staat daar weinig over opgenomen. Om te gaan voldoen aan de BIG-normen en de Europese Verordening Gegevensbescherming is het zaak om alle contracten en overeenkomsten van de gemeente Breda met externe organisaties, zoals leveranciers en beheerbedrijven van digitale systemen, partners en andere externen, te gaan toetsen op afspraken en clausules ten aanzien van informatieveiligheid, privacybescherming, eigenaarschap van gegevens e.d., zo adviseert ook de VNG. Deze afspraken en de toetsing op

[6] Zoals in sept.-okt.2016 het verspreiden van een folder omtrent de risico's, een informatiesessie, een filmpje op de koffieautomaten en placemats met informatie in de kantine.

[7] Een nettiquette omvat de richtlijnen en gedragsregels voor het gebruik van internet en ander digitaal verkeer.

de naleving hiervan verdienen nog nadere aandacht binnen de gemeente Breda. De gemeente blijft immers verantwoordelijk voor wat er met gegevens gebeurt, ook al is de verzameling en verwerking van gegevens uitbesteed aan andere organisaties.

8. *Toetsing en verantwoording*

De verantwoording aan de raad met betrekking tot de informatiebeveiliging is vrij summier en beperkt zich tot een korte paragraaf in het jaarverslag, die vooral over digitale beveiliging gaat. Ook de toetsing van de informatiebeveiliging is vooral op de digitale beveiliging gericht binnen de gemeente Breda. Toetsing en verantwoording van informatieveiligheid is echter ook op andere vlakken nodig. Zoals de VNG benadrukt heeft informatieveiligheid veel verschillende kanten en is het nodig dat gemeenten een gemeentebreed strategisch informatieveiligheidsbeleid ontwikkelen. Dat gaat ervan uit dat informatieveiligheid een belangrijke basis voor de algehele bedrijfsvoering en de bedrijfskritische processen vormt, maar ook bijvoorbeeld in de vertrouwensrelatie met de burger. Informatieveiligheid en de bescherming van de privacy verdienen daarom meer aandacht, ook bij de raad, bijvoorbeeld via een periodieke rapportage aan de raad en/of een jaarlijkse bespreking/vaststelling van het jaarplan Informatieveiligheid. Ook de Visitatiecommissie Informatieveiligheid stelt in haar rapportage over 40 gemeenten (juni 2016) dat het belangrijk is dat de raad goed betrokken is bij dergelijke belangrijke strategische vraagstukken als informatieveiligheid en privacybescherming[8].

4. Conclusies

De Rekenkamer constateert overall dat de gemeente Breda werk maakt van informatiebeveiliging, maar dat op belangrijke punten zeker nog extra inzet nodig is. Qua digitale beveiliging lijkt de gemeente Breda niet uit de toon te vallen ten opzichte van andere gemeenten: qua digitale beveiliging doet de gemeente Breda het op sommige punten relatief goed (bijvoorbeeld de beveiliging van de website en de beveiliging van SUWInet), op andere punten moeten nog extra stappen gezet worden.

Belangrijk is dat informatiebeveiliging momenteel nog te veel vooral als een ict-kwestie wordt gezien en dat het zich nog beperkt tot een relatief kleine groep van ingewijden binnen de gemeente. De gemeente Breda moet nog extra stappen zetten om te komen tot een strategisch gemeentebreed informatiebeveiligingsbeleid en een brede verankering van de uitvoering. De Visitatiecommissie Informatieveiligheid (juni 2016) stelt dat informatieveiligheid eigenlijk een vast onderdeel zou moeten zijn van alle bedrijfsprocessen en bestuurlijke vraagstukken en ‘bij iedereen moet gaan voelen als voorwaarde voor succes’. Zo ver is het in Breda nog niet.

De bevindingen in het rekenkameronderzoek en het Bredase visitatierapport van de visitatiecommissie sluiten goed op elkaar aan en beide concluderen dat de gemeente Breda bezig is om aan de landelijke normen te gaan voldoen. Daarin moeten nog wel belangrijke stappen gezet gaan worden, zo blijkt uit de bevindingen van de Rekenkamer. Naast het werken aan een breed gedragen informatieveiligheidsaanpak in de gehele organisatie, gaat het onder meer om het versterken van de urgentie en de bewustwording omtrent informatiebeveiliging intern bij alle medewerkers, een duidelijke en uitgewerkte aanpak van de privacybescherming en van de beveiligingsafspraken met externe organisaties. Gaande het rekenkameronderzoek heeft de gemeente Breda al een aantal acties ingezet (zoals langere wachtwoorden, berichten over informatieveiligheid op Intranet, mystery guest-onderzoek in de organisatie) en een aantal maatregelen/stappen voorgenomen, die in 2016-2017 uitgevoerd gaan worden. De ambities om het informatieveiligheidsbeleid zo goed mogelijk vorm te geven, zijn wel aanwezig bij de gemeente Breda. Het advies van de Rekenkamer is om de hiervoor aangegeven zaken en de voornemens in het Informatieveiligheidsplan 2016-2017 (juni 2016) nu voortvarend ter hand te gaan nemen en uit te gaan voeren.
Op basis van de bevindingen doet de Rekenkamer een aantal aanbevelingen.

[8] Het advies om de raad goed te betrekken bij een gemeentebreed strategisch informatieveiligheidsbeleid is één van de 7 lessen die de visitatiecommissie aan gemeenten wil meegeven na gesprekken in 40 gemeenten (Visitatiecommissie Informatieveiligheid, juni 2016).

5. Aanbevelingen

1. Stel als raad vast of u voldoende informatie ontvangt over de verschillende aspecten van het informatiebeveiligingsbeleid, welke informatie u eventueel verder nodig acht over informatiebeveiliging en privacybescherming , op welke strategische punten en op welke momenten de raad een verantwoordingsverslag wenst te hebben/te bespreken en welke documenten de raad zelf wenst vast te stellen (b.v. periodieke rapportage, Jaarplan Informatieveiligheid, privacy-beleidsplan). Overweeg in deze om via een aparte rapportage over informatieveiligheid en een aparte rapportage over privacybescherming geïnformeerd te worden om aan beide voldoende aandacht te kunnen geven. Spreek als raad ook af welke kaders en eventuele leertrajecten de gemeenteraad zelf nodig heeft om veilig en bewust om te gaan met informatie(systemen) en welke informatie de raad hiertoe nodig heeft.

2. Verzoek het college van B&W om in 2016-begin 2017 te komen tot de uitvoering van een strategisch gemeentebrede informatiebeveiligingsaanpak; om in deze zo spoedig mogelijk te gaan voldoen aan alle BIG normen en aan alle privacynormen/regels, zoals die landelijk zijn vastgesteld. En om in 2017 zo goed mogelijk voorbereid te zijn op de normen die in de nieuwe Europese Algemene Verordening gegevensbescherming zijn opgenomen (waar gemeenten per 1 mei 2018 aan moeten voldoen).
   Verzoek in deze om aan alle digitale en technische beveiligingsnormen te gaan voldoen, maar ook om informatiebeveiliging en privacybescherming een integraal onderdeel van ieder beleidsproces en beleidsterrein te maken en alle gegevens te classificeren op beschermingsniveau, opdat alle gegevens waar de gemeente Breda verantwoordelijk voor is, goed beveiligd zijn. Verzoek het college om voldoende budget voor een goede inbedding en uitvoering van een gemeentebreed strategisch informatieveiligheidsbeleid ter beschikking te stellen. En verzoek het college periodiek te toetsen hoe het staat met de voortgang van de verschillende aspecten van het integrale informatiebeveiligingsbeleid.

3. Verzoek het College van B&W om het informatiebeveiligingsbeleid en de benodigde acties goed in te bedden in de bredere organisatie en beter te gaan verankeren op de diverse afdelingen, om de versnippering in verantwoordelijkheden tegen te gaan en een Chief Information Security Officer, zoals bedoeld in de BIG, in de organisatie te benoemen om meer centrale sturing te geven aan de informatiebeveiliging bij de afdelingen en gemeentebreed.

4. Verzoek het College van B&W om zo snel mogelijk bewustwordings- en leertrajecten omtrent informatiebeveiliging en privacybescherming naar alle gemeentelijke medewerkers in te zetten, zodat de regels en benodigde acties bij iedereen bekend zijn en iedereen weet op welke manier zij veilig om kunnen gaan met informatie, i.c. met vertrouwelijke en privacygevoelige informatie, welke risico's bestaan en wanneer eventueel een datalek of beveiligingsrisico gemeld moet worden.
   Verzoek in deze om een helder gedragsprotocol met gedragsrichtlijnen op te stellen en een zogeheten 'nettiquette', zodat de regels, richtlijnen en procedures en risico's met betrekking tot informatieveiligheid voor alle medewerkers, raadsleden en externe organisaties duidelijk zijn en medewerkers e.a. weten op welke punten het gedrag getoetst wordt. Verzoek het meldsysteem naar alle medewerkers toe te verbeteren met betrekking tot (risico's op) incidenten, virussen, phishing mails e.d en verzoek een meldsysteem ten aanzien van datalekken op te zetten en te zorgen dat alle medewerkers de benodigde kennis hebben welke datalekken gemeld moeten worden, aan wie en op welke manier.
   Verzoek het College om het informatiebewustzijn en het gedrag regelmatig te toetsen, systematisch te werken aan het leren in de organisatie en de kennis en alertheid van medewerkers voortdurend up-to-date te houden.

5. Verzoek het College om de privacyprotocollen en de werkprocessen in het sociaal domein verder uit te schrijven en op basis van een op te stellen Privacyhandvest periodiek te toetsen hoe het staat met de privacybescherming ten aanzien van gegevens van burgers, waar de gemeente de beschikking c.q. de verantwoordelijkheid over heeft.

6. Verzoek het College om alle contracten en overeenkomsten met leveranciers, partners, externen en andere ingehuurde bedrijven/organisaties te toetsen of deze voldoende clausules en afspraken omtrent informatieveiligheid en privacy bevatten en verzoek het College om te toetsen in hoeverre die afspraken en clausules nageleefd worden door de organisaties en bedrijven. Verzoek het College in kaart te brengen waar verbeteringen nodig zijn en de CISO een coördinerende en controlerende taak te geven.

Bijlage 1 RAPPORT VAN BEVINDINGEN

Het informatiebeveiligingsbeleid van de gemeente Breda

1. Inleiding

Informatiebeveiliging is een steeds belangrijker onderwerp voor gemeenten geworden. Door de toenemende digitalisering van informatie en de grote hoeveelheid persoonsgegevens die gemeenten in beheer hebben sinds de decentralisaties op het sociaal domein (WMO, jeugdzorg en participatiewet), is een goede beveiliging van systemen en gegevens steeds noodzakelijker geworden. De kans dat een incident veel schade aanricht, wordt steeds groter. Enerzijds vindt steeds meer uitwisseling van vertrouwelijke, privacygevoelige gegevens plaats tussen personen en organisaties (o.a. in het kader van integrale zorg) en wordt meer en meer digitaal gedeeld o.a. in het kader van de Open Overheid; Anderzijds hebben gemeenten inmiddels bijna iedere dag te maken met cyberaanvallen[9], verstoringen van de informatieveiligheid, pogingen hiertoe of andere (bijna) incidenten, zo meldt de Visitatiecommissie Informatieveiligheid (2016). Het gaat hierbij om aanvallen van buitenaf via internet of email (b.v. via phishing mails of gijzelingsvirussen), onveilige verbindingen en links, virussen via besmette bestanden/computers e.d. waardoor computers, systemen en bestanden overgenomen, afgeluisterd, geblokkeerd, versleuteld of beschadigd kunnen worden. Ook gaat het om eventuele informatielekken van binnenuit (al dan niet moedwillig) en onveilig omgaan met gegevens(dragers) c.q. oneigenlijk gebruik van bestanden en (vertrouwelijke) gemeentelijke gegevens. Onderzoek laat zien dat veel provincies en gemeenten hun informatiebeveiliging nog niet geheel goed op orde hebben en op dat vlak nog veel verbeteringen aan kunnen brengen (zie b.v. NCTV, 2015; Rekenkamer Lelystad, 2016; Randstedelijke Rekenkamer, 2016; Rekenkamercommissie Eindhoven, 2016; BN de Stem, artikel 22 juli 2016).

Het verlies van gegevens, oneigenlijk gebruik en/of het manipuleren van gegevens/informatie door onbevoegden c.q. kwaadwillenden, het infiltreren van digitale systemen en het lamleggen van ICT-systemen door criminelen e.d. kan ernstige gevolgen hebben voor overheden, burgers en bedrijven. Dit kan leiden tot grote financiële schade[10], fysieke beschadiging van systemen[11] en bestanden, schade voor burgers (b.v. door identiteitsfraude) en imagoschade voor overheden. Gegevens van burgers, bedrijven en organisaties moeten bij de overheid in goede, veilige handen zijn en burgers (en de gemeenteraad) moeten ervan op aan kunnen dat gemeenten veilig omgaan met informatie. Dat maakt dat de digitale beveiliging continu gemonitord moet worden om te zien of deze goed op orde is. Daarnaast moeten gemeenten ervoor zorgen dat alle betrokkenen (medewerkers, partners e.d.) veilig omgegaan met informatie en gegevens. Het

[9] VNG Visitatiecommissie Informatieveiligheid, '180 dagen onderweg', een verslag van gesprekken in 40 gemeenten, VNG, juni 2016. Het Nationale Cyber Security Centrum (NCSC) meldt dat momenteel elke 10 dagen wel een overheid of bedrijf melding maakt van een aanval met een gijzelingsvirus, waarbij hackers losgeld vragen (Binnenlands Bestuur 25 juli 2016). Inmiddels verschijnen in de media regelmatig berichten over cyberaanvallen, gijzelingsvirussen, fraudemails, onveilige websites, privacylekken e.d..

[10] Deloitte (april 2016) berekent in een onderzoek dat het waardeverlies door cyberrisico's voor de Nederlandse publieke sector op jaarbasis op ongeveer 2,4 miljard euro bedraagt. De waardedaling voor alle Nederlandse organisaties, inclusief bedrijven, bedraagt volgens Deloitte overall zo'n 10 miljard euro door cyberaanvallen (Binnenlands Bestuur Digitaal, 4 april 2016). Allerlei organisaties lopen risico op aanvallen. Zo meldt Binnenlands Bestuur op 16 febr. 2016 dat een ziekenhuis in de VS het al een week zonder computers moet doen, omdat een aanval met zogeheten ransomware (gijzelingssoftware) het systeem volledig heeft platgelegd. De aanvallers eisen 3,6 mln. dollar, voordat zij de toegang tot het systeem herstellen. Het ziekenhuis heeft uiteindelijk betaald.

[11] In de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) wordt onder meer een voorbeeld aangehaald dat het mogelijk is om allerlei openbare voorzieningen, zoals bruggen en sluizen, van buitenaf via internet aan te vallen, stil te leggen en over te nemen, zoals een incident met de rioleringspompen in een gemeente liet zien. Hierdoor kan ook de fysieke veiligheid van burgers in het geding komen (BIG, blz. 6).

menselijk gedrag is in deze vaak de zwakste schakel, zo komt uit onderzoek naar voren [12]. Informatiebeveiliging is daardoor niet alleen een technische (ICT) kwestie, maar een zaak voor iedereen binnen de gemeente, ook voor de gemeenteraad. In feite zou informatieveiligheid standaard een belangrijk onderdeel moeten zijn van alle bedrijfsprocessen en alle bestuurlijke vraagstukken. Het is aan de gemeenteraad om de kaders in deze te stellen, om voldoende budget vast te stellen, om te controleren en toe te zien op een goede verantwoording.

Landelijk en binnen gemeenten is de laatste jaren steeds meer aandacht gekomen voor informatiebeveiliging en beveiliging van digitale systemen, netwerken en gegevens. Naast de bestaande wetgeving op het gebied van de Wet Gemeentelijke Basis Administratie Persoonsgegevens (WGBA), de Basisregistratie Adressen en gebouwen (BAG), SUWInet (Uitkeringen-, werk- en inkomensgegevens), de Paspoort Uitvoeringsregeling Nederland (PUN) en de Archiefwet 1995, heeft het Rijk wetten, regelgeving en normen voor de bescherming van de privacy en het veilig omgaan met informatie steeds verder aangescherpt en uitgebreid. Sinds begin 2015 zijn gemeenten zelf verantwoordelijk geworden voor hun informatiebeveiliging.

Vanwege het grote belang van een goede informatiebeveiliging heeft de Rekenkamer Breda in overleg met de Bredase raad in de periode dec. 2015-sept. 2016 onderzoek gedaan naar de stand van zaken van de informatiebeveiliging van de gemeente Breda. Voor de gemeenteraad is dit een relatief nieuw en complex terrein. Het doel van het onderzoek is om de raad inzicht te geven in de problematiek en in de stand van zaken binnen de gemeente Breda. De Rekenkamer heeft een deel van het onderzoek zelf verricht (informatiebeveiligingsbeleid, kaders, enquête onder afdelingshoofden). Het andere deel, te weten onderzoek naar de beveiliging van de digitale informatiesystemen van de gemeente Breda, heeft de Rekenkamer uitbesteed aan een extern gespecialiseerd bureau (Hoffmann Bedrijfsrecherche BV). Daarbij heeft het onderzoek van de Rekenkamer Den Haag (2014) naar de informatiebeveiliging als voorbeeld gediend.

Dit rapport gaat allereerst in op de onderzoeksvragen en de onderzoeksopzet. Vervolgens komen achtereenvolgens het landelijke informatiebeveiligingsbeleid en het informatiebeveiligingsbeleid van de gemeente Breda aan de orde. De resultaten uit het onderzoek naar de digitale beveiliging zijn vanwege de vertrouwelijke gegevens alleen op hoofdlijnen samengevat weergegeven in het bestuurlijke rapport.

2. De onderzoeksvragen en de onderzoeksopzet

De centrale onderzoeksvragen in het onderzoek zijn:

> ‘In hoeverre is de (digitale) informatiebeveiliging van de gemeente Breda op orde, is de gemeente Breda alert en actief genoeg om de informatiebeveiliging van de gemeente oplossingsgericht te verbeteren en kan de raad ervan op aan dat het goed gaat?’

Deze centrale onderzoeksvragen zijn onderverdeeld in de volgende deelvragen:

1. Welke kaders heeft de gemeente Breda gesteld ten aanzien van informatiebeveiliging en in hoeverre voldoet de gemeente aan de gestelde normen;
2. Hoe is de informatiebeveiliging ingericht in de organisatie, zijn verantwoordelijkheden goed belegd, worden kwetsbaarheden, lekken e.d. snel doorgegeven aan de verantwoordelijken en wordt snel actie ondernomen bij incidenten;
3. Wat doet de gemeente Breda aan informatiebeveiliging en welke beveiligingschecks en informatiebeveiligingstests heeft de gemeente Breda gedaan/laten doen (overzicht bieden);

[12] De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) constateert in een onderzoek dat er onder gemeenteambtenaren nog veel werk te verzetten is in hun alertheid op cyberaanvallen, phishing mails, inbraken en het veilig omgaan met vertrouwelijke en privacygevoelige informatie (NCTV, okt. 2015).

4. Welke kwetsbaarheden en risico's zijn te constateren in het gemeentelijke netwerk/de ICT-systemen (en subsites[13]) en welke hackmogelijkheden, eventuele virussen, sporen van phishing, mogelijke malware en mogelijke onbedoelde toegangen tot systemen en met name tot vertrouwelijke en/of privacygevoelige gegevens zijn te constateren;
5. Zijn de backups voldoende op orde, waar zijn de systemen van de gemeente Breda kwetsbaar voor uitval en wat is de inschatting van de ernst van de situatie als uitval eventueel optreedt;
6. Welke maatregelen zijn te nemen om de eventueel geconstateerde kwetsbaarheden, hackmogelijkheden en risico's technisch en/of organisatorisch te ondervangen;
7. Welke aanknopingspunten voor verdere verbetering van de informatiebeveiliging komen naar voren en welke aanbevelingen zijn aan de raad te doen.

De Rekenkamer heeft de deelvragen 1 t/m 3 onderzocht aan de hand van documentenonderzoek, gesprekken met informatie- en ICT-medewerkers, de verantwoordelijk wethouder en sleutelpersonen binnen enkele afdelingen (zoals Concerncontrol en de griffie) en een kort vragenlijstje naar alle afdelingshoofden over informatiebeveiliging. Daarnaast zijn de landelijke normen en ontwikkelingen, en de uitkomsten van enkele landelijke, provinciale en gemeentelijke onderzoeken in kaart gebracht.

De deelvragen 4 t/m 6 zijn door Bureau Hoffmann Bedrijfsrecherche BV onderzocht aan de hand van:

- Een kwetsbaarheidenscan en hackpogingen om op verschillende manieren 'binnen' te komen in de digitale systemen van de gemeente Breda, zowel van buitenaf zonder enige voorkennis, als met (enige) voorkennis. Dat laatste om te onderzoeken hoe ver iemand kan doordringen tot interne gemeentelijke (en vertrouwelijke) bestanden en informatie, als iemand eenmaal in het bezit is van een (gast)account of een toegang heeft gevonden;
- Een Forensic readiness scan, waarin onderzocht is in hoeverre de gemeente Breda voorbereid is op cyberaanvallen of lekken, hoeveel schade deze kunnen aanrichten en in hoeverre de gemeente kan achterhalen (forensisch onderzoek) door wie c.q. vanaf welke internetadres deze aanval is ingezet of het lek heeft plaatsgevonden.

Op basis van de analyses en de uitkomsten uit de deelvragen 1 t/m 6 formuleert de Rekenkamer aanbevelingen voor mogelijke verbeteringen van de informatieveiligheid (deelvraag 7).

[13] Het was de bedoeling dat 15 subsites van Breda.nl onderzocht zouden worden op beveiliging van de toegangen, uiteindelijk zijn 14 subsites onderzocht. Één site (Brimbreda) kon niet getest worden, omdat het beheer- en hostingbedrijf van die site omvangrijke voorwaarden stelde voordat zij mee wilden werken. Daar is de Rekenkamer niet mee akkoord gegaan (zie bijlage 2).

Hoofdstuk 3 Het landelijke informatiebeveiligingsbeleid

Sinds een aantal jaren stimuleert het Ministerie van Binnenlandse Zaken en Koninkrijkzaken (BZK) samen met de VNG, King en gemeenten actief een verdere professionalisering van de informatiebeveiliging bij gemeenten. De begin 2013 opgerichte landelijke Informatiebeveiligingsdienst (IBD, met daarin het ministerie van BZK, de VNG en KING) heeft daartoe onder meer een Baseline Informatiebeveiliging Gemeenten (BIG) opgesteld met basisnormen en richtlijnen voor het gemeentelijk basisbeveiligingsniveau [14]. In de BIG zijn o.a. richtlijnen voor de toegangscontroles en uitgangspunten voor toetsing van de informatieveiligheid van een organisatie opgenomen. De VNG en KING bieden in 2013 en 2014 actief ondersteuning aan gemeenten bij het opzetten van een eigen informatiebeveiligingsbeleid en het voldoen aan de BIG, o.a. door middel van een landelijke Taskforce 'Bestuur en Informatieveiligheid Dienstverlening'. Gemeenten kunnen zich bij de IBD (Informatiebeveiligingsdienst) aansluiten om verder actief ondersteund te worden met kennis en instrumenten.

In februari 2015 hebben een groot aantal lokale overheden (waaronder Breda) en partijen samen met de VNG een Convenant gesloten over de informatieveiligheid van gemeenten. Gemeenten hebben zich via een Resolutie Informatieveiligheid gezamenlijk gecommitteerd om de informatiebeveiliging professioneel op te gaan pakken en per 1 januari 2017 te voldoen aan de BIG-normen. Daartoe dienen gemeenten vóór 2017 een zogeheten GAP-analyse uit te voeren om te toetsen in hoeverre zij voldoen aan de BIG-normen en welke maatregelen nog genomen moeten worden.

In aug. 2015 heeft de VNG een landelijke visitatiecommissie Informatieveiligheid ingesteld, die in 2 jaar tijd 120 gemeenten bezoekt. Het doel van de visitatiecommissie is om op bestuurlijk niveau adviezen te geven aan gemeenten. De visitatiecommissie doet papieren onderzoek (wat is op schrift gesteld?) en voert gesprekken met de gemeenten om met name de cultuur en het omgaan met informatieveiligheid te onderzoeken. De visitatiecommissie is in januari 2016 bij de gemeente Breda geweest en heeft hierover een visitatierapport opgesteld (zie bijlage 3). In juni 2016 heeft de visitatiecommissie een verslag uitgebracht van de gesprekken bij de eerste 40 gemeenten (Visitatiecommissie Informatieveiligheid, juni 2016).

Tabel 1 De BIG-normen voor gemeenten globaal samengevat in een schema

Normen	Invulling
1. Informatiebeveiligings beleid	De gemeente dient een informatiebeveiligingsbeleid vastgesteld te hebben met de kaders, doelen, afspraken, invulling van de benodigde acties, evaluatieafspraken, bijsturingsacties en verantwoordingsafspraken.
2. De organisatie van de informatiebeveiliging	De verantwoordelijkheden, taken en verplichtingen van bestuurders, afdelingen en medewerkers moeten goed vastgelegd zijn, zodanig dat problemen, hiaten en lekken tijdig doorgegeven worden, opgepakt en opgelost worden. Speciale beveiligingsfunctionarissen (waaronder een chief information officier die direct aan de directie rapporteert) en fulltime (privacy en ICT)securityprofessionals, moeten benoemd zijn.
3. Persoonlijke en fysieke beveiliging	De toegangsbeveiliging, -beheer en –controles moeten goed op orde zijn, zowel van gebouwen, afdelingen, personen en apparatuur, als van systemen, informatie en gegevens en hoe medewerkers omgaan met informatie (o.a. clean desk policy) en met informatiedragers (zoals USB-sticks, Ipads, Smartphones e.d.).

[14] Daartoe zijn twee documenten opgesteld: 1. De Tactische Baseline Informatiebeveiliging Nederlandse gemeenten: een normenkader dat de beschikbaarheid, integriteit en exclusiviteit van gemeentelijke digitale informatiesystemen bevordert en maatregelen voorschrijft voor controle en risicomanagement;
En 2. De Strategische Baseline Informatiebeveiliging Nederlandse gemeenten: een 'kapstok' waaraan alle benodigde elementen van informatiebeveiliging opgehangen kunnen worden en waarin vooral de organisatie en verantwoording van de informatiebeveiliging centraal staan.

4. Digitale beveiliging	De beveiliging van digitale informatiesystemen en ICT-structuren moet goed op orde zijn, de informatiesystemen moeten steeds getest op kwetsbaarheden en oneigenlijk gebruik, er moet meteen alert gereageerd worden bij incidenten of misbruik en de ict-beveiliging moet continu verbeterd worden.
5. Informatiebeveiligingsbudget	Er moet voldoende budget beschikbaar zijn om de beveiliging goed uit te kunnen voeren, om risico- en kwetsbaarhedenanalyses te kunnen doen, om de beveiliging verder uit te kunnen breiden en om bijvoorbeeld leertrajecten richting gemeentelijke medewerkers op te zetten.
6. Bewustzijn van medewerkers m.b.t. veilig omgaan met informatie en bescherming privacy	Alle medewerkers dienen bewust en veilig om te gaan met papieren, mondelinge, digitale e.d. informatie[15]. De regels wat betreft vertrouwelijkheid, integriteit, beschikbaarheid en privacybescherming dienen nageleefd te worden. De gemeente moet zorgen dat iedere medewerker goed op de hoogte is van de regels, de risico's en de plicht om problemen en datalekken door te geven.
7. Afspraken m.b.t. informatiebeveiliging in overeenkomsten /contracten met externe partijen	Gemeenten dienen beveiligingsafspraken te hebben vastgelegd in overeenkomsten met ICT-gelieerde bedrijven die diensten verzorgen (leveranciers, beheer- en hosting bedrijven e.d.) en in contracten met derden /externe partijen [16]. Dit betreft afspraken over beveiliging, eigendom (o.a. van gegevens), verantwoordelijkheden, plicht tot meewerken aan beveiligingsonderzoeken, aansprakelijkheid, geheimhouding en privacyafspraken t.a.v. persoonsgegevens en rapportage over de beveiliging.
8. Verantwoording informatieveiligheid	Gemeenten dienen het beleid, de gemaakte afspraken en geplande acties te toetsen, te controleren en verantwoording af te leggen via de P&C-cyclus.

Privacybescherming
Naast de BIG-normen heeft het Rijk inmiddels de specifieke clausules omtrent privacybescherming verder aangescherpt in de Wet bescherming persoonsgegevens (Wbp 2016). De privacyclausules betekenen voor gemeenten dat: persoonlijke gegevens uitsluitend voor een specifiek omschreven en gerechtvaardigd doel mogen worden vastgelegd, gedeeld en verwerkt, en uitsluitend met uitdrukkelijke toestemming van de persoon zelf; de persoon zelf moet kunnen beschikken en de regie moet kunnen voeren over zijn/haar gegevens; en de gemeente verantwoordelijk is voor de geheimhouding, en veilige en correcte verwerking van de gegevens, ook als die gegevens bij/door externe organisaties verzameld, beheerd en gebruikt worden.

Uit onderzoeken naar privacy in het sociaal domein blijkt dat gemeenten wel aandacht hebben voor privacy, maar dat een concreet uitgewerkt privacybeleid vooralsnog vaak ontbreekt, de concrete handvatten voor uitvoerenden vaak tekort schieten om te voldoen aan de privacyeisen en de naleving van privacy nog te weinig getoetst wordt. Daardoor delen uitvoerenden veelal gegevens met anderen zonder dat zij goed weten welke grondslag daarvoor bestaat (Rekenkamer Amsterdam, maart 2016; Rkc Eindhoven, april 2016). De Autoriteit Persoonsgegevens constateert in een onderzoek onder de 41 grootste gemeenten (waaronder ook Breda) dat de meeste gemeenten nog geen duidelijk beeld hebben omtrent welke gegevens zij in het sociaal domein mogen verwerken (en delen), voor welke doelen zij dit mogen en op basis van welke grondslagen (Autoriteit Persoonsgegevens, april 2016). Ook het Sociaal en Cultureel Planbureau constateert dat nog lang niet overal binnen gemeenten en in de uitvoering van de zorg is doorgedrongen hoe een goede dienstverlening te combineren is met een correcte behandeling van de persoonsgegevens (SCP, 'Overall Rapportage Sociaal domein', mei 2016).

[15] Het gaat in deze om het veilig bewaren, vervoeren en verwerken van interne (vertrouwelijke en persoonlijke) informatie, het tegengaan van verlies van (vertrouwelijke) informatie of het laten slingeren van documenten/dossiers op bureaus, thuis, in de trein of elders en om het melden van eventuele datalekken.

[16] Gemeenten worden steeds afhankelijker van externe partijen, aangezien gemeenten genoodzaakt zijn om steeds meer uit te besteden en buitenshuis ('in the cloud') te bewaren (op externe servers), te laten beheren en te onderhouden. Met het toenemen van de specialismen en de omvang van digitale systemen/ bestanden is het ondoenlijk voor gemeenten om alle expertise zelf in huis te hebben. De externe (markt)organisaties hebben echter niet per definitie dezelfde belangen als een gemeente.

De Minister van BZK constateert op basis van deze onderzoeken dat gemeenten echt nog aan de slag moeten op dit gebied (reactie Minister op het onderzoek van het SCP, juni 2016).

Sinds 2013 zijn overheden verplicht om een Privacy Impact Assessment (PIA) uit te voeren bij ieder (wets- of beleids)voorstel dat een beperking van de grondrechten omtrent privacy zou kunnen betekenen. Aan de hand van het Toetsmodel Privacy Impact Assessment (PIA) dienen gemeenten bij ieder nieuw beleid of wijzigingen in beleid met eventuele gevolgen voor de privacy, onderzoek te doen of aan de privacynormen wordt voldaan (eerste versie PIA in 2013, aangepaste versies in 2014 en 2015). Deze PIA moet periodiek herhaald worden.

Om de privacy verder te beschermen en misbruik van persoonlijke gegevens[17] tegen te gaan, is per 1 januari 2016 de Wet Meldplicht Datalekken CBP in werking getreden als onderdeel van de aangescherpte Wet Bescherming Persoonsgegevens (WBP). Vanaf die datum zijn organisaties die werken met vertrouwelijke, privacygevoelige en persoonsgegevens, waaronder dus gemeenten, verplicht om (ernstige) leks en inbraakpogingen te melden aan het College Bescherming Persoonsgegevens (vanaf 1 jan. 2016 Autoriteit Persoonsgegevens geheten). Onder 'lekken' wordt bijvoorbeeld het in verkeerde handen vallen van gegevens, oneigenlijke toegang tot bestanden/systemen, het verlies van USB-sticks of laptops met gevoelige informatie e.d. verstaan [18]. Wordt een ernstig lek niet binnen twee werkdagen gemeld en kan een gemeente niet aantonen dat zij er alles aan hebben gedaan om goed beveiligd te zijn, dan riskeert de organisatie een boete die kan oplopen tot 810.000 euro of 10% van de omzet.

De Autoriteit Persoonsgegevens meldt in mei 2016 dat tot op heden nog weinig datalekken gemeld worden: in de periode 1 jan.- 1 mei 2016 slechts 1600 keer. "Als je bedenkt dat er 130.000 organisaties in Nederland zijn die persoonsgegevens verwerken, kan het bijna niet anders dan dat er meer datalekken zijn", aldus de AP (NOS.nl, 2016). Beveiligingsonderzoekers, die onderzoek doen naar de huidige beveiligingspraktijk bij bedrijven, bevestigen de indruk dat datalekken vaak niet worden gemeld. Er is nog onvoldoende bekendheid met en onvoldoende urgentie omtrent het melden van datalekken, zo constateert de AP.

Ook op Europees niveau zijn de richtlijnen omtrent bescherming van de privacy, het gebruik van persoonsgegevens en de bevoegdheden van toezichthouders inmiddels verder aangescherpt: op 25 mei 2016 is de Europese Algemene Verordening Gegevensbescherming (AVG) in werking getreden (EU, 2016). Overheden hebben tot 25 mei 2018 de tijd om aan de regels in deze Verordening te voldoen. De VNG raadt gemeenten aan om vóór die tijd te inventariseren welke maatregelen genomen moeten worden (o.a. ten aanzien van bewerkersovereenkomsten), om de verwerking van persoonsgegevens volledig in kaart te brengen, om een specifieker uitgewerkt Privacyhandvest op te gaan stellen, om alvast een functionaris Gegevensbescherming te benoemen en de benodigde maatregelen uit te voeren. De boetes voor het onzorgvuldig omgaan met gegevens kunnen door de Europese AVG verder gaan oplopen tot zo'n 10 mln. euro, voor bedrijven tot 20 mln..

[17] Er is immers zoals bekend een levendige handel in persoonlijke gegevens tussen allerlei marktorganisaties/bedrijven, zowel nationaal als internationaal.

[18] Enkele voorbeelden van datalekken zijn: 'het uitlekken van BSN-nummers van ongeveer 33.000 burgers in de gemeenten Rotterdam en Oegstgeest' (febr. 2016); of 'wijkteam mailt privacygevoelige informatie van 1.000 tot 1.500 zorgcliënten naar verkeerd e-mailadres' (april 2016).

Hoofdstuk 4 Het informatiebeveiligingsbeleid van de gemeente Breda

De gemeente Breda is sinds 2013 bezig om de informatiebeveiliging naar een hoger niveau te brengen en heeft diverse trajecten ingezet om het volwassenheidsniveau van de beheersmaatregelen verder te verhogen. Dit concludeert gemeenteaccountant E&Y (o.a. in hun IT-audit 2014 en de jaarcontrole 2015) en komt ook uit de gesprekken van de Rekenkamer naar voren. De gemeente Breda heeft de BIG-normen onderschreven en wil per 1 januari 2017 zoveel mogelijk voldoen aan die normen. De gemeente Breda was één van de eerste die de gezamenlijke resolutie van gemeenten ondertekende om per 1 jan. 2017 te voldoen aan de BIG-normen en één van de eerste gemeenten die zich bij de IBD (Informatiebeveiligingsdienst) aansloot voor actieve ondersteuning, instrumenten en informatie (b.v. over cyberaanvallen). Hieronder volgt per (samengevatte) BIG-norm een stand van zaken bij de gemeente Breda, zoals naar voren komt uit documenten, gesprekken en een korte enquête onder afdelingshoofden van de gemeente Breda.

1. Het Informatiebeveiligingsbeleidsplan

De gemeente Breda heeft de BIG-normen als uitgangspunt genomen bij het opstellen van een eigen gemeentelijke informatiebeveiligingsbeleidplan in 2014 (Informatie Beveiligingsbeleid, gemeente Breda, 2014). Het informatiebeleidsplan is vastgesteld door het College van B&W en ter kennisgeving naar de gemeenteraad gestuurd. In het beleidsplan staan de benodigde organisatie (functionarissen, verantwoordelijkheden), alle benodigde maatregelen ten aanzien van de BIG-normen, het beheer, de ontwikkeling en het onderhoud van informatiesystemen en informatiebeveiliging, de benodigde toetsing en het toezicht op de naleving uiteengezet [19]. Naast dit 'hoog-over'document wordt ieder jaar verder inhoud gegeven aan specifieke maatregelen in een intern uitvoeringplan (Uitvoeringsplan Informatiebeveiliging 2015 en Informatieveiligheidsplan 2016-2017). De gemeente Breda wil op het gebied van informatiebeveiliging graag zelfregulerend zijn en heeft ook aan partners en instellingen, waarmee samengewerkt wordt, opgedragen om zelfregulatie-tests te doen op veiligheid en privacykwesties. Het college van B&W van Breda zal de naleving van de PIA-verplichtingen[20] controleren en waar nodig sancties opleggen, zo stelt het Programma Veiligheid 2015-2028 (Gemeente Breda, 2014). Evaluatie van het Uitvoeringsplan Informatiebeveiliging 2015 laat zien dat nog niet alle voorgenomen acties uitgevoerd zijn en nog niet alle voorgenomen maatregelen geïmplementeerd zijn.

2. Verantwoordelijkheden in de organisatie

Inmiddels zijn de verantwoordelijkheden van bestuurders en medewerkers van de gemeente Breda omtrent informatieveiligheid uitgewerkt en formeel vastgelegd om te zorgen dat tijdig de juiste acties op het gebied van de informatiebeveiliging binnen de gemeente ondernomen worden en problemen, hiaten en lekken tijdig doorgegeven worden, opgepakt en opgelost worden. Binnen het college is één wethouder hoofdverantwoordelijk voor informatiebeveiliging (de wethouder Zorg, Onderwijs en Dienstverlening, die ook de ambtelijke organisatie in haar portefeuille heeft) en daarnaast is iedere wethouder formeel verantwoordelijk voor hun vakgebieden. De gemeentesecretaris is verantwoordelijk voor de uitvoering als geheel en in het MT wordt periodiek overlegd over informatieveiligheid. De directeur Servicebedrijf, het hoofd 'Proces en Informatie' en verschillende informatieveiligheidsmedewerkers (o.a. 2 fulltime security-ICT-medewerkers, een informatieveiligheidsadviseur en een privacy-coördinator) zijn belast met de uitvoering van het informatiebeveiligingsbeleid. Daarnaast zijn verschillende (informatie)professionals bij de bedrijfsbureaus van de directies formeel belast met de doorontwikkeling en uitvoering van de informatiebeveiliging van de door hun directie gebruikte systemen en de melding van eventuele datalekken in deze systemen. Iedere afdeling is in principe apart verantwoordelijk voor hun eigen datasystemen, hun eigen data en voor de bewustwording van hun eigen medewerkers in het veilig omgaan met gegevens en informatie. Er

[19] In het Programma Veiligheid 2015-2018 van de gemeente Breda (2014) staat informatieveiligheid eveneens als belangrijk aandachtspunt genoemd en staan verwijzingen vermeld naar de BIG-normen, de noodzaak om informatielekken te gaan identificeren en de noodzaak om de beveiliging van de digitale informatiesystemen goed op orde te hebben als gemeente Breda.

[20] PIA= Privacy Impact Assessment.

zijn binnen de gemeente Breda momenteel ongeveer 150 verschillende software- en informatiesystemen in gebruik.

Uit de gesprekken van de Rekenkamer blijkt dat binnen het College en op het hoogste managementniveau commitment bestaat om de informatiebeveiliging goed vorm te geven en uit te breiden. Periodiek wordt op dat niveau overlegd over (bepaalde punten binnen) het informatieveiligheidsbeleid. Met name bij het Servicebedrijf en de afdeling Proces en Informatie is inmiddels veel kennis aanwezig om het goed vorm te geven. De laatste tijd vinden wel veel personeelswisselingen plaats waardoor de kennis en continuïteit niet automatisch gewaarborgd is. Met name bij functies die veel specialistische (en interne) kennis vereisen, kan dit gemakkelijk tot problemen c.q. stagnatie leiden. Zo is het behouden van de medewerkers met specialistische ICT-kennis cruciaal voor de digitale beveiliging.

Een belangrijk punt is dat de beveiliging en het beheer van systemen en het omgaan met informatie versnipperd is over de gemeentelijke organisatie. De gemeente Breda heeft nog geen centrale Chief Information Security Officer, die overall coördineert en rechtstreeks rapporteert aan de directie/MT en de gemeentesecretaris. Uit de gesprekken en de enquête [21] van de Rekenkamer komt naar voren dat het informatiebeveiligingsbeleid en de eisen die dit stelt, nog niet overal goed geland is bij alle afdelingen en nog niet overal alle aandacht krijgt die het nodig heeft, laat staan dat alle benodigde acties overal bekend zijn en uitgevoerd worden. Iedere separate afdeling is echter wel zelf verantwoordelijk voor de systemen en voor bijvoorbeeld de privacybescherming en het melden van eventuele datalekken. Daar liggen derhalve nog belangrijke opgaven voor de gemeente Breda om de informatiebeveiliging en de benodigde acties verder in de organisatie bekend te laten zijn en uit te laten voeren.

3. Fysieke toegangsbeveiliging gebouwen, apparatuur, gegevens, systemen

Uit de gesprekken en de ervaring van de Rekenkamer blijkt dat de toegangsbeveiliging van het Stadskantoor redelijk goed op orde is (geautoriseerde toegangspasjes, toezicht op wie naar binnengaat), al is het onduidelijk hoeveel mensen de deur openhouden voor anderen/wellicht onbevoegden. De autorisaties met betrekking tot de toegang tot ruimten/afdelingen met vertrouwelijke informatie (Archief) of dure ICT-apparatuur kunnen verder aangescherpt worden, zo blijkt uit de gesprekken. Het is niet altijd duidelijk waarom medewerkers toegang hebben tot bepaalde ruimten/afdelingen en het blijkt vrij gemakkelijk te zijn om binnen te komen.
De ervaring is dat, als men eenmaal in het Stadskantoor binnen is, het vrij gemakkelijk is om kantoorruimten binnen te lopen. Om te voorkomen dat iedereen op die manier gemakkelijk allerlei documenten en informatie in kan zien, hanteert de gemeente Breda een clean desk policy. Dat betekent dat alle bureaus zoveel mogelijk leeg dienen te zijn, in ieder geval vrij van belangrijke interne, vertrouwelijke informatie. Omdat het niet duidelijk is hoe goed iedereen zich daaraan houdt, heeft de gemeentesecretaris in juni 2016 onderzoek hiernaar laten doen door een extern bureau (mystery guest onderzoek, juni 2016). Uit dat onderzoek bleek dat de mystery guest gemakkelijk het stadskantoor en hierbinnen vertrouwelijke ruimtes binnen was gekomen en op verschillende plekken vertrouwelijke documenten en (digitale) data in had gezien. De conclusie is dat de fysieke beveiliging verder te verbeteren is, ook van het Stadskantoor.

Ten opzichte van het Stadskantoor is de beveiliging van het stadhuis een stuk minder goed op orde, o.a. vanwege de vele openbare bijeenkomsten die daar plaatsvinden. Het camerasysteem, dat een aantal jaren geleden geïnstalleerd is, heeft de beveiliging wel verbeterd, echter optimaal is het nog niet.

Qua digitale toegangsbeveiliging heeft de gemeente Breda in december 2015 de beveiliging verder uitgebreid en zijn de verplichte wachtwoorden veel langer en ingewikkelder geworden (met hoofdletters, kleine letters, leestekens en nummers). Ook moet het wachtwoord vaker gewijzigd worden, zodat medewerkers niet lange tijd hetzelfde wachtwoord gebruiken. Onderzoek (o.a. van Symantec, 2015) wijst uit dat met name de lengte van wachtwoorden sterk de voorspelbaarheid

[21] Eind april –begin mei 2016 heeft de Rekenkamer een kort vragenlijstje naar alle afdelingshoofden van de gemeente Breda verstuurd. Ongeveer de helft van de aangeschreven personen respondeerde.

bepaalt: hoe langer het wachtwoord, hoe meer combinaties mogelijk zijn en hoe moeilijker het is om deze via gokken en testen van combinaties van wachtwoorden te achterhalen.
Verder is het belangrijk om het wijzigingsbeheer goed op orde te hebben als organisatie, zodat de autorisaties, toegangspasjes e.d. steeds up-to-date zijn, ook bij veelvuldig wijzigen van functies of in- en uitdiensttreding. Dit stond ook als speerpunt voor 2015 genoemd in het Uitvoeringsplan informatiebeveiliging 2015 (Gemeente Breda, 2015).

4. Digitale informatiebeveiliging en beveiligingsonderzoeken, audits, tests, evaluaties

De digitale beveiliging van systemen en gegevens is één van de speerpunten van de gemeente Breda in de afgelopen 2 jaar geweest. Inmiddels heeft de Gemeente Breda zelf diverse tests en beveiligingsonderzoeken verricht c.q. laten verrichten met betrekking tot de technische beveiliging van (specifieke) digitale systemen, toegangen en onderdelen van de ICT-infrastructuur. Het oppakken van de uitkomsten uit deze tests is nog wel een aandachtspunt, zo komt naar voren. Dat heeft onder meer te maken met een geringe personele bezetting op dat gebied, zo blijkt uit gesprekken. Een algehele onafhankelijke kwetsbaarheden- en penetratietest, zoals nu door bureau Hoffmann is uitgevoerd, heeft de gemeente Breda tot op heden nog niet laten uitvoeren.

De reeds verrichte audits en onderzoeken zijn:

Audits/tests	**Inhoud - uitkomsten**
1. Accountantscontrole /audit ICT	Interimcontrole beveiliging en audit accountant E&Y in 2014 [22] t.a.v. de beheersmaatregelen van de applicatie voor financiële transacties, de verwerking van uitkeringen en verwerking van salarisgegevens. Toegangsbeveiliging van i.c. financiële transacties en salarisgegevens kan beter. In 2015 en 2016 audit informatiebeveiliging E&Y: beleid is vastgesteld, volwassenheid maatregelen groeit ieder jaar.
2. DigiD beveiligingstests	Toetsing beveiliging DigiD is sinds 2013 ieder jaar verplicht[23]. In 2014 en 2015 getoetst door resp. de accountant E&Y en een extern bureau [24]. In 2014 diverse aanbevelingen om beter aan specifieke normen te voldoen. In 2015 blijken deze aanbevelingen te zijn opgevolgd.
3. GBA en SUWI beveiligingstoetsen	Toetsing beveiliging GBA en SUWI is al langer wettelijk verplicht. Uit eerdere tests kwamen nog enkele zwakke punten aan het licht in Breda, i.c. bij SUWInet. In 2015 test de Inspectie van het Ministerie van Sociale Zaken en Werkgelegenheid [25] SUWI grootschalig. Breda blijkt aan alle 7 getoetste normen te voldoen.
4. Gap-analyse	In 2015 heeft de gemeente Breda een GAP-analyse uitgevoerd: een verschillenanalyse t.a.v. de BIG-normen. Breda voldoet nog niet (geheel) aan alle BIG-normen. In het Informatiebeveiligingsplan 2015 en 2016-2017 staan maatregelen om aan deze aspecten te werken, zoals: bevordering van de bewustwording van de medewerkers, uitbreiden risicomanagement, in kaart

[22] 'Beoordeling IT beheersmaatregelen geautoriseerde gegevensverwerking, wijzigingsbeheer en logische toegangsbeveiliging van o.a. de applicaties Key2Financiën, GWS4all en Workforce', E&Y Interimcontrole 2014

[23] Het gebruik van DigiD blijft kwetsbaar, zo blijkt. Het Rijksjaarverslag 2015 van het Ministerie van BZK meldt dat in 2015 bijna 15.000 DigiD-accounts verwijderd zijn vanwege mogelijke misbruik (Ministerie van BZK, 2016).

[24] 'Heraudit DigiD-assesment digitale loket', E&Y, 2014 en 'DigiD-assesment digitale loket 2014', bureau '2 Control it', 2015 en 'Heraudit DigiD-assesment WOZ-loket', E&Y, 2014 en 'DigiD-assesment WOZ-loket 2014', bureau '2 Control it', 2015

[25] 'Onderzoek beveiliging Suwinet', Inspectie Ministerie van SZW, 2015. In SUWInet zijn gegevens van veel burgers opgeslagen, waarbij een koppeling plaatsvindt met basisregistraties van persoonsgegevens, inkomens/uitkeringsgegevens e.d.. Veel gemeenten blijken de beveiliging van SUWInet niet goed op orde te hebben.

	brengen kritieke bedrijfsprocessen en de informatieverwerking van persoonsgegevens, implementatie maatregelen BIG.
5. Zelfevaluatie Basisregistratie Personen (BRP)	In 2015 is een zelfevaluatie ingevuld door functionarissen van diverse afdelingen, die met persoonsgegevens werken, toegang hebben tot vertrouwelijke informatie en/of direct te maken hebben met beveiliging (zoals Publiekszaken, Personeelszaken, de controller Informatiebeveiliging, ICT-afdeling, Facilitaire dienst). Met name t.a.v. ICT en facilitaire dienst kwamen leerpunten naar voren.
6. Beveiligingstests van webformulieren en digitale portals	In 2015 is de beveiliging van webformulieren en enkele portals onderzocht door een extern bureau[26] (o.a. meldingsformulier Openbare ruimte, digitale aanvraag uittreksel GBA). Daaruit kwamen drie gemiddelde[27] kwetsbaarheden, dertien laag risico kwetsbaarheden en vier aandachtspunten naar voren. Daar heeft de gemeente Breda inmiddels acties op ingezet of gepland.
7. Privacy Impact Assessment (PIA)	Bij de start van de 3 decentralisaties op het sociaal domein heeft de gemeente Breda een risicoanalyse en een Privacy Impact Assessment (PIA) uitgevoerd en is gekeken welke aanvullende voorwaarden gesteld moesten worden voor de verwerking van de persoonsgegevens. Deze PIA is nog niet periodiek herhaald en wordt nog niet standaard uitgevoerd voor iedere dataset, waarin gegevens van burgers worden opgeslagen en verwerkt. Recent is een korte pilot op het sociaal domein verricht of de gestelde privacyeisen gehandhaafd worden en is een privacyprotocol voor werkprocessen opgesteld (april 2016). Deze moeten nog verder worden ingebed. De gemeente Breda heeft voorts nog geen uitgeschreven Privacyhandvest, dat als leidraad kan fungeren voor de privacytoetsing. Een dergelijk handvest wordt in 2016 opgesteld.

Incidentenmanagement
De gemeente Breda heeft wel kort in het Informatiebeveiligingsbeleidsplan 2014 beschreven hoe om te gaan met incidenten, maar heeft nog geen uitgewerktere procedures ten aanzien van incidentenmanagement. Wel heeft de gemeente Breda in de afgelopen twee jaar aan een alert incidentenmanagement gewerkt. In de afgelopen twee jaar hebben zich twee grote incidenten voorgedaan op het gebied van de digitale beveiliging (aanvallen op en uitval van een deel van het ICT-systeem). Beide keren heeft de (ICT-afdeling van) gemeente Breda snel ingegrepen, zijn de aangevallen/besmette delen geïsoleerd, verwijderd en vervangen door schone backups. De gemeentelijke organisatie heeft daar verder geen (beduidende) hinder van ondervonden. Dat geeft al aan dat op ICT-gebied de gemeente Breda serieus werk maakt van beveiliging. In het Informatiebeveiligingsplan 2016-2017 staat het nog strakker oppakken van het risicomanagement als speerpunt geformuleerd.

7. Financiering van de informatiebeveiliging

Een vijfde BIG-norm is dat gemeenten voldoende budget beschikbaar stellen voor de informatiebeveiliging en het beschermen van de privacy. De gemeente Breda geeft begin 2016 ongeveer €150.000 uit aan (in totaal 3) informatiebeveiligingsfunctionarissen. Het is moeilijk te zeggen of dat veel of weinig is, al lijkt het op het eerste gezicht wat weinig voor een grote gemeente als Breda om maar 2 ICT specialisten en 1 informatiebeveiligingsfunctionaris in huis te hebben. Daarmee kan de gemeente slechts een beperkt aantal activiteiten uitvoeren en is de gemeente bovendien kwetsbaar, in die zin dat de continuïteit al snel een probleem wordt als één van deze specialisten/functionarissen vertrekt.

[26] Madison Gurkha, 'Technisch beveiligingsonderzoek Formulierenbibliotheek gemeente Breda', aug. 2015

[27] Bij ICT kwetsbaarhedenonderzoek worden de bevindingen geclassificeerd van 'kritieke kwetsbaarheden', 'hoog risico kwetsbaarheden', 'medium/gemiddeld risico kwetsbaarheden' tot aan 'laag risico kwetsbaarheden', al naar gelang de ernst van de gevonden kwetsbaarheden en de mate waarin al dan niet gemakkelijk doorgedrongen kan worden tot gevoelige (systeem)gegevens.

Inmiddels heeft de gemeente Breda een Werkgroep Informatiebeveiliging ingesteld met medewerkers van verschillende afdelingen (zoals ICT, A&O, Communicatie, Concerncontrol). In het Informatieveiligheidsplan 2016-2017 (gemeente Breda, juni 2016) staat een bedrag van € 167.500 begroot voor de Werkgroep Informatieveiligheid en acties op het gebied van bewustwording, risicomanagement, bedrijfscontinuïteit en audits in 2016 en 2017.

In de gemeentelijke Begroting 2016 staat informatiebeveiliging niet specifiek vermeld. Bij 'Organisatie en financiering' staat voor 2016 wel een bedrag van 500.000,- euro gereserveerd voor vervanging van de gemeentelijke website, 450.000 euro voor vervanging van het Personeelsregistratiesysteem en 560.000 euro voor automatisering in het kader van 'de Digitale gemeente 2018'. Ook bij de directie Beheer is financiering voor investeringen in de automatisering (nieuwe software) opgenomen.

8. Bewustwording medewerkers/betrokkenen, leertrajecten

Vergroting van de bewustwording van alle medewerkers met betrekking tot informatiebeveiliging staat als speerpunt opgenomen in het Informatieveiligheidsplan 2015 en 2016-2017. Tot op heden is de gemeente hier nog niet erg aan toegekomen, zo komt naar voren.

Het menselijk gedrag blijkt echter vaak één van de grootste risicofactoren in het veilig omgaan met informatie. Vanuit onwetendheid, gemakzucht, onachtzaamheid of het niet volgen van de regels (al dan niet bewust) komt het veel voor dat mensen bijvoorbeeld op foute (virus/fraude)links klikken, iets naar een verkeer emailadres sturen, belangrijke informatie ergens open en bloot laten liggen, informatiedragers verliezen en/of dat onbevoegden privacygevoelige informatie verkrijgen. Daarom is het belangrijk dat iedereen in een organisatie goed weet wat de regels, procedures en afspraken zijn en welke acties van de medewerkers verwacht worden in welke situaties. Iedere organisatie zou daartoe een set aan gedragsrichtlijnen en een zogeheten netiquette[28] opgesteld moeten hebben en deze actief moeten uitdragen naar alle betrokkenen (intern en extern).

De gemeente Breda heeft nog geen gedragsrichtlijnen of netiquette opgesteld. De gemeente Breda wijst bij diverse gelegenheden wel op de noodzaak om veilig om te gaan met vertrouwelijke, geheime of persoonlijke informatie/gegevens. Zo worden (beginnende) raadsleden ingelicht over de procedures ten aanzien van vertrouwelijke/geheime documenten. Worden nieuwe medewerkers gewezen op de beroepscode en moeten medewerkers, die met gevoelige informatie te maken hebben, bij indiensttreding de Ambtseed tekenen. Daarnaast is het de bedoeling dat in werkoverleggen regelmatig aandacht wordt geschonken aan informatieveiligheid, dat beveiligingsafspraken gecommuniceerd worden aan alle medewerkers en dat periodiek gecheckt wordt of iedereen zich houdt aan de beveiligingsrichtlijnen. Maar algehele expliciete campagnes en leertrajecten gericht op alle medewerkers, raadsleden en andere betrokkenen (b.v. werkzaam buiten de gemeente Breda) over informatieveiligheid en hoe op een veilige manier om te gaan met documenten, gegevens, e-mails, internet, apps, kortom informatie en informatiedragers, heeft de gemeente Breda nog weinig opgezet. Zeer recent (sept.-okt. 2016) zijn enkele informatieacties gestart, o.a. door informatiefilmpjes op de koffieautomaten, berichten op PIP omtrent risico's en fraudemails, en een informatiesessie naar aanleiding van het verrichte mystery guest-onderzoek.

Uit de gesprekken en de enquête die de Rekenkamer onder afdelingshoofden heeft gehouden, komt naar voren dat nog nadere aandacht en acties nodig zijn om het informatiebeveiligings-bewustzijn, de kennis hieromtrent en de acties binnen de organisatie verder te vergroten. Er is nog onvoldoende bekendheid met het informatiebeveiligingsbeleid en met benodigde acties op dit gebied. Er zijn in de organisatie derhalve nadere acties nodig met betrekking tot de melding van actuele beveiligingsrisico's, incidenten, waarschuwingen voor aanvallen, het melden van lekken e.d.. Bijna alle afdelingshoofden constateren in de enquête dat meer aandacht nodig is voor de bewustwording en het gedrag ten aanzien van informatie en beveiliging. Ook de Visitatiecommissie Informatieveiligheid, die inmiddels in Breda is langs geweest, constateert dat

[28] Een netiquette of nettiquette omvat de richtlijnen en gedragsregels voor het gebruik van internet.

vergroten van kennis en bewustwording in de organisatie nog een belangrijk aandachtspunt voor de gemeente Breda is.

Reeds in 2015 was het voornemen in het Informatiebeveiligingsplan 2015 om standaardteksten op de voorpagina van (toen nog Netpresenter) intranet/PIP te zetten met belangrijke beveiligingsboodschappen en meldingen van beveiligingsincidenten en -risico's (bij incidenten als virusaanvallen, phishing mails, uitval van systemen, waarschuwing tegen en meldsysteem van lekken e.d.). Het huidige PIP-systeem leent zich echter niet goed om boodschappen standaard gemeentebreed voor langere tijd onder de aandacht te brengen. Via de (zeer kleine) nieuwsrubriek op de voorpagina van intranet staan berichten meestal maar gedurende korte tijd. Daarnaast bestaat de mogelijkheid om een melding via Yammer op PIP te zetten, echter ook die staan slechts kort op de voorpagina. De recente (juni en sept.2016) stappen met betrekking tot voorlichting over digitale aanvallen, de risico's en wat te doen, die onlangs via Yammer en de Nieuwsrubriek op PIP gezet zijn, waren daardoor na een dag niet meer op de voorpagina te zien. Medewerkers moeten daardoor in de geschiedenis[29] gaan zoeken om deze relevante documenten te kunnen vinden.

9. **Overeenkomsten, contracten, afspraken met partners,**

Informatiebeveiliging is pas twee jaar echt een gemeentelijk aandachtspunt geworden en de gemeente Breda is pas recent begonnen om in (nieuwe) contracten en overeenkomsten aandacht te besteden aan privacy en informatieveiligheid. In de oudere contracten en overeenkomsten staan daardoor nog weinig clausules en afspraken in deze opgenomen. Bovendien zijn de verantwoordelijkheden voor de systemen en bestanden versnipperd over de organisatie en niet iedere separate afdeling geeft hier zoveel prioriteit aan. Dat heeft als consequentie dat niet bij ieder nieuw softwaresysteem, dat door de afdeling zelf wordt aangeschaft in samenwerking met de afdeling Inkoop, heel scherp aan bod komt welke beveiligingseisen gesteld worden en waar het softwarebedrijf precies aan moet voldoen.

Op het sociaal domein zijn bij de start van de decentralisaties al wel afspraken in overeenkomsten en contracten opgenomen ten aanzien van gegevensuitwisseling, informatiebeveiliging en privacybescherming (zie bijlage 3 Voorbeeldovereenkomst). In het derde kwartaal van 2015 zou de werkwijze geëvalueerd worden. Het is niet duidelijk of dat gebeurd is. Uit de enquête van de Rekenkamer onder afdelingshoofden komt naar voren dat deze afspraken periodiek worden getoetst. De praktijk in het sociaal domein is echter nog voortdurend aan verandering onderhevig en pas sinds dit jaar wordt gewerkt aan digitalisering van de gegevens op het sociaal domein. De indruk bestaat uit gesprekken dat het in de praktijk moeilijk gevonden wordt om de privacyeisen te combineren met de uitgangspunten van integrale zorg. Bij integrale zorg worden immers juist zoveel mogelijk gegevens uitgewisseld, terwijl de privacyeisen juist het automatisch delen van gegevens zoveel mogelijk tegengaan.
Bovendien werkt de gemeente in het sociaal domein met uiteenlopende organisaties samen, waardoor het moeilijk is om de eisen strikt te handhaven. Zo stelt een afdelingshoofd in de rekenkamerenquête over informatieveiligheid: 'de toenemende co-creatie e.d., waarin overheid en externe organisaties steeds hechter samenwerken, levert een grijs gebied op, voor zowel privacy als informatiebeveiliging. Deze externe organisaties zijn niet altijd gerenommeerde bedrijven, maar ook vaak clubs van vrijwilligers'.

10. Verantwoording informatieveiligheid

De gemeente Breda heeft in de gemeentelijke Jaarverslagen 2014 en 2015 kort een verslag opgenomen over met name de digitale informatieveiligheid, de verrichte audits en tests, en de beheersing van de risico's. De gemeente Breda vermeldt in het Jaarverslag 2015 dat veel aandacht wordt besteed aan de digitale informatieveiligheid. De accountant constateert in de IT-audit bij het Jaarverslag 2015 dat het volwassenheidsniveau van de IT-beheersing ieder jaar stijgt in Breda.
Aan de hand van deze korte verslagen krijgt de raad slechts deels een beeld van de informatiebeveiliging. Gezien de uitgebreidheid van benodigde maatregelen en de mogelijk grote

[29] Aangezien in Yammer allerhande chat- en twitterachtige berichten van medewerkers staan, kan dat een lange zoektocht zijn.

impact van een gebrek aan informatiebeveiliging, constateert de Rekenkamer dat een uitgebreider verslag naar de raad te adviseren is. Het onderwerp is van dermate groot belang voor de bedrijfsvoering en de betrouwbaarheid van de gemeente, dat het een periodieke bespreking in de raad verdient, naast een verslag in de P&C-cylcus. Dat is ook van de lessen van de landelijke Visitatiecommissie Informatieveiligheid op basis van de eerste 40 gesprekken bij gemeenten (Visitatiecommissie, juni 2016). De Visitatiecommissie Informatieveiligheid constateert dat informatiebeveiliging eigenlijk een standaard onderdeel van ieder beleidsproces en bestuurlijk vraagstuk zou moeten zijn. Het is belangrijk dat de raad goed betrokken wordt bij dergelijke belangrijke strategische vraagstukken, aldus de Visitatiecommissie (juni 2016).

Bijlage2 Specificatie van de reikwijdte van het onderzoek naar de digitale beveiliging

De 14 **domeinnamen die binnen de scope van het onderzoek op beveiliging getest zijn:**

- bibliotheekbreda.nl
- kenjestadbreda.nl
- viabreda.nl
- stadsarchiefbreda.nl
- bredapanel.nl
- opgeruimdbreda.nl
- gemeenteraadbreda.nl
- bredaorganiccity.nl
- dotsbreda.nl
- energiekbreda.nl
- huishoudchequebreda.nl
- webmail.breda.nl
- webtoegang.breda.nl
- www.breda.nl

Diverse van deze websites (zoals Stadsarchief.breda.nl en www.breda.nl) zijn ondergebracht bij externe partijen. De domeinen kenjestadbreda.nl, bredapanel.nl, gemeenteraadbreda.nl en huishoudchechequebreda.nl zijn subpagina's van www.breda.nl en zijn daarom getest als onderdeel van www.breda.nl. Ook de domeinen opgeruimdbreda.nl en energiekbreda.nl verwijzen naar dezelfde server. Het domein bredaorganiccity.nl is op het moment van het onderzoek niet te benaderen en lijkt uit de lucht te zijn. Het contract voor dotsbreda.nl is inmiddels door de beheerder opgezegd. Hoewel deze site nog wel actief is, vond de beheerder het niet nodig om hierover apart met de hostingpartij contact over op te nemen. Zowel organiccity.nl, als dotsbreda.nl zijn daarom niet getest in het onderzoek. Ook de site www.bredabreda.nl is niet getest, omdat het hostingsbedrijf niet zonder meer een vrijwaring wilde tekenen.

BRIMBREDA.NL is niet getest

Het was de bedoeling dat ook **Brimbreda.nl** op beveiliging en op eventuele toegangen tot gemeentelijke bestanden en systemen getest zou worden. Het hosting bedrijf (waar Brimbreda.nl op de server staat) wilde echter alleen meewerken aan het onderzoek als Brimbreda.nl werd geïsoleerd werd van de andere sites, die bij dat bedrijf gehost worden, en getransporteerd naar een eigen aparte Virtual Private Server (kosten migratie ca. 900,- à 1000,- euro, aanvullende kosten setup nieuwe VPS 570,- euro) en er een nieuw maandcontract voor beheer werd afgesloten (maandlasten zouden dan 225,- euro per maand worden). Het argument van het hostingbedrijf was dat als Brimbreda.nl in de huidige situatie getest zou worden, andere klanten (van overigens onbekende sites van andere bedrijven) vanwege shared hosting mogelijk last kunnen ondervinden van de beveiligingstests. De Rekenkamer heeft hierop besloten om deze extra kosten niet aan te gaan en Brimbreda.nl daarom niet mee te nemen in het onderzoek. Wel is vermeld dat een opmerking in het onderzoek gemaakt zal worden over waarom dit onderdeel niet meegenomen is en is aan de ambtelijke organisatie en ICT doorgegeven dat er kennelijk geen nadere afspraken bestaan met alle (sub)sites van de gemeente Breda over (gratis en automatische) medewerking aan beveiligingsonderzoeken van de Gemeente Breda en het testen van eventuele toegangen tot de bestanden, systemen en gegevens van de gemeente Breda. Bovendien roept het feit dat het hostingbedrijf de site eerst wil gaan isoleren voordat het beveiligingsonderzoek kan plaatsvinden, vragen op omtrent de beveiliging van deze site bij dit hosting bedrijf. Als gewerkt wordt met shared hosting zijn misschien heel gemakkelijk toegangen mogelijk vanuit andere sites/toegangen tot Brimbreda.nl en vervolgens naar www.breda.nl. Door goede beveiliging zou het risico voor andere klanten op overlast sterk verkleind moeten zijn, zo stelt de Rekenkamer.

Misschien is het een idee om de Brimbreda site onder te brengen bij de hosting bedrijven waar al een groot deel van de Bredase sites ondergebracht zijn?

Bijlage 3 Raadsbrief Visitatierapport Breda Visitatiecommissie Informatieveiligheid

Onderwerp
Informatieveiligheid van de VNG **Datum 29-03-2016**

Geachte leden van de gemeenteraad,

Met deze brief informeren wij u over het verslag van de visitatiecommissie Informatieveiligheid van de VNG. In de bijlage treft u de aanbiedingsbrief van de visitatiecommissie en hun verslag aan. Bij de buitengewone algemene ledenvergadering van de VNG op 29 november 2013 is de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' aangenomen. Een van de onderdelen van deze resolutie is het instellen van een visitatiecommissie met als doel om het lerend vermogen op het gebied van informatieveiligheid te versterken. De doelstelling van de commissie is als volgt geformuleerd:

- Aandacht voor informatieveiligheid bij gemeenten vasthouden en stimuleren.
- Vergroten van het handelingsperspectief van gemeenten op het vlak van informatieveiligheid.
- Toetsen of het systeem van verplichtende zelfregulering werkt en hoe/waar het verbeterd kan worden.

Deze commissie heeft op 20 januari 2016 een bezoek gebracht aan de gemeente Breda.

Parallel aan deze visitatieronde wordt momenteel ook door de Rekenkamer van de gemeente Breda een onderzoek uitgevoerd naar informatieveiligheid. Dit onderzoek zal binnenkort afgerond worden. De rekenkamer heeft dit visitatierapport inmiddels ontvangen en zal deze als bijlagen bij hun onderzoek voegen en meenemen in de advisering. Wij stellen daarom voor, in overleg met de Rekenkamer, om de bespreking van het rapport van de visitatiecommissie tegelijk te agenderen met de bespreking van het rapport van de rekenkamer.

Wij hopen u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,

Burgemeester en wethouders van Breda,
Gemeentesecretaris van Breda

Het visitatierapport van de Visitatiecommissie Informatieveiligheid van de VNG

Geacht College van Burgemeester & Wethouders,

Namens de Visitatiecommissie Informatieveiligheid stuur ik u met veel plezier het definitieve gespreksverslag van ons constructief gesprek. Uw commentaar op het conceptverslag hebben wij verwerkt dan wel op gereageerd.

In het verslag hebben wij per hoofdthema een analyse gedaan van de besproken situatie in uw gemeente en daaropvolgend een advies geformuleerd. Het verslag is geordend langs de hoofdthema's van het gesprek:

- Digitalisering in het algemeen
- Besef van het belang om te werken aan informatieveiligheid
- Formele positionering van informatieveiligheid in de organisatie
- Daadwerkelijk uitvoeren van beleid en daadwerkelijk leren
- Extern leren en participeren in netwerken

Tot slot heeft de Commissie een handelingsperspectief geformuleerd. Dit handelingsperspectief is gebaseerd op de situatie in uw gemeente. Daarmee hopen wij uw gemeente van dienst te zijn bij het verder vormgeven van de informatieveiligheid.

Mede namens Maarten Ruys en Wim Blok wil ik u nogmaals hartelijk danken voor de open gedachtewisseling. Wij wensen u wijsheid toe bij het verder vormgeven aan informatieveiligheid als voorwaarde voor professionele dienstverlening.

Namens de Visitatiecommissie: Frans Backhuijs (voorzitter)
Aanwezig Visitatiecommissie: Wim Blok, Maarten Ruys, Eric Warners (secretaris)

De Commissie informatieveiligheid dankt de gemeente Breda hartelijk voor haar gastvrijheid. De commissie heeft een open gesprek kunnen voeren, wat zij zeer heeft gewaardeerd. Ze denkt een goed beeld te hebben gekregen van de wijze waarop de gemeente Breda werkt aan informatieveiligheid en wat de grootste uitdagingen zijn.

De Commissie heeft het beeld dat de gemeente Breda constructief aan het werk is met informatieveiligheid en klaar is om de volgende stap te maken. Daarbij viel de Commissie specifiek de volgende zaken positief op:

- Er is bestuurlijke en ambtelijke commitment om informatieveiligheid stap voor stap verder te brengen.
- Breda heeft tijd en capaciteit vrijgemaakt om het fundament op orde te brengen. Het beeld van de Commissie is dat Breda nu klaar is om resultaten te borgen en verder te verdiepen.
- Breda is zowel in bestuurlijke als ambtelijke netwerken actief kennis en kunde aan het verzamelen. Breda heeft met name slim gebruik gemaakt van de mogelijkheden en concrete instrumenten die de IBD biedt.
- De Commissie constateert dat de gemeente Breda het gesprek met de Raad over informatieveiligheid op een strategisch niveau voert. Dit geeft de mogelijkheid om samen met de Raad beelden te ontwikkelen over het omgaan met informatieveiligheid op de lange en korte termijn .

In dit verslag beschrijven we achtereenvolgens ons verkregen beeld, een aantal aanbevelingen voor het handelingsperspectief van de gemeente voor de komende periode en enkele slotnoties. Het beeld van de Commissie is gecategoriseerd in vijf onderdelen: 1. Digitalisering algemeen, 2. Gerichtheid, 3. Verankering, 4. Extern leren en 5. Werking.

Handelingsperspectief

Vergroot de bestuurlijk aandacht en de kennis door vanuit wisselende perspectieven te kijken

De portefeuillehouder is op bestuurlijk niveau het meest betrokken bij informatieveiligheid. De Commissie acht het belangrijk dat ook de andere Collegeleden gevoel en kennis ontwikkelen over de mogelijke impact van informatieveiligheid op andere beleidsterreinen. Denk aan de betekenis van informatieveiligheid voor de openbare orde en handhaving of voor financiën. Dit kijken vanuit wisselende perspectieven kan concreet vorm krijgen door kennissessies te beleggen over informatieveiligheid, kennisexpedities te organiseren naar bedrijven waar informatieveiligheid een cruciaal onderwerp is of hierover jaarlijks op bestuurlijk niveau kennis uit te wisselen met andere gemeenten. De jaarlijkse I-bewustzijnssessies van de VNG zijn hier een concrete gelegenheid voor.

Versterk de formele positionering van informatieveiligheid

De Commissie ziet de heroriëntatie op de organisatie-inrichting als een mooi momentum om ook stil te staan bij de formele positionering van informatieveiligheid in de organisatie. De Commissie doet de aanbeveling om in ieder geval de rol en verantwoordelijkheden van de gemeentesecretaris, directeur servicebedrijf en de adviseur informatiebeveiliging expliciet te maken. In lijn met de Baseline Informatieveiligheid Gemeenten adviseert de Commissie specifiek om de adviseur informatieveiligheid direct te laten rapporteren aan de gemeentesecretaris en daarmee als CISO te laten fungeren. Daarnaast ziet de Commissie in veel gemeenten dat het College verantwoordelijk is voor zowel de vaststelling van het beleid als de jaarplannen.

Maak gebruik van bestaande instrumenten en ervaringen op het vlak van houding en gedrag.

Het beeld is dat Breda werkt aan het verbeteren van informatieveiligheid, waarbij het accent tot nog toe lag op technische en organisatorische verbeteringen in de organisatie. Breda heeft de ambitie om komend jaar ook extra aandacht te besteden aan diverse leer- en bewustzijnsacties. De Commissie geeft graag mee dat al erg veel leermateriaal ontwikkeld is, zowel landelijk als lokaal. De Commissie raadt Breda aan om te kijken in hoeverre het bestaande materiaal herbruikbaar is. Denk aan het 1-bewustzijnsmateriaal (verkrijgbaar via de VNG Academie). De VNG kan de gemeente Breda ook helpen om in contact te komen met gemeenten die al langere tijd werken aan gedrag en bewustzijn.

De Commissie doet verder de suggestie om de aandacht voor houding en gedrag in de organisatie te intensiveren door een verdere systematisering van het leren. Door leeracties als !-bewustzijn te verbinden met opleidingsplannen en systematische aandacht voor het kennisniveau in de organisatie wordt het leren binnen de organisatie steviger ondergrond geboden. Periodieke interactie met het lijnmanagement over het verder systematiseren van het leerbeleid is daarbij wenselijk. Dit geeft de mogelijkheid om heel gericht te blijven zoeken naar de best werkende mix van interventies en acties.

1. Digitalisering algemeen (context)

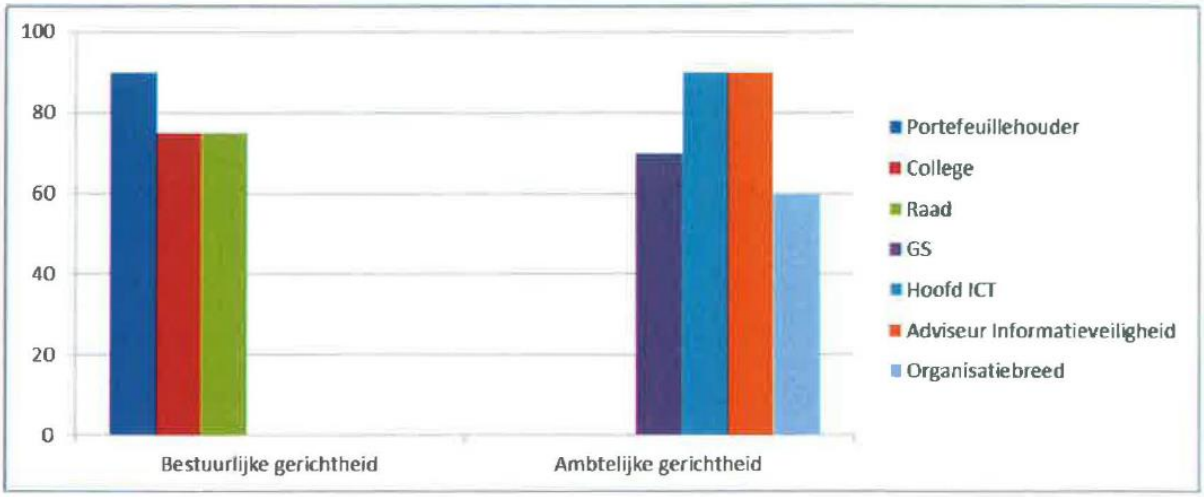
In Breda leeft digitalisering van de dienstverlening en werkprocessen sinds een aantal jaar. Met name de overstap naar digitale dienstverlening heeft een impuls gegeven aan het digitaliseringsproces. Ook wordt gewerkt aan een visie op onderwerpen als Smart Cities en Open Data.

De aandacht voor informatieveiligheid is stap voor stap toegenomen. In de afgelopen twee jaar is er capaciteit beschikbaar om te werken aan het onderwerp. In de eerste periode is vooral gewerkt aan het op orde krijgen van informatieveiligheid. In lijn met de Resolutie is veel aandacht uitgegaan naar de implementatie van de BIG. Tegenwoordig gaat ook aandacht uit naar de betekenis van meer complexe ontwikkelingen voor informatieveiligheid, zoals het gebruik van de Cloud.

Bij de start van nieuwe digitaliseringsprojecten wordt informatieveiligheid geborgd door de betrokken 1-adviseur. Als informatieveiligheid naar verwachting sterke vereisten stelt aan de inrichting van het proces, wordt van tevoren een impactanalyse uitgevoerd. De positieve ontwikkeling in de gemeente Breda is dat informatieveiligheid steeds meer al vanaf de start van een project expliciet op de agenda staat.

2. Besef van het belang van werken aan informatieveiligheid (gerichtheid)

Het beeld van de Commissie is dat gerichtheid op bestuurlijk niveau aanwezig is. Men onderkent het belang van informatieveiligheid en geeft vervolg aan onderkenning door het onderwerp te agenderen. De Raad toont ook betrokkenheid bij het onderwerp, waarbij de Commissie positief is over de proactieve handelswijze van de Raad waar het gaat om *informatieveiligheid. Ambtelijk is men vooral op tactisch/operationeel niveau sterk betrokken bij het onderwerp. In de breedte van de organisatie zijn met betrekking tot bewustzijn in ieder geval nog stappen te maken.*



Figuur 1: mate van bestuurlijke en ambtelijke gerichtheid

De portefeuillehouder onderkent het belang van informatieveiligheid en toont betrokkenheid. De betrokkenheid blijkt onder meer uit de regelmatige bespreking van informatieveiligheid tijdens stafoverleg.

Ook in het College onderkent men het belang van informatieveiligheid, maar de betrokkenheid bij het onderwerp kan verder vergroot worden. De Commissie heeft het beeld dat de bespreking van het onderwerp zich nog vooral richt op de vaststelling van het beleid en de jaarplannen. In mindere mate wordt samen een visie gevormd op de omgang met informatieveiligheid.

De Commissie is positief over de betrokkenheid van de Raad bij het onderwerp. De Raad agendeert zelf het onderwerp en vraagt om verantwoording door het College. Daarnaast is het beeld dat de Commissie proactief de strategische discussie zoekt met het College langs de lijnen van nieuwe ontwikkelingen, zoals Big Data, Open Data en Smart Cities.

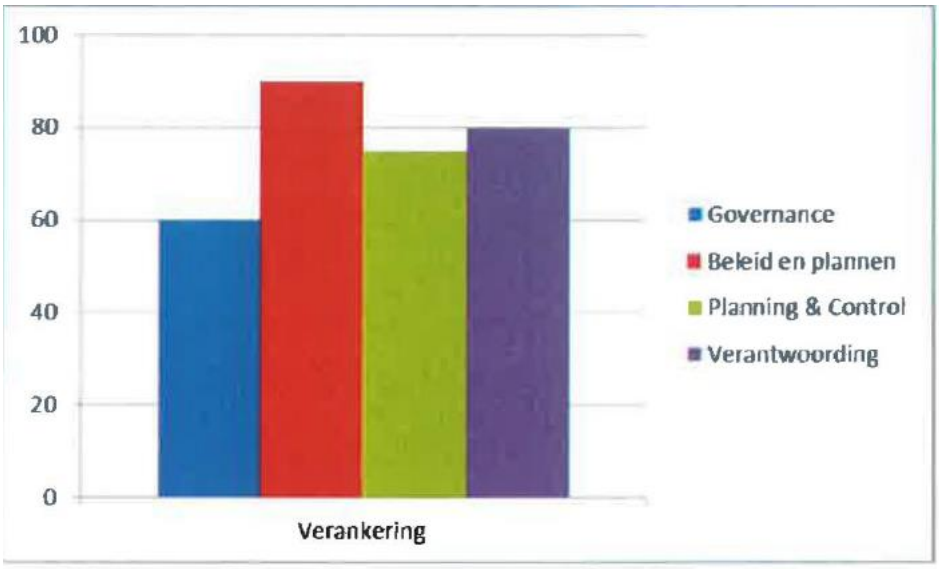
Daarnaast is ook de Raad sinds januari volledig digitaal gaan werken . Er bestaat bij de Raadsleden behoefte aan ondersteuning bij deze overgang, waarbij ook aandacht uitgaat naar informatieveilige omgang met documenten. Breda geeft aan met name tevreden te zijn over de manier waarop met de Raad gesproken wordt over de omgang met geheime informatie en de afspraken die daaruit volgen.

Op topambtelijk niveau is met name op operationeel/tactisch niveau sterke gerichtheid op het onderwerp. Er zijn twee fulltime adviseurs informatiebeveiliging die kennis hebben van en betrokken zijn bij het onderwerp. Ook de gemeentesecretaris acht het onderwerp van belang en ziet het als een vraagstuk waardoor de gemeente Breda als één organisatie aan gewerkt moet gaan worden.

In de breedte van de organisatie is informatieveiligheid nog weinig aan de orde, met uitzondering van de afdelingen waar informatieveiligheid van oudsher een belangrijk thema is. Het plan is om in het komend jaar extra aandacht te besteden aan het bewustzijn en het leren in de organisatie.

3. Formele positionering in bestuur, organisatie en in P&C cyclus (verankering)

Breda heeft het onderwerp in de reguliere lijn gepositioneerd. Dit betekent dat er formeel geen CISO (maar een adviseur informatiebeveiliging) is en ook de andere verantwoordelijkheden en bevoegdheden niet expliciet zijn gemaakt. Er is beleid en een jaarplan. In het jaarverslag staat een paragraaf opgenomen over informatieveiligheid.



Figuur 2: mate van bestuurlijke en ambtelijke verankering

De governance-structuur van de gemeente Breda ziet er als volgt uit:

- Bestuurlijk is de portefeuillehouder verantwoordelijk voor informatieveiligheid.
- De gemeentesecretaris is verantwoordelijk voor het functioneren van de organisatie en daarmee impliciet ook voor informatieveiligheid.
- De gemeente kent vijf directies. Elke directeur is verantwoordelijk voor informatieveiligheid in zijn of haar directie.
- Eén van de directies is het servicebedrijf. Onderdeel van het servicebedrijf is de afdeling Proces en Informatie (PI). De adviseur informatiebeveiliging is medewerker bij de afdeling PI. De adviseur informatiebeveiliging rapporteert aan het Hoofd PI.

De adviseur informatiebeveiliging is in de lijn gepositioneerd en heeft nu formeel geen directe toegang tot de gemeentesecretaris dan wel het College (informeel werkt dit anders; zie 5.Werking). Op operationeel/tactisch niveau is een werkgroep gevormd.

De werkgroep richt zich op de onderling verbonden onderwerpen : digitalisering, persoonsgegevens, privacy, DIV en informatieveiligheid. De werkgroep is de uitvoeringskracht waar het gaat om digitalisering, en specifiek informatieveiligheid.

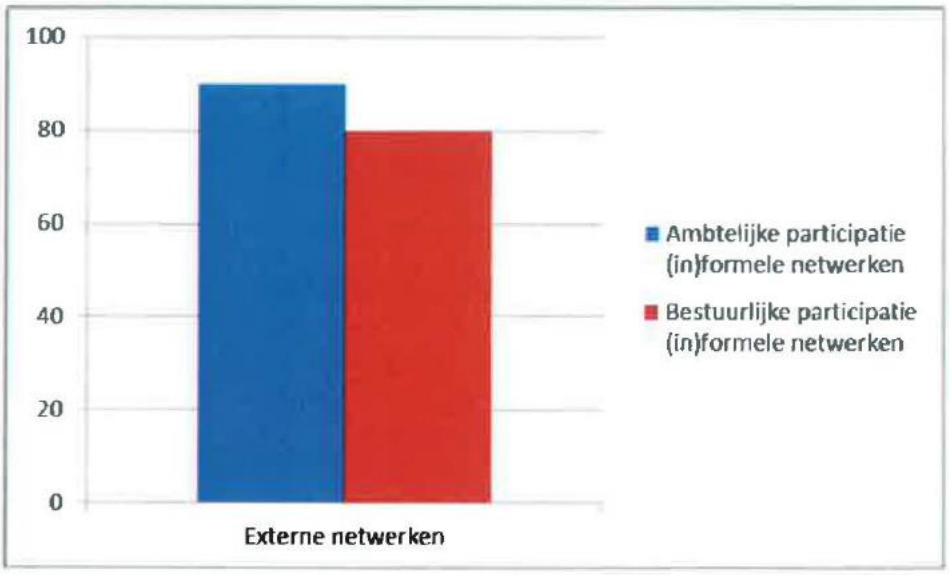
Gemeente Breda geeft aan te werken aan een heroriëntatie op de interne inrichting. De heroriëntatie richt zich op het verkennen van een sturingsvorm die de uniformiteit binnen de gemeente vergroot.

Breda heeft informatiebeleid opgesteld en vastgesteld door het College van Burgemeester en Wethouders. Het informatiebeleid is ter kennisname gebracht aan de Commissie Bestuur van de Raad. Elk jaar wordt er op basis van de bevindingen uit de GAP-analyse en de risicoanalyse een jaarplan opgesteld. Afgelopen jaar is dat jaarplan (2015) vastgesteld door de Directeur Servicebedrijf. Het jaarplan voor 2016 is in concept klaar. Er is nog geen keuze gemaakt over wie het jaarplan vaststelt, waarbij ook de keuze om dit bestuurlijk te laten vaststellen overwogen wordt.

Breda voert jaarlijks de verplichte audits en controles uit. Daarnaast is informatieveiligheid onderdeel van de jaarlijkse IT-audit ten behoeve van het jaarverslag. In het jaarverslag staat expliciet een paragraaf opgenomen over informatieveiligheid.

4. Extern leren

Breda is één van de eerste gemeenten die zich aansloot bij de IBD. Daarnaast is men bestuurlijk en ambtelijk erg actief in zowel regionale als landelijke netwerken waar het onderwerp informatieveiligheid op de agenda staat.



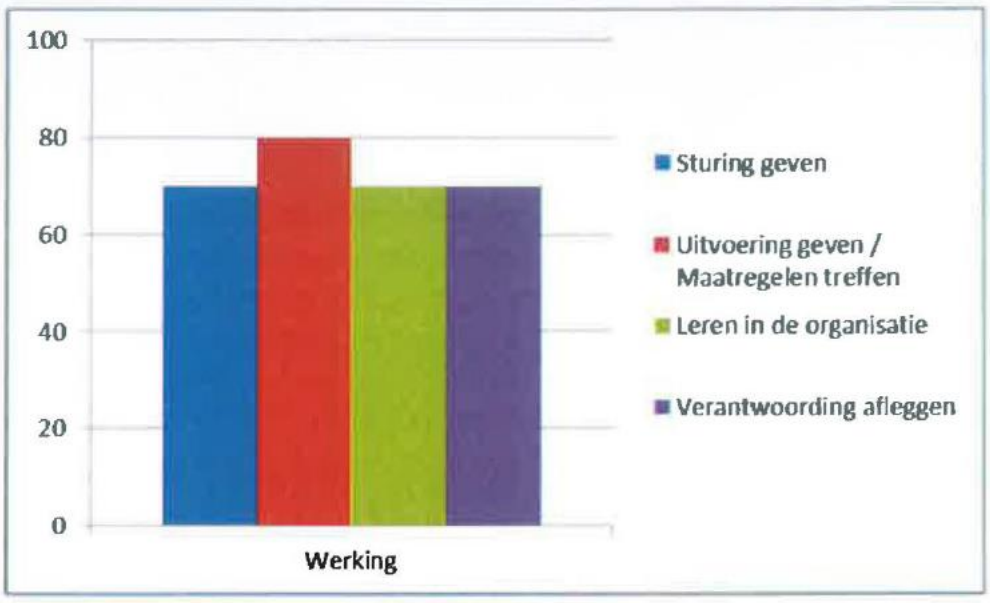
Breda is volledig aangesloten bij de IBD. Er wordt veel gebruik gemaakt van IBD-kennis en -instrumenten. Daarnaast is ambtelijk contact met de VNG en is men actief in diverse KINGnetwerken.

Ook voor de oprichting van de IBD was Breda al lid van Govcert. Breda is één van de gemeenten die experimenteert met honeypots: een systeem dat bewust is opgezet om te hacken met als bedoeling hackers te verleiden en zo inzicht in werkwijzen te krijgen.

Op bestuurlijk niveau gaat de wethouder regelmatig in gesprek over informatieveiligheid, vooral om verhalen en inspiratie op te halen die verder richting kunnen geven aan de praktijk in Breda. Ook is de wethouder aanwezig bij congressen zoals het VNG-KING jaarcongres, om nieuwe kennis te verzamelen.

5. Daadwerkelijk leren, daadwerkelijk beleid uitvoeren (werking)

Het beeld van de Commissie is dat in de praktijk informele verbindingen zijn ontstaan tussen de belangrijkste betrokkenen op tactisch operationeel-niveau, topambtelijk niveau en bestuurlijk niveau. Basis voor de uitvoering in 2016 is het jaarplan. De ambitie is om *het institutioneel leren als één organisatie verder te versterken. Daarnaast wil men in 2016 specifiek inzetten op bewustwording in de breedte van de organisatie. Er is sprake van systematische verantwoording aan de Raad via het jaarverslag.*



Figuur 3: mate van werking van de verankering en het leren

De governance-structuur werkt in de praktijk als volgt:

- Er is tweewekelijks overleg tussen het Hoofd Proces en Informatie en de adviseur informatieveiligheid over de vorderingen op het vlak van informatieveiligheid. Het jaarplan fungeert hierbij als leidraad.
- Daarnaast is wekelijks teamoverleg ICT, waarbij eventuele incidenten ook worden besproken.
- Hoofd PI rapporteert periodiek aan de Directeur Servicebedrijf, waarbij informatieveiligheid één van de onderwerpen is.
- Parallel blijkt behoefte te bestaan bij de betrokken portefeuillehouder om over dit onderwerp regelmatig geïnformeerd te worden. De afgelopen maanden is vier keer overleg geweest over informatieveiligheid tussen de wethouder en in ieder geval de adviseur. informatiebeveiliging en Hoofd PI over relevante ontwikkelingen en vorderingen.
- Daarnaast komt de projectgroep informatieveiligheid regelmatig bij elkaar om de voortgang op tactisch/operationeel niveau in de breedte van de organisatie te bespreken.

De uitvoering verloopt conform het jaarplan. In het jaarplan is specifieke aandacht voor de relatie met leveranciers. Uit de BIG zijn een aantal normen geselecteerd waaraan leveranciers aanvullend dienen te voldoen. Dit wordt getoetst aan de hand van NEN-certificeringen dan wel Third-Party Mededelingen. Dergelijke vereisten worden meegenomen in de aanbestedingen. In de komende periode gaat extra aandacht worden besteed aan het bewustzijn in de breedte van de organisatie.

Reguliere controles en de IT audit vormen de basis van de controle-cyclus. Bevindingen en ervaringen worden zoveel mogelijk omgezet tot actie.

Dit gebeurt tot nog toe vooral binnen de afdelingen waar leerpunten worden geconstateerd. De behoefte bestaat om aan de hand van incidenten (dan wel simulaties) ook het organisatiebreed leren verder vorm te geven.

Verantwoording aan de Raad gebeurt via het jaarverslag. De rapportages over informatieveiligheid zijn inhoudelijk beknopt. Door de Raad zijn geen aanvullende vragen gesteld.

6. Tot slot

- Gemeente Breda heeft het gesprek met de Visitatiecommissie als plezierig ervaren.
- De gezamenlijke voorbereiding van het gesprek aan de hand van de vragenlijst heeft de gemeente Breda geholpen om het huidige werken aan informatieveiligheid scherp te krijgen.
- Er bestaat bij de gemeente Breda behoefte aan een gecombineerde audit, gebaseerd op de BIG.
- Op bestuurlijk niveau bestaat behoefte aan meer inspiratie en verhalen die richting geven aan de bestuurlijke discussie over informatieveiligheid.
  (zie: http://www.taskforcebid.nl/fileadmin/bestandentaskforce/pdfllnspiratiebundel Taskforce LR.pdf voor een inspiratiebundel over informatieveiligheid).
- De gemeente Breda vraagt aandacht voor de verwevenheid van informatieveiligheid in allerlei informatieketens. Dit is een belangrijk perspectief op het informatieveiligheidsvraagstuk dat nadere verdieping vraagt.
- De gemeente Breda heeft aangegeven het verslag met het College te willen bespreken en de Raad te informeren mede in relatie met een lopend rekenkameronderzoek naar informatieveiligheid.

Bijlage 4 Voorbeeld van Privacy clausules, werkwijze casussen WMO

Uit: 'Standaard Resultaatovereenkomst dienstverlening Begeleiding', Gemeente Breda 24-09-2014

Blz. 16 *Casusoverleg*

4.1. Dienstverlener zorgt dat de Generalist op de hoogte is van eventuele bijstellingen op de uitvoering van het ondersteuningsplan en van onvoorziene problemen bij de uitvoering van dat plan. Zodat de Generalist als regisseur op hoofdlijnen kan volgen wat er daadwerkelijk gebeurt. Te denken valt aan voorgestelde aanpassingen van het te bereiken resultaat, looptijd van het plan, signalen over het niet medewerken door Client, ingediende klacht, et cetera. Doel is het informeren van een collega hulpverlener, die een regisserende taak heeft.

Blz. 17 *Kaders voor gegevensuitwisseling*

6.1 Informatievoorziening. Dienstverlener conformeert zich aan standaarden op het gebied van informatievoorziening en berichtenverkeer zoals deze landelijke en specifiek voor de/het sector/domein waarin hij werkzaam is zijn vastgesteld. Denk hierbij o.a. aan gebruik van basisgegevens als BSN, standaarden voor berichtenuitwisseling zoals iWMO, iJW, CORV en het gebruik van het gegevensknooppunt.

6.2 Informatiebeveiliging. Dienstverlener conformeert zich aan standaarden en uitgangspunten op het gebied van informatiebeveiliging zoals deze landelijke en specifiek voor de/het sector/domein waarin hij werkzaam is zijn vastgesteld. Denk hierbij o.a. aan gebruik van basisgegevens als BSN, standaarden voor berichtenuitwisseling zoals iWMO, iJW, CORV en het gebruik van het gegevensknooppunt.

6.2 Informatiebeveiliging. Dienstverlener conformeert zich aan standaarden en uitgangspunten op het gebied van informatiebeveiliging zoals deze landelijk en voor de/het sector/domein waarin hij werkzaam is zijn vastgesteld c.q. zijn geaccepteerd. Denk voor gemeenten hierbij aan de Baseline "Informatiebeveiliging Nederlandse Gemeenten (BIG)" van de "Informatie Beveiligings Dienst (IBD), denk voor andere sectoren/domeinen onder andere aan NEN 27001, NEN 27002 of aan de algemeen aanvaarde procedures betreffende informatiebeveiliging waaronder o.a. vallen beveiligde toegang tot systemen cq. gegevens en beveiligd berichtenverkeer.

6.3 Privacy

Dienstverlener conformeert zich aan landelijke kaders en standaarden op het gebied van het verwerken, beheren en delen van persoonsgegevens binnen het sociaal domein. Denk hierbij o.a. aan de Participatiewet, de Jeugdwet, de Wet maatschappelijke ondersteuning, maar ook de Wet bescherming persoonsgegevens.

In het proces van dienstverlening treedt de gemeente op als regisseur. In die rol beschikt de gemeente over informatie die nodig is om de regiefunctie uit te oefenen. Dat wil zeggen dat de gemeente zich laat adviseren door dienstverleners en daarbij antwoord krijgt van die dienstverleners op vragen die voor het sturen van het proces van hulpverlening nodig zijn. De regie-informatie is bij de gemeente en behoort ook in het geval dat regietaken worden uitbesteed, onder de verantwoordelijkheid van de gemeente. Het inhoudelijke dossier met hulpverleningsgegevens blijft bij de dienstverlener; dat dossier volgt de cliënt.

Na het aflopen of beëindigen van deze overeenkomst of in het geval van faillissement of overname, is de Dienstverlener verplicht om de regie-informatie, zoals bovengenoemd, digitaal in een door de gemeente dan vast te stellen formaat, over te dragen aan de Gemeente zodat deze ingelezen kan worden in een informatiesysteem.

Op verzoek van de gemeente dient een dienstverlener medewerking te verlenen medewerking te verlenen aan een audit op het gebied van gegevensverwerking of een Privacy Impact Analyse.

In onderling overleg wordt in het derde kwartaal van 2015 bovenstaande werkwijze geëvalueerd. Zo nodig worden afspraken bijgesteld.

Blz. 20 **Ontwikkelopgave**

Privacy

Omdat de dienstverleners onderling actief informatie delen, stellen partijen gezamenlijk voor 1 juli 2015 een Privacy Protocol op en conformeren zich daaraan. Een dergelijk protocol bevat minimaal:

- het doel waarom en de wijze waarop informatie wordt vergaard, geregistreerd, doorgegeven, bewaard en vernietigd;
- de wijze waarop bij de dienstverlener een zorgvuldige verwerking van persoonsgegevens binnen het werkproces wordt gewaarborgd (casusregie, procesregie, kwalificaties personeel, software etc.);

- een analyse van de risico's op (onbedoelde) privacy en beveiligings- schendingen door ongeclausuleerde informatievergaring en –verwerking;
- de eisen van subsidiariteit, proportionaliteit en doelmatigheid aan het verzamelen en bewerken van informatie, waarmee onbedoelde privacy schendingen in de processen worden voorkomen.

Met aandacht voor:
- aan cliënt voldoende, maar niet meer persoonlijke informatie vragen dan noodzakelijk om taak uit te kunnen oefenen;
- aan cliënt om toestemming vragen voor het delen van informatie als daarvoor een rechtmatige grondslag ontbreekt;
- afpaling van het domein waar de (diverse rollen) van medewerkers toegang hebben tot informatie, delen en bewerken van gegevens;
- gegevens over cliënten moeten op één centrale plek worden vastgelegd en opgeslagen en eenvoudig opgevraagd kunnen worden door geautoriseerde professionals;
- dossiergegevens over cliënten zijn te allen tijde raadpleegbaar dan wel opvraagbaar door de cliënten zelf, met in achtneming van de wettelijke regels hieromtrent.

Bijlage 5 Begrippenlijst

- **Autoriteit Persoonsgegevens (AP)**=
  De Autoriteit Persoonsgegevens is een zelfstandig bestuursorgaan, dat rapporteert aan het Ministerie van Veiligheid en Justitie. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving. Iedere lidstaat van de Europese Unie is via de Wbp verplicht een privacyautoriteit te hebben die onafhankelijk toezicht houdt op het gebruik van persoonsgegevens.
- **AVG**=
  Europese Algemene Verordening Gegevensbescherming. In mei 2016 is de Europese Verordening Gegevensbescherming in werking getreden, die striktere eisen stelt betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
- **BAG**=
  Basisregistratie Adressen en Gebouwen.
- **BIG**=
  Baseline Informatiebeveiliging Nederlandse Gemeenten door de Informatiebeveiligingsdienst van het Ministerie van BZK opgesteld.
- **College Bescherming Persoonsgegevens (CBP)**=
  Tot aan 1 januari 2016 heette de Autoriteit Persoonsgegevens (AP) het College Bescherming Persoonsgegevens.
- **DigiD**=
  Digitale identiteit. Met een persoonlijke DigiD kan ingelogd worden op websites van de overheid en bijvoorbeeld in de zorg om persoonlijke (vertrouwelijke) gegevens door te geven of op te vragen.
- **Firewall**=
  Is een systeem dat een netwerk of computer beschermt tegen misbruik van buitenaf, bijvoorbeeld tegen aanvallen van hackers en computerkrakers, inbraken en/of uitbraken van computervirussen, spyware, spam en *denial of service attacks*.
- **GAP-analyse**=
  Een analyse van verschillen tussen de huidige en de gewenste situatie. In dit geval bedoeld als een analyse in hoeverre de gemeentelijke BIG-normen gehaald worden en waar nog hiaten zijn.
- **IBD**=
  Informatiebeveiligingsdienst van het Ministerie van Binnenlandse Zaken en Koninkrijkszaken, samen met KING en de VNG.
- **Machtigingen apps**=
  Smartphones geven veelal automatisch machtigingen aan alle gratis apps, die gebruikt worden, om over alle informatie in de smartphone te kunnen beschikken. Als de apps-machtigingen niet uitgeschakeld zijn (zie Instellingen: Privacy, apps machtigingen), kunnen alle gegevens qua berichten, contacten, agenda, foto's, microfoon e.d. vrijelijk gebruikt worden door de bedrijven achter de gratis apps en doorverkocht worden aan andere bedrijven. Allerlei bedrijven en organisaties beschikken op die manier automatisch, zonder dat de mensen daar zelf erg in hebben, over alle persoonlijke en alle werkgegevens van de gebruikers. Personen kunnen op die manier overal gevolgd worden en hun informatie kan door de bedrijven vrijelijk gebruikt worden voor allerlei doeleinden.
  Zie http://www.npo.nl/3doc-addicted-to-my-phone/24-10-2016/AT_2068495
- **Malware**=
  Software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen. Het woord is een samentrekking van het Engelse malicious software (kwaadaardige software, soms schadelijke software). Malware veronderstelt kwade opzet.
- **MT**=
  Managementteam.
- **Mystery guest onderzoek**=
  Door middel van een mystery guest onderzoek kan de beveiliging van gebouwen, ruimtes en bestanden/informatie worden getest. Daarbij wordt een bureau ingehuurd om pogingen te doen om (zonder toegangspasje of uitnodiging) een beveiligd gebouw binnen te komen, om

hierbinnen zoveel mogelijk beveiligde ruimtes binnen te komen, vertrouwelijke documenten in te zien, toegang tot beveiligde bestanden (bijvoorbeeld GBA, uitkeringssysteem e.d.) te verkrijgen etc..

- **NCSC**=
  Het Nationaal Cyber Security Centrum is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland en valt onder het Ministerie van Veiligheid en Justitie.
- **NCTV**=
  De Nationale Coördinator Terrorismebestrijding en Veiligheid heeft als taak om Nederland tegen bedreigingen te beschermen, die de maatschappij kunnen ontwrichten (zoals terroristische aanslagen, cybercriminaliteit e.d.). De NCTV valt onder het Ministerie van Veiligheid en Justitie.
- **Spyware**=
  Is de naam voor computerprogramma's (of delen daarvan) die informatie vergaren over een computergebruiker en deze doorsturen naar een externe partij. Het doel van spyware is meestal om geld te verdienen. De term komt van het Engelse woord *spy*, dat spion betekent, en het achtervoegsel *ware*, dat aangeeft dat het om software gaat.
- **Phishing**=
  Is een vorm van oplichting op het internet. De slachtoffers worden vaak via een email benaderd. In de mail staat een link die het slachtoffer naar een valse website lokt. Zo'n email lijkt te komen van een betrouwbare instantie, bijvoorbeeld een creditcardmaatschappij of een bank. Het verzoek van de oplichter is meestal om 'de inloggegevens te controleren'. Via een echt lijkende website, die met de link verbonden is, kan de oplichter inloggegevens en persoonsgegevens in handen krijgen. Daarmee kan de oplichter bijvoorbeeld op naam van die persoon spullen kopen en/of geld van de betreffende bankrekening halen.
- **Phishing mails**=
  Emails die als doel hebben om gegevens van personen of bedrijven te verkrijgen, waarmee fraude gepleegd kan worden.
- **PIA**=
  Een Privacy Impact Assessment (PIA) is een onderzoek dat zich richt op de mogelijke impact op de privacy in gevallen waarin verwerkingen van persoonsgegevens betrokken zijn. Vanaf 1 september 2013 is het uitvoeren van een PIA voor de Rijksdienst verplicht. In het buitenland bestaat al een langere historie van het uitvoeren van PIA's en wordt hier ook op gehandhaafd. Vanuit het oogpunt van het beperken van aansprakelijkheid is het uitvoeren van PIA's zeer aan te raden. In het kader van het de Wet Meldplicht Datalekken is het verstandig regelmatig PIA's uit te voeren. In de Europese Algemene Verordening Gegevensbescherming wordt het uitvoeren van een PIA in meer gevallen expliciet verplicht gesteld dan nu.
- **Ransomware**=
  Is een chantagemethode op internet door middel van malware. Letterlijk vertaald betekent ransom: losgeld. Ransomware is een programma dat een computer (of gegevens die erop staan) blokkeert en vervolgens geld van de gebruiker vraagt om de computer weer te 'bevrijden'. Het wordt daarom ook wel 'gijzelingsvirus' genoemd.
- Valse-email@fraudehelpdesk.nl=
  Helpdesk waar valse, frauduleuze emails/phishing mails aan doorgegeven kunnen worden. De helpdesk is onderdeel van de Stichting Aanpak Financieel-Economische Criminaliteit in Nederland.
- **Wbp**=
  De Wet bescherming persoonsgegevens bevat alle regels en richtlijnen ter bescherming van persoonsgegevens. Per 1-1-2016 is deze wet aangescherpt en is hier de Wet Meldplicht Datalekken aan toegevoegd.
- **Wet Meldplicht Datalekken**=
  Per 1-1-2016 is de Wet Meldplicht Datalekken in werking getreden en vanaf die datum zijn organisaties, die werken met vertrouwelijke, privacygevoelige en persoonsgegevens, verplicht om (ernstige) leks en inbraakpogingen te melden aan de Autoriteit Persoonsgegevens. Wordt een ernstig datalek niet binnen twee werkdagen gemeld en kan een organisatie niet aantonen er alles aan gedaan te hebben om goed beveiligd te zijn, dan riskeert de organisatie een boete die kan oplopen tot 810.000 euro of 10% van de omzet.

Literatuurlijst

- Autoriteit Persoonsgegevens, ‘Onderzoek toestemming sociaal domein’, april 2016
- Binnenlands Bestuur Digitaal, 'Ambtenaren niet bewust genoeg van belang informatieveiligheid', 30 sept. 2016
- Binnenlands Bestuur Digitaal, ‘Overheden veelvuldig doelwit van cyberaanvallen’, 14 okt. 2015
- Binnenlands Bestuur Digitaal, 'Rijk verantwoordelijkheid voor slechte gegevensbeveiliging', 18 aug. 2016
- Binnenlands Bestuur Digitaal, ‘Rijksambtenaren digitaal alerter dan lokale ambtenaren’, 28 okt 2015
- Binnenlands Bestuur Digitaal, ‘Wijkteam mailt gegevens cliënten naar verkeerde’, april 2016
- Binnenlands Bestuur Digitaal, ‘Ziekenhuis VS al week plat door aanval ransomware’, 16 febr. 2016
- Bureau 2 Control it, ‘DigiD-assesment digitale loket 2014’, 2015
- Bureau 2 Control it, ‘DigiD-assesment WOZ-loket 2014’, 2015
- Centraal Planbureau en het Nationaal Cyber Security Centrum, ‘Risicorapportage cyberveiligheid’, juli 2016
- Deloitte, ‘Cyber value at risk in The Netherlands’, april 2016
- Ernst & Young, ‘Beoordeling IT beheersmaatregelen geautoriseerde gegevensverwerking, wijzigingsbeheer en logische toegangsbeveiliging van o.a. de applicaties Key2Financiën, GWS4all en Workforce’, 2014
- Ernst & Young, ‘Heraudit DigiD-assesment digitale loket’, 2014
- Ernst & Young, ‘Heraudit DigiD-assesment WOZ-loket’, 2014
- Ernst & Young, ‘Rapport van bevindingen bij Jaarverslag 2015 van de Gemeente Breda’, 2016
- Europese Unie, ‘Europese Algemene Verordening Gegevensverwerking’, april 2016
- Gemeente Breda, ‘Actieplan 2016-2018 ‘Open data maakt mogelijk’, juni 2016
- Gemeente Breda, ‘Begroting 2016’, 2015
- Gemeente Breda, ‘Informatie Beveiligingsbeleid’, 2014
- Gemeente Breda, ’Informatieveiligheidsplan 2016-2017’, juni 2016
- Gemeente Breda, ‘Jaarverslag 2014’, 2015
- Gemeente Breda, ‘Jaarverslag 2015’, 2016
- Gemeente Breda, “Programma Veiligheid 2015-2018’, 2014
- Gemeente Breda, ‘Raadsbrief 29032016 Verslag Visitatiecommissie informatieveiligheid VNG’, 2016
- Gemeente Breda, ‘Standaard Resultaatovereenkomst dienstverlening Begeleiding’, 2014
- Gemeente Breda, ‘Uitvoeringsplan informatiebeveiliging 2015’, 2015
- Informatiebeveiligingsdienst, ‘Strategische Baseline Informatiebeveiliging Nederlandse gemeenten’, 2013 (met updates in 2015 en 2016)
- Informatiebeveiligingsdienst, ‘Tactische Baseline Informatiebeveiliging Nederlandse gemeenten’, 2013 (met updates in 2015 en 2016)
- Inspectie Ministerie van Sociale Zaken en Werkgelegenheid, ‘Onderzoek beveiliging Suwinet’, 2015.
- Madison Gurkha, ‘Technisch beveiligingsonderzoek Formulierenbibliotheek gemeente Breda’, aug. 2015
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, ‘Rijksjaarverslag 2015’, 2016
- Ministerie van Wonen en Rijksdienst, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het Ministerie van Veiligheid en Justitie, ‘Toetsmodel Privacy Impact Assessment (PIA), 2013 (met updates in 2014 en 2015)
- Ministerie van Veiligheid en Justitie, ‘Wet bescherming Persoonsgegevens’, versie 1-1-2016
- Nationale Coördinator Terrorismebestrijding en Veiligheid (NCTV), ‘Cybersecurity 2015 Awareness, gedrag & digitaal verantwoord ondernemen’, sept. 2015
- Nationaal Cyber Security Centrum (NCSC), ‘Grootschalige verspreiding malware via email’, juni 2016
- NOS.nl, ‘Privacywaakhond: datalekken worden niet gemeld’, 13 mei 2016
- Randstedelijke Rekenkamer, ‘Informatieveiligheid in de Provincies Flevoland, Noord-Holland, Utrecht en Zuid-Holland’, juli 2016
- Rekenkamer Amsterdam, ‘Privacy van burgers met een hulpvraag’, maart 2016;
- Rekenkamer Den Haag, ‘Bestuurlijk rapport digitale veiligheid’, 2014

- Rekenkamer Lelystad, ‘Lelystad op weg naar de BIG. Quickscan informatiebeveiliging gemeente Lelystad’, maart 2016
- Rekenkamercommissie Eindhoven, ‘Een open deur, informatiebeveiliging en privacy in het sociaal domein’, april 2016;
- Sociaal en Cultureel Planbureau, ‘Overall Rapportage Sociaal domein’, juni 2016
- VNG Visitatiecommissie Informatieveiligheid, ‘180 dagen onderweg, een verslag van gesprekken in 40 gemeenten’, juni 2016