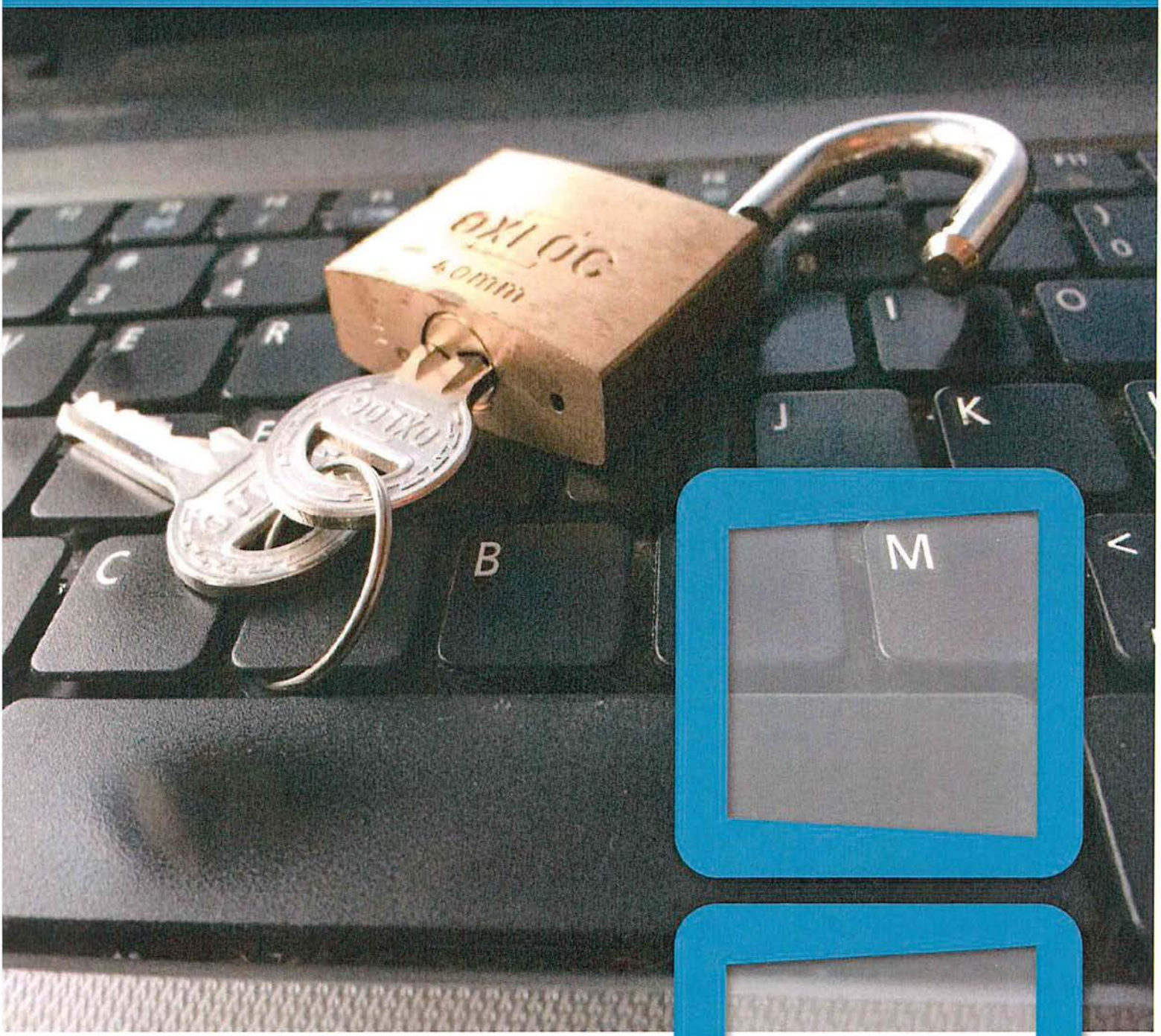
in onveilige handen

onderzoek informatiebeveiliging van gevoelige informatie



Rekenkamer
ROTTERDAM

Rekenkamer
ROTTERDAM

voorwoord

Het overheidshandelen is de afgelopen jaren in rap tempo aan het veranderen door de steeds groter wordende afhankelijkheid van de alsmaar sneller ontwikkelende ICT. Waar voorheen gegevens met betrekking tot zowel interne bedrijfsvoering als primaire processen nog grotendeels in fysieke vorm werden verwerkt, is dat tegenwoordig vrijwel nergens meer het geval. Gegevens zijn digitaal van vorm en daarmee via internet en intranet in principe altijd benaderbaar en veranderbaar. Dat maakt de bescherming daarvan een meer dan essentieel onderdeel van het overheidsbeleid, zeker waar het de bijzondere persoonsgegevens betreft van burgers, die al dan niet verplicht zijn om deze gegevens aan diezelfde overheid aan te leveren.

In Rotterdam voldoet de bescherming van deze kwetsbare gegevens grotendeels niet aan de eisen die daar aan mogen worden gesteld. Deze harde conclusie is voor de rekenkamer op zich al voldoende reden geweest om een afweging te maken met betrekking tot de vraag of het rapport al dan niet vertrouwelijk naar de gemeenteraad moet worden verzonden. Leidend daarbij is de wet, in dit geval de bepalingen van de Gemeentewet (artikel 185, lid 1 en 5), waarin wordt gesteld dat rekenkamerrapporten openbaar zijn. Los hiervan weegt naar het oordeel van de rekenkamer het belang van de Rotterdamse burger om te weten op welke wijze de gemeente omgaat met zijn of haar bijzondere persoonsgegevens en het belang van de gemeenteraad om in de volle openbaarheid hierover een debat te kunnen voeren, zwaarder dan mogelijke risico's voor de gemeente. In de afweging speelt tevens een belangrijke rol mee dat de gemeente al lange tijd op de hoogte was van de aangetoonde kwetsbaarheden en alle tijd heeft gehad om die te dichten. Dat dit niet heeft plaatsgevonden neemt de rekenkamer de gemeente erg kwalijk. Dat is geen fijne boodschap, maar de rekenkamer is nadrukkelijk van mening dat er op het punt van informatiebeveiliging nu echt grote stappen moeten worden genomen.

Voor haar onderzoek heeft de rekenkamer veel informatie verzameld. De rekenkamer is de contactpersonen en geïnterviewden zeer erkentelijk voor hun medewerking. Het onderzoek werd verricht door Rolf Willemse (projectleider), Nicole Kuijpers, Rosa Ridderhof en Job Stierman (externe inhuur).

Paul Hofstra
directeur Rekenkamer Rotterdam

Rekenkamer ROTTERDAM

Rekenkamer ROTTERDAM

bestuurlijke nota

Rekenkamer ROTTERDAM

1 inleiding

1-1 aanleiding

Het onderwerp ‘kwaliteit van de informatiebeveiliging’ was opgenomen in het onderzoeksprogramma van de rekenkamer voor 2016. Aanleiding was het gegeven dat als gevolg van de decentralisaties in het sociaal domein de gemeente Rotterdam steeds meer (bijzondere) persoonsgegevens[1] in beheer heeft. Ook wordt steeds meer informatie digitaal opgeslagen en overgedragen en worden systemen en data steeds vaker aan elkaar gekoppeld. Het belang om de informatiebeveiliging op orde te hebben en weerbaar te zijn tegen dreigingen als cybercrime, is als gevolg van deze ontwikkelingen aanzienlijk toegenomen.

In februari 2016 werd de gemeente Rotterdam geconfronteerd met een datalek waarbij (bijzondere) persoonsgegevens als namen, adressen en burgerservicenummers (BSN) uit belastingbestanden van de gemeente (periode 1996-2004) via het internet openbaar benaderbaar zijn geweest. Naar aanleiding hiervan heeft de gemeenteraad op 17 maart 2016 een motie aangenomen waarin de rekenkamer wordt verzocht direct te starten met het beoogde onderzoek naar de informatiebeveiliging van de gemeente Rotterdam en daarin het datalek mee te nemen. De rekenkamer heeft per brief van 23 maart 2016 aan de raad aangegeven gehoor te geven aan dit verzoek.

1-2 doel- en vraagstelling

De rekenkamer beoogt met dit onderzoek na te gaan of de gemeente adequaat opvolging heeft gegeven aan het datalek in februari 2016 en in bredere zin na te gaan of gevoelige informatie zoals (bijzondere) persoonsgegevens bij de gemeente Rotterdam in veilige handen is.

De centrale onderzoeksvraag luidt als volgt:
Heeft de gemeente Rotterdam adequaat opvolging gegeven aan het datalek in februari 2016 en is gevoelige informatie, zoals (bijzondere) persoonsgegevens, bij de gemeente Rotterdam in veilige handen?

1-3 leeswijzer

Deze bestuurlijke nota bevat de conclusies en aanbevelingen die volgen uit het onderzoek. In de nota van bevindingen staan de feitelijke bevindingen uit het onderzoek die als basis dienen voor de conclusies in de bestuurlijke nota. Samen vormen de bestuurlijke nota en de nota van bevindingen het rekenkamerrapport.

1 Een persoonsgegeven is iedere vorm van informatie die direct over iemand gaat of naar deze persoon te herleiden is. Bij bijzondere persoonsgegevens gaat het om BSN-nummers en informatie over iemands godsdienst of levensovertuiging, ras, politieke voorkeur, gezondheid, seksuele leven, lidmaatschap van een vakbond of strafrechtelijk verleden. Bijzondere persoonsgegevens mogen niet verwerkt worden, tenzij daarvoor een wettelijke uitzondering geldt. Bron: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens

Rekenkamer
ROTTERDAM

2 conclusies en aanbevelingen

2-1 hoofdconclusies

1 Over het algemeen is gevoelige informatie, zoals (bijzondere) persoonsgegevens, bij de gemeente Rotterdam onvoldoende in veilige handen. Er is namelijk sprake van een combinatie van:
   a een tekortschietende beveiliging van digitale informatiesystemen voor aanvallen van binnenuit,
   b falende fysieke beveiliging van meerdere kantoorlocaties en
   c een tekort aan benodigde 'social & security awareness' bij medewerkers.

2 De gemeentelijke informatiesystemen zijn in technische zin beter beveiligd tegen cyberaanvallen van buiten uit, onverlet kleinere kwetsbaarheden.

3 Door de tekortschietende informatiebeveiliging bestaan er reële risico's op identiteitsfraude, fysieke onveiligheid van politiek-bestuurlijke ambtsdragers, verstoring van de openbare orde, verstoring van de publieke dienstverlening en misbruik van publieke middelen.

4 In opzet is de verdeling van taken, bevoegdheden en verantwoordelijkheden over het algemeen adequaat voor een goede informatieveiligheid. Deze sluit aan bij algemeen aanvaarde professionele standaarden.

5 Desalniettemin heeft onvoldoende centrale sturing plaatsgevonden op informatieveiligheid.
   a De in het beleid voorgeschreven PDCA-cyclus wordt niet gevolgd. Er wordt onvoldoende gemonitord op tussentijdse resultaten en daarnaar gehandeld.
   b Er zijn tal van beveiligingsmaatregelen genomen, maar het ontbreekt aan passende maatregelen die volgen uit systematische en actuele risicoanalyses. Deze laatste worden namelijk niet integraal en volledig uitgevoerd, ondanks het juiste voornemen van het college om dit wel te doen.
   c De voorgeschreven dataclassificaties hebben niet juist en volledig plaatsgevonden. Hierdoor is onbekend welke gegevens kwetsbaar zijn voor misbruik.
   d Sinds geruime tijd zijn tekortkomingen in de informatiebeveiliging bekend, maar (voorgenomen) verbetermaatregelen hebben klaarblijkelijk niet kunnen voorkomen dat de informatiesystemen voor kwaadwillenden nog steeds gemakkelijk toegankelijk zijn.

6 De kwaliteit van de informatiebeveiliging van afzonderlijke systemen kent grote verschillen. Ook hier ontbreekt het aan centrale toetsing aan het gemeentelijk beleid.

7 In het geval van het datalek zijn te weinig mogelijke lessen getrokken.

2-2 toelichting hoofdconclusies

1 *Over het algemeen is gevoelige informatie, zoals (bijzondere) persoonsgegevens, bij de gemeente Rotterdam onvoldoende in veilige handen. Er is namelijk sprake van een combinatie van:*
   a een tekortschietende beveiliging van digitale informatiesystemen voor aanvallen van binnenuit,
   b falende fysieke beveiliging van meerdere kantoorlocaties en
   c een tekort aan benodigde 'social & security awareness' bij medewerkers.

- De rekenkamer heeft een gespecialiseerd bureau opdracht gegeven deze vormen van beveiliging te toetsen. De uitkomst is dat de informatieveiligheid binnen de gemeente Rotterdam ernstig tekortschiet.

a tekortschietende beveiliging van binnenuit

- In een zogeheten interne penetratietest wordt geprobeerd vanaf gemeentelijke werkplekken en vanuit de gemeentelijke digitale omgeving oneigenlijke toegang tot kwetsbare informatiesystemen te verkrijgen. Uit deze test kwamen zo'n 700 kritieke technische kwetsbaarheden (te herleiden tot 46 unieke kwetsbaarheden) bij specifieke systemen of applicaties naar voren.
- Daarnaast zijn er kwetsbaarheden in de IT-infrastructuur geconstateerd die het eenvoudig maken om oneigenlijke toegang tot het gemeentelijke netwerk te krijgen.
- Eenmaal in het gemeentelijke netwerk is veel informatie, waaronder persoonsgegevens, toegankelijk. Het bleek zelfs mogelijk beheerrechten te verkrijgen, waarmee nagenoeg alle systemen toegankelijk werden.
- Bovendien bleken veel systemen en applicaties verouderd.

b falende fysieke beveiliging

- Bij een toereikende fysieke beveiliging van kantoorlocaties, zouden de gemeentelijke informatiesystemen in principe alleen kwetsbaar zijn voor oneigenlijke toegang door kwaadwillende medewerkers.
- Het bleek uit inlooptesten echter eenvoudig om ongeautoriseerd toegang te krijgen tot vier gemeentelijke panden. Eenmaal binnen was er vrije toegang tot gevoelige locaties en (vertrouwelijke) informatie.
- De onderzoekers die ongeautoriseerd binnen waren gekomen, werden niet door medewerkers van de gemeente Rotterdam aangesproken.
- Het is dus voor kwaadwillenden van buiten de gemeente mogelijk om van binnenuit oneigenlijke toegang tot de gemeentelijke informatiesystemen te krijgen.

c tekort aan 'social & security awareness'

- Zoals aangegeven werden tijdens de inlooptesten de onrechtmatige bezoekers niet door medewerkers van de gemeente aangesproken.
- Tijdens de inlooptesten hebben de desbetreffende onderzoekers "lokmiddelen" achtergelaten. Een aantal is door medewerkers gebruikt, waardoor oneigenlijke toegang aan derden kon worden verschaft.
- Via een zogeheten 'spear phishing mail' bleek het mogelijk een medewerker te verleiden een verdachte link te openen. Dit leidde niet tot schade.

2 *De gemeentelijke informatiesystemen zijn in technische zin beter beveiligd tegen cyberaanvallen van buiten dan tegen aanvallen van binnenuit, onverlet kleinere kwetsbaarheden.*

- Het is niet gelukt om binnen de beschikbare tijd van vier dagen via het internet binnen te dringen in systemen van de gemeente Rotterdam.

- Wel blijkt het voor aanvallers mogelijk via internet informatie (bijvoorbeeld netwerkadressen en webmailsessies) te vergaren, die voor een hack gebruikt zouden kunnen worden.
- De technische staat van de informatiebeveiliging verhoedt niet dat 'spear phishing' mogelijk blijft.

3 *Door de tekortschietende informatiebeveiliging bestaan er reële risico's op identiteitsfraude, fysieke onveiligheid van politiek-bestuurlijke ambtsdragers, verstoring van de openbare orde, verstoring van de publieke dienstverlening en misbruik van publieke middelen.*

- Door toegang te hebben tot informatiesystemen met (bijzondere) persoonsgegevens kunnen kwaadwillenden zich naw-gegevens en BSN-nummers toe-eigenen. Dit zijn noodzakelijke (hoewel nog niet voldoende) gegevens om identiteitsfraude te plegen.
- Met inzicht in de agenda van een bestuurder wordt kennis opgedaan van zijn of haar gangen. Hier kan misbruik van worden gemaakt.
- Door toegang te hebben tot informatiesystemen kunnen bijvoorbeeld bruggen en verkeerslichten op afstand bediend worden en het verkeer worden lamgelegd. Dat kan vandalisme zijn, maar ook met het doel van ontwrichting worden gedaan.
- Met de genoemde toegang kunnen primaire processen van de gemeente worden platgelegd, waardoor bijvoorbeeld uitkeringen of parkeervergunningen niet (op tijd) worden verstrekt.
- Ook is het mogelijk persoonsgegevens te wijzigen, zodat een kwaadwillende onrechtmatig uitkeringen kan doen of ontvangen.

4 *In opzet is de verdeling van taken, bevoegdheden en verantwoordelijkheden over het algemeen adequaat voor een goede informatieveiligheid. Deze sluit aan bij algemeen aanvaarde professionele standaarden.*

- In het IB-beleid zijn de verantwoordelijkheden ten aanzien van informatiebeveiliging duidelijk beschreven. Deze verantwoordelijkheden zijn in lijn met het in de Baseline Informatiebeveiliging Gemeenten (BIG) vastgelegde uitgangspunt dat iedere lijnmanager verantwoordelijk is voor de integrale informatiebeveiliging van zijn of haar onderdeel. De BIG is een in professionele kring en bij overheden algemeen aanvaarde richtlijn voor informatiebeveiliging.
- Taken voor informatiebeveiliging worden vooral uitgevoerd door de CISO, security manager, information security officers, security coördinatoren en functioneel beheerders. Deze taken worden als onduidelijk ervaren. Zo is bijvoorbeeld niet duidelijk wat precies tot het takenpakket van de information security officers behoort. De clusters MO en W&I beschikken over een privacy officer. De andere clusters hebben een dergelijke functie niet.

5 *Desalniettemin heeft onvoldoende centrale sturing plaatsgevonden op informatieveiligheid.*
a De in het beleid voorgeschreven PDCA-cyclus wordt niet gevolgd. Er wordt onvoldoende gemonitord op tussentijdse resultaten en daarnaar gehandeld.

- In het door het college vastgestelde concern IB-beleid is opgenomen dat de zogeheten PDCA-cyclus zal worden gevolgd. In deze cyclus worden continu acties gepland (P), uitgevoerd (D), beoordeeld op resultaat (C) en eventueel ingegrepen (A).
- Het ontbreekt evenwel aan structurele rapportagelijnen richting de verantwoordelijke clusterdirecties.
- De concernbrede rapportage over informatiebeveiliging bevat vooral informatie op hoofdlijnen. Ook blijkt uit de rapportages niet welke voortgang er ten opzichte van de voorgaande periode is geboekt. De realisatie van de BIG blijkt niet uit de rapportages.

- De rekenkamer heeft geen systematische sturing van het college op de uitvoering van het concern IB-beleid aangetroffen.
- In de afgelopen jaren zijn verschillende audits en onderzoeken uitgevoerd op het gebied van informatiebeveiliging, maar onduidelijk is of naar aanleiding van de uitkomsten altijd verbeteracties zijn ingezet.

b *Er zijn tal van beveiligingsmaatregelen genomen, maar het ontbreekt aan passende maatregelen die volgen uit systematische en actuele risicoanalyses. Deze laatste worden namelijk niet integraal en volledig uitgevoerd, ondanks het juiste voornemen van het college om dit wel te doen.*

- De gemeente heeft zowel technische als organisatorische beveiligingsmaatregelen getroffen. Technische maatregelen zijn bijvoorbeeld firewalls, virusscanners en toegangspasjes. Organisatorische maatregelen zijn naast de meer algemene beleidsdocumenten diverse uitwerkingen in procedures en richtlijnen (zoals een handreiking dataclassificatie en een procedure voor het aanvragen van externe dataverbindingen).
- De organisatorische maatregelen zijn onder meer in navolging van de voornoemde BIG getroffen. Genomen maatregelen vloeien niet direct voort uit een risicoanalyse.
- Het college heeft in het 'Concern Informatiebeveiligingsbeleid' (november 2013) vastgelegd dat de gemeente op basis van risicoanalyses tot passende beveiligingsmaatregelen wil komen. Voor een goede en doelmatige informatieveiligheid is dit een juiste beleidslijn.
- De gemeente heeft echter onvoldoende risicoanalyses ten aanzien van informatiebeveiliging gemaakt. Niet van alle informatiesystemen is een risicoanalyse gemaakt. De risicoanalyses die wel zijn uitgevoerd zijn inhoudelijk niet compleet en consistent. Daarnaast ontbreekt vaak een koppeling tussen risico's en te treffen beveiligingsmaatregelen.
- Hierdoor is de gemeente niet in staat om op basis van geïdentificeerde risico's en de inschatting van kans en impact daarvan, te bepalen welke beveiligingsmaatregelen genomen moeten worden.
- Ook betekent het dat van de beveiligingsmaatregelen die wel zijn genomen, het niet volledig is vast te stellen of deze gelet op de beveiligingsrisico's wel passend en effectief zullen zijn.

c *De voorgeschreven dataclassificaties hebben niet juist en volledig plaatsgevonden. Hierdoor is onbekend welke gegevens kwetsbaar zijn voor misbruik.*

- In 'Concern Informatiebeveiligingsbeleid' (november 2013) heeft het college ook vastgelegd dat er dataclassificaties moeten worden opgesteld.
- Echter, noch op concernniveau, noch binnen de clusters worden dataclassificaties structureel en kwalitatief goed uitgevoerd. Evenmin heeft de gemeente een overzicht van alle processen waarin (gevoelige) persoonsgegevens worden verwerkt.
- Door het ontbreken hiervan is de gemeente niet in staat vast te stellen welke gegevens kwetsbaar zijn en welke passende beveiligingsmaatregelen getroffen moeten worden.

d *Sinds geruime tijd zijn tekortkomingen in de informatiebeveiliging bekend, maar (voorgenomen) verbetermaatregelen hebben klaarblijkelijk niet kunnen voorkomen dat de informatiesystemen voor kwaadwillenden nog steeds gemakkelijk toegankelijk zijn.*

- De kwetsbaarheden die bleken uit de interne penetratietest (zie hoofdconclusie 1a), zijn ook opgemerkt tijdens een vergelijkbare penetratietest die in 2015 in opdracht van de gemeente is uitgevoerd.

- Ook de accountant van de gemeente Rotterdam heeft tijdens de jaarrekeningcontrole 2015 kritische opmerkingen gemaakt over de informatiebeveiliging. Zo is gewezen op het risico van ongeautoriseerde toegang tot systemen en onderliggende data, alsmede op een verhoogd risico op datalekken.
- Omdat de informatieveiligheid niet is vergroot, is de gemeente er sinds 2015 klaarblijkelijk niet in geslaagd effectieve verbeteringen door te voeren.

6 *De kwaliteit van de informatiebeveiliging van afzonderlijke systemen kent grote verschillen. Ook hier ontbreekt het aan centrale toetsing aan het gemeentelijk beleid.*

- De rekenkamer heeft de beveiliging van vijf applicaties op acht aspecten beoordeeld. Aangezien in deze 'kroonjuwelen' veel (privacy)gevoelige informatie wordt opgeslagen en verwerkt, dient de beveiliging van deze systemen zonder meer op orde te zijn.
  De beveiliging van geen enkele onderzochte applicatie is op alle acht aspecten volledig op orde. Wel zijn er grote verschillen tussen de applicaties.

- Er zijn ook grote verschillen waar het de beoordeelde aspecten betreft. Aan de eis dat er een service level agreement (SLA) met rapportageafspraken over informatiebeveiliging, voldoet geen enkele onderzochte applicatie. De consequentie is dat de verantwoordelijke afdeling geen inzicht krijgt in de staat van de informatieveiligheid.
- Ook ontbreekt bij alle onderzochte applicatie een onafhankelijke assurance over de kwaliteit van de dienstverlening rond het technisch beheer. Ook dit betekent dat de verantwoordelijke afdeling geen inzicht krijgt in de staat van de informatieveiligheid.
- Bij geen van de applicaties is een recente risicoanalyse van voldoende kwaliteit aangetroffen. Wel is er bij twee applicaties sprake van een goed risicobewustzijn bij betrokken management en medewerkers. Deze risico's zijn inzichtelijk gemaakt via self-assessments of audits.
- Niet bij alle applicaties wordt bij testwerkzaamheden gebruikgemaakt van geanonimiseerde data. Dit betekent dat privacygevoelige informatie wordt blootgesteld aan onbevoegden (systeemontwikkelaars en testers).
- Bij twee van de vijf onderzochte applicaties wordt het eigenaarschap van de applicatie en de data betekenisvol ingevuld door het management. Bij de overige applicaties ontbreekt het aan actief toezicht op de beveiliging en het beheer van gegevens.
- Alle applicaties hebben verfijnde functionaliteit om rechten toe te kennen op basis van rollen (zoals beheerder of uitvoerder) die zijn afgeleid van de functies van medewerkers. De mate waarin (periodiek) toezicht wordt gehouden op de juiste toekenning van autorisaties verschilt.
- Back-up procedures zijn bij alle onderzochte applicaties in orde. Wel bestaat bij twee applicaties die door externe partijen worden gehost een groter risico op ongecontroleerde raadpleging door derden.

- Een verklaring voor de verschillen tussen de applicaties is dat er (gelet op de eigen verantwoordelijkheid van het lijnmanagement) een zekere vrijheid bestaat in de uitvoering van het informatiebeveiligingsbeleid. Er is echter geen dwingend toezicht op de naleving van de gemeentelijke voorschriften en op de kwaliteit van informatiebeveiliging op decentraal niveau.

7 In het geval van het datalek zijn te weinig mogelijke lessen getrokken.

- Door het datalek in februari 2016 waren persoonsgegevens van 32.000 personen tijdelijk via internet te bereiken. Zowel de medewerker die het lek veroorzaakte als de gemeente hebben na het bekend worden van het datalek meteen acties ondernomen om het lek te dichten en relevante partijen te informeren.
- Het college heeft het datalek afdoende technisch laten onderzoeken. Er is gekeken naar de aard, omvang, potentiële en daadwerkelijke consequenties van het datalek. Organisatorische aspecten zijn niet onderzocht.
- Maatregelen om soortgelijke datalekken in de toekomst te voorkomen, zijn vooral gericht op het creëren van algemene bewustwording bij medewerkers (bijvoorbeeld door middel van een brief en aandacht in het functioneringsgesprek).
- Naar aanleiding van het onderzoek naar het datalek zijn geen technische maatregelen genomen.
- In de communicatie aan de raad over de afhandeling van het datalek legt het college daarentegen nadruk op reeds bestaande documenten en maatregelen en het benoemt geen nieuwe maatregelen.

2-3 aanbevelingen aan B en W

Uit het rekenkameronderzoek komt naar voren dat het voor kwaadwillenden gemakkelijk is om oneigenlijke toegang tot de informatiesystemen van de gemeente Rotterdam te verkrijgen. Dit is opvallend, omdat de gemeente op papier wel een beleid en organisatie voor de informatiebeveiliging heeft opgesteld dat over het algemeen voldoet aan geldende professioneel standaarden. Dat de gemeente zich niettemin grote zorgen moet maken om de informatieveiligheid, is omdat de uitvoering daarvan en in het bijzonder de centrale sturing daarop, tekortschiet. De navolgende aanbevelingen aan het college van B en W vloeien uit deze analyse voort.

1 Zorg voor een krachtige centrale sturing op informatiebeveiliging binnen de gemeente.
   - Draag zorg voor voldoende ‘awareness’ en expertise bij het lijnmanagement en de medewerkers die verantwoordelijk zijn voor de informatiehuishouding;
   - Beoordeel of de CISO in financieel en functioneel opzicht effectieve doorzettingsmacht heeft om op decentraal niveau goede informatiebeveiliging en compliance aan centrale voorschriften af te dwingen.
   - Laat regelmatig onafhankelijke audits uitvoeren op de beveiliging van informatiehuishouding en handel naar de bevindingen.
2 Pas de in het beleid voorgeschreven dataclassificaties op alle informatiesystemen volledig en juist toe.
3 Leg vast welke informatiesystemen voor misbruik kwetsbare gegevens bevatten. Maak voor deze systemen periodiek een risicoanalyse, waarbij:
   - een inschatting wordt gemaakt van de kans dat een risico zich voordoet;
   - een inschatting wordt gemaakt van de impact als een risico zich voordoet; hierbij gaat het niet alleen om gevolgen voor de gemeentelijke organisatie, maar met name ook voor de burgers;
   - bij de risico’s behorende beveiligingsmaatregelen en inschatting van de benodigde financiële middelen worden geformuleerd.
4 Stel voor de uit te voeren beveiligingsmaatregelen de benodigde middelen ter beschikking, voer de maatregelen daadwerkelijk onverkort uit en laat per kwartaal rapporteren over de voortgang en de resultaten daarvan. Grijp in als de resultaten afwijken van de verwachting.

Rekenkamer ROTTERDAM

Met de opvolging van de bovenstaande vooral organisatorische aanbevelingen wordt uitvoering gegeven aan een op termijn adequate en duurzame informatiebeveiliging, Het rekenkameronderzoek heeft daarnaast diverse meer concrete kwetsbaarheden aangetroffen die op korte termijn verholpen dienen te worden. De volgende aanbevelingen aan het college vloeien hieruit voort.

5 Pak systematisch en gericht de diverse kwetsbaarheden aan die uit de interne penetratietest naar voren zijn gekomen en monitor dit door middel van een kwartaalrapportage. Beoordeel uiterlijk na een jaar aan de hand van een nieuwe interne penetratietest uit of de kwetsbaarheden naar behoren zijn aangepakt.
6 Verbeter de toegangsbeveiliging op kantoorlocaties, daarbij gebruikmakend van de uitkomsten van de inlooptesten van de rekenkamer. Beoordeel uiterlijk na een jaar met nieuwe inlooptesten of de zwakke plekken zijn verholpen.

7 Versterk het bewustzijn van medewerkers ten aanzien van informatiebeveiliging. Beoordeel met testen in welke mate het awareness programma effectief is geweest.
8 Neem alle mogelijke organisatorische en technische maatregelen om (onbewust) slordig omgaan met vertrouwelijke informatie door medewerkers, en daarmee een soortgelijk datalek als in februari 2016, te voorkomen.

9 Neem maatregelen tegen de kwetsbaarheden die uit de externe penetratietest van de rekenkamer naar voren zijn gekomen.
10 Beoordeel uiterlijk na een jaar met een nieuwe externe penetratietest of er nog kwetsbaarheden in de beveiliging tegen cyberaanvallen zitten en neem eventuele passende maatregelen.

11 Verbeter de informatiebeveiliging van de onderzochte applicaties in lijn met de BIG en daarmee het gemeentelijk beleid. Realiseer daartoe in ieder geval het volgende:
- Zorg voor actieve betrokkenheid van het management als (gemandateerde) eigenaars van de gegevens.
- Richt volwassen servicemanagement in, inclusief verantwoording, zodat de algemene beheersing over de applicatie beoordeeld kan worden.
- Vul eigenaarschap van gegevens in, zoals bijvoorbeeld het beheer over het aanmaken, wijzigen, raadplegen, verwijderen, inclusief de vertrouwelijkheidsclassificatie.
- Voer periodiek een risicoanalyse uit.
  Een hulpmiddel hierbij kan een uitgebreide applicatie audit zijn, zoals bijvoorbeeld is uitgevoerd bij de in de nota van bevindingen genoemde applicatie D.

Rekenkamer ROTTERDAM

3 reactie college en nawoord rekenkamer

Zoals artikel 11 van de Verordening Rekenkamer Rotterdam voorschrijft, heeft de rekenkamer het college in de gelegenheid gesteld om een reactie te geven op de onderzoeksresultaten. Het college heeft in een brief van 22 maart 2017 zijn reactie gegeven. Het geeft daarin aan het overgrote deel van de conclusies te herkennen en alle aanbevelingen over te nemen. Uit de gegeven toelichtingen blijkt dat het college ook daadwerkelijk goeddeels in lijn van de aanbevelingen gaat handelen. De rekenkamer is hierover verheugd, vanwege de ernst van de gesignaleerde tekortkomingen. Waar de 1,5 jaar geleden door de gemeente zelf geconstateerde gebreken niet verholpen zijn, moet er nu vanuit kunnen worden gegaan dat de tekortkomingen wél voortvarend worden opgepakt. In zijn reactie heeft het college aangegeven dat er in het kader van de opvolging van de aanbevelingen een investeringsprogramma zal worden opgesteld. De rekenkamer zal de uitvoering van dit programma de komende jaren nauwlettend volgen.

openbaarheid rapport

Het investeringsprogramma zal het college niet openbaar maken. Ook de reactie op het rekenkamerrapport heeft het college als geheim bestempeld. De reden is dat een groot deel van het rekenkamerrapport (in het bijzonder hoofdstuk 6 van de nota van bevindingen en de daarvan afgeleide hoofdconclusies) vertrouwelijk zou moeten worden gehouden. Volgens het college zou de rekenkamer met het openbaar maken onverantwoorde veiligheidsrisico's nemen.

Over de noodzaak van het openbaar maken van het rapport verschilt de rekenkamer fundamenteel van mening met het college. Hiervoor zijn de volgende argumenten. Ten eerste is de rekenkamer van oordeel dat eventuele gevolgen van tekortschietende informatiebeveiliging de rekenkamer niet kan en mag worden aangerekend. Het college is immers verantwoordelijk voor een goede veiligheid van bij de gemeente berustende (privacy) gevoelige informatie. De rekenkamer heeft de verantwoordelijkheid om de kwaliteit van de bedrijfsvoering van de gemeente voor eenieder transparant te maken, in dit geval de informatiebeveiliging. Deze verantwoordelijkheid vloeit rechtstreeks voort uit de bepaling in de Gemeentewet dat rapporten van de rekenkamer openbaar *zijn* (artikel 185, lid 5).

Diezelfde Gemeentewet stelt wel enige restricties aan wat een rekenkamer in zijn rapport kan opnemen, namelijk geen naar haar aard vertrouwelijke informatie (artikel 185, lid 1). In het rapport van de rekenkamer zijn echter geen persoonsgegevens en commerciële informatie opgenomen en ook raakt het niet de staatsveiligheid.

Los hiervan kan nog een afweging worden gemaakt tussen de belangen van openbaarmaking en de belangen van het college. De rekenkamer is van oordeel dat de belangen van het college niet onevenredig worden geschaad. De exacte wijze waarop de onderzoekers zich toegang hebben verschaft tot de informatiesystemen, wordt namelijk niet in het te publiceren rapport beschreven. Dit staat wel in een technische

onderliggende analyse. Deze blijft nadrukkelijk vertrouwelijk en zal onder geen beding door de rekenkamer openbaar worden gemaakt en met derden worden gedeeld. Het is enkel met de verantwoordelijke ambtenaren gedeeld.

In het rapport worden wel tekortkomingen benoemd en wordt uitgelegd wat dat precies betekent voor de gemeentelijke organisatie, de lokale samenleving en de Rotterdammer. Deze duiding van mogelijke gevolgen is cruciaal, omdat het inzicht geeft in de ernst van de bevindingen. Met deze keuzen kan worden voldaan aan het voor de rekenkamer geldende uitgangspunt dat een rekenkamerrapport de raad in staat moet stellen om binnen de raad en met het college een openbaar politiek-bestuurlijk debat te voeren over de bevindingen, conclusies en aanbevelingen.

Bij het oordeel dat dit ook een *openbaar* rapport vereist, heeft de rekenkamer zich overigens niet alleen laten leiden door de Gemeentewet. Het onderzoek heeft zich grotendeels gericht op systemen waarin gegevens over Rotterdammers zijn opgeslagen. Burgers moeten erop kunnen vertrouwen dat (persoons)gegevens die zij – vaak verplicht of gedwongen – hebben toevertrouwd aan de gemeente, daar ook in veilige handen zijn. Bovendien behoren zij te mogen weten of dat ook daadwerkelijk het geval is, in dit geval via het rekenkamerrapport. Diezelfde burgers moeten er ook op kunnen vertrouwen dat áls er problemen met de veiligheid van hun gegevens zijn, de gemeente deze voortvarend oppakt. Dit is nu juist niet het geval. Het onderzoek laat ernstige tekortkomingen zien, die reeds geruime tijd bekend waren uit een door de gemeente zelf in 2015 geïnitieerd onderzoek. Deze bleken dus daarna niet te zijn opgelost.

dreiging kort geding

Alles afwegende heeft de rekenkamer de raad en het college in een brief van 23 maart 2017 laten weten het rapport te zullen openbaren. Naar aanleiding van dit besluit heeft het college zijn bestuurlijke reactie naar de raad gestuurd. Omdat deze ook nu als geheim is bestempeld, kan de rekenkamer in dit rapport hier niet verder inhoudelijk op ingaan.

Op 31 maart 2017 heeft het college bij de rekenkamer een bezwaarschrift tegen openbaring ingediend. Mocht de rekenkamer volharden in haar besluit tot openbaar maken, dan zou de rechter in kort geding worden gevraagd dit te voorkomen. De rekenkamer heeft hierop in een brief van 3 april 2017 aangegeven publicatie uit te stellen en zich te beraden op het bezwaarschrift en de door het college bestreden passages.

De rekenkamer heeft in de daarop volgende dagen met extern technisch en juridisch advies de door het college bestreden (en ten behoeve van de rekenkamer gemarkeerde) passages kritisch tegen het licht gehouden. Daarbij gold als cruciaal uitgangspunt dat de bestuurlijke conclusies en oordelen transparant en navolgbaar moeten zijn naar onderliggende bevindingen.[2] In dat licht heeft de rekenkamer diverse additionele voorbeelden die ter onderbouwing van de conclusies dienden, alsnog geschrapt. Een minimum van onderbouwende bevindingen dient evenwel

2 Dit is een algemeen aanvaard principe voor audit gerelateerde onderzoeken. Op de noodzaak hiervan is gewezen in een extern evaluatie van de Rekenkamer Rotterdam van september 2014 ('Evenwicht bij tegenwicht') en is ook vastgelegd het Kwaliteitshandvest waarin de Rekenkamer Rotterdam zich heeft gecommitteerd (voor beide documenten: www.rekenkamer.rotterdam.nl).

aanwezig te zijn, dus grote delen van de nota van bevindingen zijn ongemoeid gelaten. Dit heeft naar het oordeel van de rekenkamer wel consequenties voor de leesbaarheid en toegankelijkheid van het rapport. De rekenkamer heeft hieraan meer concessies gedaan dan haar lief is.

Op 6 april 2017 publiceerde de Volkskrant een groot artikel over het rapport, daarbij gebruik makend van vertrouwelijke conceptrapportages die klaarblijkelijk gelekt waren. Hierop besloot de rekenkamer het aangepaste rapport zo snel mogelijk te publiceren.

moment van openbaarmaking
In de discussie met het college over openbaar making is ook het moment van openbaren aan de orde geweest. Het college gaf in zijn bezwaarschrift aan geen bezwaren tegen publicatie na zes maanden te hebben. Dat zou voldoende tijd bieden om de ernstigste kwetsbaarheden op te lossen. In een brief aan de raad van 23 maart 2017 stelt het college bovendien dat de rekenkamer 'bij de start van het onderzoek getekend heeft voor het niet openbaar delen van informatie die de integriteit van onze informatiehuishouding kan schaden.' De rekenkamer heeft in het kader van het onderzoek twee overeenkomsten met de gemeente getekend, namelijk een vrijwaringsovereenkomst voor de inlooptesten en een vrijwaringsovereenkomst voor de penetratietesten. Hierin zijn géén afspraken gemaakt over het al dan niet openbaar maken van bevindingen. Dit zou de rekenkamer gelet op haar wettelijke taak en onafhankelijkheid ook niet kunnen doen.

Daarnaast wijst het college in dezelfde brief op het principe van "responsible disclosure" volgens welke informatie over beveiligingsproblemen niet met anderen wordt gedeeld totdat het is opgelost. De rekenkamer wijst er echter op dat juist in dit kader de gemeente reeds op 26 oktober 2016 over de meest kritieke kwetsbaarheden is geïnformeerd. Over de overige kwetsbaarheden is zij in januari 2017 geïnformeerd. Los van het feit dat veel kwetsbaarheden toen al zeker 1,5 jaar bekend waren, heeft de rekenkamer de gemeente dus ruim vijf maanden de tijd gehad om de (meest kritieke) beveiligingslekken al voor de publicatie van het rapport te dichten. Deze termijn moet zonder meer voldoende zijn. Volgens de 'Leidraad om te komen tot een praktijk van responsible disclosure' van het Nationaal Cyber Security Centrum (2013) is 'een redelijke standaardtermijn die kan worden gehanteerd voor kwetsbaarheden in software 60 dagen.' Deze termijn is ruimschoots overschreden. Dat het college aangeeft vanaf april nog eens zes maanden nodig te hebben, baart de rekenkamer grote zorgen.

Rekenkamer
ROTTERDAM

nota van bevindingen

Rekenkamer ROTTERDAM

1 inleiding

1-1 aanleiding

Het onderwerp ‘kwaliteit van de informatiebeveiliging’ was opgenomen in het onderzoeksprogramma van de rekenkamer voor 2016. In februari 2016 werd de gemeente Rotterdam geconfronteerd met een datalek waarbij (bijzondere) persoonsgegevens als namen, adressen en burgerservicenummers (BSN) uit belastingbestanden van de gemeente (periode 1996-2004) via het internet openbaar benaderbaar zijn geweest. Naar aanleiding hiervan heeft de gemeenteraad op 17 maart 2016 een motie aangenomen waarin de rekenkamer wordt verzocht direct te starten met het beoogde onderzoek naar de informatiebeveiliging van de gemeente Rotterdam en daarin het datalek mee te nemen. De rekenkamer heeft per brief van 23 maart 2016 aan de raad aangegeven gehoor te geven aan dit verzoek.

1-2 belang van informatiebeveiliging

Als gevolg van de decentralisaties in het sociaal domein hebben gemeenten steeds meer (bijzondere) persoonsgegevens[3] in beheer. Ook wordt steeds meer informatie digitaal opgeslagen en overgedragen en worden systemen en data steeds vaker aan elkaar gekoppeld. Het belang van gemeenten om de informatiebeveiliging op orde te hebben en weerbaar te zijn tegen dreigingen als cybercrime, is als gevolg van deze ontwikkelingen aanzienlijk toegenomen.

Daarnaast hebben alle bedrijven en overheden die persoonsgegevens gebruiken een wettelijke plicht om deze goed te beveiligen. Artikel 13 van de Wet bescherming persoonsgegevens (Wbp) schrijft voor dat organisaties hiertoe passende technische en organisatorische maatregelen moeten nemen.

artikel 13 Wet bescherming persoonsgegevens (Wbp)

De tekst van artikel 13 Wbp luidt als volgt: “De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.”

3 Een persoonsgegeven is iedere vorm van informatie die direct over iemand gaat of naar deze persoon te herleiden is. Bij bijzondere persoonsgegevens gaat het om BSN-nummers en informatie over iemands godsdienst of levensovertuiging, ras, politieke voorkeur, gezondheid, seksuele leven, lidmaatschap van een vakbond of strafrechtelijk verleden. Bijzondere persoonsgegevens mogen niet verwerkt worden, tenzij daarvoor een wettelijke uitzondering geldt. Bron: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens.

In de 'Richtsnoeren beveiliging persoonsgegevens' heeft de Autoriteit Persoonsgegevens nader toegelicht wat onder een passend niveau van beveiliging wordt verstaan. Uitgangspunten die de Autoriteit Persoonsgegevens hanteert zijn onder andere dat:[4]

- beveiliging van persoonsgegevens gedurende de hele levensduur van een informatiesysteem punt van aandacht moet zijn, van het eerste ontwerp tot het wissen van het laatste back-up bestand;
- beveiliging ingebed moet zijn in een plan-do-check-act cyclus waarin risico's worden beoordeeld, gebruik wordt gemaakt van algemeen geaccepteerde beveiligingsstandaarden en regelmatig controle en evaluatie plaatsvindt.

Sinds 1 januari 2016 is de meldplicht datalekken van kracht. Als sprake is van een datalek en uit toetsing door de Autoriteit Persoonsgegevens blijkt dat niet is voldaan aan de wettelijke regels, dan kan de autoriteit een boete opleggen die kan oplopen tot maximaal € 810.000.

1-3 doel- en vraagstelling

1-3-1 doelstelling

De rekenkamer beoogt met dit onderzoek na te gaan of de gemeente adequaat opvolging heeft gegeven aan het datalek in februari 2016 en in bredere zin na te gaan of gevoelige informatie zoals (bijzondere) persoonsgegevens bij de gemeente Rotterdam in veilige handen is.

1-3-2 onderzoeksvragen

De centrale onderzoeksvraag luidt als volgt:
Heeft de gemeente Rotterdam adequaat opvolging gegeven aan het datalek in februari 2016 en is gevoelige informatie, zoals (bijzondere) persoonsgegevens, bij de gemeente Rotterdam in veilige handen?

De centrale onderzoeksvraag is uitgewerkt in de volgende deelvragen: [5]

1 Beschikt de gemeente Rotterdam over een adequaat informatiebeveiligingsbeleid en is sprake van een goed georganiseerde informatiebeveiligingsfunctie?
2 Welke maatregelen heeft de gemeente Rotterdam genomen na het datalek in februari 2016 en zijn deze voldoende om dergelijke incidenten in de toekomst redelijkerwijs te voorkomen?
3 Heeft de gemeente Rotterdam in brede zin een goed beeld van de belangrijkste risico's op het gebied van informatiebeveiliging en in het bijzonder gevoelige informatie zoals (bijzondere) persoonsgegevens?
4 Heeft de gemeente Rotterdam voldoende maatregelen getroffen om gevoelige informatie te beschermen tegen de belangrijkste veiligheidsrisico's?

4 Autoriteit Persoonsgegevens, 'Richtsnoeren beveiliging persoonsgegevens', februari 2013.

5 De eerste vraag was niet opgenomen in de oorspronkelijke opzet, maar bleek wel noodzakelijk te beantwoorden. Aan de laatste vraag was oorspronkelijk toegevoegd "en welke gevolgen kan dit hebben voor de burger?". Dit bleek tijdens het onderzoek vooral een theoretische vraag te zijn. Wel zullen in deze nota eventuele gevolgen globaal worden geschetst. Voor het overige zijn enkele redactionele wijzigingen in de onderzoeksvragen doorgevoerd.

5 Is het mogelijk oneigenlijke toegang te krijgen tot gevoelige informatie die de gemeente Rotterdam in beheer heeft?

1-4 aanpak

In het kader van deelvraag 2 heeft de rekenkamer gebruik gemaakt van de resultaten van de onderzoeken die in opdracht van de gemeente zijn uitgevoerd naar het datalek. In het kader van deelvraag 4 heeft de rekenkamer zowel maatregelen betrokken die op niveau van het concern zijn getroffen, als maatregelen binnen de individuele clusters. Daarbij zijn tevens zowel technische als organisatorische beveiligingsmaatregelen in ogenschouw genomen. In het kader van deelvraag 5 heeft de rekenkamer getest of het mogelijk is oneigenlijke toegang te krijgen tot (bijzondere) persoonsgegevens in systemen van de gemeente Rotterdam en tot andere gevoelige informatie die de gemeente in beheer heeft (onder meer via een zogeheten penetratietest). In de afzonderlijke hoofdstukken wordt voor zover nodig nader ingegaan op de gevolgde methode. In bijlage 1 wordt eveneens ingegaan op de gevolgde onderzoeksmethoden.

1-5 leeswijzer

In hoofdstuk 2 komen het informatiebeveiligingsbeleid en de informatiebeveiligingsfunctie van de gemeente aan de orde (onderzoeksvraag 1). Vervolgens behandelt de rekenkamer in hoofdstuk drie de opvolging die is gegeven aan het datalek (onderzoeksvraag 2). In hoofdstuk vier beoordeelt de rekenkamer of de gemeente voldoende zicht heeft op de belangrijkste risico's op het gebied van informatiebeveiliging (onderzoeksvraag 3). In hoofdstuk vijf komen de maatregelen aan de orde die de gemeente op het gebied van informatiebeveiliging heeft getroffen (onderzoeksvraag 4). Ten slotte worden in hoofdstuk 6 (onderzoeksvraag 5) de resultaten behandeld van de hack die de rekenkamer heeft laten uitvoeren. Hiermee wordt inzicht gegeven in de effectiviteit van de beveiligingsmaatregelen, die zijn getroffen om oneigenlijke toegang tot gemeentelijke systemen te voorkomen.

De nota van bevindingen bevat de analyses en feiten die horen bij de onderzoeksvragen. Bij deelvragen één (hoofdstuk 2), twee (hoofdstuk 3), drie (hoofdstuk 4) en vier (hoofdstuk 5) wordt getoetst in hoeverre wordt voldaan aan normen en criteria. De normen zijn vermeld in de inleiding van hoofdstuk twee, drie, vier en vijf. Deelvraag 5 (hoofdstuk 6) is beschrijvend van aard. Hierop zijn geen normen van toepassing.

In bijlage 1 is een onderzoeksverantwoording opgenomen. Bijlage 2 bevat een lijst met aangehaalde documentatie. Bijlage 3 bevat een lijst van veelgebruikt begrippen. Bijlage 4 bevat ten slotte een lijst met gebruikte afkortingen.

schuingedrukte teksten
In de nota van bevindingen beginnen paragrafen met een cursieve tekst. Deze cursieve tekst vormt de korte conclusie van de betreffende (sub)paragraaf aan de hand van de gehanteerde normen. Bij afwezigheid van normen vormt de cursieve tekst een samenvatting van de paragraaf.

gekleurde kaders
In de nota zijn geelgekleurde en groengekleurde tekstblokken te vinden. De geelgekleurde tekstblokken bevatten aanvullende informatie die voor de

oordeelsvorming niet essentieel is, maar een nadere toelichting geeft over bijvoorbeeld gebruikte begrippen en instrumenten. De groengekleurde tekstblokken bevatten nadere informatie of uitleg over feiten waarover in het rapport wordt geoordeeld.

2 beleid en organisatie

2-1 inleiding

Dit hoofdstuk gaat in op het informatiebeveiligingsbeleid (hierna IB-beleid) van de gemeente Rotterdam en de wijze waarop informatiebeveiliging binnen de gemeente is georganiseerd. De volgende onderzoeksvraag staat hierbij centraal:

Beschikt de gemeente Rotterdam over een adequaat informatiebeveiligingsbeleid en is sprake van een goed georganiseerde informatiebeveiligingsfunctie?

De normen die de rekenkamer in het kader van deze onderzoeksvraag heeft gehanteerd zijn weergegeven in tabel 2-1.

tabel 2-1: normen beleid en organisatie informatiebeveiliging

normen	criteria	paragraaf
de gemeente beschikt over een actueel overkoepelend informatiebeveiligingsbeleid dat op onderdelen is uitgewerkt in specifieke procedures en/of richtlijnen	• er is een overkoepelend informatiebeveiligingsbeleid dat bestuurlijk is vastgesteld	2-2-1
	• de inhoud van het informatiebeveiligingsbeleid sluit aan bij good practices zoals de Baseline Informatiebeveiliging Gemeenten (BIG)	2-2-2
	• het informatiebeveiligingsbeleid wordt minimaal vierjaarlijks geëvalueerd en waar nodig geactualiseerd	2-2-2
	• indien veranderingen in de gemeentelijke organisatie hiertoe aanleiding geven wordt het informatiebeveiligingsbeleid geactualiseerd	2-2-3
	• de gemeente beschikt over procedures en of richtlijnen waarin diverse onderdelen van het informatiebeveiligingsbeleid nader invulling hebben gekregen	
taken en verantwoordelijkheden rond informatiebeveiliging en de bescherming van (bijzondere) persoonsgegevens zijn duidelijk belegd binnen de gemeentelijke organisatie	• taken en verantwoordelijkheden voor informatiebeveiliging zijn zichtbaar belegd binnen de gemeentelijke organisatie	2-3-1
	• taken en verantwoordelijkheden m.b.t de bescherming van (bijzondere) persoonsgegevens zijn zichtbaar belegd binnen de organisatie	2-3-2

de gemeente geeft adequaat invulling aan de PDCA[6]-cyclus rond het informatiebeveiligingsbeleid	• in het informatiebeveiligingsbeleid is beschreven hoe invulling wordt gegeven aan de PDCA-cyclus rond informatiebeveiliging • de PDCA-cyclus krijgt in de praktijk uitvoering zoals beschreven in het beleid	2-4
de gemeente heeft in het kader van informatiebeveiliging een actueel overzicht van alle ICT-middelen van de gemeente en de mate van vertrouwelijkheid van de informatie die daarin wordt verwerkt	• er is een up-to-date overzicht van systemen, applicaties en dergelijke. waarin de gemeente informatie verwerkt • de gemeente classificeert de informatie die zij verwerkt naar mate van vertrouwelijkheid	2-5

In de volgende paragraaf worden het concerninformatiebeveiligingsbeleid en aanverwante procedures en richtlijnen beschreven. In paragraaf 2-3 komt de verdeling van taken en verantwoordelijkheden ten aanzien van informatiebeveiliging aan bod. In paragraaf 2-4 wordt de PDCA (plan-do-check-act)-cyclus rond informatiebeveiliging beschreven. Tot slot staan de gemeentelijke ICT-middelen en dataclassificatie centraal in paragraaf 2-5.

2-2 informatiebeveiligingsbeleid

In december 2013 heeft het college het concern IB-beleid vastgesteld. Het beleid is in opzet adequaat. Het beleid is risk-based: de gemeente beoogt beveiligingsmaatregelen te treffen op basis van risicoanalyse. Het IB-beleid was eind 2016 nog niet geactualiseerd, terwijl er wel organisatieveranderingen zijn geweest die hier aanleiding toe geven.

Naast het IB-beleid gelden er verschillende andere procedures en richtlijnen voor informatiebeveiliging. Regels voor het gebruik van ICT-middelen zijn uitgewerkt in de regeling ICT en informatiegebruik. Uit de component architectuur IB is af te leiden welke beveiligingsmaatregelen genomen moeten worden in relatie tot de dataclassificatie die data-eigenaren moeten toekennen.

De baseline DIA beschrijft het standaard niveau van beveiliging voor de ICT-voorzieningen waarvoor de directie IIFO het technisch beheer verzorgd. Niet alle clusters beschikken over een eigen informatiebeveiligingsplan dat als basis kan dienen voor afspraken met IIFO over aanvullende beveiligingsmaatregelen.

Concernbreed gelden tot slot procedures voor het aanvragen van externe dataverbindingen, het melden van datalekken en regels voor de beveiliging van mobiele apparatuur. Ook is er een beleidsregel voor gegevensverwerking in het sociaal domein.

2-2-1 concerninformatiebeveiligingsbeleid

De gemeente Rotterdam beschikt over een concerninformatiebeveiligingsbeleid, dat op 10 december 2013 door het college is vastgesteld. Daarnaast zijn er diverse procedures en regelingen waarin ook kaders zijn vastgelegd voor de wijze waarop informatiebeveiliging binnen de gemeente moet worden geborgd.

6 Plan-Do-Check-Act.

De doelstelling van het concern IB-beleid is als volgt geformuleerd:[7]

'Dit concern IB beleid is het kader voor passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen dat de gemeente voldoet aan relevante wet- en regelgeving. Rotterdam streeft ernaar om 'in control' te zijn en daarover op professionele wijze verantwoording af te leggen.'

Het concern IB-beleid is hoofdzakelijk gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG). Daarmee is het beleid gebaseerd op een good practice. Tabel 2-2 geeft een overzicht van de onderwerpen die in het concern IB-beleid zijn uitgewerkt. Dit zijn onderwerpen die ook in de BIG zijn opgenomen.

tabel 2-2: onderwerpen concern IB-beleid

onderwerp	kaders voor
organisatie informatiebeveiliging	toedeling van verantwoordelijkheden, taken en rollen, inrichting PDCA-cyclus etc.
gebruik van middelen en informatie	het gebruik van (privé)middelen en gemeentelijke informatie, wijze van classificatie van gegevens
personeel	organisatorische aspecten t.a.v. personeel en bewustwording rond informatiebeveiliging
fysieke beveiliging	toegang tot gebouwen, terreinen, werkplekken etc.
beveiliging apparatuur en informatie	correct en veilig gebruik van ICT-voorzieningen, o.a. systeemplanning- en acceptatie, back up en recovery, logging
logische toegangsbeveiliging	toegang tot informatie, o.a. authenticatie en autorisatie, toegang externe partijen, thuiswerken
beveiliging van informatiesystemen	integrale beveiliging van informatiesystemen, o.a. softwareontwikkeling en onderhoud, encryptie
beveiligingsincidenten	melding en registratie en opschaling bij grote incidenten
bedrijfscontinuïteit	voorkomen van onderbreking van bedrijfsactiviteiten en bescherming van kritische informatiesystemen
naleving	voldoen aan wet- en regelgeving en toetsing op naleving IB-beleid

In het concern IB-beleid staat het voornemen om informatiebeveiliging risk-based aan te pakken; de gemeente beoogt beveiligingsmaatregelen te treffen op basis van risicoanalyse.[8] Op de invulling die het risicomanagement rond informatiebeveiliging in de praktijk krijgt wordt nader ingegaan in hoofdstuk 4.

7 Gemeente Rotterdam, 'concern informatiebeveiligingsbeleid 2014', 10 december 2013.

8 Gemeente Rotterdam, 'concern informatiebeveiligingsbeleid 2014', 10 december 2013, pag. 4.

2-2-2 (periodieke) evaluatie en actualisatie IB-beleid

Zoals eerder aangegeven is het huidige concern IB-beleid op 10 december 2013 door het college vastgesteld. In september 2015 is de start van een actualisatie van het concern IB-beleid aangekondigd. Het bestaande beleid was aan herziening toe vanwege interne organisatieveranderingen, de meldplicht datalekken en nieuw beleid voor mobiel werken.[9] Organisatorische veranderingen die na de vaststelling van het concern IB-beleid eind 2013 zijn doorgevoerd zijn onder andere:

- De afschaffing van een separate CIO-functie en het onderbrengen van de CIO-office bij IIFO met ingang van 2016;
- De omvorming van de RSO en delen van de Bestuursdienst met ingang van 2016 naar het cluster BCO;
- De aanstelling van decentrale information security officers halverwege 2016 ten behoeve van de clusters MO, SO, SB, DV en BCO.[10]

In de rapportage Programma Generieke ICT (september 2016) is gemeld dat de actualisatie van het informatiebeveiligingsbeleid is vertraagd. De genoemde organisatorische veranderingen zijn daardoor vooralsnog niet verwerkt in het concern IB-beleid. Hierdoor sluit het beleid niet aan op de huidige inrichting van de organisatie.

2-2-3 nadere procedures en richtlijnen

De gemeente Rotterdam beschikt naast het concern IB-beleid over diverse concernbrede procedures, richtlijnen en handreikingen waarin aan informatiebeveiliging gerelateerde onderwerpen (nader) zijn uitgewerkt. De rekenkamer heeft de volgende documenten aangetroffen:

- regeling ICT en informatiegebruik (2012);
- component architectuur informatiebeveiliging (2014);
- handreiking dataclassificatie (2011);[11]
- baseline DIA (2013);
- procedure aanvragen externe dataverbindingen (2016);
- protocol meldplicht datalekken (2016);
- beveiliging mobiele apparatuur (2016);
- beleidsregel gegevensverwerking in het sociaal domein (2016).

De inhoud van deze documenten wordt hierna toegelicht.

regeling ICT en informatiegebruik 2012

Deze regeling bevat de regels die gelden voor de medewerkers van de gemeente Rotterdam bij het gebruik van ICT-middelen en gemeentelijke informatie. De regeling geeft ook aan binnen welke kaders er controle op het gebruik kan plaatsvinden. Aanleiding voor het opstellen van de regeling was de ontwikkeling van het nieuwe werken. De regeling is ook van toepassing op het gebruik van privé-middelen ten behoeve van werkzaamheden. In het kader van informatiebeveiliging is artikel 4 van

9 Gemeente Rotterdam, 'Tweede tertaalrapportage concern informatiebeveiliging 2015', 4 september 2015, pag. 2.

10 Het cluster W&I beschikte reeds over een decentrale security officer.

11 De handreiking is vervallen, de inhoud hiervan is opgenomen in de component architectuur informatiebeveiliging.

de regeling relevant. Dit artikel betreft de toegang tot en de beveiliging van gemeentelijke informatie (zie onderstaand kader).

Artikel 4 Toegang tot en beveiliging van gemeentelijke informatie

1 De medewerker verschaft zich uitsluitend toegang tot die gegevens waartoe hij geautoriseerd is.
2 Het is de medewerker verboden om anderen dan daartoe geautoriseerde medewerkers toegang tot gemeentelijke informatie te verlenen.
3 De medewerker neemt passende technische en organisatorische maatregelen om gemeentelijke informatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatige gebruik.
4 De medewerker houdt hierbij in ieder geval rekening met:
   a. de beveiligingsclassificatie van de informatie;
   b. de door de gemeente gestelde beveiligingsvoorschriften;
   c. aan de werkplek verbonden risico's;
   d. het risico door het benaderen van gemeentelijke informatie met andere dan door de gemeente verstrekte of goedgekeurde ICT-apparatuur.
5 De medewerker dient geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten onverwijld te melden bij de functionaris informatiebeveiliging.
6 Ingeval van dringende redenen kan het hoofd van dienst, of bij diens afwezigheid de functionaris informatiebeveiliging, dan wel de algemeen directeur van de Servicedienst besluiten tot het nemen van noodmaatregelen voor de informatiebeveiliging. Deze noodmaatregelen kunnen, voor zover dit noodzakelijk is, betrekking hebben op privé-middelen en privé-bestanden.
7 De medewerker is gerechtigd advies of ondersteuning van de functionaris informatiebeveiliging te vragen.
8 De medewerker is verplicht advies of ondersteuning van de leidinggevende of de functionaris informatiebeveiliging te vragen indien de medewerker onvoldoende in staat is de beveiligingsvoorschriften uit te voeren of te beoordelen.
9 De beveiligingsclassificatie en de beveiligingsvoorschriften als bedoeld in het derde lid, zijn op te vragen bij de functionaris informatiebeveiliging.

component architectuur informatiebeveiliging 2014

De component architectuur (vastgesteld in december 2014) is een technische uitwerking van het concern IB-beleid. De component architectuur bevat een leidraad voor ontwerpbeslissingen, (technische) oplossingen en investeringen in informatiebeveiliging.[12] Uitgangspunt van de component architectuur is *comply or explain*; de architectuur is voorschrijvend, afwijken is alleen toegestaan op basis van een zorgvuldige risicoafweging door het verantwoordelijk management.[13] In de component architectuur zijn de hoofdprincipes voor informatiebeveiliging (vertrouwelijkheid, integriteit en beschikbaarheid) uitgewerkt in beveiligingsmaatregelen gekoppeld aan de classificatieniveaus (geen – laag – midden – hoog) voor data die het concern IB-beleid onderscheidt.

12 Gemeente Rotterdam, 'Concern informatiebeveiliging component architectuur', 15 december 2014, pag. 4.

13 Gemeente Rotterdam, 'Concern informatiebeveiliging component architectuur', 15 december 2014, pag. 4.

hoofdprincipes informatiebeveiliging en classificatieniveaus[14]

- ***vertrouwelijkheid:*** de data-eigenaar verschaft alleen geautoriseerde gebruikers toegang tot vertrouwelijke gegevens. De bevoegdheid en mogelijkheid tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie is beperkt tot een gedefinieerde groep van gerechtigden.
- ***integriteit:*** de data-verantwoordelijke waarborgt de integriteit van gegevens, zodat informatie in overeenstemming is met de werkelijkheid en gegarandeerd is dat niets wordt achtergehouden of verdwijnt.
- ***beschikbaarheid:*** de beschikbaarheid van informatie en IT voldoet aan de gemaakte continuïteitsafspraken. Informatie is toegankelijk en kan gebruikt worden.

De koppeling tussen de hoofdprincipes en classificatieniveaus voor data is hieronder weergegeven:

Niveau	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Geen	**Openbaar** informatie mag door iedereen worden ingezien *(de gemeentelijke website)*	**Niet zeker** informatie mag worden veranderd *(templates en sjablonen)*	**Niet nodig** gegevens kunnen zonder gevolgen niet beschikbaar zijn *(tools)*
LAAG	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie *(het intranet)*	**Beschermd** het bedrijfsproces staat enkele (integriteits-)fouten toe *(rapportages)*	**Nodig** informatie mag (incidenteel) niet beschikbaar zijn *(administratieve gegevens)*
MIDDEN	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep *(de belastingadministratie)*	**Hoog** het bedrijfsproces staat zeer weinig fouten toe *(vergunningverlening)*	**Belangrijk** informatie moet vrijwel altijd beschikbaar zijn *(sociale dienst systeem)*
HOOG	**Geheim** informatie is alleen toegankelijk voor direct geadresseerde(n) *(de basisregistratie personen)*	**Absoluut** het bedrijfsproces staat geen fouten toe *(de gemeentelijke website)*	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen *(gegevensmagazijn)*

In de component architectuur is bepaald dat de data-eigenaren verantwoordelijk zijn voor de classificatie van data. Op basis van het toegekende classificatieniveau kunnen de data-eigenaren uit de component architectuur afleiden welke beveiligingsmaatregelen getroffen moeten worden.

Het proces van classificeren start met het inventariseren van wettelijke eisen ten aanzien van de data. Vervolgens moeten de verantwoordelijkheden ten aanzien van de data in kaart worden gebracht,[15] evenals de waarde van de data en het belang van het bedrijfsproces waarin de data wordt verwerkt. Tot slot volgt de toekenning van een classificatieniveau en de daarmee gepaard gaande keuze voor passende beveiligingsmaatregelen. In hoofdstuk 4 wordt ingegaan op de mate waarin dataclassificatie in de praktijk is uitgevoerd.

baseline DIA 2013

Het technisch beheer op de applicaties die binnen de gemeente in gebruik zijn wordt verzorgd door het Cluster BCO – directie IIFO (voorheen RSO - Dienstencentrum Informatie en Automatisering (DIA)). In de baseline DIA 2013 is het standaardniveau van beveiliging beschreven dat moet worden toegepast bij de ICT-voorzieningen

14 Gemeente Rotterdam, 'Concern informatiebeveiliging component architectuur', 15 december 2014, pag. 8.

15 Het gaat dan bijvoorbeeld om wie de er allemaal gebruik maken van de data en welke rechten zij hebben.

waarvan het beheer bij de directie IIFO is ondergebracht. De baseline bevat beveiligingsmaatregelen in de volgende categorieën:

- fysieke toegangsbeveiliging;
- beheer van communicatie- en bedieningsprocessen;
- toegangsbeveiliging;
- verwerving, ontwikkeling en onderhoud van systemen;
- beheer van informatiebeveiligingsincidenten;
- bedrijfscontinuïteitsbeheer;
- naleving (o.a. wettelijke voorschriften).

In de baseline is vermeld dat alle clusters moeten beschikken over een eigen informatiebeveiligingsplan op basis waarvan afspraken worden gemaakt over eventuele aanvullende beveiligingsmaatregelen voor bepaalde ICT-voorzieningen. Hoewel de baseline DIA is vastgesteld in 2013 constateert de rekenkamer dat, met uitzondering van het cluster W&I, de clusters in 2016 nog niet over een eigen informatiebeveiligingsplan beschikten. Ten aanzien van het informatiebeveiligingsplan 2015-2016 van het cluster W&I constateert de rekenkamer dat dit plan niet duidelijk maakt welke aanvullende beveiligingsmaatregelen dit cluster nodig acht ten opzichte van de baseline DIA.

procedure aanvragen externe dataverbindingen (2016)
In dit document staat de procedure beschreven voor de totstandkoming van dataverbindingen waarmee externe partijen toegang tot het gemeentelijke netwerk kunnen krijgen. Een ander uitgangspunt van de procedure is dat externe toegang alleen is toegestaan als risico's zijn gemitigeerd doordat er voldoende passende maatregelen zijn getroffen. Uitgangspunt in de procedure is dat elke aanvraag voor externe toegang moet worden onderzocht op mogelijke risico's. De security manager van het cluster BCO dient deze risicoanalyse te toetsen, alvorens hij een besluit neemt over de toekenning van de verbinding.

protocol meldplicht datalekken
Per 1 januari 2016 is de meldplicht datalekken van kracht. Met het oog op deze meldplicht is eind 2015 het protocol meldplicht datalekken vastgesteld. Het protocol schrijft voor wanneer een (vermoeden van) een datalek moet worden gemeld en welke acties dan moeten worden uitgevoerd.

wat is een datalek?
Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. Er is sprake van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens, zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens. Voorbeelden van datalekken zijn een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.[16]

16 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

Iedere medewerker van de gemeente is verplicht melding te maken als sprake is van:[17]

- verlies of diefstal van gegevensdragers (bijv. smartphone, usb-stick etc.);
- verlies van papieren documenten met persoonsgegevens;
- hacking van een database met persoonsgegevens;
- ongeautoriseerde toegangsverschaffing tot bestanden met persoonsgegevens;
- verbreking van een geheimhoudingsplicht m.b.t. persoonsgegevens;
- al dan niet doelbewuste verstrekking van persoonsgegevens aan onbevoegden;
- alle andere gevallen waarin beveiligingsmaatregelen voor persoonsgegevens geen bescherming bieden.

Ook is in het protocol opgenomen dat bij uitbesteding van de verwerking van persoonsgegevens aan derden, in een bewerkersovereenkomst opgenomen moet worden dat de bewerker verplicht is een datalek direct aan de gemeente te melden.

beveiliging mobiele apparatuur
In 2016 is een aantal documenten opgesteld over de beveiliging van verschillende typen telefoons en andere mobiele apparatuur, die medewerkers in het kader van hun werkzaamheden gebruiken.[18] Ook is in een document uitgewerkt hoe te handelen bij verlies of diefstal van een mobile device.

beleidsregel gegevensverwerking in het sociale domein
Deze beleidsregel gaat in op de verwerking en uitwisseling van persoonsgegevens in het kader van de uitvoering van de gedecentraliseerde taken in het sociaal domein. In de beleidsregel zijn de uitgangspunten uiteen gezet die de gemeente in dit verband hanteert. Een uitgangspunt is bijvoorbeeld dat gegevensverwerking plaatsvindt op basis van 'need to know'; alleen gegevens die gezien het doel van de uitgevoerde taak noodzakelijk zijn worden verwerkt. Een andere uitgangspunt is dat gegevensverwerking plaatsvindt op basis van 'toestemming, tenzij'; toestemming van de burger voor een behandeling impliceert daarbij ook toestemming voor het delen van gegevens met zorgverleners die bij de behandeling zijn betrokken. Ten aanzien van het borgen van een veilige gegevensuitwisseling is in de beleidsregel opgenomen dat de gemeente aansluit bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Van ketenpartners verwacht de gemeente dat zij dezelfde eisen aan hun beveiliging stellen.[19]

2-3 taken en verantwoordelijkheden

In het IB-beleid zijn de verantwoordelijkheden ten aanzien van informatiebeveiliging duidelijk beschreven. Hierbij zijn specifieke verantwoordelijkheden voor het lijnmanagement benoemd. Taken op het gebied van informatiebeveiliging worden als onduidelijk ervaren. Zo is bijvoorbeeld niet duidelijk wat precies tot het takenpakket van de information security officers behoort. Taken voor informatiebeveiliging worden vooral uitgevoerd door de CISO, security manager, information security officers, security coördinatoren en functioneel beheerders.
De bescherming van persoonsgegevens is de verantwoordelijkheid van de data-eigenaren. In aanloop naar de invoering van de nieuwe Europese verordening gegevensbescherming (AVG) is

17 Gemeente Rotterdam, 'Protocol meldplicht datalekken', 8 december 2015.

18 https://rio.rotterdam.nl/Project/ConcernInformatiebeveiliging/Documents#!/path=%7CVeilig%20werken%20met%20mobiele%20apparatuur/

19 Gemeente Rotterdam, 'Beleidsregel gegevensverwerking in het sociaal domein', 2015.

een kwartiermaker functionaris gegevensbescherming aangesteld. De clusters MO en W&I beschikken over een privacy officer. De andere clusters hebben een dergelijke functie niet.

2-3-1 taken en verantwoordelijkheden t.a.v. informatiebeveiliging

Het concern IB-beleid van de gemeente gaat uit van de volgende verantwoordelijkheidsverdeling:[20]

- Het college is integraal verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente;
- De concerndirectie is verantwoordelijk voor kaderstelling en sturing;
- De clusterdirecties zijn vanuit een vragende rol[21] verantwoordelijk voor de integrale beveiliging van hun organisatieonderdelen;
- De directie van het cluster BCO (in het IB-beleid nog aangeduid als RSO) is verantwoordelijk voor de uitvoering van de beveiligingsmaatregelen.

Uit gesprekken is naar voren gekomen dat de uitvoering van beveiligingsmaatregelen niet enkel een verantwoordelijkheid van het cluster BCO is. De afdeling beheer (BCO – IIFO) verzorgt het technisch beheer voor de applicaties. Het functioneel beheer is een verantwoordelijkheid van de clusters zelf. In de praktijk betekent dit dat de afdeling beheer (BCO – IIFO) verantwoordelijk is voor het technisch juist functioneren van applicaties, waaronder het juist toepassen van technische beveiligingsmaatregelen. Het functioneel beheer ten aanzien van de applicaties vindt voor het merendeel van de applicaties plaats binnen de clusters.[22] Functioneel beheer is o.a. verantwoordelijk voor de verdere inrichting van de applicaties en het beheer van autorisaties.

technisch vs. functioneel beheer

Het technisch beheer richt zich op het in stand houden, beheren en onderhouden van de IT-infrastructuur; de basis waarop applicaties kunnen draaien, bestaande uit het netwerk, de computers, operating systems en overige apparatuur. Het functioneel beheer omvat de beheertaken die samenhangen met het dagelijks gebruik van specifieke applicaties. Het gaat dan bijvoorbeeld om het beheren van de autorisaties, het doorvertalen van gebruikerswensen naar de applicatie, het testen van doorgevoerde wijzigingen in de applicatie.

In de beleidsdocumenten is geen nadere verdeling van taken voor informatie-beveiliging beschreven. Ook geven meerdere geïnterviewden aan dat er geen specifieke functiebeschrijving is waarin hun taken en verantwoordelijkheden helder zijn omschreven.

Op basis van de gesprekken die in het kader van dit onderzoek zijn gevoerd, constateert de rekenkamer dat de taken ten aanzien van informatiebeveiliging in de dagelijkse praktijk primair bij de volgende functionarissen zijn belegd:

- Chief information security officer (CISO);
- Information security officers (ISO's);

20 Gemeente Rotterdam, 'Concern informatiebeveiligingsbeleid 2014', 10 december 2013, pag. 5.

21 De clusters maken hun behoeften richting BCO kenbaar.

22 IIFO verzorgt het functioneel beheer voor de generieke concernbrede systemen. Het functioneel beheer voor specifieke systemen en applicaties vindt in de regel binnen de clusters zelf plaats, met uitzondering van enkele specifieke applicaties waarvoor IIFO ook het functioneel beheer verzorgt.

- Security managers;
- Security coördinatoren[23], tevens technisch beheerders;
- Functioneel beheerders;
- Lijnmanagers.

De taken die deze functionarissen op het gebied van informatiebeveiliging uitvoeren worden onderstaand toegelicht.

chief information security officer (CISO)
Binnen de gemeente Rotterdam is de CISO (1 FTE) gepositioneerd binnen het cluster BCO – IIFO, bij de afdeling strategie en ondersteuning, onder de programmadirecteur IIFO. In de Baseline Informatievoorziening Gemeenten is beschreven dat de CISO de beveiliging bevordert en gevraagd en ongevraagd advies geeft, rapportages verzorgt over de status van de beveiliging, de naleving van maatregelen controleert, evalueert en voorstellen doet tot implementatie c.q. aanpassing van plannen op het gebied van informatiebeveiliging. Het takenpakket dat van de CISO van de gemeente Rotterdam komt overeen met omschrijving in de baseline. De gemeentelijke CISO geeft op strategisch niveau invulling aan de concernbrede informatiebeveiliging. Taken die tot het werkpakket van de CISO behoren zijn het uitwerken van beleidskaders, opstellen van het meerjarenplan informatiebeveiliging, bevorderen van de awareness binnen het concern en het opstellen van tertaalrapportages over informatiebeveiliging. De CISO vervult een kaderstellende rol richting de beheerorganisatie bij het Cluster BCO.[24]

information security officers
Binnen de gemeente Rotterdam zijn in de verschillende clusters information security officers aangesteld. De information security officers maken deel uit van de afdeling informatiemanagement bij het cluster BCO (IIFO). Vanuit deze afdeling verrichten de information security officers werkzaamheden voor de clusters.

Vanaf halverwege 2016 hebben alle clusters een information security officer tot hun beschikking. Daarvoor bestond deze functie alleen binnen het cluster W&I. In 2015 heeft de CISO om extra capaciteit gevraagd, zodat binnen ieder cluster 1 FTE als information security officer aangesteld kon worden. Deze capaciteitsclaim kwam voort uit de wens om de uitvoering van het meerjarenplan informatiebeveiliging te verbeteren. Voor de gevraagde versterking kon niet voldoende financiële dekking worden gevonden. Uiteindelijk heeft de concerndirectie € 200.000 beschikbaar gesteld voor extra capaciteit en besloten dat het meerjarenplan gefaseerd moest worden uitgevoerd.[25] Dit was niet voldoende om voor ieder cluster 1 FTE aan te stellen. De clusters MO en W&I hebben daardoor nu ieder 1 FTE beschikbaar voor de ISO-functie, de overige clusters 0,5 FTE.

benodigde capaciteit voor informatiebeveiliging
Het is lastig precies te benoemen hoeveel capaciteit een organisatie nodig heeft om informatiebeveiligingstaken goed uit te kunnen voeren. Dit is onder meer afhankelijk van het

23 Securitycoördinator is een rol die verschillende beheerders vervullen naast hun reguliere werkzaamheden.

24 In het kader demand & supply geeft de CISO hiermee invulling aan de demand-zijde.

25 Gemeente Rotterdam, impressie concerndirectie, 30 september 2015.

volwassenheidsniveau dat de organisatie reeds heeft bereikt op het gebied van informatiebeveiliging, de mate waarin medewerkers en lijnmanagement zich verantwoordelijk voelen voor goede informatiebeveiliging en het daar bijbehorende gedrag vertonen, en van extra uitdagingen die zich voordoen zoals de invoering van nieuwe wet- en regelgeving. De rekenkamer heeft geen bruikbare benchmark aangetroffen waarmee beoordeeld kan worden of de gemeente Rotterdam genoeg capaciteit inzet voor informatiebeveiliging.

De information security officers vervullen een adviserende rol ten aanzien van de clusters. Daarnaast geven de ISO's aan dat het bevorderen van de awareness, het uitwerken van IB-plannen voor de clusters, het uitvoeren van risicoanalyses, het afhandelen van incidenten en datalekken en het regelen van externe dataverbindingen tot hun takenpakket behoren. Uit gesprekken met de ISO's komt naar voren dat o.a. door het ontbreken van een functiebeschrijving niet volledig helder is wat wel en niet onder de taken en verantwoordelijkheden van de ISO's valt. Zo gaf één van de ISO's bijvoorbeeld aan dat hij veel operationele zaken uitvoert, zoals het regelen van externe dataverbindingen, maar het de vraag is of dergelijke zaken tot het takenpakket van de ISO's moeten horen.[26]

security manager
De security manager is onderdeel van het team ontwikkeling en projecten (cluster BCO – IIFO). De security manager richt zich op de technische invulling van informatiebeveiliging en bevordert de awareness en het veilig gedrag van medewerkers binnen IIFO. Ten tijde van dit onderzoek was er 1 FTE als security manager actief en stond er 1 FTE open voor het aanstellen van een tweede security manager. De openstaande FTE is ingevuld door (tijdelijke) externe inhuur. Het takenpakket van de security manager is beperkt tot de technische kant van informatiebeveiliging; het bevorderen van awareness en veilig gedrag valt niet onder de verantwoordelijkheden van de security manager. Tot de taken van de security manager behoren bijvoorbeeld het toetsen van oplossingen aan de component architectuur beveiliging, het adviseren over- en goedkeuren van voorgestelde technische maatregelen, adviseren t.a.v. projecten, opstellen van proces- en procedurebeschrijvingen, en het leveren van input t.b.v. aanbestedingsprocedures. De security manager verzorgt de beveiliging die door de CISO en de clusters wordt gevraagd.[27]

Ten opzichte van de CISO geeft de security manager invulling aan de supply-zijde, door de technische invulling te verzorgen van de beveiliging die door de CISO en de clusters wordt gevraagd (demand). Er vindt samenwerking plaats tussen de CISO en de security manager.

security coördinatoren
Security coördinator is geen functie binnen de gemeente Rotterdam, maar een rol die technisch beheerders van het cluster BCO (IIFO, afdeling beheer) naast hun reguliere werkzaamheden vervullen. In totaal zijn er circa 30 technisch beheerders die de rol van security coördinator vervullen. De securitycoördinatoren zijn o.a. betrokken bij de realisatie van de technische beveiligingsmaatregelen die op grond van het beleid en

26 Interview, 19 juli 2016.

27 In het kader van demand & supply geeft de security manager daarmee invulling aan de supply-zijde.

specifieke wensen van de clusters worden getroffen. Er is geen sprake van een hiërarchische relatie tussen de security manager en de securitycoördinatoren, aangezien de security coördinatoren werkzaam zijn binnen de afdeling beheer en de security manager werkzaam is voor de afdeling ontwikkeling en projecten.

functioneel beheerders
Binnen de verschillende clusters zijn functioneel beheerders aangesteld die de inrichting verzorgen van de applicaties die de clusters gebruiken. In relatie tot informatiebeveiliging hebben zij een belangrijke taak als het gaat om het ontwerpen en beheren van functionele rollen die in een applicatie kunnen worden onderscheiden. Daarbij werken zij ook de bijbehorende autorisatiematrix uit en houden toezicht op de toekenning van autorisaties.

lijnmanagers
Uitgangspunt van de Baseline Informatiebeveiliging Gemeenten is dat iedere lijnmanager verantwoordelijk is voor de integrale informatiebeveiliging van zijn of haar onderdeel. Ten aanzien van de rol van het lijnmanagement is in het IB-beleid vermeldt dat zij moeten sturen op informatieveiligheid en naleving van het beleid. Daarnaast zijn in het concern IB-beleid de volgende specifieke verantwoordelijkheden voor het lijnmanagement benoemd:

- Het lijnmanagement is verantwoordelijk voor het juist afhandelen van beveiligingsaspecten van het aangaan, wijzigen en beëindigen van een dienstverband of een overeenkomst met externen.
- Het lijnmanagement bepaalt welke rol(len) de medewerker moet vervullen en welke autorisaties voor het raadplegen, opvoeren, muteren en afvoeren van gegevens moeten worden verstrekt.
- Het lijnmanagement bevordert dat medewerkers (en externe gebruikers van gemeentelijke systemen) zich houden aan beveiligingsrichtlijnen.

2-3-2 taken en verantwoordelijkheden t.a.v. bescherming persoonsgegevens

De bescherming van (bijzondere) persoonsgegevens is primair de verantwoordelijkheid van de data-eigenaren binnen de clusters. Deze verantwoordelijk hangt samen met de verantwoordelijkheid die zij dragen voor de uitvoering van primaire processen. Daarnaast is er binnen de gemeente Rotterdam een aantal functionarissen waarvan de taken en verantwoordelijkheden zich richten op het borgen van privacy bij het verwerken van persoonsgegevens.

kwartiermaker functionaris gegevensbescherming
Vanaf 25 mei 2018 wordt de Algemene Verordening Gegevensbescherming (AVG) van kracht, die iedere overheidsorganisatie verplicht een functionaris gegevensbescherming aan te stellen. Vooruitlopend op deze verplichting heeft de gemeente Rotterdam in mei 2016 een kwartiermaker functionaris gegevensbescherming benoemd. Deze kwartiermaker heeft een drieledige opdracht gekregen: (1) het beoordelen en melden van datalekken, (2) kwartiermaken voor de functie van functionaris gegevensbescherming en (3) het vervullen van een ‘aanjaagrol’ in het kader van de implementatie van de AVG.

privacy officers clusters W&I en MO
Naar aanleiding van de decentralisaties in het sociaal domein is in 2015 bij het cluster MO een privacy officer aangesteld. Bij het cluster W&I is vanaf mei 2016 ook een

privacy officer aangesteld.[28] De overige clusters beschikken niet over een dergelijke functie.

De privacy officers, de information security officers en juridisch controllers van de clusters MO en W&I vormen samen een privacy office. Dit privacy office richt zich op een drietal zaken:[29]

1 zorgen voor bewustwording rond privacy onder medewerkers binnen het sociaal domein;
2 de basis op orde; inzicht krijgen in alle processen waarin persoonsgegevens omgaan;
3 ondersteunen van de 'door-ontwikkel-opgaven' binnen het sociaal domein.

Daarnaast worden de privacy officers ook ingezet op ad-hoc zaken en werkzaamheden in het kader van de afhandeling van datalekken, het beoordelen van informatieverzoeken die in het kader van (wetenschappelijk) onderzoek worden gedaan, het inventariseren van gegevensuitwisselingen en het opstelling van privacy impact analyses bij het in gebruik nemen van nieuwe applicaties. De privacy officers werken ook in dit verband samen met de ISO's.

2-4 PDCA-cyclus

De opzet van de PDCA-cyclus rond informatiebeveiliging is beschreven in het IB-beleid. In de praktijk wordt aan deze cyclus onvoldoende invulling gegeven. Het ontbreekt met name aan structurele rapportagelijnen richting de verantwoordelijke clusterdirecties. De concernbrede rapportage over informatiebeveiliging bevat enkel informatie op hoofdlijnen en onduidelijk is op welke manier opvolging wordt gegeven aan deze rapportage. In de afgelopen jaren zijn verschillende audits en onderzoeken uitgevoerd op het gebied van informatiebeveiliging, maar onduidelijk is of n.a.v. de uitkomsten hiervan altijd verbeteracties zijn ingezet.

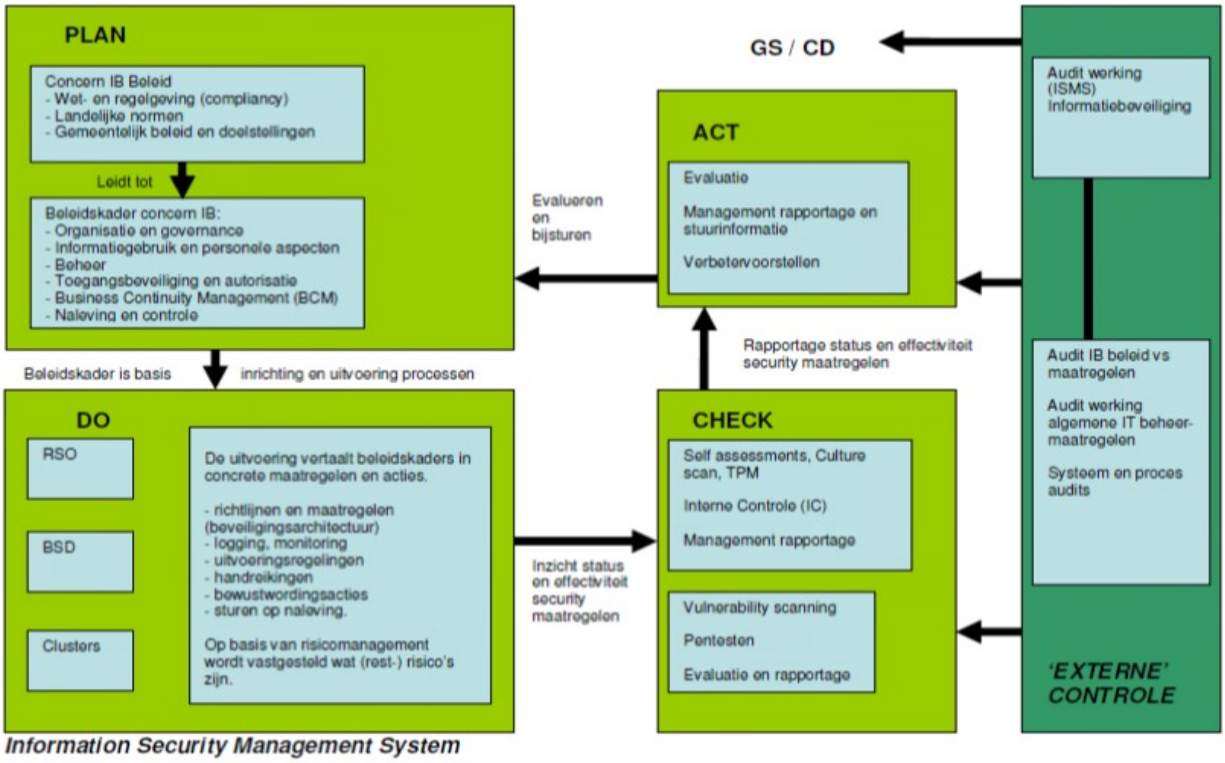
In het concern IB-beleid is de PDCA-cyclus[30] rond informatiebeveiliging als volgt weergegeven:

28 De aanstelling van de privacy officer betrof een pilot waarbij eind 2016 besloten zou worden of de functie wordt voortgezet.

29 Interview, 13 juli 2016.

30 Met dit principe wordt aangegeven dat voor het bereiken van een hogere kwaliteit een continue cyclus op gang moet worden gebracht van het plannen van acties, het ten uitvoer brengen van geplande acties, het checken of de resultaten van de acties werkelijk zijn zoals was beoogd, en het bijsturen of bijstellen van de uitvoering of plannen naar aanleiding van de checkresultaten.

figuur 2-1: PDCA-cyclus informatiebeveiliging



bron: gemeente Rotterdam, 'Meerjarenplan informatiebeveiliging'.

In het meerjarenplan informatiebeveiliging (maart 2015) is vermeld dat de PDCA-cyclus nog niet volledig wordt doorlopen en concernbreed nog in de kinderschoenen staat. Daarbij is aangegeven dat dit met name geldt voor de 'Check'. Volgens het meerjarenplan informatiebeveiliging is er onvoldoende grip op wat er wordt uitgevoerd en is er uitsluitend sprake van verantwoording op afzonderlijke wettelijk verplichte onderwerpen, zoals DigiD en Suwinet.[31] Daarnaast is in het meerjarenplan geconstateerd dat er geen structurele rapportagelijnen binnen de clusters zijn, waardoor er onvoldoende basis is om een eenduidige verantwoordingscyclus uit te kunnen voeren. Het beeld dat naar voren komt uit het meerjarenplan komt overeen met het beeld dat naar voren komt uit de gesprekken die de rekenkamer in het kader van dit onderzoek heeft gevoerd. Tussen de CISO, security manager, security information officers en privacy officers is sprake van collegiaal overleg, maar structurele rapportagelijnen richting de directies ontbreken.[32]

concernbrede rapportages over informatiebeveiliging

Onderdeel van het concern IB-beleid is dat de CISO periodiek rapporteert over de concernbrede stand van zaken op het gebied van informatiebeveiliging. De security manager en de clusters leveren informatie aan ten behoeve van deze rapportage.

31 Gemeente Rotterdam, 'Meerjarenplan Concern IB', 2 maart 2015, pag. 11.

32 In het kader van ambtelijk wederhoor van de nota van bevindingen geeft de ambtelijke organisatie aan dat rapportagelijnen voor één bepaalde applicatie (SUWI) zijn geformaliseerd. Daarnaast zouden voor de clusters Maatschappelijke Ontwikkeling en Werk en Inkomen portefeuillehouders voor informatiebeveiliging en privacy aangesteld zijn. Dit gegeven alleen zorgt nog niet voor structurele rapportagelijnen.

In de rapportages die vanaf 2012 zijn verschenen komen standaard de volgende onderwerpen terug: de voortgang van het meerjarenplan IB, stand van zaken rond de algemene verordening gegevensbescherming, de meldplicht datalekken, stand van zaken in de clusters, incidenten en 'audits en onderzoeken'. De rapportages zijn beperkt in omvang, er wordt ten aanzien van de verschillende onderwerpen op hoofdlijnen gerapporteerd. Ook blijkt uit de rapportages niet welke voortgang er ten opzichte van de voorgaande periode is geboekt. Onduidelijk is of de rapportages binnen het concern worden besproken. De rekenkamer heeft geen aanwijzingen dat de rapportages aanleiding zijn geweest voor het inzetten van verbeteracties.

audits en andere onderzoeken
De afgelopen jaren zijn op het gebied van informatiebeveiliging diverse audits en onderzoeken uitgevoerd.

Concern Auditing heeft diverse audits uitgevoerd die gericht waren op informatiebeveiliging in brede zin of op specifieke applicaties. In 2013 heeft Concern Auditing een nulmeting uitgevoerd op de sturing en beheersing rond informatiebeveiliging. In opvolging van deze audit is in 2014 en 2015 een aantal audits in samenhang uitgevoerd, resulterend in auditrapportages over management control rond IB en IB-processen (SUWI, DigiD en BRP) en een overkoepelende rapportage. Ook heeft Concern Auditing een audit uitgevoerd op de applicatie leerling-basis-administratie.

Over de gegevensuitwisseling via Suwinet moeten gemeenten jaarlijks verantwoording afleggen aan het ministerie van SZW. In dit verband heeft Concern Auditing audits uitgevoerd op de beveiliging van Suwinet-inkijk. Ook over de beveiliging van DigiD moet de gemeente jaarlijks verantwoording afleggen aan het ministerie. In dit verband heeft Concern Auditing DigiD-beveiligingsassesments uitgevoerd. Over de inrichting, werking en beveiliging van de basisregistratie personen moet ook jaarlijks verantwoording worden afgelegd aan het Rijk. Daartoe voert het cluster dienstverlening jaarlijks een zelfevaluatie uit.

In het kader van de jaarrekeningcontrole worden jaarlijks de IT-general controls getoetst. Dit gebeurt intern door Financial Audit, waarna de externe accountant een review uitvoert.

In 2015 heeft de gemeente een penetratietest laten uitvoeren door een extern gespecialiseerd onderzoeksbureau. Met een penetratietest wordt inzichtelijk gemaakt in hoeverre kwetsbaarheden in de beveiliging kunnen worden uitgebuit en er van buitenaf ingebroken kan worden in de gemeentelijke systemen. Ook zijn er in opdracht van de gemeente Rotterdam audits uitgevoerd op Rotterdam.nl, op de Wifi en op de thuiswerkomgeving van de gemeente.

In 2016 zijn er binnen verschillende clusters (SO, MO, DV) GAP-analyses uitgevoerd op systemen en processen. Doel van de GAP-analyses is inzichtelijk te maken welke maatregelen uit de Baseline Informatiebeveiliging Gemeenten zijn geïmplementeerd. Cluster Maatschappelijke Ontwikkeling heeft in haar beveiligingsplan opvolging gegeven aan de bevindingen uit de GAP-analyses. Onduidelijk is welke opvolging de overige clusters hebben gegeven aan de bevindingen uit de GAP-analyses.

2-5 overzicht applicaties en dataclassificatie

Er bestaat geen actueel centraal overzicht van welke informatie in welke applicaties wordt verwerkt. De gemeente heeft circa 1.000 applicaties in gebruik. Er bestaat een concernclassificatietabel waarin circa 300 applicaties zijn geclassificeerd. Deze tabel dateert uit maart 2014[33].

De gemeente Rotterdam heeft in totaal 785 applicaties in gebruik. De afdeling technisch beheer beschikt over een database waarin de applicaties en andere ICT-middelen zijn opgenomen. Hierin is bijvoorbeeld vastgelegd wie de eigenaar van een applicatie is. De rekenkamer heeft in het kader van dit onderzoek geconstateerd dat deze gegevens niet altijd actueel zijn.

Er is binnen de gemeente geen totaaloverzicht van welke informatie in welke systemen of applicaties wordt verwerkt. Er bestaat een concernclassificatietabel waarin zo'n 300 applicaties zijn opgenomen, die zijn geclassificeerd. Het gaat om de applicaties die de clusters als belangrijk hebben aangemerkt. Daarin is niet vermeld welke informatie in deze applicaties omgaat. Van de overige applicaties die de gemeente in gebruik heeft, heeft de rekenkamer geen classificatie aangetroffen.

In de concernclassificatietabel is een classificatie toegekend aan de aspecten beschikbaarheid-integriteit-vertrouwelijkheid. Uitgangspunt van het IB-beleid is dat de classificaties van alle bedrijfskritische applicaties centraal worden vastgelegd door de CISO en jaarlijks gecontroleerd worden door de clusters. De concern-classificatietabel dateert echter uit 2013 en is daarna niet meer geactualiseerd.

33 Cluster W&I heeft haar gedeelte van de concernapplicatietabel in 2015 geactualiseerd.

Rekenkamer ROTTERDAM

3 maatregelen datalek

3-1 inleiding

Zoals in hoofdstuk 1 is aangegeven, heeft zich in februari 2016 bij de gemeente een datalek voorgedaan. Bij een datalek gaat het om ongewenste toegang tot persoonsgegevens bij een organisatie. In dit specifieke geval betrof het bij de gemeentelijke belastingdienst in beheer zijnde persoonsgegevens, die ruim een maand via internet benaderbaar waren. In dit hoofdstuk beoordeelt de rekenkamer de opvolging die is gegeven aan het datalek.

De desbetreffende onderzoeksvraag luidt als volgt:
Welke maatregelen heeft de gemeente Rotterdam genomen na het datalek in februari 2016 en zijn deze voldoende om dergelijke incidenten in de toekomst redelijkerwijs te voorkomen?

Bij de beantwoording van deze vraag hanteert de rekenkamer normen, die in de onderstaande tabel staan weergegeven.

tabel 3-1: normen en criteria opvolging datalek

normen	criteria	paragraaf
het college heeft de oorzaken en gevolgen van het datalek in februari 2016 afdoende onderzocht	• het college heeft een onderzoek uitgevoerd naar het datalek	3-3
	• dit onderzoek behandelt tenminste aard, omvang, potentiële consequenties en de daadwerkelijke gevolgen van het datalek	3-3
	• in het onderzoek zijn organisatorische en technische aspecten meegenomen	3-3
	• van het onderzoek bestaat verslaglegging	3-3
op basis van de onderzoeksbevindingen heeft het college maatregelen getroffen die een soortgelijk datalek in de toekomst redelijkerwijs kunnen voorkomen	• de gemeente detecteert vergelijkbare kwetsbaarheden en treft maatregelen om te voorkomen dat deze tot nieuwe datalekken leiden	3-4
	• er zijn acties ingezet ter beïnvloeding van houding en gedrag wat betreft veilig gebruik van vertrouwelijke gegevens	3-4

In de volgende paragraaf wordt dieper ingegaan op de waarneming, aard en afhandeling van het datalek. In paragraaf 3-3 wordt specifiek ingegaan op het onderzoek naar het datalek (de eerste norm), waarna in paragraaf 3-4 de vraag aan de orde komt welke maatregelen zijn genomen om toekomstige soortgelijke lekken te voorkomen.

3-2 aard en afhandeling datalek

Door het datalek in februari 2016 waren persoonsgegevens (namen, adressen en BSN-nummers) van 32.000 personen tijdelijk via internet benaderbaar. Zowel de medewerker die het lek veroorzaakte als de gemeente hebben na het bekend worden van het datalek meteen acties ondernomen om het lek te dichten en relevante partijen te informeren.

De Informatiebeveiligingsdienst (IBD) van de Vereniging Nederlandse Gemeenten (VNG) werd in februari 2016 getipt over een datalek met gegevens afkomstig van de gemeente. De veroorzaker van het lek, een ingehuurde medewerker, is op 25 februari door de IBD geïnformeerd dat het mogelijk was om persoonsgegevens via het internet te benaderen. Deze gegevens stonden oorspronkelijk op een externe harde schijf van de medewerker. Deze schijf was gekoppeld aan een thuisnetwerk dat via een router tijdelijk was opengesteld voor benadering vanaf het internet. Er was geen beveiliging (bijvoorbeeld met een wachtwoord) op dit thuisnetwerk ingesteld. De inhoud van de schijf was na openstelling opgemerkt door de zoekmachines van Google.[34] Omdat iemand via Google de gegevens tegenkwam, is het lek min of meer bij toeval gedetecteerd, herkend en gemeld bij de IBD. De precieze periode dat de gegevens benaderbaar waren is onbekend, maar begon waarschijnlijk in januari 2016 en duurde tot eind februari 2016.

hoe kwamen de data op de externe harde schijf?
Tussen 1996 en 2004 werkte de veroorzaker van het datalek voor de gemeente Rotterdam aan automatiseringsprojecten. Daarbij werd software ontwikkeld die moest worden getest. Hiervoor werden gegevens van de gemeente gebruikt. Deze werkbestanden voor testdoeleinden zijn na gebruik in 2004 niet verwijderd. Bij het maken van een back-up werden ze (al jaren geleden) op een externe harde schijf opgeslagen.

Na de constatering van het datalek zijn zowel door de ambtenaar die het lek heeft veroorzaakt, als vanuit de gemeente, verschillende acties ondernomen. Zo heeft de medewerker na de waarschuwing van de IBD, nog dezelfde dag zijn leidinggevende bij de gemeente op de hoogte gesteld. Ook heeft hij het lek gedicht door de apparatuur uit te zetten. Verder heeft hij de gemeente inzicht gegeven in de bestanden die op de harde schijf opgeslagen stonden. Hieruit bleek dat naast Rotterdamse bestanden, ook data van de gemeente Oegstgeest toegankelijk zijn geweest. Ten slotte leverde de medewerker zijn privé-apparatuur in voor nader onderzoek.

Naar aanleiding van de constatering dat naast Rotterdamse bestanden ook data van de gemeente Oegstgeest toegankelijk zijn geweest, heeft de gemeente Rotterdam de

[34] De gegevens waren al openbaar, maar door het zogenaamde indexeren door Google ook vindbaar gemaakt door zoeken op trefwoorden.

gemeente Oegstgeest hierover geïnformeerd.[35] Vanaf maandag 29 februari 2016 is de aard en omvang van het lek door de gemeente nader bekeken. Er werd vastgesteld dat het lek toegang verleende tot privacygevoelige gegevens van Gemeentebelastingen uit de periode 1996-2004. Het betrof namen, adresgegevens en BSN-nummers.[36] Deze gegevens werden indertijd door de medewerker gebruikt als niet-geanonimiseerde testdata. Uit een vergelijking met de Basis Registratie Persoonsgegevens bleek dat het gegevens van ongeveer 32.000 personen betrof.

Vervolgens zijn selecties gemaakt van diverse groepen, zoals overledenen en personen die naar een andere gemeente of het buitenland zijn vertrokken. Per categorie werd communicatie ontwikkeld met uitleg over het datalek.[37] De desbetreffende burgers werden geïnformeerd via een brief en de gemeentelijke website. Extra informatie opvragen was mogelijk via informatienummer 14010 (eerstelijnshulp) en via een tweedelijnsteam voor complexere vraagstukken. Ook is een speciale webpagina opgezet (www.rotterdam.nl/persoonsgegevens) met veel gestelde vragen en antwoorden. De capaciteit van het informatienummer 14010 is naar aanleiding van het datalek tijdelijk uitgebreid. Dinsdag 8 maart 2016 is een brief aan betrokkenen (ca. 15.300 Rotterdammers en in totaal ca. 25.000 personen in Nederland) verzonden. Sommige categorieën hoefden volgens de wettelijke bepalingen niet persoonlijk te worden geïnformeerd (bijvoorbeeld personen die naar het buitenland zijn vertrokken).

Op vrijdag 11 maart 2016 is de melding van het datalek bij de Autoriteit Persoonsgegevens definitief gemaakt. Bij politie werden alle leidinggevenden van de afdelingen Intake en Service in de regio geïnformeerd in verband met mogelijke aangiften van identiteitsfraude.

datalekken gemeente Rotterdam

Over de periode januari tot en met augustus 2016 heeft de gemeente Rotterdam negentien datalekken gemeld bij de Autoriteit Persoonsgegevens.[38] Naast het datalek bij Gemeentebelastingen ging het bijvoorbeeld om een gestolen telefoon met emailverkeer waarin persoonsgegevens van zeventien burgers voorkwamen, een verloren telefoon met e-mails over ingediende bezwaarschriften (betrof 146 personen) en 26 opleidingsaccounts waarbij mogelijk persoonsgegevens waren ingezien door cursisten van Werk en Inkomen.

Ook vóór 2016 kwamen datalekken voor binnen de gemeente Rotterdam. Zo is in een rapportage over informatiebeveiliging uit 2015 een incident gemeld waarbij documenten met daarin persoonsgegevens uit het raam waren gewaaid en niet meer teruggevonden konden worden. De meldplicht was toen echter nog niet van toepassing, waardoor dergelijke incidenten niet algemeen bekend werden.

Naast de beschreven acties om het lek te dichten en om de direct belanghebbenden te informeren, heeft de gemeente verschillende onderzoeken in gang gezet. Eén betreft een technisch onderzoek naar de gevolgen van het datalek en een tweede een interne evaluatie van de afhandeling van het datalek. Het technische onderzoek komt in de

35 De behandeling van het datalek door Oegstgeest is in dit onderzoek verder buiten beschouwing gelaten.

36 Brief directeur gemeentebelastingen over gelekte persoonsgegevens aan getroffen burgers, 7 maart 2016.

37 Zie hiervoor ook paragraaf 3-4.

38 Collegebrief m.b.t. datalekken, 13 september 2016.

volgende paragraaf aan de orde, de interne evaluatie (voor zover relevant voor de onderzoeksvraag) in paragraaf 3-4.[39]

3-3 onderzoek datalek

Het college heeft het datalek afdoende technisch laten onderzoeken. Er is gekeken naar de aard, omvang, potentiële en daadwerkelijke consequenties van het datalek. Organisatorische aspecten zijn niet onderzocht.

Vast staat dat persoonsgegevens tijdelijk via het internet toegankelijk zijn geweest. Of er op het internet daadwerkelijk actieve raadplegingen hebben plaatsgevonden is op het moment van het datalek onduidelijk, maar de IBD schrijft hierover: “Het is volgens onze experts hoogst onwaarschijnlijk dat de gegevens benaderbaar zijn geweest zonder een zeer gerichte en specialistische zoekactie. Het zoeken naar een BSN-nummer zou hierbij niet voldoende zijn geweest.”

Om hierover meer duidelijkheid te krijgen heeft een gespecialiseerd bedrijf in opdracht van de gemeente nader onderzoek uitgevoerd. De rekenkamer heeft het geheime rapport van dit onderzoek ingezien, om vast te kunnen stellen of het college de oorzaak en gevolgen van het datalek afdoende heeft onderzocht. De aanpak en gebruikte techniek waren forensisch, dat wil zeggen gericht op het verzamelen van bewijzen van eventuele raadpleging van de persoonsgegevens. In de rapportage is stap voor stap de aanpak en uitkomst na te lezen.

Ten behoeve van het technisch onderzoek door het bureau zijn van de harde schijf en andere hardware forensische kopieën gemaakt. De hardware zelf is voorlopig beveiligd opgeslagen, in afwachting van vernietiging. Vervolgens zijn de harde schijf en de router van de medewerker onderzocht. Hierbij is nagegaan of de gegevens zijn geraadpleegd, door te zoeken naar sporen op het internet. Dat kon niet worden vastgesteld. Omdat niet kon worden vastgesteld of de gegevens extern zijn benaderd, kon ook niet worden vastgesteld door wie dat dan zou zijn gedaan. Volgens het onderzoeksbedrijf zijn de logging-gegevens[40] op de router die daarover mogelijk uitsluitsel hadden kunnen geven, verloren gegaan bij het dichten van het lek. Dit is, meteen nadat de veroorzaker van het datalek kennis had gekregen van het datalek, gebeurd door de uitschakeling van de router en de harde schijf.

Desgevraagd meldde het onderzoeksbureau aan de rekenkamer dat nadere inspectie van het interne geheugen van de router (door demontage) zinloos was, omdat de geheugenchip na onderbreking van de elektriciteitstoevoer niet direct extreem was gekoeld. Dit is noodzakelijk om de data op de chip te behouden. Het onderzoeksbureau ontving een router die al enige dagen niet van stroom was voorzien. Daarmee was de kans dat nog bruikbare loggegevens uitleesbaar waren, volgens het onderzoeksbureau nihil. De conclusie was al met al dat niet viel uit te sluiten dat de gegevens extern zijn geraadpleegd. Tegelijkertijd werd de kans daartoe door de IBD als zeer klein ingeschat, omdat alleen met heel gerichte zoektermen

39 Daarnaast is, zoals gebruikelijk in dit soort kwesties, een integriteitsonderzoek naar de betreffende medewerker verricht. Dat is hier verder buiten beschouwing gelaten.

40 Een registratie van de transacties in een systeem, zoals in een logboek.

iemand bij de gegevens zou kunnen komen. Er zijn geen voorvallen bekend waaruit blijkt dat de gegevens inderdaad extern zijn geraadpleegd.

identiteitsfraude
Van identiteitsfraude is sprake als iemand de identiteit van een ander voorwendt om hieraan financieel of ander voordeel te ontlenen. De persoonsgegevens die bij het datalek zijn vrijgekomen betreffen namen, adressen en BSN-nummers. Deze gegevens zijn in veel gevallen op zichzelf niet voldoende om identiteitsfraude mee te plegen. Als iemand erin slaagt deze gegevens te verrijken met andere persoonlijke informatie (bijvoorbeeld bankgegevens, emailadres etc.) van betrokkenen kan wel misbruik worden gepleegd. Een kwaadwillende kan dan bijvoorbeeld een uitkering op naam van iemand anders aanvragen of contracten afsluiten en aankopen doen onder een valse naam.

Het onderzoek van het externe bureau richtte zich op de technische aspecten van het datalek en niet op organisatorische aspecten, zoals de omstandigheden waardoor het datalek kon ontstaan. Dat behoorde niet tot de opdracht van de gemeente aan het bureau. De gemeente heeft hier ook zelf geen afzonderlijk onderzoek aan gewijd. Zij had evenwel kunnen onderzoeken of er bij de medewerkers voldoende “awareness” is wat betreft informatiebeveiliging. Het college startte, zoals aangegeven, wel een interne evaluatie naar de afhandeling van het datalek (zie paragraaf 3-4).

3-4 maatregelen naar aanleiding van datalek

Naar aanleiding van het datalek heeft het college enkele maatregelen genomen om soortgelijke datalekken in de toekomst te voorkomen. Getroffen maatregelen zijn vooral gericht op het creëren van bewustwording bij medewerkers (door middel van een brief). Technische maatregelen zijn niet genomen. In de communicatie aan de raad over de afhandeling van het datalek legt het college nadruk op reeds bestaande documenten en maatregelen en benoemt geen nieuwe maatregelen.

Na het bekend worden van het datalek, op 15 maart 2016, stuurde het college een brief aan de raad, waarin het aangaf welke beveiligingsmaatregelen waren getroffen. Het college verwijst daarbij naar een aantal generieke maatregelen en documenten, zoals het eind 2013 vastgestelde informatiebeveiligingsbeleid en het Meerjarenplan Concern Informatiebeveiliging. Het college verwijst in zijn brief ook naar voortgangs-rapportages over informatiebeveiliging. In aanvulling hierop worden nog enkele technische maatregelen genoemd, zoals ‘follow-me-printing’[41], het gebruik van tokens voor thuiswerken en dergelijke. Het betreft hier allemaal zaken met betrekking tot informatiebeveiliging die al van kracht waren. De opsomming betreft geen specifieke maatregelen die als reactie op het datalek zijn genomen ter voorkoming van toekomstige lekken. Ook is de gemeente niet nagegaan of kwetsbaarheden voorkomen die vergelijkbaar zijn met de oorzaken van het datalek.

Maatregelen die wél zijn genomen om soortgelijke datalekken in de toekomst te voorkomen, betreffen vooral de sociale kant van informatiebeveiliging, namelijk houding en gedrag van de medewerkers. Zo heeft het college op 8 april 2016 aan alle ambtenaren een brief met uitleg over gegevensbescherming en het belang van

41 Follow me printing houdt onder meer in dat de printer pas afdrukt na identificatie door de gebruiker.

informatiebeveiliging gestuurd. Daarbij is gewezen op de geldende protocollen en procedures. Ook hebben alle leidinggevenden een e-mail ontvangen met het verzoek informatiebeveiliging aandacht te geven binnen hun afdeling. Verder is op de gemeentelijke intranetsite RIO aandacht het datalek geschonken, waarbij op het belang van informatiebeveiliging wordt gewezen. De directeur Gemeentebelastingen heeft in maart 2016 een mail heeft verstuurd aan alle medewerkers. Hierin zijn de medewerkers geïnformeerd en verzocht te controleren of zij privacy gevoelige gegevens op privé apparatuur of opslagmedia hadden staan. Ook de extern ingehuurde medewerkers zijn benaderd om dit te controleren en zo nodig te verwijderen. Daarnaast is door de ICT afdeling van Gemeentebelastingen een verplichte workshop gegeven aan alle medewerkers waarin alle concernregels, risico's en maatregelen zijn uitgelegd. Verder zijn er binnen het cluster Dienstverlening enkele lezingen gegeven om het Datalek onder de aandacht te brengen van het management. Voorts treffen de Informatie Security Officers voorbereidingen voor een zogeheten ‘awareness programma’. Hoewel dit laatste niet zozeer naar aanleiding van het datalek is opgezet, is de urgentie ervan met het datalek wel toegenomen.

Een technische maatregel die genomen is betreft het invoeren van Mobile Application Management, waardoor op mobiele apparaten een afgeschermd gedeelte komt, zodat de gemeente het mobiele apparaat op afstand kan bedienen en beheren, zonder privé informatie te wissen. Deze maatregel is niet specifiek naar aanleiding van het datalek getroffen, maar draagt wel effectief bij aan informatiebeveiliging.

De gemeente is niet nagegaan hoe groot de kans is dat een datalek zoals bij gemeentebelastingen in de toekomst nog een keer voor zal komen. Er is bijvoorbeeld niet nagegaan of er vaker testgegevens door medewerkers mee naar huis zijn genomen. Dat opnieuw een datalek zal ontstaan via een privé-opslagmedium dat aan het internet wordt verbonden, valt niet uit te sluiten. De gemeente heeft naar aanleiding van het datalek echter geen specifieke technische maatregelen genomen om dit te voorkomen. Een beveiligingsmaatregel die de gemeente bijvoorbeeld had kunnen nemen is dat technisch wordt afgedwongen dat medewerkers gegevens moeten classificeren, bijvoorbeeld bij het aanmaken van een document. Als data als vertrouwelijk zijn geclassificeerd, kan technisch worden ingeregeld wat er met deze data is toegestaan (bijvoorbeeld alleen lezen na invoer van een wachtwoord, verhinderen dat de data wordt geprint, gekopieerd of verzonden etc.).

evaluatie afhandeling datalek

Zoals in paragraaf 3-3 werd opgemerkt heeft de gemeente naar aanleiding van de gang van zaken gedurende het datalek een interne evaluatie uitgevoerd. Daaruit is bekend hoeveel en wat voor soort vragen er door burgers zijn gesteld. Er zijn geen schadeverzoeken ingediend. In het evaluatierapport wordt verder geconcludeerd dat het Protocol Melding Datalekken in de praktijk toepasbaar is. In het evaluatierapport staan ook aanbevelingen voor verbetering. De belangrijkste zijn de volgende:

- Het gebruikte protocol Meldplicht Datalekken is gericht op het doen van een melding. Het protocol biedt nog geen handvatten hoe te handelen nadat de melding is gedaan. Daarom dient het protocol uitgebreid te worden met een paragraaf “Dichtplicht datalekken” waarin de stappen na de melding benoemd worden.
- Opstellen van scenario’s van verschillende soorten datalek-incidenten.
- Borg advisering van deskundigen op het gebied van communicatie en juridische zaken.

4 risicoanalyse

4-1 inleiding

In dit hoofdstuk beoordeelt de rekenkamer de wijze waarop de gemeente Rotterdam risico's op het gebied van informatiebeveiliging beheerst. Daarmee wordt een antwoord gegeven op de volgende onderzoeksvraag:

Heeft de gemeente Rotterdam in brede zin een goed beeld van de belangrijkste risico's op het gebied van informatiebeveiliging en in het bijzonder gevoelige informatie zoals (bijzondere) persoonsgegevens?

Bij de beantwoording van deze vraag hanteert de rekenkamer normen, die in de onderstaande tabel staan weergegeven.

tabel 4-1: normen en criteria risicoanalyse

normen	criteria	paragraaf
op concernniveau en binnen de individuele clusters worden met voldoende frequentie risicoanalyses en/of dreigingsanalyses gemaakt. In de risicoanalyses en/of dreigingsanalyses zijn de belangrijkste risico's geïdentificeerd	• het uitvoeren van risicoanalyses is onderdeel van het informatiebeveiligingsbeleid	4-2 en 4-3
	• het informatiebeveiligingsbeleid (of een aanvullend document) schrijft voor op welke momenten en op welke wijze risicoanalyses uitgevoerd moeten worden	4-3-1
	• op concernniveau worden periodiek de gemeentebrede risico's op het gebied van informatiebeveiliging en het beheer van vertrouwelijke informatie in kaart gebracht	4-3-1
	• ieder cluster brengt periodiek de specifieke risico's voor het cluster in kaart op het gebied van informatiebeveiliging en het beheer van vertrouwelijke informatie	4-3-1
	• risicoanalyses worden met passende frequentie herhaald	4-3-1
de risicoanalyses en/of dreigingsanalyses geven inzicht in specifieke risico's m.b.t. het beheer van (bijzondere) persoonsgegevens	• er bestaat per cluster inzicht in welke (bijzondere) persoonsgegevens worden vastgelegd en bewerkt	4-3-2
	• concernbreed zijn risico's ten aanzien van het beheer van (bijzondere) persoonsgegevens in kaart gebracht	4-3-2
	• binnen de clusters zijn risico's ten aanzien van het beheer van (bijzondere) persoonsgegevens benoemd in risicoanalyses	4-3-2

In de volgende paragraaf wordt de risk-based aanpak van het informatiebeveiligingsbeleid toegelicht (paragraaf 4-2). Vervolgens wordt ingegaan op risicoanalyse en dataclassificatie (paragraaf 4-3).

4-2 risk-based informatiebeveiligingsbeleid

Zoals reeds aan de orde is geweest in hoofdstuk 2, gaat het concern IB-beleid uit van een risk based aanpak: beveiligingsmaatregelen worden getroffen op basis van risicoanalyse. De te nemen beveiligingsmaatregelen moeten volgens het concern IB-beleid worden afgestemd op de risico's. Naarmate gegevens een vertrouwelijker karakter hebben, of gezien de context waarin ze gebruikt worden een groter risicoprofiel kennen, dienen zwaardere eisen aan de beveiliging te worden gesteld.[42] De baseline DIA gaat uit van eenzelfde risicobenadering: bij het ontwerp, de selectie of de ontwikkeling van nieuwe informatiesystemen worden de benodigde beveiligingseisen op basis van een risicoanalyse vastgesteld.

In het concern IB-beleid is bepaald dat proceseigenaren de kwetsbaarheid van hun werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident moeten inventariseren. Daarbij moeten ze rekening houden met de beschermingseisen van de informatie die in het proces omgaat.[43] De beschermingseisen volgen uit het classificatieniveau (geen – laag – midden – hoog) dat op grond van de dataclassificatie moet worden toegekend. Vervolgens moet de proceseigenaar een inschatting maken van de kans dat een beveiligingsincident zich voordoet en de impact daarvan op het werkproces (risico = kans x impact). Aan de hand van de uitkomsten van de risicoanalyse moet de proceseigenaar vervolgens bepalen welke beveiligingsmaatregelen nodig zijn. In het informatiebeveiligingsbeleid is niet aangegeven met welke frequentie de proceseigenaren een risicoanalyse moeten opstellen. Het is gebruikelijk dit van tijd tot tijd te evalueren en aan te passen.

In de volgende paragrafen komt aan de orde in welke mate en op welke wijze risicoanalyses en dataclassificaties in de praktijk worden uitgevoerd binnen de verschillende clusters en op concernniveau. Daarbij wordt specifiek ingegaan op de wijze waarop de clusters inzicht krijgen in risico's ten aanzien van het beheer van (bijzondere) persoonsgegevens.

4-3 risicoanalyse en dataclassificatie

Het beleid schrijft een risico gestuurde informatiebeveiliging voor. Noch op concernniveau, noch binnen alle clusters worden risicoanalyses, dataclassificaties en privacy impact assessments structureel en kwalitatief goed uitgevoerd. Evenmin heeft de gemeente een overzicht van alle processen waarin (gevoelige) persoonsgegevens worden verwerkt. Door het ontbreken van deze inzichten en overzichten is de gemeente niet in staat op basis van geïdentificeerde risico's en de inschatting van kans en impact te bepalen welke beveiligingsmaatregelen genomen moeten worden.

42 Gemeente Rotterdam, 'concern informatiebeveiligingsbeleid', december 2013, pag. 11.

43 Gemeente Rotterdam, 'concern informatiebeveiligingsbeleid', december 2013, pag. 11.

4-3-1 risicoanalyse

Op concernniveau is geen sprake van een gestructureerd proces van risicoanalyse. Concernbrede risico's op het gebied van informatiebeveiliging worden niet periodiek geïdentificeerd en gekwantificeerd in termen van kans en impact. In het meerjarenplan informatiebeveiliging 2015-2017 is wel een beschrijving opgenomen van risico's. Deze zijn weergegeven in onderstaand groen kader. De rekenkamer merkt op dat in deze opsomming niet alleen risico's zijn vermeld, maar soms ook maatregelen zijn benoemd. Daarnaast constateert de rekenkamer dat de benoemde risico's niet zijn gekwantificeerd in termen van kans en impact.

in meerjarenplan informatiebeveiliging 2015-2017 genoemde risico's

- Taken en verantwoordelijkheden worden onvoldoende ingevuld.
- Aanpak is incident gedreven en niet gericht op continue verbetering.
- Er is onvoldoende sturing op naleving. Rotterdam is niet in control.
- Niet voldoen aan wetgeving schaadt rechten van burgers en bedrijven, ons vertrouwen en wordt (in de toekomst) zeer zwaar gesanctioneerd.
- Incidenten verdwijnen 'onder de radar', risico's worden onvoldoende beheerst.
- Een cyclische aanpak van IB is randvoorwaardelijk voor goede control en professionele verantwoording. De druk op dit laatste neemt toe met de komst van nieuwe normenkaders en wetgeving.
- Goede rapportage is randvoorwaardelijk voor sturen en bijsturen.
- Onvoldoende risicobewustzijn verhoogt de kans op incidenten, zoals verlies van (gevoelige) data, mogelijk zonder dat wij het weten.
- Onvoldoende control bij calamiteiten: uitval van kritische bedrijfsfuncties, personeel.
- Zonder goede control is geen goede verantwoording mogelijk, dit schaadt vertrouwen en kan (zwaar) worden gesanctioneerd.
- Het ontbreken van logging belemmert het kunnen herleiden van incidenten. Monitoring is essentieel voor detectie: zonder dat blijven incidenten 'onder de radar'.
- Het ontbreken van generieke beveiligingsniveaus vergroot de complexiteit en beheerlast. Incidenten blijven onopgemerkt.
- Zonder management van (onbeheerde) mobiele apparatuur is gemeentelijke informatie relatief onbeschermd.
- Kwetsbaarheden in software vormen een groot risico. Privacygevoelige informatie kan worden gecompromitteerd met verstrekkende gevolgen (imagoschade, claims, aangifte).
- Structureel testen reduceert risico's aanzienlijk.

Ook bevat het meerjarenplan een overzicht van dreigingen (zie onderstaande tabel). Deze dreigingen zijn afgeleid uit een dreigingsanalyse van de Nationaal Coördinator Terrorismebestrijding en Veiligheid. De rekenkamer merkt hierbij op dat de dreigingen in algemene termen zijn benoemd en niet zijn gespecificeerd naar de Rotterdamse situatie. Eveneens ontbreekt een inschatting van kans en impact.

Zoals in hoofdstuk 2 reeds is vermeld, is op concernniveau ook geen actuele classificatie beschikbaar van de data die omgaan in de applicaties die binnen het concern worden gebruikt. Het meest actuele overzicht dat de rekenkamer heeft aangetroffen dateert uit september 2013. In dit overzicht zijn circa 300 van de 785 applicaties die de gemeente in gebruik heeft, geclassificeerd op beschikbaarheid,

integriteit en vertrouwelijkheid (BIV-aspecten). Betrokkenen konden niet aangeven wat er met deze classificaties is gedaan.[44]

figuur 4-1: dreigingen benoemd in meerjarenplan IB-beleid

Actor	Dreiging voor Rotterdam	Weerbaarheid nu	Weerbaarheid ambitie
Beroepscriminelen	Verstoring ICT	Midden	Midden
	Diefstal en publicatie of verkoop van informatie	Laag	Midden
	Manipulatie van informatie	Laag	Laag
	Overname ICT	Midden	Midden
Staten	Digitale Spionage	Laag	Midden
	Offensieve cybercapaciteiten	Laag	Laag
Terroristen	Verstoring/overname ICT	Laag	Laag
Cybervandalen	Diefstal informatie	Hoog	Hoog
	Verstoring ICT	Midden	Hoog
Cyberonderzoekers	Verkrijging en publicatie van informatie	Midden	Hoog
Hacktivisten	Verstoring ICT	Midden	Hoog
	Diefstal en publicatie verkregen informatie	Midden	Midden
	Defacement	Midden	Midden
	Overname ICT	Midden	Midden
Interne actoren (bewust)	Diefstal en publicatie of verkoop verkregen informatie	Laag	Hoog
	Verstoring ICT	Laag	Midden
Intern (niet bewust)	Verstoring ICT (malware/spam)	Hoog	Hoog
	Verstoring ICT online diensten	Midden	Hoog
	Onbewust gegevens lekken	Laag	Hoog
Private organisaties	Verkrijging van informatie	Midden	Midden
Geen actor	Uitval ICT	Midden	Midden

bron: gemeente Rotterdam, 'Meerjarenplan informatiebeveiliging'.

risicoanalyse clusters

Ook in de gemeentelijke clusters worden de risico's ten aanzien van informatiebeveiliging niet gestructureerd in kaart gebracht. Risicoanalyse vindt in de clusters alleen incidenteel plaats, voornamelijk wanneer sprake is van een aanvraag voor een externe verbinding of bij het in gebruik nemen van nieuwe systemen of applicaties. Betrokkenen zijn zich in het algemeen wel bewust van potentiële risico's. Behalve het cluster W&I, kon geen enkel cluster in het kader van dit onderzoek een totaaloverzicht aanleveren van de risicoanalyses die ten aanzien van informatiebeveiliging zijn opgesteld.

In het kader van het opstellen van informatiebeheerplannen voor de clusters zijn de afgelopen jaren diverse processen geclassificeerd op de BIV-aspecten van informatiebeveiliging. Hierbij is echter geen gebruik gemaakt van de methode die de dataclassificatie in de component architectuur informatiebeveiliging voorschrijft. Onduidelijk is wat de scores die bij deze classificatie zijn toegekend aan de BIV-aspecten betekenen en wat er met de uitkomsten van deze classificatie is gedaan. De rekenkamer heeft in het kader van dit onderzoek geen voorbeelden aangetroffen van dataclassificaties die zijn uitgevoerd, zoals voorgeschreven in het concern IB-beleid en de component architectuur informatiebeveiliging.[45]

44 In ambtelijk wederhoor is onder meer aangegeven dat de classificatietabel onder andere is gebruikt om aan het Management Team van IIFO de noodzaak van netwerksegmentatie te laten zien. Ook is de classificatie van de applicaties opgenomen in Planon. Dit stelt beheerders in staat bij incidenten en wijzigingen op applicaties direct te zien wat de gevoeligheid is en kunnen hun gedrag aanpassen.

45 Tijdens de uitvoering van het onderzoek heeft de rekenkamer gevraagd naar dataclassificaties. De ontvangen voorbeelden waren vaak onvolledig ingevuld. In het ambtelijk wederhoor heeft de rekenkamer één ander voorbeeld ontvangen. Ook deze was niet volledig omdat in de managementsamenvatting de belangrijkste conclusies, aanbevelingen en risico's niet zijn benoemd.

4-3-2 risicoanalyses t.a.v. bescherming van persoonsgegevens

Eén van de hoofdprincipes van informatiebeveiliging is vertrouwelijkheid. Dit is in het bijzonder van belang bij (bijzondere) persoonsgegevens. Een voorwaarde om goed inzicht te krijgen in de risico's ten aanzien van het beschermen van (bijzondere) persoonsgegevens, is dat er overzicht bestaat van alle processen en/of systemen waarin (bijzondere) persoonsgegevens omgaan. Dit overzicht is zowel op concernniveau als binnen de verschillende clusters niet aanwezig. In 2016 is het cluster MO in dit verband wel gestart met een nulmeting, waarin alle processen waarin persoonsgegevens worden verwerkt in kaart worden gebracht.

Een Privacy Impact Assessment (PIA) is een instrument om risico's ten aanzien van het beheer van privacygevoelige informatie inzichtelijk te maken. Hoewel de hoeveelheid privacygevoelige informatie die de clusters in beheer hebben de afgelopen jaren sterk is gegroeid, worden nog nauwelijks PIA's uitgevoerd. Vooralsnog hebben alleen de clusters MO en W&I op zeer beperkte schaal gebruik gemaakt van dit instrument. In het informatiebeveiligingsbeleid 2013-2014 van het cluster W&I is wel opgenomen dat altijd een PIA moet worden uitgevoerd bij de aanschaf van nieuwe informatiesystemen, maar in de praktijk wordt hieraan nog nauwelijks invulling gegeven.[46]

46 Interview, 22 juli 2016.

5 beveiligingsmaatregelen

5-1 inleiding

In dit hoofdstuk beoordeelt de rekenkamer de beveiligingsmaatregelen die de gemeente heeft getroffen en de wijze waarop de gemeente Rotterdam risico's op het gebied van informatiebeveiliging beheerst. Daarmee wordt een antwoord gegeven op de volgende onderzoeksvraag:

Heeft de gemeente Rotterdam voldoende maatregelen getroffen om gevoelige informatie te beschermen tegen de belangrijkste veiligheidsrisico's?

Bij de beantwoording van de onderzoeksvraag hanteert de rekenkamer de onderstaande normen.

tabel 5-1: normen en criteria beveiligingsmaatregelen

normen	criteria	paragraaf
De gemeente heeft maatregelen getroffen die de risico's doen afnemen. Het totaal aan maatregelen geeft voldoende waarborgen voor een goede bescherming van de (bijzondere) persoonsgegevens die de gemeente in beheer heeft.	• De gemeente heeft technische maatregelen genomen.	5-2
	• De gemeente heeft organisatorische maatregelen genomen.	5-2
	• De getroffen maatregelen vloeien logisch voort uit uitgevoerde risicoanalyses.	5-2 en 5-3
	• In ieder geval de belangrijkste risico's zijn voorzien van beveiligingsmaatregelen.	5-2 en 5-3
	• Persoonsgegevens in de onderzochte applicaties zijn goed beveiligd.	5-3

De volgende paragraaf gaat in op maatregelen die gemeente heeft genomen in het kader van informatiebeveiliging. Daarna richt de rekenkamer zich op vijf specifieke applicaties, zogeheten 'kroonjuwelen' waarin (bijzondere) persoonsgegevens worden verwerkt. In die gevallen zal de rekenkamer op acht aspecten beoordelen of de informatiebeveiliging op orde is.

5-2 maatregelen op basis van risicoanalyse

Omdat de gemeente onvoldoende risicoanalyses ten aanzien van informatiebeveiliging heeft gemaakt, ontbreekt de koppeling tussen risico's en getroffen beveiligingsmaatregelen. Er zijn zowel technische als organisatorische beveiligingsmaatregelen getroffen. Van de beveiligingsmaatregelen die zijn genomen, is niet volledig vast te stellen of deze gelet op beveiligingsrisico's effectief zijn.

In hoofdstuk 4 is vastgesteld dat de gemeente haar beleidsvoornemen om risico-gebaseerd beveiligingsmaatregelen te treffen, niet toepast. Omdat het op concernniveau en binnen de clusters ontbreekt aan voldoende risicoanalyses, dataclassificaties en privacy impact assessments, ontbreekt de koppeling tussen risico's en de getroffen maatregelen. Dit laat onverlet er binnen de gemeente allerlei maatregelen zijn genomen om informatie te beveiligen. In hoofdstuk 2 en 3 staan voorbeelden van organisatorische maatregelen. Deze zijn onder meer in navolging van de BIG (Baseline Informatiebeveiliging Gemeenten) genomen.

Daarnaast zijn er tal van technische maatregelen getroffen. Deze maatregelen dragen onmiskenbaar bij aan effectieve informatiebeveiliging. Deze maatregelen vloeien niet direct voort uit een risicoanalyse. Voorbeelden zijn:

- toekenning van uniek gebruikersaccount, beveiligd met wachtwoord dat aan kwaliteitseisen moet voldoen;
- beveiliging van het gemeentelijk netwerk met firewalls;
- inrichting van een veilige werkplek met virusscanners;
- de mogelijkheid om gegevens op telefoons op afstand te wissen;
- verlenen van toegang tot gebouwen met persoonsgebonden pasjes;
- beveiligde en geklimatiseerde ruimte voor computerapparatuur met brandveilige wanden.

Omdat risico's niet systematisch in kaart zijn gebracht, is niet goed te beoordelen of altijd de juiste maatregelen zijn genomen. Ook is onduidelijk hoe de kosten van de maatregelen zich verhouden tot de risico's.

De gemeente kon geen overzicht geven van de mate waarin de technische maatregelen uit de Baseline DIA (zie paragraaf 2-2-3) daadwerkelijk zijn geïmplementeerd. Tijdens interviews is opgemerkt dat er geen verslag wordt opgemaakt van de afgeronde zaken in het licht van de Baseline omdat het aan capaciteit ontbreekt. De rekenkamer heeft hierdoor geen beeld gekregen van het totale pakket aan beveiligingsmaatregelen dat in werking is. Wel is duidelijk dat niet alle maatregelen uit de baseline effectief worden toegepast. Onderstaand kader geeft hiervan een voorbeeld.

voorbeeld niet effectief toegepaste beveiligingsmaatregel

Een beveiligingsmaatregel is dat gebruikers van systemen hun wachtwoord regelmatig moeten wijzigen. Er bestaat de technische mogelijkheid om af te dwingen dat wachtwoorden voor kritische functies vaker moeten worden gewijzigd en dat deze wachtwoorden een zekere complexiteit kennen. In praktijk wordt dit onderscheid tussen 'gewone' en 'sensitieve' gebruikers binnen de gemeente niet gemaakt. Dit doet afbreuk aan de potentiële effectiviteit van de beveiligingsmaatregel.

Voorgaande was aanleiding om een selectie van applicaties te maken waarin vertrouwelijke gegevens worden verwerkt. Bij deze 'kroonjuwelen' heeft de rekenkamer de beveiliging onderzocht. Hiermee beoogt de rekenkamer een beeld te geven van de effectiviteit van de beveiliging van deze applicaties.

5-3 informatiebeveiliging 'kroonjuwelen'

De beveiliging van vijf applicaties is beoordeeld op acht verschillende aspecten.

Bij twee applicaties ontbreekt een service level agreement (SLA). Slechts bij één applicatie is informatiebeveiliging een onderwerp in de SLA. Over de bestaande SLA's is niet gerapporteerd. Wel zijn bij twee applicaties rapportages in ontwikkeling. Bij deze applicaties bestaat duidelijk aandacht voor de beveiliging.

Back-up procedures zijn bij alle applicaties in orde. Wel bestaat bij twee applicaties die door externe partijen worden gehost een groter risico op ongecontroleerde raadpleging door derden. Alle applicaties hebben de functionaliteit om rechten toe te kennen op basis van rollen die zijn afgeleid van de functies van medewerkers. De mate waarin (periodiek) toezicht wordt gehouden op de juiste toekenning van autorisaties verschilt.

Bij twee van de vijf applicaties wordt het eigenaarschap van de applicatie en de data betekenisvol ingevuld door het management. Bij de overige applicaties ontbreekt het aan actief toezicht op de beveiliging en het beheer van gegevens.

Bij geen van de applicaties is een recente risicoanalyse van voldoende kwaliteit aangetroffen. Bij twee applicaties is echter wel sprake van een goed risicobewustzijn bij betrokken management en medewerkers en zijn risico's inzichtelijk gemaakt via self-assessments of audits.

Onafhankelijke assurance over de kwaliteit van de dienstverlening rond het technisch beheer van de applicaties ontbreekt bij alle applicaties.

Slechts bij twee applicaties wordt bij testwerkzaamheden gebruikgemaakt van geanonimiseerde data.

5-3-1 selectie 'kroonjuwelen'

De rekenkamer heeft in het kader van dit onderzoek de beveiliging beoordeeld van een aantal applicaties waarin de gemeente (bijzondere) persoonsgegevens verwerkt of opslaat. Omdat de clusters geen totaaloverzicht konden verstrekken van de applicaties die zij gebruiken waarin (bijzondere) persoonsgegevens omgaan, heeft de rekenkamer uiteindelijk een selectie gemaakt op basis van een overzicht dat is ontvangen van de afdeling ICT-beheer. In dit overzicht zijn de applicaties opgenomen die de clusters als vitaal voor hun bedrijfsvoering hebben aangemerkt; verstoring van deze applicaties is in hoge mate onwenselijk. Uit dit overzicht van vitale applicaties heeft de rekenkamer de belangrijkste applicaties geselecteerd waarin (bijzondere) persoonsgegevens worden verwerkt en die in die zin beschouwd kunnen worden als 'kroonjuwelen' van de gemeente. In deze systemen worden grote hoeveelheden persoonsgegevens opgeslagen, zoals zorg-, inkomens-, detentie- en naw-gegevens. Deze systemen zijn door honderden medewerkers raadpleegbaar.

Tabel 5-2 geeft een overzicht van de uitkomsten van de beoordeling van de applicaties op verschillende beveiligingsaspecten, die later in deze paragraaf nader worden toegelicht. Hierbij worden tevens de bevindingen gepresenteerd die uit de beoordeling van de rekenkamer naar voren zijn gekomen.

De legenda bij tabel 5-2 is:
- rood: beveiliging is niet op niveau;
- oranje: beveiliging is gedeeltelijk op niveau;

- groen: beveiliging is grotendeels op niveau.

tabel 5-2: overzicht beveiligingsaspecten informatiebeveiliging kroonjuwelen

applicatie	service level agreement (SLA)	backups	gebruikers-management	eigenaar-schap	incident management	risico-management	onafhankelijke assurance	anoniem testen
A								
B								
C								
D								
E								

5-3-2 service level agreement (SLA)

Service level agreements zijn dienstverleningsovereenkomsten tussen de gebruiker van de applicatie (de clusters) en de organisatie die de applicatie aanbiedt en beheert (het cluster BCO of externe leveranciers). In deze overeenkomst zijn bijvoorbeeld afspraken vastgelegd over beschikbaarheid van de applicatie, afhandeling van wijzigingsverzoeken, responsetijd[47] en dergelijke. De rekenkamer heeft ten aanzien van de geselecteerde applicaties onderzocht of er SLA's zijn afgesloten en zo ja, of het naleven van het gemeentelijke IB-beleid en melden van beveiligingsincidenten onderdeel uitmaken van de afspraken in de SLA's. Ook is de rekenkamer nagegaan of in het kader van de SLA's verantwoording wordt afgelegd over de naleving van het IB-beleid en beveiligingsincidenten die hebben plaatsgevonden.

Het risico van het ontbreken van informatiebeveiliging als onderwerp in de SLA is dat afspraken rond de beveiliging van een applicatie niet duidelijk zijn en er wanneer rapportages ontbreken geen inzicht is bij de gebruiker in de mate waarin het IB-beleid wordt nageleefd door de organisatie die de applicatie levert.

Bij B en A is geen SLA aangetroffen, niet van de applicatie als geheel noch van beveiligingsaspecten. Daardoor is niet goed na te gaan of en hoe de eigenaar van de applicatie (het management) zicht heeft op de prestaties in het algemeen en van beveiligingsaspecten in het bijzonder. Daarom is de beoordeling op dit aspect 'niet op niveau'.

Voor de applicatie E bestaat er een SLA. Hiervan maakt beveiliging geen deel uit. Over de uitvoering van de afspraken in de SLA wordt niet gerapporteerd. Ook deze applicatie is op dit aspect daarom niet op niveau.

Voor Dis er een service level overeenkomst afgesloten met IIFO. Hier is beveiliging geen apart onderwerp. De rapportages zijn in ontwikkeling. Bij C is er een SLA opgesteld waarin aandacht is voor beveiliging. Er zijn afspraken opgenomen over periodieke rapportages. Omdat de applicatie nog maar kort in productie is zijn er nog geen rapportages uitgebracht. Bij D en C bleek duidelijk interesse in en bemoeienis met het wel en wee van de applicatie vanuit het management. Uit de gesprekken die in het kader van dit onderzoek zijn gevoerd en ontvangen documentatie bleek

47 De tijd die een applicatie, computer, server, helpdesk of iets anders nodig heeft om te reageren op een actie van een gebruiker.

bijvoorbeeld betrokkenheid bij de inrichting, verificatie van de maatregelen en overleg over incidenten. Daarom is de beoordeling: beheersing is gedeeltelijk op niveau.

5-3-3 back-ups

Ten aanzien van het aspect 'back-ups' beperkt de beoordeling van de rekenkamer zich tot de mate waarin back-ups veilig worden uitgevoerd en geborgd is dat onbevoegden geen toegang hebben op de data die in de back-ups is opgeslagen. De rekenkamer heeft andere aspecten die samenhangen met het maken van back-ups, zoals het (oefenen) van uitwijk bij calamiteiten, niet beoordeeld.

Gebruikelijk is dat van de data in systemen en applicaties periodiek (bijv. dagelijks of wekelijks) een kopie in de vorm van een back-up wordt gemaakt. Als gegevens kwijt raken of een database corrupt raakt, kan de meest recente back-up worden teruggeplaatst zodat zo min mogelijk data verloren gaat. Om de vertrouwelijkheid van gegevens te borgen is het noodzakelijk dat rond het maken van back-ups passende beveiligingsmaatregelen worden genomen. Er moet geen onbeperkte toegang tot de back-ups zijn, de back-ups moeten beschermd worden opgeslagen en het terugzetten van kopieën dient gecontroleerd plaats te vinden.

Het risico in relatie tot informatiebeveiliging is dat via back-ups vertrouwelijke gegevens onbedoeld toegankelijk zijn voor ongeautoriseerde personen.

Volgens de functioneel beheerders van alle beoordeelde applicaties worden er periodiek back-ups gemaakt, die veilig worden opgeslagen en die alleen volgens bepaalde procedures kunnen worden opgevraagd. Omdat C en E dit proces hebben uitbesteed acht de rekenkamer het risico op raadpleging door derden bij deze applicaties relevant. Zoals in paragraaf 5-3-7 aan de orde zal komen, ontbreken onafhankelijke assurance-verklaringen. Daarom beoordeelt de rekenkamer C en E op het aspect back-ups als 'gedeeltelijk op niveau'.

5-3-4 gebruikersmanagement

Bij gebruikersmanagement gaat het om het aanmaken, wijzigen en verwijderen van gebruikersaccounts, verleende autorisaties en wachtwoorden. De beheersing van dit aspect is van groot belang om geautoriseerde toegang tot applicaties te faciliteren en misbruik in de vorm van ongeautoriseerde toegang tegen te gaan. De rekenkamer is bij de geselecteerde applicaties het proces van het aanmaken van nieuwe accounts, het verlenen van toegang tot gegevens in de applicaties, wijzigingen van autorisaties (bijvoorbeeld bij verandering van functie) en het afsluiten van accounts nagegaan. Belangrijk hierbij is bijvoorbeeld dat een gebruikersaccount uniek en persoonsgebonden is, wachtwoorden niet te eenvoudig zijn, er een periodieke verplichting tot het wijzigen van het wachtwoord is en mutaties in autorisaties worden gelogd (wie wijzigt wat op welk moment). Ook is de rekenkamer nagegaan of het management toezicht houdt op het geautoriseerd gebruik van applicaties, bijvoorbeeld door na te gaan of de functioneel beheerders hun werkzaamheden op dit terrein naar behoren uitvoeren en te checken of iedereen die toegang tot een applicatie heeft daadwerkelijk in dienst is.

Wanneer het gebruikersmanagement niet adequaat wordt uitgevoerd, bestaat het risico dat er gebruikers zijn die onterecht geautoriseerd zijn en daardoor onterecht toegang hebben tot vertrouwelijke gegevens.

De onderzochte applicaties hebben allemaal de functionaliteit om verfijnde autorisaties toe te kennen; er kan bijvoorbeeld onderscheid gemaakt worden tussen autorisaties waarbij alleen gegevens in de applicatie geraadpleegd mogen worden of autorisaties waarbij gegevens in de applicatie ingevoerd, gewijzigd of verwijderd kunnen worden. Zo ontstaan rollen die bestaan uit een stapeling van rechten binnen een applicatie. Een rol kan bestaan uit meer dan honderd specifieke rechten. Hierdoor is het beheer een omvangrijke taak.

De rekenkamer neemt tussen de applicaties verschillen waar in de wijze waarop het beheer wordt uitgevoerd. Bij de applicatie B is bijvoorbeeld enige vervuiling van rechten ontstaan door achterstallig onderhoud. Bij de applicaties A, C en D bestaat veel aandacht voor de juistheid van autorisaties. Van tijd tot tijd wordt de juistheid en volledigheid van toegekende autorisaties voorgelegd aan (afdelings-)managers met het verzoek deze kritisch te beschouwen en de juistheid te bevestigen. Daarom beoordelen we deze applicaties op dit aspect als veilig. Deze controle ziet de rekenkamer niet bij E en B. Het management houdt bij deze applicaties geen toezicht op de juistheid van toegekende autorisaties.

De mogelijkheid bestaat om hoge eisen te stellen aan de kwaliteit van wachtwoorden, zodat ze moeilijk te raden zijn. De bestaande praktijk bij de een deel van de onderzochte applicaties is dat er beperkt gebruik wordt gemaakt van de technische mogelijkheden die op de punt bestaan. Bij C en D worden behoorlijke eisen gesteld aan de complexiteit van de wachtwoorden, maar bij de andere applicaties is dit niet het geval. De frequentie waarmee gebruikers hun wachtwoord verplicht moeten veranderen beloopt bij de onderzochte applicaties in de regel een te korte periode voor applicaties waarin vertrouwelijke gegevens worden verwerkt.

Een goede praktijk heeft de rekenkamer gezien bij D, waar failed logons werden opgemerkt (bijvoorbeeld als herhaaldelijk een verkeerd wachtwoord wordt geprobeerd bij een poging tot braak). Dit bleek tijdens de hack uitgevoerd door een gespecialiseerd bureau. Bij de andere applicaties wordt bij onterechte (hack-)pogingen tot toegang automatisch het account geblokkeerd. Dit wordt niet structureel gemonitord en het management wordt hierover niet geïnformeerd.

5-3-5 eigenaarschap

In algemene zin merkt de rekenkamer op dat de informatie over wie de eigenaren van de onderzochte ‘kroonjuwelen’ zijn, niet altijd up-to-date bleek. De ambtenaren die bij technisch beheer stonden geregistreerd als eigenaar van een applicatie, bleken in de praktijk die rol niet te vervullen, bijvoorbeeld omdat ze van functie waren veranderd. Dit brengt het risico met zich mee dat in het geval zich een incident of een verstoring voordoet, technisch beheer niet direct in contact kan treden met de eigenaar van de applicatie.

In het kader van informatiebeveiliging en de bescherming van (bijzondere) persoonsgegevens is het van belang dat het eigenaarschap ten aanzien van de data in een applicatie betekenisvol wordt ingevuld. De eigenaar dient zicht te hebben op de getroffen beveiligingsmaatregelen en dient zich te (laten) informeren over de werking van deze maatregelen en incidenten die zich hebben voorgedaan.

Het risico van geen of gedeeld eigenaarschap van gegevens is dat bij beveiligingsincidenten onduidelijk is wie waarvoor verantwoordelijk is en dat

(daardoor) onvolledige of onjuiste maatregelen zijn getroffen ten aanzien van de beveiliging.

De rekenkamer heeft geen betekenisvol eigenaarschap aangetroffen bij B, A en E. De managers of directeuren van de clusters waar vertrouwelijke informatie wordt verwerkt zijn de eigenaren van de data. Deze verklaarden echter niet te weten of en welke passende beveiligingsmaatregelen zijn getroffen. Er werd verwezen naar de functioneel beheerder of de informatieadviseur. Actief toezicht op de functioneel beheerders door leidinggevenden ontbrak. Of de beveiligingsmaatregelen effectief zijn en passend voor het gewenste niveau van vertrouwelijkheid wordt niet van tijd tot tijd door het management geëvalueerd – er bestaat een impliciet vertrouwen in. Daarom is de beveiliging bij B en E op dit aspect als onvoldoende beoordeeld. Voor A bestaat enige compensatie voor het gebrek aan managementaandacht door de consciëntieuze zorg voor informatiebeveiliging door de functioneel beheerders. Daarom is bij deze applicatie de beveiliging gedeeltelijk op niveau op dit aspect.

Bij C wordt het eigenaarschap actief ingevuld door het management, dat zich hierin laat bijstaan door een team van functioneel beheerders.

Bij D is het niet goed mogelijk ondubbelzinnig eigenaarschap aan te wijzen vanwege het karakter van de organisatie; de data is eigendom van verschillende samenwerkingspartners. Dit is ondervangen door een aantal bewerkersovereenkomsten tussen ketenpartners, waarin afspraken over gebruik en raadpleging zijn vastgelegd. In het algemeen is het management van de bij betrokken applicatie organisatie nauw betrokken bij het juiste gebruik en professioneel beheer van de gegevens.

5-3-6 incidentmanagement

Bij incidentmanagement gaat het om een goede monitoring, registratie en opvolging van beveiligingsincidenten, bijvoorbeeld het verliezen van een mobiele telefoon. Incidenten die hebben plaatsgevonden dienen adequaat onderzocht te worden en structureel te worden opgelost. Tot slot dient hierover aan het management te worden gerapporteerd.

Als beveiligingsincidenten niet worden opgevolgd en niet structureel worden opgelost, bestaat het risico dat incidenten zich herhaaldelijk voor blijven doen en er bijvoorbeeld langdurig sprake is van ongeautoriseerde toegang tot vertrouwelijke gegevens. Een ander risico is dat er niet wordt geleerd van incidenten die zich hebben voorgedaan.

De servicedesk bij het cluster BCO registreert incidenten. Er bestaat verslaglegging van incidenten van de verschillende applicaties. De mate van vastlegging verschilt per applicatie. Van de applicatie D, vindt een aparte registratie van beveiligingsincidenten plaats. De beoordeling van de rekenkamer is bij B en A dat de beheersing gedeeltelijk op orde is. Immers, BCO pakt structurele incidenten op en daarmee waarschijnlijk ook beveiligingsincidenten. Het ontbreken van formele verslaglegging sluit niet uit dat incidenten worden opgelost.

Bij E en C is het proces rond de afhandeling van incidenten in de SLA opgenomen. In beide SLA's worden beveiligingsincidenten niet apart benoemd. Zoals eerder aangegeven wordt bij E niet gerapporteerd over de uitvoering van de SLA. Voor C is in

de SLA opgenomen hoe er over incidenten wordt gerapporteerd. Rapportages zijn echter nog niet verschenen omdat de applicatie nog maar kort in gebruik is. Onduidelijk is daardoor of specifiek over beveiligingsincidenten wordt gerapporteerd.

5-3-7 risicomanagement

Zoals in eerdere hoofdstukken is beschreven gaat het concern IB-beleid uit van een risk-based aanpak, die veronderstelt dat beveiligingsmaatregelen worden getroffen op basis van risicoanalyse. De rekenkamer is voor de geselecteerde applicaties nagegaan of er risicoanalyses en/of privacy impact analyses zijn uitgevoerd en of deze van goede kwaliteit zijn.

Wanneer beveiligingsrisico's onvoldoende in kaart worden gebracht bestaat het risico dat er onvoldoende of niet de juiste maatregelen worden getroffen om de risico's voldoende af te dekken.

De rekenkamer heeft bij geen van de onderzochte applicaties een recente risicoanalyse aangetroffen waarin de kans en impact van beveiligingsrisico's zijn ingeschat en waarbij is aangegeven welke maatregelen worden getroffen om de risico's te mitigeren.

Bij de applicatie E is een risicoanalyse opgesteld door de leverancier van de applicatie. Uit de risicoanalyse van de leverancier blijkt dat er risico's zijn waarvoor de gemeente maatregelen moet treffen. Het betreffende cluster heeft niet aan kunnen tonen of aan deze gesignaleerde risico's opvolging is gegeven. In maart 2015 heeft het cluster zelf een risicoanalyse opgesteld. Daarin is een beperkt aantal maatregelen genoemd, waarvan onduidelijk is of deze werkelijk geïmplementeerd zijn.

Bij de overige applicaties is, ondanks dat een risicoanalyse ontbreekt, wel met risico's rekening gehouden. Betrokken medewerkers tonen zich risicobewust. Maar de koppeling tussen getroffen beveiligingsmaatregelen en risico's ontbreekt. Ook bestaat er geen inzicht of aanwezige beveiligingsmaatregelen de risico's voldoende afdekken.

De applicaties D en C zijn in 2016 nieuw opgeleverd. De opzet en inrichting duidt op 'security & privacy by design'.[48] Er is bij beide applicaties ook een aantal self-assessments/audits uitgevoerd die risico's en kwetsbaarheden blootleggen. Naar aanleiding hiervan zijn verbeteringen uitgevoerd of gepland.[49] Daarom beoordeelt de rekenkamer het aspect risicomanagement bij deze applicaties als op niveau.

Bij de applicatie A moet verantwoording aan het rijk worden afgelegd via self-assessments. Daarbij kunnen ook risico's en kwetsbaarheden aan het licht komen. Omdat er op deze manier toch enig inzicht in risico's bestaat, beoordeelt de rekenkamer deze applicatie op dit aspect als gedeeltelijk op niveau.

5-3-8 onafhankelijke assurance

Het is een goede praktijk om zekerheid te verkrijgen over de beschikbaarheid, continuïteit en vertrouwelijkheid door middel van een onafhankelijke onderzoek

48 Zie hiervoor het Concern Informatie Component Architectuur, 14 december 2014.

49 C is nog niet volledig operationeel. Voor verschillende processen wordt nog de voorganger F gebruikt. De beveiliging van F heeft de rekenkamer niet beoordeeld, maar de indruk is dat deze minder goed op orde is.

(bijvoorbeeld uitgevoerd door een register IT-auditor). Dat geldt voor zowel de interne als externe verwerking van gegevens. De verantwoording hierover vindt zijn weerslag in een zogenaamde third party mededeling ('TPM') of in een International Standard on Assurance Engagements 3402-statement (ISAE-3402).[50] Van belang is dat in het kader van de TPM of ISAE3402 niet alleen wordt vastgesteld dat beveiligingsmaatregelen op papier bestaan, maar dat ook de werking kan worden aangetoond.

Wanneer onafhankelijke assurance ontbreekt, bestaat het risico dat onopgemerkt blijft dat de interne leverancier (BCO) of de externe leverancier ontoereikende maatregelen heeft getroffen voor de beschikbaarheid, continuïteit en vertrouwelijkheid van de gegevens in de applicaties te waarborgen.

Bevestiging van de kwaliteit van de dienstverlening bij derden of bij het cluster BCO in de vorm van een TPM of ISAE3402-statement heeft de rekenkamer bij geen van de onderzochte applicaties aangetroffen. Bij E en C hebben de leveranciers een ISO-27001 certificering. Deze certificering zegt echter alleen iets over de opzet van beveiligingsmaatregelen en niet over de effectieve werking daarvan.

5-3-9 anoniem testen

In het kader van informatiebeveiliging is het van belang dat bij het testen van nieuwe applicaties of wijzigingen in bestaande applicaties, gebruik wordt gemaakt van geanonimiseerde gegevens. Dit om te voorkomen dat tijdens testwerkzaamheden vertrouwelijke gegevens ten onrechte worden ingezien. Ook voorkomt het testen met geanonimiseerde gegevens dat een situatie kan ontstaan zoals bij het datalek in februari 2016 bij Gemeentebelastingen, waarbij niet-geanonimiseerde testgegevens via internet toegankelijk waren. Wanneer voor testwerkzaamheden niet-geanonimiseerde persoonsgegevens worden gebruikt wordt privacyregelgeving geschonden. Het is namelijk niet toegestaan om persoonsgegevens te gebruiken voor testwerkzaamheden.[51]

De functionarissen die de rekenkamer heeft gesproken hebben aangegeven dat testwerkzaamheden worden uitgevoerd met geanonimiseerde testgegevens. De rekenkamer heeft onvoldoende materiaal aangetroffen om dit te verifiëren.

Bij D wordt getest met geanonimiseerde gegevens. De gegevens in de testomgeving zijn gescrambled. In de laatste testfase (de gebruikersacceptatietest) wordt wel met echte data getest, namelijk met een kopie van de productiegegevens. Dit is een gebruikelijke werkwijze.

Bij B bestaat een aparte testomgeving, maar hierin worden echte data gebruikt.

Bij A worden bij nieuwe releases door de leverancier ~~Centric~~ software ter beschikking gesteld die de gemeente in een eigen OTAP installeert. Hierbij is een testprocedure van toepassing. Of testgegevens geanonimiseerd worden is niet duidelijk. In totaal zijn er vier functioneel beheerders die het testwerk uitvoeren voor A. Er kan dus een beperkt aantal mensen bij de testgegevens.

50 Dit is een audit standaard voor rapportage over uitbestede processen.

51 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens

Bij de ontwikkeling van C is het testen gebeurd met een bestaande geanonimiseerde dataset. Door het projectteam is getest of de applicatie in functionele zin voldeed. Daarna is een acceptatietest uitgevoerd door gebruikers inclusief acceptatietestverslag.

Bij E is er een aparte testomgeving ‘pre-productie’ waarin nieuwe releases worden getest. Testen worden meestal met echte (niet-geanonimiseerde) gegevens uitgevoerd.

Rekenkamer ROTTERDAM

6 resultaten hack

6-1 inleiding

In dit hoofdstuk staat de volgende onderzoeksvraag centraal:

Is het mogelijk oneigenlijke toegang te krijgen tot gevoelige informatie die de gemeente Rotterdam in beheer heeft?

De rekenkamer heeft deze vraag via drie wegen beantwoord. Ten eerste is een externe penetratietest uitgevoerd. Daarbij is geprobeerd vanuit een niet-gemeentelijke locatie via internet in de gemeentelijke informatieomgeving (de infrastructuur, applicaties en data) door te dringen. Ten tweede is een interne penetratietest uitgevoerd, waarbij vanuit een gemeentelijke locatie (een werkruimte, vergaderzaal) geprobeerd is oneigenlijke toegang te verkrijgen. Ten slotte is een social engineering test gedaan, waarin de “awareness” van medewerkers is getoetst. De bevindingen uit de uitgevoerde testen geven inzicht in hoeverre het totaal aan beveiligingsmaatregelen dat de gemeente heeft getroffen, voldoet om te voorkomen dat onbevoegden kunnen doordringen tot de gemeentelijke informatieomgeving. In het volgende groene kader is een aantal voorbeelden opgenomen van scenario’s die kunnen optreden als onbevoegden toegang weten te krijgen tot de gemeentelijke informatieomgeving.

voorbeelden scenario’s gevolgen oneigenlijke toegang

- Als de mailbox van een bestuurder wordt gehackt, is het mogelijk om uit zijn of haar naam e-mails te versturen. Dit kan tot verwarring leiden en gevaarlijke gevolgen hebben. Als de agendagegevens van de desbetreffende gezagsdrager toegankelijk zijn, vormt dit een veiligheidsrisico voor hem- of haarzelf en zijn/haar omgeving. Als in e-mails het veiligheidsprotocol voor een evenement is beschreven, kan dat worden gebruikt om zwakke plekken in de beveiliging op te sporen en te misbruiken.
- Als een hacker toegang verkrijgt tot de basisregistratie personen kunnen bijvoorbeeld geboortedata worden aangepast, zodat iemand eerder AOW krijgt. Of iemand kan aangifte doen van de geboorte van meerdere kinderen om zo een hogere kinderbijslag te ontvangen.
- Als toegang wordt verkregen tot besturingssystemen van verkeersobjecten, kan de besturing van bruggen, tunnels en stoplichten worden ontregeld. Het gevolg kan een verkeerschaos zijn waardoor hulp- en veiligheidsdiensten niet langer juist en tijdig hun werk kunnen uitvoeren.

Voor de uitvoering van de testen heeft de rekenkamer gebruikgemaakt van een extern, gespecialiseerd, bureau. Omdat de werkzaamheden – hacks – formeel gezien strafbaar zijn, is tussen de gemeente, dit bureau en de Rekenkamer Rotterdam een vrijwaringsovereenkomst getekend. Daarmee heeft de gemeente toestemming voor de hacks gegeven. Van de zijde van het ingehuurde bureau en de rekenkamer gold onder meer de verplichting de gemeentelijke informatiesystemen niet te ondermijnen en eventueel ontdekte cruciale beveiligingslekken meteen bij de CISO te melden. Hierover en over de social engineering test heeft de rekenkamer op 5 oktober 2016 een brief aan

de raad en het college verzonden. Daarin is tevens aangegeven dat in het geval van de social engineering test de rekenkamer geen (interne) vastlegging doet van de namen van de personen via wie al dan niet oneigenlijke toegang tot informatie is verkregen.

Zoals is vermeld in paragraaf 2-4, heeft de gemeente begin 2015 zelf een (ander) gespecialiseerd bureau ingehuurd voor een interne penetratietest. Daarbij is geprobeerd om vanuit een gemeentelijke kantoorlocatie in de gemeentelijke systemen binnen te dringen Hierbij kwamen verschillende tekortkomingen aan het licht, waarvan verschillende met een zeer hoog risico. Naar aanleiding hiervan is een projectleider aangesteld die aan de slag is gegaan om de geconstateerde kwetsbaarheden op te lossen. Op basis van de uitkomsten van de interne penetratietest die in het kader van dit rekenkameronderzoek is uitgevoerd, is de rekenkamer voor zover mogelijk nagegaan of de kwetsbaarheden die in 2015 zijn geconstateerd, voldoende zijn verholpen.

bevindingen accountant t.a.v. informatiebeveiliging

Ook de accountant van de gemeente Rotterdam heeft tijdens de jaarrekeningcontrole 2015 kritische opmerkingen gemaakt ten aanzien van de informatiebeveiliging.[52] De accountant heeft bijvoorbeeld gewezen op het risico dat ongeautoriseerd toegang en handelingen plaatsvinden binnen systemen en onderliggende data en op een verhoogd risico op datalekken.

Van de penetratietesten die de rekenkamer heeft laten uitvoeren is een gedetailleerde rapportage gemaakt. Deze rapportage bevat veel technische bevindingen die laten zien hoe al dan niet toegang kan worden verkregen tot de gemeentelijke informatiesystemen. Omdat dit gevoelige informatie betreft, is de rapportage als vertrouwelijk aangemerkt. De vertrouwelijke rapportage, die ook technische aanbevelingen voor verbetering bevat, is wel toegezonden aan de CISO.

In dit hoofdstuk wordt een beeld geschetst van de bevindingen uit de testen. Daarbij wordt in algemene zin een indruk gegeven van de aard van de bevindingen, het daarbij behorende risico en de mogelijke consequenties. Tevens wordt aangegeven of tekortkomingen reeds in de eerdere penetratietesten waren opgemerkt.

6-2 resultaten externe penetratietest

Er zijn geen aanwijzingen dat de gemeente onvoldoende is beveiligd tegen aanvallen van buiten. Het is niet gelukt om binnen de beschikbare tijd van vier dagen via het internet binnen te dringen in systemen van de gemeente Rotterdam. Wel zijn er kwetsbaarheden geconstateerd die aanvallers in staat stellen via het internet bruikbare informatie te vergaren en bleek het mogelijk webmailsessies te volgen. Ook bleek een aantal systemen onnodig via het internet benaderbaar, waardoor het risico bestaat dat de controle over deze systemen van buitenaf wordt overgenomen. Tot slot is het mogelijk misbruik te maken van een aantal gemeentelijke websites en zo de gemeente imagoschade toe te brengen.

Bij de externe penetratietest is geprobeerd zonder voorkennis via het internet toegang te verkrijgen tot systemen van de gemeente Rotterdam. Binnen de beschikbare tijd

52 PWC, tweede boardletter tussentijdse bevindingen controle 2015, 25 maart 2016.

van vier dagen is het niet gelukt om deze toegang te verkrijgen. Wel zijn er bij deze externe penetratietest kwetsbaarheden aan het licht gekomen. Tabel 6-1 geeft een overzicht van deze kwetsbaarheden.

tabel 6-1: bevindingen externe penetratietest

kwetsbaarheid	risico
systemen lekken informatie	laag
onveilige login pagina's	hoog
systemen onnodig benaderbaar vanaf internet	gemiddeld
verouderde DNS verwijzingen	laag
cross site scripting	hoog
verouderde webmail installatie	kritiek

Figuur 6-1 licht de verschillende risiconiveaus (laag-gemiddeld-hoog-kritiek) toe die van toepassing zijn op de verschillende kwetsbaarheden die aan het licht zijn gekomen. Hierin wordt geïllustreerd dat bij een kritiek risico zowel de waarschijnlijkheid dat een kwetsbaarheid zal worden uitgebuit, als de impact daarvan (in termen van schade), zijn ingeschat op hoog.

figuur 6-1 risiconiveaus gedetecteerde kwetsbaarheden

Risico = Waarschijnlijkheid * Impact				
Impact	Hoog	Gemiddeld	Hoog	Kritiek
	Gemiddeld	Laag	Gemiddeld	Hoog
	Laag	Informatief	Laag	Gemiddeld
		Laag	Gemiddeld	Hoog
	Waarschijnlijkheid			

Hierna worden de verschillende geconstateerde kwetsbaarheden nader toegelicht.

systemen lekken informatie (laag risico)
Een aantal systemen lekt informatie via uitgebreide foutmeldingen die op het internet worden weergegeven. Deze informatie biedt bijvoorbeeld inzicht in de structuur van (netwerk)mappen, interne IP-adressen, databases en namen van medewerkers. Deze informatie kan kwaadwillenden handvatten bieden om een hack te starten. Aanvallers krijgen middels dit soort informatie bijvoorbeeld een beeld van hoe het interne netwerk eruit ziet of ze kunnen gericht medewerkers benaderen met phishing-mails en zo meer informatie vergaren die bruikbaar is bij een poging de gemeente te hacken.

onveilige login pagina's (hoog risico)
Er zijn twee gemeentelijke websites aangetroffen waarop gebruikers moeten inloggen, waarbij geen sprake is van een versleutelde https-verbinding. Het slotje in de adresbalk waaraan https-verbindingen herkenbaar zijn ontbreekt bij deze websites. In

slecht beveiligde netwerken (zoals openbare WIFI-hotspots) is het mogelijk om bij deze login-pagina's gebruikersnamen en wachtwoorden 'af te luisteren'.

systemen onnodig benaderbaar vanaf internet (gemiddeld risico)
Een aantal systemen is onnodig vanaf internet benaderbaar. Dit betreft bijvoorbeeld een camerasysteem en een systeem voor klimaatcontrole. De onderzoekers zijn er niet in geslaagd binnen de tijd die zij beschikbaar hadden daadwerkelijk toegang te verkrijgen tot deze systemen. Wanneer dergelijke systemen via het internet benaderbaar zijn is echter niet uit te sluiten dat aanvallers in staat zijn gebruikersnamen en wachtwoorden te achterhalen en zo de controle over een systeem over kunnen nemen.

verouderde DNS verwijzingen (laag risico)
Er zijn verouderde DNS-verwijzingen aangetroffen.

DNS
Het Domain Name System (DNS) is het systeem- en netwerkprotocol dat op het internet gebruikt wordt om namen van computers naar numerieke adressen (IP-adressen) te vertalen en omgekeerd. Het DNS-protocol is kwetsbaar voor misbruik. Onder meer door middel van zogenaamde 'DNS cache pollution'-aanvallen is het DNS om de tuin te leiden. Als gevolg hiervan kunnen argeloze gebruikers bijvoorbeeld naar een valse, malafide website worden gestuurd.

Via social engineering kan ~~zo~~ controle worden verkregen over systemen, die vervolgens ingezet kunnen worden voor een phishing aanval. Dit kan tot imagoschade voor de gemeente leiden.

cross site scripting (hoog risico)
Eén gemeentelijke website bleek gevoelig voor Cross Site Scripting. Het is dan mogelijk het uiterlijk van de website te veranderen door bijvoorbeeld valse login schermen op te zetten op de website of kwaadaardige scripts uit te voeren. Zo kunnen kwaadwillenden betrouwbaar ogende phishing aanvallen opzetten en bezoekers van de website verleiden een valse link te bezoeken waarmee vervolgens bijvoorbeeld malware geïnstalleerd kan worden op de computer van de bezoeker.

verouderde webmailinstallatie (kritiek risico)
Er is een verouderde met internet verbonden webmailinstallatie aangetroffen. Via deze installatie bleek het mogelijk willekeurige bestanden en belangrijke systeemwachtwoorden op te vragen. De onderzoekers kregen zo leestoegang tot bestanden op de webserver en konden zo sessies van webmailgebruikers volgen.[53] In het vertrouwelijke rapport over de penetratietest is hiervan nadere bewijsvoering opgenomen.

6-3 resultaten interne penetratietest

Uit de interne penetratietest kwamen zo'n 700 kritieke technische kwetsbaarheden bij specifieke systemen of applicaties, te herleiden tot 46 unieke kwetsbaarheden. Daarnaast zijn

53 Het gaat om een sporadisch gebruikt systeem met vijf actieve medewerkers die geen gebruik maakten van burger gerelateerde gegevens.

er kwetsbaarheden in de IT-infrastructuur geconstateerd die het eenvoudig maken om oneigenlijke toegang tot het gemeentelijke netwerk te krijgen. Eenmaal in het gemeentelijke netwerk is veel informatie toegankelijk. Veel systemen en applicaties bleken verouderd en niet meer ondersteund te worden. Uiteindelijk bleek het mogelijk beheerrechten te verkrijgen waarmee nagenoeg alle systemen toegankelijk werden.

De kwetsbaarheden die bij deze interne penetratietest aan het licht kwamen, zijn ook opgemerkt tijdens een penetratietest die in 2015 in opdracht van de gemeente is uitgevoerd. De gemeente is er niet in geslaagd in de tussenliggende periode op deze punten verbeteringen door te voeren.

De rekenkamer heeft 20.000 kwetsbaarheden gedetecteerd bij specifieke systemen of applicaties, waarvan zo'n 700 kritiek, 600 hoog, 13.000 medium en 5.000 met een lage kwetsbaarheidsgraad. Het gaat om 482 unieke kwetsbaarheden waarvan 46 kritiek en 89 hoog.

De rekenkamer merkt op dat deze hackactiviteiten door de beheerders van de applicatie D werden opgemerkt. Vervolgens hebben zij hiervan melding van gemaakt bij de CISO. Dit is een good practice. Voor de overige applicaties zijn er geen meldingen gedaan en lijken de activiteiten onopgemerkt gebleven.

Systeembeheerders hebben gedurende de pentest hackpogingen opgemerkt. Zij hebben de plek van waar dit gebeurde kunnen lokaliseren en hebben de pentesters gestoord in hun activiteiten. De pentesters hadden op dat moment al cruciale informatie verzameld om op een later moment (op een andere locatie) verder te kunnen gaan. De onderbreking hangt samen met de methodiek van de pentesters. Als deze in korte tijd wordt uitgevoerd, laat dit relatief veel sporen achter.[54]

kwetsbaarheden in IT-infrastructuur
Het bleek voor de onderzoekers vrij eenvoudig om oneigenlijke toegang tot het gemeentelijke netwerk te krijgen. Dit is het gevolg van kwetsbaarheden die zijn geconstateerd met betrekking tot de IT-infrastructuur. Deze kwetsbaarheden worden hierna summier toegelicht. Een nadere onderbouwing en toelichting staan in een technisch rapport dat vertrouwelijk blijft.

geen netwerkauthenticatie (gemiddeld risico)
Als sprake is van netwerkauthenticatie krijgt een gebruiker pas toegang tot het bekabelde netwerk nadat de gebruiker is ingelogd. Hiervan wordt binnen de gemeente geen gebruik gemaakt. Ook uit de penetratietest uit 2015 is gebleken dat de netwerkauthenticatie tekortschiet.

onvoldoende filtering in het netwerk (gemiddeld risico)
Er is onnodig vrije netwerktoegang tot diensten en protocollen, waardoor ~~vergroot~~ het aanvalsoppervlak dat kwaadwillenden tot hun beschikking krijgen als ze zich toegang hebben verschaft tot (een deel van) het netwerk, wordt vergroot.

54 De insteek van de pentesters was om in zo'n kort mogelijke tijd zoveel mogelijk eventuele kwetsbaarheden bloot te leggen. Een werkelijk kwaadwillende hacker zal voor een manier kiezen die minder in het oog loopt ~~(langzamer en meer proberen geen sporen achter te laten).~~

In de penetratietest die de gemeente begin 2015 heeft laten uitvoeren is ook geconstateerd dat netwerkfiltering in onvoldoende mate is toegepast. Volgens het plan van aanpak dat de gemeente na deze penetratietest heeft opgesteld, is dit probleem deels opgelost met de implementatie van nieuwe werkplekken in het eerste kwartaal van 2016. Daarnaast heeft het project 'inrichten ICT beveiliging cf. nieuwe concern IB architectuur' dat is opgenomen in het meerjarenplan informatiebeveiliging 2015-2017, tot doel het interne netwerk te segmenteren op basis van classificaties.

beperkte beveiliging werkstations (kritiek risico)
Doordat werkstations een beperkte beveiliging hebben was het mogelijk om ~~de~~ gebruikers te bespieden door mee te kijken op hun scherm en/of toetsaanslagen vast te leggen, zonder dat dit werd opgemerkt. In de penetratietest die in 2015 is uitgevoerd kwamen bevindingen van dezelfde strekking naar voren.

verouderde en niet meer ondersteunde systemen en applicaties (kritiek risico)
Er is een groot aantal systemen en applicaties aangetroffen dat niet meer wordt ondersteund door de leverancier en/of waarbij beschikbare beveiligingsupdates niet bleken te zijn toegepast. Verouderde besturingssystemen en applicaties bevatten daardoor vaak kwetsbaarheden. Door de aangetroffen kwetsbaarheden te misbruiken hebben de onderzoekers beheerrechten verkregen waarmee nagenoeg alle Windows-systemen, netwerkmappen, gebruikersmappen, mailboxen en andere systemen toegankelijk werden, waaronder het account van een bestuurder. Ook konden de onderzoekers bestandsnamen doorzoeken en zo bestanden achterhalen waarin naar alle waarschijnlijkheid vertrouwelijke persoonsgegevens zijn opgeslagen.

De risico's van het gebruik van verouderde en niet ondersteunde software zijn ook gesignaleerd bij de penetratietest die de gemeente begin 2015 heeft laten uitvoeren. In het plan van aanpak dat na deze penetratietest is uitgewerkt is ten aanzien van deze risico's opgenomen een 'legacy' project te starten en applicatie life cycle management in te voeren. Dit zijn in opzet adequate oplossingen. Desondanks kwamen deze kwetsbaarheden ook naar voren in de penetratietesten die de rekenkamer heeft laten uitvoeren.

6-4 social engineering test

Het bleek eenvoudig om ongeautoriseerd toegang te krijgen tot gemeentelijke panden. Eenmaal binnen was er vrije toegang tot kwetsbare ruimtes en (vertrouwelijke) informatie.

Tijdens de inlooptesten hebben de desbetreffende onderzoekers "lokmiddelen" achtergelaten. Een aantal hiervan is door medewerkers gebruikt, waardoor oneigenlijke toegang aan derden kon worden verschaft.

Via een spear phishing mail bleek het mogelijk een medewerker te verleiden een verdachte link te openen. Dit leidde niet tot schade.

De social engineering test bestond uit drie componenten: inlooptesten, achtergelaten lokmiddelen en spear phishing mails. Hierna worden per onderdeel de bevindingen toegelicht.

inlooptesten
In het kader van de inlooptesten hebben onderzoekers ongeautoriseerde toegang ~~te~~ gekregen tot vier gemeentelijke locaties. De onderzoekers kwamen daarbij vertrouwelijke (fysieke) informatie tegen en hadden toegang tot voor sabotage kwetsbare ruimtes.

Waar de onderzoekers ongeautoriseerd toegang hebben verkregen, was het mogelijk (vergader)ruimtes met netwerkaansluitingen te betreden. De onderzoekers konden vrij bewegen en verblijven binnen de verschillende panden, zonder dat zij werden aangesproken. De onderzoekers hadden van de gelegenheid gebruik kunnen maken het netwerk van de gemeente aan te vallen.

achtergelaten lokmiddelen
Tijdens de inlooptesten hebben de onderzoekers op verschillende plaatsen ~~USB-sticks~~ lokmiddelen achtergelaten. Enkele achtergelaten lokmiddelen werden door medewerkers van de gemeente gebruikt, waardoor onbedoeld digitaal toegang kon worden verschaft aan kwaadwillenden. Enkele lokmiddelen zijn ingeleverd bij security officers, omdat medewerkers deze verdacht vonden.

spear phishing mails
Er zijn twee gerichte 'spear phishing' emails verstuurd waarmee geprobeerd is de ontvangers te verleiden om kwaadaardige links te volgen. Op één email is geen reactie gekomen. Bij de andere email bleek het mogelijk de betreffende medewerker te verleiden een verdachte link te openen. Het bezoek aan de website leverde in dit geval geen gebruikersnaam en wachtwoord op.

6-5 totaalbeeld

Met de interne en externe penetratietest, de social engineering test en de applicatiereviews heeft de Rekenkamer Rotterdam zicht gekregen op de effectiviteit van het IB-beleid van de gemeente Rotterdam. De rekenkamer constateert dat het tot nu toe gevoerde IB-beleid onvoldoende heeft bijgedragen aan een goede informatieveiligheid, in het bijzonder van (bijzondere) persoonsgegevens. Er bestaat een uitgeschreven beleid. Dit is nader uitgewerkt in diverse procedures en richtlijnen. Het beleid hanteert een risk based aanpak. In de praktijk wordt hier aan geen invulling gegeven omdat risicoanalyses veelal ontbreken. Er is geen koppeling tussen de bestaande maatregelen en de risico's. De maatregelen worden niet consequent binnen de organisatie toegepast en schieten soms kwalitatief tekort.

De rekenkamer heeft kritieke kwetsbaarheden in de informatiebeveiliging vastgesteld. Ook dit onderschrijft dat de beveiligingsmaatregelen onvoldoende effectief zijn. Dit beeld wordt versterkt door het gegeven dat 1,5 jaar voor het rekenkameronderzoek de gemeente zelf al een interne penetratietest heeft laten uitvoeren. Hieruit bleken kritieke kwetsbaarheden, waarvan verschillende ook nu door de rekenkamer zijn vastgesteld. Eventuele verbetermaatregelen die de gemeente naar aanleiding van eerdere testen heeft genomen zijn klaarblijkelijk niet effectief.

Het algemene beeld uit het door de rekenkamer uitgevoerde onderzoek is dat het voor een kwaadwillende gemakkelijker is om van binnenuit in de informatiesystemen van de gemeente te komen, dan van buitenaf. Het is relatief eenvoudig gebleken om vanaf een gemeentelijke locatie informatiesystemen te misbruiken. Deze toegang wordt

vergemakkelijkt doordat ook de fysieke beveiliging tekortschiet. De beveiliging ~~met~~ is verre van waterdicht. Eenmaal fysiek een gemeentelijk pand binnengekomen, is er geringe sociale controle; onbevoegden worden niet aangesproken door medewerkers van de gemeente. Door de combinatie van een tekort aan digitale en fysieke beveiliging en gebrekkige 'security awareness', is gevoelige informatie binnen de gemeente kwetsbaar.

Een positieve uitkomst van het onderzoek is dat gemeentelijke informatiesystemen voor aanvallen van buitenaf in technisch opzicht behoorlijk zijn beschermd. Incidenten kunnen echter nooit worden uitgesloten. Medewerkers blijken namelijk niet ongevoelig voor het openen van spear phishing mails en lokmiddelen, die zijn achtergelaten in gemeentelijke locaties. Ook hierdoor kunnen kwaadwillenden de digitale systemen van de gemeente in.

De potentiële consequenties van de geschetste tekortkomingen zijn divers en groot. Eenmaal zowel fysiek als digitaal binnengekomen, blijkt het relatief eenvoudig wachtwoorden te verkrijgen en mee te kijken met gebruikers, tot en met de agenda van een bestuurder toe. Van deze gegevens kan misbruik worden gemaakt. Zo zouden systemen platgelegd kunnen worden, waardoor bijvoorbeeld uitkeringen niet kunnen worden verstrekt of parkeervergunningen niet kunnen worden verleend. Met dergelijke toegang kunnen kwaadwillenden zich bovendien verrijken door geld aan zichzelf over te maken en zich ook (bijzondere) persoonsgegevens toe te eigenen. Hacks kunnen dus grote gevolgen voor individuele burgers hebben. Verder kan het overnemen van de bediening van stoplichten, bruggen etc. de verkeersorde flink verstoren.

Tot op heden hebben zich nog geen grootschalige cyber-incidenten met grote maatschappelijke gevolgen voorgedaan. Met de huidige staat van de informatiebeveiliging is de gemeente Rotterdam – zowel het bestuur en organisatie, haar inwoners – echter onvoldoende weerbaar tegen misbruik en de maatschappelijke gevolgen daarvan.

Rekenkamer ROTTERDAM

bijlagen

Rekenkamer ROTTERDAM

bijlage 1 onderzoeksverantwoording

inleiding
Het onderzoek naar informatiebeveiliging Rotterdam is uitgevoerd in de periode van mei 2016 tot en met januari 2017. Het rapport is gebaseerd op een documentstudie, interviews met betrokken ambtenaren van de gemeente, een nadere beoordeling van de beveiliging van vijf belangrijke applicaties waarin persoonsgegevens worden verwerkt en een ethical hack.

documentstudie
De rekenkamer heeft onder meer de volgende documenten geraadpleegd:
- documenten die inzicht geven in het beleid van de gemeente op het terrein van informatiebeveiliging;
- rapportages van onderzoeken die zijn uitgevoerd naar het datalek uit februari 2016;
- rapportages van onderzoeken en penetratietesten die eerder in opdracht van de gemeente zijn uitgevoerd;
- documenten die inzicht geven in de staat van informatiebeveiliging van de vijf onderzochte applicaties.

In bijlage 2 staan de documenten opgesomd die in dit rapport staan genoemd.

interviews
De rekenkamer heeft met diverse personen binnen en buiten de gemeente Rotterdam gesproken of per e-mail contact gehad.

Binnen de gemeente Rotterdam is gesproken met:
- de CISO;
- de security information officers;
- de security manager;
- ambtenaren van de afdeling IIFO (o.a. van technisch beheer);
- ambtenaren van de verschillende clusters (BCO, Dienstverlening, Maatschappelijke Ontwikkeling, Stadsbeheer, Werk en Inkomen en Stadsontwikkeling) die betrokken zijn bij de vijf onderzocht applicaties;
- directeur Gemeentebelastingen;
- kwartiermaker functionaris gegevensbescherming;
- ambtenaren van Concern Auditing.

analyse kroonjuwelen
De rekenkamer heeft vijf applicaties geselecteerd waarin veel persoonsgegevens omgaan en de staat van informatiebeveiliging bij deze applicaties nader onderzocht. De rekenkamer heeft in dit verband gesprekken gevoerd met de functioneel beheerders van de applicaties en andere bij de applicaties betrokken medewerkers, waaronder eigenaren van de data die in de applicaties omgaat. Ook heeft de rekenkamer alle onderzochte applicaties ingezien.

ethical hack
De rekenkamer heeft door een gespecialiseerd bureau een ethical hack laten uitvoeren. Ten eerste is een externe penetratietest uitgevoerd. Daarbij is geprobeerd vanuit een niet-gemeentelijke locatie via internet in de gemeentelijke informatiesystemen door te dringen. Ten tweede is een interne penetratietest uitgevoerd, waarbij vanuit een gemeentelijke locatie (een werkruimte, vergaderzaal)

geprobeerd is oneigenlijke toegang te verkrijgen. Ten slotte is een social engineering test gedaan, waarin de “awareness” van medewerkers is getoetst. De social engineering test bestond uit een inlooptest, het achterlaten van USB-sticks en het versturen van phising-mails.

procedures

De opzet van het onderzoek is op 9 mei 2016 ter kennisname aan de raad verstuurd. De voorlopige onderzoeksresultaten zijn opgenomen in een concept nota van bevindingen. Deze is op 26 januari 2017 voor ambtelijk wederhoor voorgelegd aan de CISO. Na verwerking van de op 10 februari 2017 ontvangen ambtelijke reactie is een bestuurlijke nota opgesteld. Deze omvat de voornaamste conclusies en aanbevelingen van de rekenkamer. De bestuurlijke nota, met de nota van bevindingen als bijlage, is op 23 februari 2017 voor bestuurlijk wederhoor voorgelegd aan het college van B en W. Op 22 maart 2017 heeft de rekenkamer de reactie van B en W vertrouwelijk ontvangen. Omdat deze ook vertrouwelijk naar de raad is verzonden, is zij niet integraal in het rapport opgenomen. Logischerwijze ontbreekt daarmee ook een inhoudelijk nawoord op het rapport. Het definitieve rapport wordt door toezending aan de gemeenteraad en B en W openbaar.

Rekenkamer ROTTERDAM

bijlage 2 geraadpleegde documenten

In deze bijlage staan de aangehaalde documenten opgesomd, die zijn geraadpleegd voor dit rapport. Dat neemt niet weg dat voor het onderzoek ook andere hier niet aangehaalde bronnen zijn gebruikt, waaronder inzage in vertrouwelijke documenten.

gemeentelijke documenten

- Gemeente Rotterdam, cluster Maatschappelijk Ontwikkeling, 'Actie en besluitenlijst overleg bewustwording privacy en IS', 7 juni 2016.
- BRP inclusief proces autoriseren en controleren', 11 april 2016.
- Gemeente Rotterdam, 'Beheerregeling gemeentelijke basisregistratie personen Rotterdam 2014, 17 december 2013.
- Gemeente Rotterdam, 'Beleidsregel gegevensverwerking in het sociale domein', ongedateerd.
- Gemeente Rotterdam, 'Besluit Informatiebeheer Rotterdam 2013', vastgesteld op 6 september 2013.
- Gemeente Rotterdam, 'Bijlage protocol meldplicht datelekken contactpersonen', ongedateerd.
- Gemeente Rotterdam, 'Bundel gespreksverslagen in het kader van de procesevaluatie van het datalek bij het cluster Dienstverlening gemeld op 25 februari 2016', mei 2016.
- Gemeente Rotterdam, 'Concern informatiebeveiliging component architectuur', 15 december 2014.
- Gemeente Rotterdam, 'Concern informatiebeveiligingsbeleid 2014', 10 december 2013.
- Gemeente Rotterdam, 'Factsheet handreiking privacy voor professionals', april 2015.
- Gemeente Rotterdam, 'Factsheet meldplicht datalekken', ongedateerd.
- Gemeente Rotterdam, 'Factsheet Regeling ICT- en informatiegebruik 2012', ongedateerd.
- Gemeente Rotterdam, 'Handreiking data classificatie', 11 januari 2011.
- Gemeente Rotterdam, 'I-agenda gemeente Rotterdam', 12 maart 2013.
- Gemeente Rotterdam, 'Impressie concerndirectie', 30 september 2015.
- Gemeente Rotterdam, 'Informatiebeveiliging Baseline DIA 2013', februari 2013.
- Gemeente Rotterdam, 'Meerjarenplan Concern IB', 2 maart 2015.
- Gemeente Rotterdam, 'Meerjarenplan Concern Informatiebeveiliging ontwikkelpad 2015-2017', 2 maart 2015.
- Gemeente Rotterdam, 'Notitie dekking meerjarenplan concern informatiebeveiliging', 15 september 2015.
- Gemeente Rotterdam, 'Opdracht tot integriteitsonderzoek', 3 maart 2016.
- Gemeente Rotterdam, 'P&O circulaire invoering integriteits- en geheimhoudingsverklaring', 26 augustus 2008.
- Gemeente Rotterdam, 'Plan van Aanpak security problemen, ongedateerd.
- Gemeente Rotterdam, 'Procedure aanvraag externe dataverbindingen', 22 januari 2016.
- Gemeente Rotterdam, 'Procesevaluatie van het op 25 februari 2016 bij het cluster Dienstverlening gemelde datalek', mei 2016.
- Gemeente Rotterdam, 'Protocol meldplicht datalekken 2016', 8 december 2015.
- Gemeente Rotterdam, 'Protocol meldplicht datalekken', 8 december 2015.

- Gemeente Rotterdam, 'Regeling ICT- en informatiegebruik 2012', vastgesteld op 17 april 2012.
- Gemeente Rotterdam, 'Resultaten GAP-analyse 2016 cluster Dienstverlening', 26 mei 2016.
- Gemeente Rotterdam, 'Resultaten GAP-analyse 2016 cluster Maatschappelijke Ontwikkeling', 7 juni 2016.
- Gemeente Rotterdam, 'Resultaten GAP-analyse 2016 cluster Stadsontwikkeling', 15 juni 2016.
- Gemeente Rotterdam, 'Tweede tertaalrapportage concern informatiebeveiliging 2015', 4 september 2015.
- Gemeente Rotterdam, cluster Bestuurs- en Concern Ondersteuning, 'Communicatieplan Bewustwording informatiebeveiliging', 24 mei 2016.
- Gemeente Rotterdam, cluster Bestuurs- en Concernondersteuning, 'Plan van aanpak organisatieontwikkeling', 8 juni 2016.
- Gemeente Rotterdam, cluster Maatschappelijk Ontwikkeling, 'Noodscenario wijkteam handmatig registreren', 29 augustus 2016.
- Gemeente Rotterdam, cluster Maatschappelijke Ondersteuning, 'PSA t.b.v. de projectactiviteiten voor het eerste plateau van Eén informatieplatform 3D cluster MO', 30 juli 2014.
- Gemeente Rotterdam, cluster Werk & Inkomen, 'Beknopt informatiebeveiligingsplan werk en inkomen 2015-2016', 21 augustus 2015.
- Gemeente Rotterdam, cluster Werk & Inkomen, 'Controleplan Suwinet-inkijk', 3 maart 2015.
- Gemeente Rotterdam, cluster Werk & Inkomen, 'Informatiebeveiligingsbeleid Werk en Inkomen 2013-2014', 27 juli 2014.
- Gemeente Rotterdam, cluster Werk & Inkomen, 'TBV - Taken, bevoegdheden en verantwoordelijkheden
- Gemeente Rotterdam, cluster Werk & Inkomen, 'Totstandkoming rapportages Suwinet raadplegingen', 20 maart 2015.
- Gemeente Rotterdam, cluster Werk & Inkomen, directienotitie 'Vaststellen informaitebeveiligingsbeleid 2013-2014 cluster W&I ivm herzieningen', 21 juni 2014.
- Gemeente Rotterdam, cluster Werk & Inkomen, directienotitie 'Vastellen beknopt informatiebeveiligingsplan 2015-2016 cluster W&I', 21 augustus 2015.
- Gemeente Rotterdam, cluster Werk & Inkomen, directienotitie 'Vaststellen Informatiebeveiligingsbeleid 2015 cluster W&I ivm herzieningen', 27 februari 2015.
- Gemeente Rotterdam, cluster Werk & Inkomen, memo 'Diversen informatiebeveiliging', 16 april 2015.
- Gemeente Rotterdam, cluster Werk & Inkomen, memo 'Diversen informatiebeveiliging', 1 augustus 2014.
- Gemeente Rotterdam, cluster Werk & Inkomen, memo 'Overzicht achterstand informatiebeveiligingsplan 2013-2014', 28 juli 2014.
- Gemeente Rotterdam, concerndirectie, diverse exemplaren van 'Uit de concerndirectie', van jaar 2012 tot en met jaar 2016.
- Gemeente Rotterdam, Service organisatie, 'Dienstverleningsovereenkomst voor generieke ICT basisdienstverlening 2015 CIO en Dienstencentrum I&A', 18 december 2014.
- Veiligheidshuis Rotterdam-Rijnmond, 'Afspraken en handswijze Marconistraat', oktober 2015.
- Veiligheidshuis Rotterdam-Rijnmond, 'Algemeen privacyreglement Veiligheidshuis Rotterdam-Rijnmond', 1 januari 2016.

- Veiligheidshuis Rotterdam-Rijnmond, 'Bijlage bij het Algemeen privacyreglement Veiligheidshuis Rotterdam-Rijnmond Casusreglement Huiselijk geweld', ongedateerd.
- Veiligheidshuis Rotterdam-Rijnmond, 'Bijlage bij het Algemeen privacyreglement Veiligheidshuis Rotterdam-Rijnmond Casusreglement Overvallers 18+ Rotterdam en regio Zuid-Holland Zuid', ongedateerd.
- Veiligheidshuis Rotterdam-Rijnmond, 'Bijlage bij het Algemeen privacyreglement Veiligheidshuis Rotterdam-Rijnmond Casusreglement Hit tafel Veiligheidshuis Rotterdam-Rijnmond', 1 februari 2014.
- Veiligheidshuis Rotterdam-Rijnmond, 'Bijlage bij het Algemeen privacyreglement Veiligheidshuis Rotterdam-Rijnmond Casusreglement Veelplegers 18+ misdrijven', 2015.
- Veiligheidshuis Rotterdam-Rijnmond, 'Bijlage bij het Algemeen privacyreglement Veiligheidshuis Rotterdam-Rijnmond Casusreglement Weegploeg en casusoverleg radicalisering', 1 januari 2016.
- Veiligheidshuis Rotterdam-Rijnmond, 'Bijlage bij het Algemeen privacyreglement Veiligheidshuis Rotterdam-Rijnmond Casusreglement Rotterdam Veeplegers 18+ overlast kanton', 2015.
- Veiligheidshuis Rotterdam-Rijnmond, 'Informatiebeveiligingsbeleid Veiligheidshuizen Rotterdam-Rijnmond en Zuid-Holland Zuid', 9 november 2016.
- Veiligheidshuis Rotterdam-Rijnmond, 'Pers- en PR-beleid Veiligheidshuis Rotterdam-Rijnmond', ongedateerd.
- Veiligheidshuis Rotterdam-Rijnmond, 'Toelichting bij het Algemeen privacyreglement Veiligheidshuis Rotterdam-Rijnmond', 16 november 2015.

brieven

- Burgemeestersbrief, 'Mogelijk vrijkomen persoonsgegevens', 6 september 2016.
- Collegebrief, 'Brief aan CBP n.a.v. onderzoek gegevensverwerking in sociaal domein', 11 juni 2015.
- Collegebrief, 'Datelekken', 13 september 2016.
- Collegebrief, 'Persoonsgegevens', 15 maart 2016.
- Collegebrief, 'Persoonsgegevens', 8 maart 2016.
- Collegebrief, 'Uitgangspuntennotitie doorontwikkeling welzijn, zorg en jeugdhulp 2018', 4 maart 2016.
- Collegebrief, 'Update persoonsgegevens', 1 juni 2016.
- Collegebrief, 'Vertrouwelijke inzage samenvatting technisch onderzoek datatlek', 10 mei 2016.
- Gemeente Rotterdam, brief aan burgers van directeur gemeentebelastingen 'Persoonsgegevens', 7 maart 2016.
- Wethoudersbrief, 'Beveiliging van e-mail', 8 juni 2016.
- Wethoudersbrief, 'Melding aan AP', 23 maart 2016.

rapportages concernauditing

- Financial Audit, 'Adviesrapport IT general controls (ITGC)', 9 juni 2016.
- Concern Auditing, 'Deelrapportage audit informatiebeveiliging fase 1 management control IB', 19 februari 2015.
- Concern Auditing, 'Deelrapportage IB processen audit informatiebeveiliging', 29 mei 2015.
- Concern Auditing, 'Eindrapportage onderzoek informatiebeveiliging 2014', 29 mei 2015.

- Concern Auditing, 'Informatiebeveiliging 2016 LBA: IB eisen en afspraken leverancier', 25 juli 2016.
- Concern Auditing, 'Rapportage ICT beveiligingsassessment DigiD 2013', 27 september 2013.
- Concern Auditing, 'Rapportage ICT beveiligingsassessment DigiD 2014, 30 april 2015.
- Concern Auditing, 'Rapportage Informatiebeveiliging (nulmeting sturen en beheersen), 16 april 2013.
- Financial Audit, 'Rapportage uitkomsten ITGC 2015', 2 februari 2016.
- Financial Audit, 'Samen verder: verbeteradviezen op de ITGC', 4 mei 2016.
- Concern Auditing, 'Zelfevaluatie basisregistraties', 1 juli 2016.

overige documenten

- College Bescherming Persoonsgegevens, 'CBP Richtsnoeren beveiliging van persoonsgegevens', februari 2013.
- Gemeente Rotterdam en EPA partners (Ipse de Bruggen, Stichting Pameijer, NIFP Rotterdam Dordrecht, Stichting PerspeKtief, Zorgorganisatie ASVZ), 'Aanvullend privacyreglement EPA aanpak, 1 januari 2016.
- Gemeente Rotterdam, 'Concern Classificatietabel (van bedrijfskritische applicaties)', september 2013.
- Gemeente Rotterdam, 'GAP analyse systeem F', 13 mei 2016.
- Gemeente Rotterdam, 'Informatiebeheerplannen', ongedateerd.
- Gemeente Rotterdam, 'Inventarisatie kwetsbare functies W&I 2013, ongedateerd.
- Gemeente Rotterdam, 'Risicoanalyse nalatenschaponderzoek', ongedateerd.
- Gemeente Rotterdam, 'Vragen GAP analyse clusters', ongedateerd.
- Gemeente Rotterdam, cluster Werk & Inkomen, diverse exemplaren van incidentenrapportages, 'Incidentenrapportage', uit jaar 2009 tot en met jaar 2015.
- Gemeente Rotterdam, diverse exemplaren van rapportage informatiebeveiliging, 'Rapportage informatiebeveiliging', uit jaar 2012 tot en met jaar 2016.
- Gemeente Rotterdam, inzake applicatie B, 'Autorisaties medewerker budgetbeheer', ongedateerd.
- Gemeente Rotterdam, inzake applicatie B, 'Autorisaties schuldbemiddelaar', ongedateerd.
- Gemeente Rotterdam, inzake applicatie B, 'Gebruikers B', ongedateerd.
- Gemeente Rotterdam, inzake applicatie B, 'Overzicht 2016 wachtwoorden en accounts B', ongedateerd.
- Gemeente Rotterdam, inzake applicatie B, 'Risico's autorisaties', ongedateerd.
- Gemeente Rotterdam, inzake applicatie B, 'Rollen', ongedateerd.
- Gemeente Rotterdam, inzake applicatie B, 'Selectie zaterdag en zondag SZW', ongedateerd.
- Gemeente Rotterdam, inzake applicatie B, 'Uittreksel en managementrapportage zelfevaluatie vragenlijst BRP 2016', ongedateerd.
- Gemeente Rotterdam, inzake applicatie B, 'Vragenlijst BRP', ongedateerd.
- Gemeente Rotterdam, inzake applicatie C, 'C rollen naar rechten itemgroepen', ongedateerd.
- Gemeente Rotterdam, inzake applicatie E, 'Autorisatie E', 10 juni 2016.
- Gemeente Rotterdam, inzake applicatie E, 'Autorisatiematrix', ongedateerd.
- Gemeente Rotterdam, inzake applicatie E, 'Autorisatiematrix E', 19 september 2016.
- Gemeente Rotterdam, inzake applicatie E, 'Deactiveren gebruikers MC VW's en WT's', 19 september 2016.
- Gemeente Rotterdam, inzake applicatie E, 'Evidence t.a.v. werking autorisatiematrix', ongedateerd.

- Gemeente Rotterdam, inzake applicatie E, 'Geleverde dienstverlening Q1 irt normen SLA', ongedateerd.
- Gemeente Rotterdam, inzake applicatie E, 'Interne audit rapportage ISO27001 en NEN 7510', ongedateerd.
- Gemeente Rotterdam, inzake applicatie E, 'Rapportage overzicht restrisico's', november 2015.
- https://rio.rotterdam.nl/Project/ConcernInformatiebeveiliging/Documents#!/path=%7CVeilig%20werken%20met%20mobiele%20apparatuur/, geraadpleegd op 27 december 2016.
- Informatiebeveiligingsdienst, 'Handreiking dataclassificatie', oktober 2013.
- Informatiebeveiligingsdienst, 'Status informatiebeveiliging op basis van BIG gemeente Rotterdam', 29 juli 2014.
- Informatiebeveiligingsdienst, 'Strategische baseline informatiebeveiliging Nederlandse gemeenten', ongedateerd.
- Informatiebeveiligingsdienst, 'Tactische baseline informatiebeveiliging Nederlandse gemeenten', 27 juli 2015.
- Lost Lemon B.V., 'Toegangsbeveiligingsbeleid Lost Lemon B.V.', 14 maart 2015.
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 'Baseline Informatiebeveiliging Rijksdienst tactisch normenkader (TNK)', 1 december 2012.
- Overeenkomst tussen gemeente Rotterdam en NVSI inzake applicatie E, 9 januari 2014.
- Service level agreement C gemeente Rotterdam en Conclusion Digital, 8 december 2016.
- Service level agreement gemeente Rotterdam en E NVSI, 2 november 2015.

bijlage 3 lijst met begrippen

back-up	een veiligheidskopie van programma`s en data
persoonsgegevens	elk gegeven dat te herleiden is tot een persoon
bijzondere persoons-gegevens	BSN-nummers en gegevens m.b.t. ras, godsdienst, politieke voorkeur, gezondheid, seksueel leven, lidmaatschap van vakbond en strafrechtelijk verleden
comply or explain	pas toe of leg uit
cross-site scripting	een fout in de beveiliging van een webapplicatie
cybercrime	criminaliteit op of via het internet
datalek	wanneer (persoons)gegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben
hacken	illegaal inbreken op computers
logging	het bijhouden van loggegevens
penetratietest	onderzoek naar kwetsbaarheden in computersystemen
social engineering	een persoon verleiden om informatie vrij te geven die in principe niet toegankelijk zijn voor derden
thin client	computersysteem zonder externe opslag, dat wordt geplaatst in een netwerk met een centrale server met terminals

Rekenkamer ROTTERDAM

bijlage 4 lijst met afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BCO	Bestuurs- en Concernondersteuning
BIG	Baseline Informatiebeveiliging Gemeenten
BIG	Baseline Informatiebeveiliging Nederlandse Gemeenten
BIV	Beschikbaarheid, integriteit en vertrouwelijkheid
BRP	Basisregistratie personen
BSN	Burgerservicenummer
CIO	Chief Information Officer
CISO	Chief information security officer
DIA	Dienstencentrum Informatie en Automatisering
DigiD	Digitale Identiteit
DNS	Domain Name System
DV	Dienstverlening
DVO	Dienstverleningsovereenkomst
fte	full time equivalent
IB	informatiebeveiliging
IBD	Informatiebeveiligingsdienst
ict	informatie- en communicatietechnologie
IIFO	Innovatie, Informatievoorziening, Facilitair en Onderzoek
IP	Internet Protocol
ISO	Information security officers
IT	Informatie Technologie
MO	Maatschappelijke Ontwikkeling
PDCA	Plan-do-check-act
PIA	Privacy Impact Assessment
SB	Stadsbeheer
SLA	Service level agreement
SO	Stadsontwikkeling
SUWI	Structuur Uitvoering Werk en Inkomen
TPM	Third party mededeling
VNG	Vereniging Nederlandse Gemeenten
W&I	Werk & Inkomen
Wbp	Wet bescherming persoonsgegevens
WiFi	Wireless Fidelity
Wmo	Wet maatschappelijke ondersteuning
Wob	Wet openbaarheid van bestuur