Rekenkamer
Den Haag

Retouradres: Postbus 19157, 2500 CD Den Haag

Raadscommissie Bestuur
Mevrouw Michels-Spee, voorzitter

Uw kenmerk

Ons kenmerk
RK/2013.38
Doorkiesnummer
070-3532048
E-mailadres
rekenkamer@denhaag.nl
Aantal bijlagen
1
Datum
2 oktober 2013

Onderwerp:
Aankondiging onderzoek Quick Scan Digitale Veiligheid

Geachte voorzitter,

Hierbij ontvangt u het onderzoeksplan 'Quick Scan Digitale Veiligheid'

De rekenkamer wil met deze quick scan bijdragen aan de beveiliging van gevoelige informatie over burgers en bedrijven bij de gemeente Den Haag, de bewustwording van het belang van informatiebeveiliging en het vergroten van kennis over de staat van de informatiebeveiliging van de gemeente.

Bij de uitvoering van dit onderzoek werkt de rekenkamer samen met een extern bureau met relevante expertise.

De aard van het onderzoek en de gevoeligheid van bij het onderzoek betrokken informatie alsmede mogelijk gevoelige uitkomsten van het onderzoek zijn voor de rekenkamer aanleiding in de uitvoering en bij de rapportage van dit onderzoek te zoeken naar een bij het onderwerp passende vorm. In het kader van dit onderzoek zal de rekenkamer een deel van de bevindingen aan de raad rapporteren in de vorm van een vertrouwelijke bijlage bij het onderzoeksrapport. De rekenkamer zal, wanneer daar vanuit de commissie behoefte aan is, de bevindingen toelichten in een besloten vergadering van de commissie Bestuur.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

Ing Yoe Tan
Lid-rapporteur en waarnemend voorzitter

Rekenkamer Den Haag

Onderzoeksplan Quick Scan digitale veiligheid

30 september 2013

1. Aanleiding, probleemschets

Veiligheid van informatisering is steeds relevanter als gevolg van de toenemende informatisering in de samenleving. Niet alleen in de bedrijfsvoering, maar recent ook in de dienstverlening van overheid naar burger, neemt de informatisering drastisch toe. Informatieoverdracht tussen overheid en burgers gebeurt steeds meer digitaal. Tegelijkertijd werken overheden, en daarmee ook de gemeente Den Haag, intern aan het verregaand koppelen van data en processen. Dit alles dient veel doelen: het efficiënter maken van de gemeentelijke organisatie, verbeteren van de dienstverlening, maar ook het doeltreffender maken van beleid en bijvoorbeeld gerichter kunnen sanctioneren van burgers die zich niet aan regels houden.

Deze ontwikkelingen leiden er toe dat er steeds meer informatie digitaal wordt opgeslagen en dat gegevens, die mogelijk privacygevoelig zijn, steeds vaker en meer met elkaar gekoppeld worden. Processen, applicaties en netwerken worden complexer. Daarnaast verandert de manier waarop data wordt ontsloten. Door flexwerken, werken vanuit huis en mobiele toepassingen neemt het aantal ingangen naar toepassingen en data binnen de organisatie toe. Burgers krijgen meer toegang tot gegevens en netwerken via bijvoorbeeld 'mijndenhaag.nl' of het digitale loket op de website van de gemeente Den Haag. De kwetsbaarheid neemt toe met de complexiteit van systemen en door de toenemende toegankelijkheid van informatie. En met de toename van de hoeveelheid gedigitaliseerde informatie (en de koppeling daarvan) wordt de gevoeligheid van opgeslagen informatie hoger.

Een belangrijke vraag is of de beveiliging de trend van toenemende digitalisering voldoende bijhoudt. Binnen de gemeente Den Haag wordt gewerkt aan het professionaliseren van de informatiebeveiliging, onder meer met het aanstellen van een Concern Information Security Officer en met een beveiligingsparagraaf in de gemeentelijke I-visie. Niettemin blijft het de vraag of daarmee de bij gemeenten opgeslagen (gevoelige) informatie ook daadwerkelijk veilig is. Recente gebeurtenissen zoals de landelijke 'Diginotar-crisis' en 'Lektober' laten zien dat de veiligheid nog onvoldoende is gewaarborgd. Dat de gemeente Den Haag recent ten onrechte gemeentelijke bekendmakingen niet publiceerde is een voorbeeld van (nog) niet 'in control' zijn over de automatisering. Gemeenten worden telkens verrast door incidenten en risico's terwijl zij beschikken over grote hoeveelheden privacygevoelige informatie van burgers.
De rekenkamer wil daarom een proef op de som nemen door te laten onderzoeken in hoeverre gevoelige informatie van buitenaf te verkrijgen is.

2. Regelgeving, beleid en organisatie

- Wet- en regelgeving

De wettelijke basis voor beveiliging van digitale informatie bij overheden ligt in de Algemene Wet Bestuursrecht (AWB), afdeling 2.3 'verkeer langs elektronische weg'[1]. In artikel 2:14, derde lid is vastgelegd dat: 'Indien een bestuursorgaan een bericht elektronisch verzendt, geschiedt dit op een voldoende betrouwbare en vertrouwelijke manier'. Het begrip 'verzenden' moet hier breed worden geïnterpreteerd: het gaat om elke vorm van gegevens uitwisseling met een andere partij[2].
Daarnaast wordt in de Wet Bescherming Persoonsgegevens (WBP) artikel 13 bepaald: 'De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking'.

Beide uitgangspunten zijn op verschillende aspecten uitgewerkt in wettelijke kaders of richtlijnen. Een nadere omschrijving van het in de AWB gebruikte 'betrouwbaarheid' is uitgewerkt in de handreiking 'Betrouwbaarheidsniveaus voor elektronische overheidsdiensten'[3]. Een ander voorbeeld is de Wet Elektronische Handtekeningen op basis waarvan in het Burgerlijk Wetboek vereisten zijn opgenomen waaraan een elektronische handtekening moet voldoen, wil deze rechtsgeldig zijn.
In de 'Wet algemene bepalingen Burgerservicenummer' zijn specifiek richtlijnen opgenomen voor het gebruik en de verificatie van het Burgerservicenummer. Alle overheidsdiensten kunnen het Burgerservicenummer gebruiken. Belangrijke vereiste is de 'vergewisplicht': de organisatie die het nummer wil gebruiken dient zich ervan te vergewissen dat het nummer daadwerkelijk bij de betreffende persoon hoort[4].

Samenwerkingsverbanden en relevante partijen

Naar aanleiding van een aantal grote incidenten met gevolgen op landelijk schaalniveau, onder meer de Diginotar-crisis en het zogenaamde 'Lektober'[5], is er landelijk aandacht voor de beveiliging van gemeentelijke informatiesystemen. Samenwerkingsverbanden tussen gemeenten onderling en met bijvoorbeeld de Nationaal Coördinator Terrorismebestrijding (NCTB) zijn opgezet en vanuit het Rijk worden eisen gesteld aan gemeenten om de informatiebeveiliging te verbeteren. Belangrijke partijen in de samenwerking zijn het Kwaliteitsinstituut Nederlandse Gemeenten (KING), het Nationaal Cyber Security Center (NCSC), het Forum Standaardisatie[6] en sinds 1 januari 2013 de Informatie Beveiligingsdienst (IBD), een samenwerking tussen de gemeenten en Rijk met als doel een gestandaardiseerde informatiebeveiliging bij gemeenten te realiseren.

---

[1] artikelen 2:13 tot en met 2:17 hebben betrekking op 'elektronisch verkeer' tussen overheden en burgers en overheden onderling.
[2] 'Betrouwbaarheidsniveaus voor elektronische dienstverlening', Forum standaardisatie, p. 33
[3] Forum Standaardisatie en Logius, januari 2012.
[4] Wet algemene bepalingen Burgerservicenummer, artikel 12.
[5] Diginotar-crisis: het bedrijf Diginotar verstrekte digitale authenticatie certificaten, digitale handtekeningen. Na een hack bij dit bedrijf kwamen valse digitale handtekeningen in omloop waarmee wereldwijd gevoelige websites werden gehacked. Lektober: in oktober 2011 komt in het nieuws dat de websites van een groot aantal Nederlandse gemeente 'open' staan voor buitenstaanders. Het is mogelijk om via de websites (gevoelige) informatie uit gemeentelijke systemen op te halen of te veranderen.
[6] Het Forum Standaardisatie is een initiatief van de Rijksoverheid. Doelstelling is de digitale samenwerking (interoperabiliteit) tussen overheden onderling en tussen overheid, bedrijfsleven en publiek te bevorderen door het opstellen van standaarden voor informatie en informatiebeveiliging)

Relevante documenten en acties

Vanuit de hierboven beschreven instituten zijn vooralsnog drie relevante producten gerealiseerd. Ten eerste is afgesproken dat het Digid jaarlijks door elke gemeente getest moet worden. Wanneer gemeenten niet voldoen aan gestelde eisen, of de test niet uitvoeren, kunnen ze door het Rijk worden uitgesloten van het gebruik van Digid. Ten tweede is er een handreiking gepubliceerd die een standaard neerlegt voor het bepalen van betrouwbaarheidsniveaus van informatie. Daarmee wordt de vraag beantwoord wat bedoeld wordt met het begrip 'voldoende betrouwbaar' uit de AWB (zie hierboven). Tenslotte is recent door het IBD de Baseline Informatiebeveiliging Gemeenten (BIG) opgesteld. Dit is een normenkader volgens ISO standaarden voor het implementeren en onderhouden van informatiebeveiliging bij gemeenten[7].

- Gemeentelijk beleid

In november 2011 heeft het college de gemeentelijke I Visie (2011-2014) vastgesteld[8] met een perspectief op hoofdlijnen over de volle breedte van de gemeentelijke ICT. Onderdeel van de I visie is het beleid ten aanzien van beveiliging van ICT, dat zich richt op de onderwerpen 'vertrouwelijkheid', 'beschikbaarheid' en 'integriteit'. Vertrouwelijkheid gaat over de bescherming van gegevens, de beschikbaarheid betreft de beveiliging tegen het uitvallen van systemen en integriteit gaat over de betrouwbaarheid van gegevens. De gemeentelijke ambities met betrekking tot veiligheid van ICT zijn[9]:

- Blijvende borging van veilige digitale communicatie tussen burgers/ bedrijven en gemeente.
- Verbetering van de beschikbaarheid van kritische ICT-systemen, vooral op het gebied van
- de dienstverlening aan burgers en bedrijven.
- Een afgewogen beveiligingsbeleid en een slagvaardige informatiebeveiligingsorganisatie.

De I visie sluit aan op landelijke richtlijnen, zoals de 'Handreiking betrouwbaarheidsniveaus elektronische dienstverlening'[10].

In de commissiebrief 'Stand van zaken informatiebeveiliging' van oktober 2012[11] gaat de verantwoordelijke portefeuillehouder in op de vorderingen op het gebied van beveiliging. Het betreft het waarborgen van de beschikbaarheid en de continuïteit van 10 kritische processen, het omgaan met grote incidenten en het 'in control' zijn door diensten bij de verschillende informatie beheer processen en procedures. Doelstelling is dat in de loop van 2013 noodzakelijke verbetering doorgevoerd zijn en dat in tweede helft van 2013 deze verbeteringen worden getoetst.
Op 18 juni 2013 is de eerste voortgangsrapportage bij de I-Visie door het college naar de raad gestuurd[12] waarin ook de stand van zaken op het gebied van informatiebeveiliging is weergegeven[13].

---

[7] Strategische respectievelijk Tactische Baseline Informatiebeveiliging Nederlands Gemeenten, Informatiebeveiligingdienst/ KING/VNG, mei 2013.
[8] RIS 181621, 'Get connected – sluit je aan', gemeentelijk I Visie, 1 november 2011.
[9] I Visie, p. 15.
[10] I Visie, p. 14. Hier wordt gesproken over "Handreiking Classificatie van overheidsdiensten en bepaling van het daarvoor vereiste betrouwbaarheidsniveau". De in de tekst hierboven opgenomen titel is van de definitieve versie van deze handreiking. Deze handreiking wordt in dit onderzoeksplan besproken bij 'Wet en regelgeving'
[11] RIS 253203, 30 oktober 2012.
[12] RIS 260175, 'Voorgangsrapportage I Visie, Get connected – Sluit je aan', 18 juni 2013.
[13] RIS 260175, p. 5-6.

De rapportage levert op hoofdlijnen geen aanvullende informatie ten opzichte van de hierboven genoemde commissiebrief 'Stand van zaken informatiebeveiliging'. Wel wordt er melding gemaakt van een aantal specifieke vorderingen, zoals het benoemen van cyber security risico's (in maart 2013), tweejaarlijks actualiseren van software (vanaf 2013) en het operationaliseren van hulpmiddelen om kwetsbaarheden in software op te sporen (vanaf eerste kwartaal 2013).

- Organisatie van de gemeentelijke beleidsuitvoering

Sinds 2011 heeft de gemeente een Chief Information Officer (CIO), die met het Gemeentelijk Management Team (GMT) en de directeur van het Intern Diensten Centrum (IDC) de IT Board vormt. De CIO geeft leiding aan de concern brede 'ICT governance'[14]. Hij organiseert maandelijks een concernoverleg informatievoorziening, waarin de informatiemanagers van alle diensten zitting hebben. Informatiebeveiliging is op een vergelijkbare wijze georganiseerd met een Concern Information Security Officer (CISO), verantwoordelijk voor de concern brede aanpak van informatiebeveiliging en Dienst Information Security Officers bij alle diensten. Deze structuur komt overeen met de normen voor verantwoordelijkheidsverdelingen en rollen zoals neergelegd in de Baseline Informatiebeveiliging Gemeenten[15].

3. Relevantie

- Financieel belang

Den Haag geeft per jaar ongeveer 70 miljoen euro uit aan ICT, verspreid over alle diensten. Specifieke bedragen voor informatiebeveiliging zijn niet bekend. In totaal werken binnen de gemeente circa 350 FTE binnen het ICT-werkveld[16].
Het is niet bekend hoe groot de financiële schade kan zijn door problemen met informatiebeveiliging. Een raming door de landelijke Informatiebeveiligingsdienst geeft aan dat de schade voor alle gemeenten jaarlijks 300 miljoen euro zou kunnen bedragen[17], maar de financiële belangen bij diensten die met digitale systemen worden geleverd kunnen nog groter zijn. Zo worden met het systeem 'Socrates' alle Haagse uitkeringen overgemaakt. De gemeentelijke basisadministratie is een bestand dat door bijvoorbeeld de belasting wordt gebruikt bij het toekennen en uitkeren van toeslagen. Er is daardoor (latent) een financieel belang voor mogelijke indringers bij het ophalen of manipuleren van gegevens die bij de gemeente in beheer zijn.

- Maatschappelijk belang

De gemeente beschikt over veel vertrouwelijke informatie over burgers. Die informatie moet in veilige handen zijn bij de gemeente, moet juist zijn (bijvoorbeeld actueel) en niet beschikbaar zijn voor personen anders dan de burger zelf of ambtenaren die deze informatie voor hun werk in moeten zien. Daarnaast is het voor de gemeente en burgers van belang dat de dienstverlening niet verstoord kan worden, bijvoorbeeld door hackers die de website van de gemeente 'platleggen' of het systeem voor het verstrekken van uitkeringen verstoren. Informatiebeveiliging heeft dan ook als doel de beschikbaarheid, de integriteit en de vertrouwelijkheid van informatie en processen te waarborgen[18].

---

[14] I Visie p. 2.
[15] In het voorbereidend onderzoek voor dit onderzoeksplan is niet geanalyseerd of de organisatiestructuur volgens BIG volledig is overgenomen
[16] Bron middelen en Fte's: gemeentelijke I-Visie, RIS 181621, p. 5.
[17] Strategische Baseline Informatiebeveiliging, IBD, mei 2013, p. 3.
[18] Tactische Baseline Informatiebeveiliging, IBD, mei 2013, p. 7

- Politiek/ bestuurlijk belang

Informatiebeveiliging is een breed gedragen onderwerp. Er zijn geen politieke belangen of tegenstrijdigheden in de belangen van afzonderlijke partijen ten aanzien van het principe dat gegevens bij de gemeente veilig moeten zijn.
Aan (digitale) informatie en processen is wel een bestuurlijk risico verbonden. De publiciteit en raadsvragen naar aanleiding van het niet publiceren van gemeentelijke bekendmakingen en het kwijtraken van twee dozen met aktes van de burgerlijke stand laten zien dat problemen met informatisering veel aandacht genereren richting gemeentebestuur[19].

4. Toegevoegde waarde

Er is nog weinig onderzoek naar digitale veiligheid gedaan door onafhankelijke onderzoeksinstituten, of door lokale rekenkamers[20]. Zowel op Rijksniveau als binnen de gemeente wordt op ambtelijk niveau wel onderzoek gedaan ten behoeve van de informatiebeveiliging.

Rijksniveau

De Rijksoverheid heeft naar aanleiding van de Diginotar-crisis verschillende (interne) onderzoeken gedaan. Het Diginotar incident is ook onderzocht door de Onderzoeksraad voor de Veiligheid[21]. De onderzoeksraad richt zich met het rapport en de aanbevelingen op de organisatie-beheersaspecten en de bestuurlijke verantwoordelijkheid voor digitale veiligheid.
Het Nationaal Cyber Security Centrum brengt periodiek een 'Cybersecuritybeeld Nederland' uit, met de meest actuele stand van zaken op het gebied van bedreigingen van informatisering in Nederland[22].

Gemeentelijk niveau

De gemeente Den Haag voert audits, assessments en penetratietesten uit naar de beveiliging van informatie. Er worden ook interne rapportages opgesteld over de voortgang op het gebied van verbetering van de informatiebeveiliging (in het kader van de uitvoering van de I-Visie). Deze rapportages volgen onder meer het proces van veranderingen waarmee diensten 'in control' moeten worden van de informatisering.
De Amsterdamse gemeentelijke accountantsdienst (ACAM)[23] doet jaarlijks een audit naar de beheersaspecten in de samenwerking tussen de sociale diensten van de G4 (Wego4it). Onderdeel daarvan is een audit specifiek voor de beheersaspecten van Socrates, de applicatie waarmee sociale diensten uitkeringen verstrekken. De GAD gaat in de toekomst de 'in control statements' controleren, die diensten als onderdeel van de I visie eind 2013 af moeten geven.

---

[19] Door een fout in een systeem publiceerde de gemeente tussen maart 2012 en maart 2013 533 gemeenteberichten per ongeluk niet. In februari raakte de gemeente twee dozen met akten uit de burgerlijke stand kwijt. Dit had publiciteit tot gevolg en vragen die door de raad aan de verantwoordelijke wethouder werden gesteld (bron: Binnenlands Bestuur, 29 maart 2013, 'Den Haag is aktes en publicaties kwijt').
[20] In de lijst rekenkamerrapporten op de site van de NVRR is geen rapport opgenomen over dit onderwerp.
[21] 'Het diginotar incident – waarom digitale veiligheid de bestuurstafel te weinig bereikt', Onderzoeksraad voor de Veiligheid, 28 juni 2012.
[22] 'Cybersecuritybeeld Nederland', Nationaal Cyber Security Centrum, juni 2012.
[23] Vanuit Den Haag is een medewerker van de Gemeentelijke Accountantsdienst (GAD) lid van de auditcommissie die deze onderzoeken uitvoert.

Het Rijk verplicht gemeenten jaarlijks een Digid-assessment te doen. Deze verplichting is één van de acties naar aanleiding van de Diginotar-crisis. Gemeenten die niet tijdig het assessment doen of die niet voldoen aan de gestelde eisen, kunnen door de minister van Binnenlandse Zaken uitgesloten worden van Digid.

Als onderdeel van het gemeentelijke ICT beleid, worden zoals aangegeven penetratietesten uitgevoerd op processen en systemen van alle diensten. Bij een penetratietest worden de zwakheden in het netwerk en of de systemen voor beveiliging gezocht en getest. Deze testen zijn minder diepgaand dan het *hacken* van een systeem. Er wordt bijvoorbeeld niet gekeken naar niet digitale manieren waarmee systemen of informatie benaderd kunnen worden, bijvoorbeeld door medewerkers van de gemeente zelf. Ook wordt niet gekeken naar de risico's die voortkomen uit de gevonden zwakheden. Penetratietesten worden gezien als 'een eerste stap' op weg naar een goede beveiliging[24]. *Hackers* maken gebruik van een veel breder scala aan mogelijkheden voor het openbreken van systemen. Een quick scan waarbij een breder scala aan middelen wordt ingezet voor het verkrijgen van toegang sluit beter aan op de daadwerkelijke risico's.

Rekenkamer

Een Quick Scan door de rekenkamer waarbij de beveiliging feitelijk getoetst wordt, heeft als meerwaarde dat het inzicht geeft in de concrete realiteit van de informatiebeveiliging. Waar rapporten vanuit het Rijk en de gemeente zich richten op beheersaspecten of randvoorwaarden voor informatiebeveiliging, kan een gerichte simulatie waarbij geprobeerd wordt door de beveiliging heen te komen, informatie geven over de feitelijke stand van zaken van de informatiebeveiliging en over mogelijke zwakke schakels in die beveiliging.

5. Doel en probleemstelling, onderzoeksvragen

De rekenkamer wil met deze quick scan bijdragen aan de beveiliging van gevoelige informatie over burgers en bedrijven bij de gemeente Den Haag, de bewustwording van het belang van informatiebeveiliging en het vergroten van kennis over de staat van de informatiebeveiliging van de gemeente.

Probleemstelling

Welke waarborgen bieden de genomen maatregelen tegen oneigenlijk benaderen van gevoelige informatie bij de gemeente Den Haag?

De probleemstelling is uitgewerkt in de volgende onderzoeksvragen:

- is het mogelijk oneigenlijke toegang tot (belangrijke) systemen en bestanden te krijgen?
- wat zijn de zwakke plekken in de beveiliging tegen het oneigenlijk benaderen van gevoelige informatie bij de gemeente?
- welke informatiesystemen (netwerken, infrastructuur en applicaties) zijn te identificeren als 'zwakke schakels'?
- welke factoren afgezien van informatie technologie zijn te identificeren als 'zwakke schakels' in de beveiliging van gevoelige informatie?

[24] Informatieblad 'penetratietest', Fox-it security (via www.fox-it.com)

6. Aanpak

De rekenkamer verstrekt voor de uitvoering van dit onderzoek opdracht aan een bedrijf dat in staat is met de nieuwste technieken in te breken in de systemen en bestanden van de gemeente Den Haag. Er is een aantal van dit soort bedrijven in Nederland actief, met onder andere ervaring bij andere gemeenten en overheden. Aan drie bedrijven is een offerteverzoek gedaan. Na vergelijking van de voorstellen heeft de rekenkamer opdracht verleend aan een gespecialiseerd bureau op het gebied van dergelijke onderzoeken.
De rekenkamer realiseert zich terdege de gevoeligheden en risico's die verbonden zijn met een dergelijk onderzoek. Zij stelt daarom de volgende randvoorwaarden voor het garanderen van de zorgvuldigheid:

- De opzet en uitvoering van dit onderzoek wordt in nauw overleg gedaan met verantwoordelijke bestuurder(s) en ambtenaren. De rekenkamer rekent daartoe in ieder geval: de verantwoordelijke portefeuillehouder, betrokken sector- of algemeen directeuren bij gemeentelijke diensten, de Chief Information Officer en de Concern Information Security Officer.
- De opdrachtnemer voldoet aan de volgende vereisten:
    - ervaring met vergelijkbaar onderzoek bij tenminste drie andere overheidsinstellingen
    - screening van de medewerkers door de politie
    - voldoen aan vereisten wet particulier beveiligingsbedrijven en recherchebureaus
    - aansluiting bij een relevante beroepsvereniging

Voor de Quick Scan zullen minimaal twee systemen of databases benaderd worden. In overleg met de opdrachtnemer zal worden bepaald hoe de quick scan het best ingericht kan worden zodat aanbevelingen zo breed mogelijk toepasbaar kunnen zijn.

Voor de uitvoering van het onderzoek zijn de volgende scenario's geschetst:

- Een test naar de mogelijkheid om via de website www.denhaag.nl toegang te krijgen tot daaraan verbonden systemen/ processen/ data
- Een test naar de mogelijkheid om via het wifi-netwerk in het stadhuis toegang te krijgen tot gemeentelijke systemen/ processen data
- Een test om met een standaard gebruikers account toegang te krijgen tot gemeentelijke systemen/ processen/ data
- Toepassen van phishing/ peer phishing. Hierbij wordt geprobeerd inloggegevens van medewerkers te verkrijgen door het rondsturen van mails met ogenschijnlijk veilige verzoeken tot het geven van informatie of in het tweede geval het tussen systeem en gebruiker plaatsen van op het origineel gelijkende website pagina's.
- Het plaatsen van sensoren in gemeentelijke systemen. Hiermee wordt onderzocht in hoeverre er al besmetting is en bijvoorbeeld al backdoors bestaan waarmee derden toegang hebben tot gemeentelijke systemen.
- Inloop tests, waarbij via social engineering (rondlopen, medewerkers informatie proberen te laten geven) en het inpluggen van laptops/ usb sticks of gebruik maken van netwerkstations van medewerkers proberen toegang te krijgen.

Verschillende methoden kunnen parallel aan elkaar worden uitgevoerd. Een doorlooptijd van 4 tot 6 weken voor het uitvoeren van het onderzoek lijkt haalbaar.

7. Planning en organisatie

Fase	Activiteiten	Periode in de tijd
Voorbereiding	Aankondiging onderzoek Offertetraject(selectie externen)	juli-oktober 2013
Feitenonderzoek	Onderzoeksactiviteiten zoals benoemd in paragraaf 6	half oktober - november
Rapportage	Feitenrapport en ambtelijke reactie Bestuurlijk rapport, bestuurlijke reactie	december - januari 2014
Publicatie		februari 2014

Bij dit onderzoek zijn betrokken:
De heer Rabin Baldewsingh, verantwoordelijk portefeuillehouder ICT
De heer Gerard Boot, directeur concern bedrijfsvoering
De heer Jan Willem Duijzer, Chief Information Officer
De heer Jilles van Harselaar, Concern Security Information Officer
De heer Pablo Hunnego, directeur IDC
Afhankelijk van de definitieve keuze ten aanzien van de aanpak van het onderzoek, en de te onderzoeken systemen, de daarvoor verantwoordelijk portefeuillehouder(s) en de verantwoordelijken op dienstniveau.

Mevrouw Ing Yoe Tan (tijdelijk): lid rapporteur rekenkamer
Mevrouw Mirjam Swarte: secretaris
De heer Thijs Bosma: onderzoeker/ projectleider rekenkamer
Contactpersoon opdrachtnemer

Bijlage 1 Verantwoording voorbereidingsfase/ literatuur

Bij het opstellen van dit onderzoekplan is van de volgende bronnen gebruik gemaakt:

- Algemene wet bestuursrecht (vooral artikel 2.14)
- Algemene wet bescherming persoonsgegevens (artikel 13)
- Burgerlijk wetboek artikel 15 a en b/ Wet elektronische handtekeningen
- Algemene beginselen van behoorlijk IT-gebruik. Kamerstukken II 2001/02, 28 483, nr. 3, p. 15.
- Handreiking 'Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten' (januari 2012), Forum Standaardisatie.
- Strategische- en Tactische Baseline informatiebeveiliging Nederlandse gemeenten (mei 2013), Informatie Beveiligings Dienst (IBD).
- VNG ledenbrief 'Informatiebeveiliging' (6 juni 2013), VNG.
- RIS 181621, 'Get connected – sluit je aan', gemeentelijk I Visie, 1 november 2011 (inclusief toelichtende commissiebrief).
- RIS 260175, 'Voorgangsrapportage I Visie, Get connected – Sluit je aan', 18 juni 2013 (inclusief toelichtende commissiebrief).
- RIS 253203, commissiebrief 'Stand van zaken informatiebeveiliging', 30 oktober 2012.
- 'Het diginotar incident – waarom digitale veiligheid de bestuurstafel te weinig bereikt' (28 juni 2012) Onderzoeksraad voor de Veiligheid.
- Informatieblad 'penetratietest', Fox-it security (via www.fox-it.com/ 16 juni 2013 geraadpleegd)

Er is gesproken met de volgende personen:
De heer Jan Willem Duijzer (Chief information officer)
De heer Jilles van Harselaar (Chief information security officer)
De heer Hans Kortekaas (Hoofd afdeling interne audits dienst SZW)
De heer Marco van Beek (ACAM) met betrekking tot audits bij Wego4it onder leiding van ACAM.
Vertegenwoordigers van drie bureaus gespecialiseerd in informatiebeveiliging.