Rekenkamer
Den Haag

Digitale veiligheid

Digitale veiligheid

Colofon

Rekenkamer Den Haag

Leden
- de heer Watze de Boer, voorzitter
- mevrouw Ing Yoe Tan (tot 1 mei 2014)
- de heer Pieter Welp (tot 1 mei 2014)
- mevrouw Pauline Reeuwijk (per 1 mei 2014)
- de heer Wicher Schönau (per 1 mei 2014)

Aan dit onderzoek hebben meegewerkt
- Mirjam Swarte, secretaris rekenkamer
- Thijs Bosma, senior onderzoeker
- Hoffmann ICT Security

Fotografie
Foto omslag: Shutterstock

Contactgegevens
Rekenkamer Den Haag
Postbus 19157
2500 CD Den Haag
Telefoon 070 - 353 20 48
www.rekenkamerdenhaag.nl

Bezoekadres
Stadhuis
Spui 70
2511 BT Den Haag

Datum
Juli 2014

Ontwerp
Studio Buffalo

Voorwoord

Digitale veiligheid staat meer nog dan voorheen in de belangstelling van overheid en bedrijfsleven. Inbreuken op digitale veiligheid leiden tot grote financiële en/ of imagoschade. De gemeente maakt in toenemende mate gebruik van gedigitaliseerde informatie en communicatie in haar contacten met burgers, bedrijven en instellingen. Daarmee ontwikkelt de overheid zich van een eOverheid naar een iOverheid, aldus de WRR in haar rapportages uit 2008 en 2011. De verantwoordelijkheid die de overheid draagt voor de fysieke veiligheid zou in gelijke mate moeten gelden voor de digitale veiligheid. Gegevens van burgers, bedrijven en instellingen moeten bij de gemeente in goede handen zijn. Dat is de essentie van het vertrouwen dat men in de overheid moet kunnen stellen.

Bovenstaande vormde mede aanleiding voor ons onderzoek naar de digitale veiligheid van de gemeente Den Haag. Door Hoffmann ICT Security hebben wij daarom penetratietesten op de ICT-infrastructuur van de gemeente laten uitvoeren. Hierbij kwam een groot aantal kwetsbaarheden in de beveiliging aan het licht. Sommigen daarvan waren naar ons oordeel dermate urgent dat wij, in afwijking van de gangbare procedure bij rekenkameronderzoek, hebben gemeend de organisatie en het college al in december 2013 van onze bevindingen op de hoogte te moeten stellen. Dit om, daar waar nodig, de organisatie de gelegenheid te bieden direct actie te ondernemen ten einde de meest urgente kwetsbaarheden weg te nemen. Door onze onderzoekers werden hiertoe aanbevelingen voor de korte termijn geformuleerd zodat de gemeente direct aan de slag kon.

Op grond van artikel 185 lid 1 van de Gemeentewet hebben wij gemeend het rapport van bevindingen in zijn geheel als vertrouwelijk te moeten bestempelen. Wat u hierna aantreft is dus uitsluitend onze bestuurlijke rapportage. Deze biedt naar ons oordeel voldoende inzicht in hoe het met de digitale veiligheid is gesteld en welke acties nog ondernomen zouden moeten worden. De reactie van het college laat zien dat alle aanbevelingen worden overgenomen en sommige al in uitvoering zijn. Het is nu aan de raad om dit te bevestigen en het onderwerp hoog op de agenda te plaatsen en te houden. Als thuishaven van ‘The Hague Security Delta’ zou de gemeente een voortrekkersrol moeten nemen op het gebied van digitale veiligheid.

100% veiligheid bestaat niet. Dat geldt zeker ook in de digitale wereld. De beveiliging hiervan is een dynamisch proces dat continu vraagt om aanscherping van maatregelen door nieuwe ‘dreigingen’, zoals het college het in zijn reactie terecht formuleert. Daarbij moet worden afgewogen welke capaciteit en deskundigheid de gemeente in eigen huis heeft of kan ontwikkelen en welke taken beter aan externe experts met actuele kennis van cybersecurity kunnen worden overgelaten.

De raad zal (aangepaste) kaders moeten stellen voorzien van passende budgetten en moeten toezien op een adequate verantwoording. De rekenkamer zal de ontwikkelingen in deze met belangstelling blijven volgen.

Inhoudsopgave

Inleiding

1.1 Aanleiding

Wettelijke plicht informatiebeveiliging

De gemeente beschikt over veel vertrouwelijke informatie van burgers en bedrijven. Die informatie moet in veilige handen zijn bij de gemeente. Zij moet volgens de Wet bescherming persoonsgegevens (Wbp) deze gegevens beveiligen en hiervoor passende technische en organisatorische maatregelen nemen. Informatie moet vertrouwelijk worden behandeld (niet in te zien dan door bevoegden), betrouwbaar zijn (juist en actueel) en beschikbaar zijn (systemen vallen niet uit).[1] De wet Basisregistratie personen geeft aan dat de verantwoordelijkheid voor de informatiebeveiliging van persoonsgegevens ligt bij het college van burgemeester en wethouders.[2] Gebruik van bij de gemeente aanwezige informatie anders dan waartoe deze beschikbaar is gesteld kan leiden tot grote schade voor burgers, bedrijven en voor de gemeente zelf. Zo kunnen criminelen met deze informatie identiteitsfraude plegen, waarvan burgers slachtoffer kunnen worden, bijvoorbeeld wanneer op hun naam leningen worden aangevraagd of een uitkering wordt verstrekt. Iedereen moet er op kunnen vertrouwen dat zijn of haar persoonsgegevens door de overheid voldoende worden beveiligd.

Figuur 1: definitie 'veilig' bij digitale informatie[3]

1 De wet bescherming persoonsgegevens (Wbp) geeft aan: 'de verantwoordelijke [voor bewaarde privacygevoelige informatie] legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking'. Daarnaast zijn bestuursorganen volgens de Algemene wet bestuursrecht (Awb) verplicht informatie voldoende betrouwbaar en vertrouwelijk te behandelen.

2 Artikel 1.9 tot en met 1.11 BRP: Het college van burgemeester en wethouders is verantwoordelijk voor de inrichting en beveiliging van de persoonsregistraties.

3 Bron: RIS 181621, 'Get connected – sluit je aan', gemeentelijk I-visie, 1 november 2011, p. 14.

Hoeveelheid gevoelige informatie neemt sterk toe

De omgang met en het belang van digitaal opgeslagen of uitgewisselde informatie groeit iedere dag.[4] Overheden, en daarmee ook de gemeente Den Haag, werken intern aan het koppelen van data en processen. En de communicatie met burgers en bedrijven gebeurt steeds vaker (alleen nog maar) digitaal. ICT is niet meer een interne aangelegenheid in de 'backoffice', maar behoort door het toenemende belang ervan tot de primaire processen van de gemeente, waarvan de maatschappelijke relevantie vergelijkbaar is met processen als het verstrekken van uitkeringen of het handhaven van regelgeving.

Het beveiligen van (digitale) informatie is van een ICT vraagstuk veranderd in een bestuurlijk relevant onderwerp en daarmee een verantwoordelijkheid van de gemeenteraad, die kaders zou moeten stellen en het college controleren op het uitvoeren van zijn taken op dit gebied. *'Digitale veiligheid is van een operationele een strategische kwestie geworden'.*[5]

Een actuele ontwikkeling is de taakverzwaring die gemeenten vanaf 2015 krijgen met de decentralisaties in het sociaal domein. De hoeveelheid informatie over burgers in beheer bij de gemeente zal daardoor sterk toenemen en de koppeling van die gegevens ook. Het is nu nog onduidelijk welke praktische gevolgen dit heeft. Zo is bijvoorbeeld nog onduidelijk in hoeverre koppeling van bestanden juridisch gezien generiek kan gaan gebeuren of alleen als maatwerk voor specifieke doelgroepen. Daarbij moet een balans gevonden worden tussen benodigde informatie voor het bereiken van een efficiënte beleidsuitvoering en het beschermen van privacy van burgers. Ook op bestuurlijk niveau tussen het Rijk en gemeenten is deze discussie nog niet afgerond.[6]

Bewustwording de afgelopen jaren

Naar aanleiding van onder meer de Diginotar-crisis en Lektober in 2011 is gebleken dat de informatiebeveiliging bij gemeenten niet altijd even goed op orde was. Landelijk zijn daarop verschillende initiatieven genomen waarmee deze beveiliging verbeterd kan worden. Sinds 1 januari 2013 werkt bijvoorbeeld de Informatie Beveiligings Dienst (IBD), een samenwerking tussen het ministerie van BZK en de gemeenten, aan het realiseren van een gestandaardiseerde informatiebeveiliging bij gemeenten. Het IBD heeft een Baseline Informatiebeveiliging Gemeenten (BIG)[7] opgesteld, waarmee gemeenten kunnen voldoen aan een basis beveiligingsniveau. Eén van de operationele producten op basis van de BIG is een 'Informatiebeveiligingsplan' waarin gemeenten algemene beleidsuitgangspunten vast kunnen leggen zoals classificatie van informatie, doelstellingen en maatregelen op het gebied van informatiebeveiliging.[8] Daarnaast werkt de Taskforce Bestuur en Informatieveiligheid Dienstverlening sinds februari 2013 aan het prominent op de bestuurlijke agenda krijgen van het onderwerp informatiebeveiliging. Met de Vereniging Nederlandse Gemeenten wordt ingezet op een 'verplichte zelfregulering'. Einddoel hiervan is dat vanuit gestelde kaders op landelijk- en koepelniveau in iedere gemeentelijke organisatie een jaarlijkse cyclus is geborgd waarin

4 Cyber Security Beeld Nederland 3, juli 2013, Nationaal Cyber Security Centrum, p. 9.
5 Patrick de Graaf, Capgemini, in: 'Opmars Cybersecurity', Fd.nl, 18 april 2014.
6 Bron: F. Blankena,'Privacy-vraagstuk rond decentralisaties ligt weer bij gemeenten', 17 maart 2014, website Binnenlands Bestuur.
7 Baseline Informatiebeveiliging Gemeenten, IBD, 2013. Deze Baseline bestaat uit een 'Strategisch' en een 'Tactisch' deel en biedt een volledig overzicht van uitgangspunten en maatregelen waarmee informatiebeveiliging gerealiseerd kan worden. In het eerste deel wordt ingegaan op de organisatie en de verantwoording over informatiebeveiliging, in het tweede deel worden normen en maatregelen beschreven voor controle en risicomanagement conform ISO/IEC 27002:2007.
8 Voorbeeld Informatiebeveiligingsbeleid Gemeenten, IBD, augustus 2013.

ambtelijke- en bestuurlijke oordeelsvorming over informatieveiligheid plaatsvindt. Dit einddoel is uitgewerkt in een resolutie die door de ledenvergadering van de VNG is vastgesteld (november 2013). Concreet houdt deze resolutie in dat gemeenten een informatiebeveiligingsbeleid vaststellen aan de hand van de Baseline Informatiebeveiliging Gemeenten.

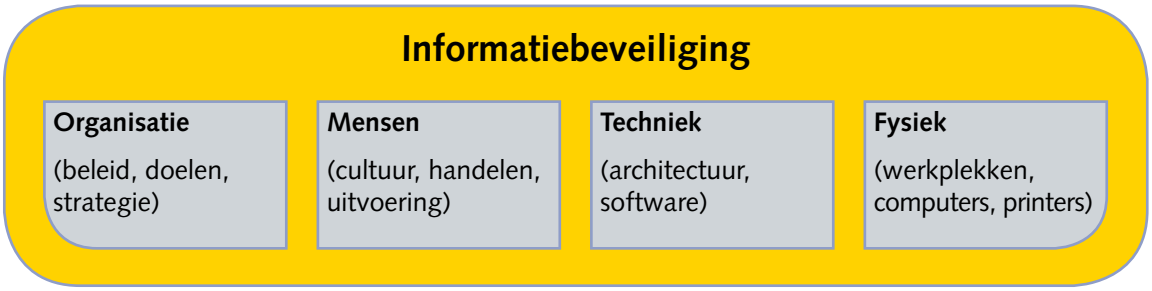
Het belang van informatiebeveiliging en de bescherming van privacygevoelige informatie is regelmatig in het nieuws. Incidenten hebben gevolgen voor burgers en voor de beheerders van informatie. Recent bleek dat zowel de Nederlandse Zorgautoriteit (NZa) als de Inspectie voor de Gezondheidszorg (IGZ) jarenlang onzorgvuldig waren geweest met privacygevoelige informatie.[9]
Eigen medewerkers hadden bij beide instellingen via een intern informatiesysteem vrij toegang tot gegevens die ze wettelijk niet in mogen zien. In april 2014 sloot de gemeente Velsen uit voorzorg haar digitale loket. Gebleken was dat hierin een kwetsbaarheid zat waarmee het mogelijk is ogenschijnlijk veilig internet verkeer tussen gemeente en burgers 'af te luisteren'.[10] Burgers moesten daarom weer langskomen op het stadhuis of bellen met de gemeente voor informatie over diensten van de gemeente. Uit bovenstaande voorbeelden wordt duidelijk dat onvoldoende kennis van bedreigingen en een langzame reactie op incidenten tot ernstige schending van vertrouwelijkheid kan leiden en flinke imagoschade voor instellingen en overheden. Risico's zijn nooit volledig uit te sluiten, ook 'digitaal' bestaat volledige veiligheid niet. Bij het uitvoeren van informatiebeveiliging gaat het daarom niet alleen om preventieve maatregelen, kennis van bedreigingen en kwetsbaarheden, maar ook om monitoring van systemen op oneigenlijk gebruik en een alerte reactie bij incidenten of misbruik.

Informatiebeveiliging is complex

Er zijn verschillende vormen van oneigenlijk gebruik van gegevens. Personen kunnen moedwillig van buitenaf proberen gegevens te bemachtigen, zogenaamde 'cybercrime', met als doel bijvoorbeeld identiteitsfraude of het belemmeren van dienstverlening door systemen uit te schakelen. Misbruik kan ook van binnen de organisatie komen. Al dan niet kwaadwillig kunnen gegevens worden benaderd door medewerkers van de gemeente die voor hun werk deze gegevens niet nodig hebben. De gemeente is wettelijk verplicht ook dergelijke schendingen van de privacy van burgers te voorkomen. Kwaadwillenden kunnen op veel verschillende manieren proberen toegang te krijgen tot de ICT-systemen van de gemeente en tot privacygevoelige informatie van burgers en bedrijven. Dat zou kunnen gaan via vanaf het internet bereikbare systemen zoals de gemeentelijke website of routers die in verbinding staan met aan de gemeente gelieerde systemen, via het bemachtigen van inlog- en wachtwoord gegevens of via het overnemen van een pc van medewerkers. Methoden die kunnen worden toegepast zijn het aanvallen van de website, het verzenden van phishing- emails[11], maar ook het binnenlopen van kantorenlocaties en benutten van aanwezige apparatuur of het via WIFI benaderen van het interne netwerk. Medewerkers kunnen toegang hebben tot informatie, delen van het netwerk of applicaties die ze niet of niet meer voor hun werk nodig hebben. Ze kunnen gegevens inzien die vertrouwelijk zijn of toegang proberen te krijgen tot systemen die bijvoorbeeld cruciale infrastructuur aansturen. Informatiebeveiliging bevat daarom verschillende aspecten, waarvan technische maatregelen zoals virusscanners en firewalls onderdeel zijn, maar ook de wijze waarop het interne netwerk toegankelijk is voor de verschillende gebruikers. Het gaat daarnaast om de fysieke beveiliging van werkplekken, om het gedrag van medewerkers en om organisatorische aspecten

9 'Wanorde bij NZa: medische gegevens onveilig, klokkenluider genegeerd', 10 april 2014, website NRC.nl; 'Ook intern privacylek bij Inspectie voor de Gezondheidszorg', 19 april 2014, website VPRO/Argos.
10 'Gemeente getroffen door beveiligings-bug Heartbleed', 14 april 2014, website RTVSeaport.
11 Met een phishing email wordt geprobeerd software met een ongewenste functie te activeren op het systeem van de ontvanger of kan worden geprobeerd inloggegevens te bemachtigen.

zoals een duidelijk beleid op het gebied van informatiebeveiliging (zie figuur 2).[12] Bij dat alles moet een balans gevonden worden tussen de beveiliging en de gebruikswaarde of gebruiksvriendelijkheid van gegevens en systemen. De toenemende digitalisering van gegevens en processen heeft immers tot doel effectiever en efficiënter te kunnen werken en een betere dienstverlener te kunnen zijn voor burgers en bedrijven.



Figuur 2. Vier aspecten van informatiebeveiliging.[13]

1.2 Gemeentelijk beleid

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 (2011-2014).[14] De I-visie geeft een perspectief op hoofdlijnen over de volle breedte van de gemeentelijke ICT. Ten aanzien van beveiliging van ICT gaat de I-visie in op de onderwerpen 'vertrouwelijkheid', 'beschikbaarheid' en 'integriteit' (betrouwbaarheid van gegevens).

De gemeentelijke ambities met betrekking tot veiligheid van ICT zijn[15]:

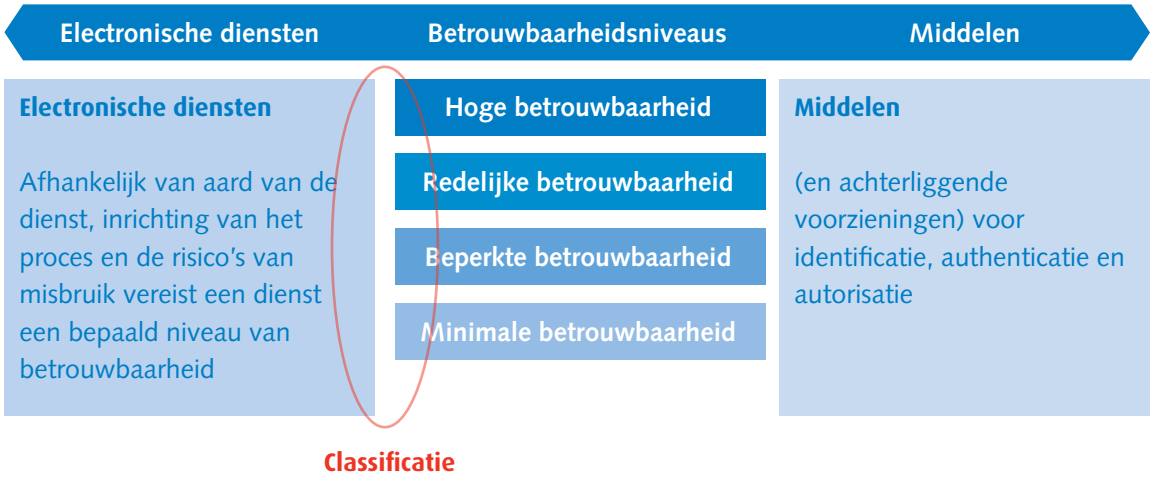
- Blijvende borging van veilige digitale communicatie tussen burgers/ bedrijven en gemeente.
- Verbetering van de beschikbaarheid van kritische ICT-systemen, vooral op het gebied van de dienstverlening aan burgers en bedrijven.
- Een afgewogen beveiligingsbeleid en een slagvaardige informatiebeveiligingsorganisatie.

Naar aanleiding van de I-visie zijn onder meer bij de 10 meest kritieke bedrijfsprocessen[16] maatregelen genomen om de continuïteit te kunnen waarborgen (afgerond in 2013). Eind 2013 hebben daarnaast alle diensten verklaard 'in control' te zijn bij de reguliere informatie beheer processen en procedures. Voor het overige wordt in de I-visie vooral aandacht besteed aan de beschikbaarheid en functionaliteit van ICT. Den Haag geeft per jaar ongeveer € 70 miljoen uit aan ICT, waarvan een onbekend bedrag aan beveiliging. De gemeente heeft circa 350 FTE in het werkveld van ICT. Ook daarvan is onbekend hoeveel capaciteit beschikbaar is voor digitale veiligheid.

12 Bron: Tactische Baseline Informatiebeveiliging, IBD, 2013
13 Afbeelding gemaakt door Rekenkamer Den Haag
14 RIS 181621, 'Get connected – sluit je aan', gemeentelijk I-visie, 1 november 2011.
15 I-visie, p. 15.
16 Dit gaat bijvoorbeeld om het proces van verstrekken paspoorten en rijbewijzen, of om de gemeentelijke website.

Informatiebeveiliging wordt in de I-Visie niet integraal afgewogen bij de afzonderlijke maatregelen voor verbetering van de ICT. Zo geeft de I-visie aan dat gewerkt wordt aan het creëren van een centraal domein waarmee het tijd- en plaatsonafhankelijk werken op pc's binnen alle panden van de gemeente en in mobiele situaties mogelijk wordt gemaakt.[17] Daarbij wordt echter geen melding gemaakt van een afweging tussen de voordelen (werkbaarheid, efficiency) en de mogelijke nadelen op het gebied van veiligheid. De I-visie is niet door de gemeenteraad vastgesteld en er is geen afzonderlijk door de raad vastgesteld kader voor informatiebeveiliging. Daarmee is er op dat niveau ook geen risicoanalyse en categorisering van niveaus van betrouwbaarheid, op basis waarvan inzet van (digitale) beveiligingsmaatregelen afgewogen kan worden.

Een dergelijke categorisering wordt in de 'Handreiking betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten'[18] voorgesteld (zie figuur 3). Op ambtelijk niveau is deze classificatie wel overgenomen. Voor afzonderlijke onderwerpen, ondermeer de gemeentelijke basisadministratie en Suwinet (gegevensuitwisseling bij verstrekken van uitkeringen) en bij gemeentelijke diensten, zijn ook informatiebeveiligingsplannen opgesteld. De gemeente voert op afzonderlijke systemen tests uit ter controle van de veiligheid en is verplicht audits uit te voeren voor DigiD[19] en Suwinet[20].



Figuur 3: betrouwbaarheidsniveaus. Bron: handreiking betrouwbaarheidsniveaus voor authenticatie bij electronische overheidsdiensten, p. 8.

17 I-visie, p. 14.
18 'Handreiking betrouwbaarheidsniveaus voor authenticatie bij electronische overheidsdiensten', Forum standaardisatie, januari 2012.
19 DigiD: beveiligd inloggen voor burgers bij overheidsinstellingen.
20 Suwinet: wordt door overheden gebruikt voor het uitwisselen van persoonsgegevens bij het verstrekken van uitkeringen.

1.3 Het onderzoek

Doel en onderzoeksvragen

De rekenkamer heeft een onderzoek gedaan naar de staat van de informatiebeveiliging bij de gemeente Den Haag. In het onderzoek stond de vraag centraal welke waarborgen genomen maatregelen bieden tegen het benaderen van gevoelige informatie. De rekenkamer wil met dit onderzoek bijdragen aan de beveiliging van gevoelige informatie van burgers en bedrijven bij de gemeente, de bewustwording van het belang van informatiebeveiliging en het vergroten van kennis over de staat van de informatiebeveiliging van de gemeente.

In het onderzoek zijn de volgende vragen gesteld:

- 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?

Aanpak

Het onderzoek heeft zich gericht op de ICT-infrastructuur van de gemeente Den Haag. Deze is getest op kwetsbaarheden waarmee hackers of kwaadwillenden onrechtmatig over bedrijfsgevoelige gegevens of gegevens van burgers zouden kunnen beschikken. Daarbij is gekeken naar de technische, maar ook fysieke waarborgen voor het veilig bewaren van gegevens.

In het onderzoek zijn de volgende tests uitgevoerd:

- Een blackbox test: hierbij is zonder kennis vooraf geprobeerd toegang te verkrijgen tot systemen. Tijdens de blackbox test zijn aan internet gekoppelde systemen waaronder de website www.denhaag.nl, een aantal aan de gemeente gelieerde websites, het interne netwerk van de gemeente[21] en het WIFI netwerk in het Stadhuis onderzocht. Ook is onderzocht in hoeverre het mogelijk is zonder autorisatie toegang te verkrijgen tot het interne netwerk (onder meer phishing en gebruiken van aanwezige hardware op werkplekken).
- Een greybox test: bij de greybox test is gebruik gemaakt van een door de gemeente beschikbaar gesteld gebruikersaccount met wachtwoord. Met deze informatie is de beveiliging van het interne netwerk van de gemeente onderzocht, zowel vanaf een werkplek in het stadhuis als door op afstand in te loggen (thuiswerk optie).
- Een netwerktap: hierbij is een deel van het dataverkeer op een knooppunt in het gemeentelijk interne netwerk onderzocht op aanwezigheid van malware.[22] Er is steekproefsgewijs onderzocht of hackers zich al toegang hebben verschaft tot systemen van de gemeente.

21 In de blackbox test is onderzocht of het interne netwerk te benaderen is door onbevoegden. Daarbij is eerst gekeken op welke wijze toegang gekregen kan worden en vervolgens of het mogelijk was op het interne netwerk informatie van burgers en bedrijven te vinden.

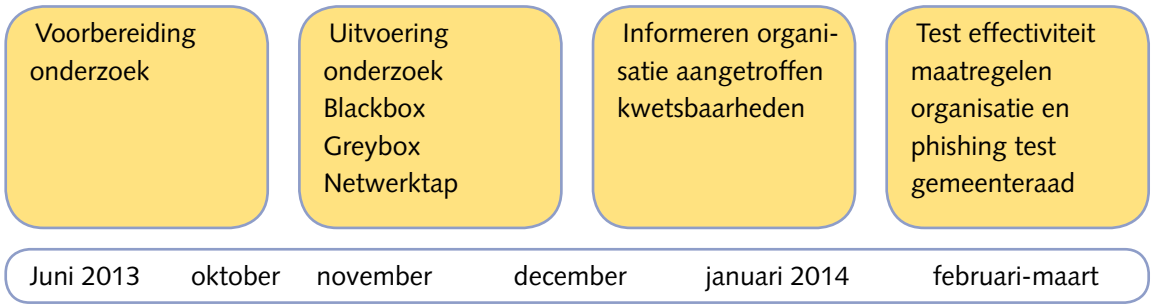
22 Malware: software met ongewenste functies zoals virussen en trojans (uit: Tactisch Baseline Informatiebeveiliging Gemeenten, IBD, 2013, p. 70.).

Proces en afstemming met gemeente

Voorafgaand aan en tijdens het onderzoek is afgestemd met de gemeentelijke organisatie en de verantwoordelijke portefeuillehouder. Daarbij is vanuit de gemeente medewerking verleend aan het onderzoek, voor zover dat voor de betreffende onderdelen noodzakelijk was. Zo is meegewerkt bij het plaatsen van de netwerktap en is een medewerkeraccount met thuiswerkmogelijkheid beschikbaar gesteld aan de rekenkamer.

Het onderzoek is uitgevoerd in de maanden november en december 2013. Vanwege de ernst van een aantal van de gevonden kwetsbaarheden is door de rekenkamer besloten de bevindingen direct na de uitvoering van het onderzoek kenbaar te maken aan de gemeentelijke organisatie en niet, zoals gebruikelijk, pas na afronding en vaststelling van het feitenrapport. Half december zijn de bevindingen uit het onderzoek gedeeld met de gemeentelijke organisatie.[23] Op basis van deze bevindingen heeft de gemeentelijke organisatie vanaf december 2013 de urgentste kwetsbaarheden gerepareerd en is een plan van aanpak opgesteld voor het oplossen van achterliggende, structurele, oorzaken. De aanpak is tevens door een extern deskundige op het gebied van informatiebeveiliging gevalideerd (in opdracht van de gemeente). De rekenkamer is op de hoogte gesteld van de aanpak en de prioritering daarbij.

Ter afsluiting van het onderzoek is in de laatste week van februari 2014 door de rekenkamer een hertest uitgevoerd waarbij een selectie van de bevindingen is nagelopen. Het doel was te achterhalen of kwetsbaarheden, waarvan de organisatie had aangegeven deze opgelost te hebben, nog benut konden worden. Tenslotte is in maart, ter vergroting van de bewustwording over het onderwerp, een nep-phishingmail[24] verzonden aan de leden van de gemeenteraad.



Figuur 4. Planning onderzoek digitale veiligheid

De gevonden feiten in het onderzoek vormen de basis voor de conclusies en aanbevelingen in dit rapport. In de volgende paragraaf wordt op hoofdlijnen ingegaan op de bevindingen. De beschreven bevindingen zijn door de gemeente inmiddels verholpen. Vanwege de gevoeligheid van de bevindingen voor de informatiebeveiliging worden de overige gevonden kwetsbaarheden niet gepubliceerd.

23 De rekenkamer heeft op 18 december 2013 de portefeuillehouder voor dit onderwerp mondeling ingelicht over de aard van de bevindingen en vervolgens het college van B&W schriftelijk geïnformeerd. Op dezelfde dag is een inhoudelijke toelichting gegeven aan de voor dit onderwerp verantwoordelijke ambtenaren.

24 Deze nep-phishingmail bevatte geen malware, maar een link naar een niet bestaande website, waarmee alleen geteld werd hoeveel ontvangers op de link hebben geklikt.

1.4 Overzicht bevindingen

Denhaag.nl is veilig, interne netwerk vertoont ernstige kwetsbaarheden

In de beveiliging van de gemeentelijke website (www.denhaag.nl) zijn ten tijde van het onderzoek geen ernstige kwetsbaarheden aangetoond.
In het onderzoek is gebleken dat het interne netwerk van de gemeente de zwakke schakel is in de beveiliging. Enerzijds is het relatief eenvoudig en op verschillende manieren mogelijk toegang te krijgen tot het interne netwerk en anderzijds kent het netwerk zelf ernstige kwetsbaarheden.[25] In de analyse van de netwerktap zijn geen sporen gevonden van aanwezige malware of van oneigenlijk gegevensverkeer. Er is daarmee geen aanwijzing dat 'indringers' actief waren op het interne netwerk.

Netwerktap
Bij een netwerktap wordt een deel van de data die over het netwerk gaat gekopieerd en vervolgens geanalyseerd. Door dit niet 'real time' te doen is het mogelijk zeer nauwkeurig de gegevens te analyseren. Gekeken wordt onder meer naar de aanwezigheid van malware zoals virussen of naar het downloaden van oneigenlijke bestanden van internet. Bij het analyseren van de netwerktap tijdens het onderzoek zijn geen sporen van malware of oneigenlijk gegevensverkeer gevonden. De gegevens uit de netwerktap zijn na afloop van het onderzoek vernietigd door de gemeente.

Eenvoudig onbevoegd toegang te krijgen tot interne netwerk

Tijdens het onderzoek was het zonder inloggegevens op verschillende manieren mogelijk toegang te krijgen tot het interne netwerk. Hoewel een aantal van de mogelijkheden inmiddels door de gemeente is weggenomen, blijft dit een kwetsbare schakel in de beveiliging waardoor het voor buitenstaanders zonder veel technische kennis eenvoudig is toegang te verkrijgen tot het interne netwerk van de gemeente Den Haag. Daarbij speelt de cultuur met betrekking tot informatiebeveiliging bij medewerkers een rol, de open werkomgeving op het stadhuis en de behoefte ICT-voorzieningen zo gebruiksvriendelijk mogelijk te maken.

Kwetsbaarheden intern netwerk

Onderzoekers van de rekenkamer waren in het greybox scenario op basis van een standaard medewerker account in staat 14 dagen lang ongemerkt systemen op het interne netwerk aan te vallen, waarbij zij zich toegang konden verschaffen tot delen van de ICT infrastructuur die alleen voor beheerders bereikbaar dienen te zijn. De onderzoekers konden daardoor grote hoeveelheden vertrouwelijke informatie inzien. Er zijn onder meer GBA gegevens gevonden van ruim 690.000 burgers (naam, Burgerservicenummer, administratienummer).

25 Ernstige kwetsbaarheden: (onnodige) blootstelling aan risico op het misbruiken van gegevens door onbevoegden. Een inschatting van het daadwerkelijke risico valt buiten de reikwijdte van dit onderzoek.

Privacygevoelige informatie, GBA gegevens
De gemeente beheert van burgers en bedrijven gegevens zoals naam, adres en Burgerservicenummers. Een belangrijk databestand is de Gemeentelijke Basis Administratie (GBA). Onderzoekers waren tijdens het onderzoek in staat in te loggen op een applicatie waarmee wijzigingen in het GBA worden doorgevoerd. Daarbij was het ook mogelijk een groot GBA bestand in te zien. Er is niet geprobeerd hierin wijzigingen door te voeren.

Tijdens het onderzoek waren, op basis van standaardautorisatie voor medewerkers, op printers opgeslagen bestanden in te zien, waaronder enkele kopieën van identiteitsbewijzen van burgers. Daarnaast is gebleken dat op het netwerk grote hoeveelheden informatie zonder beperking in te zien zijn, die alleen beschikbaar zouden mogen zijn voor het primaire proces en voor medewerkers belast met specifieke taken. Ook hier gaat het om onder meer GBA gegevens van burgers.[26]

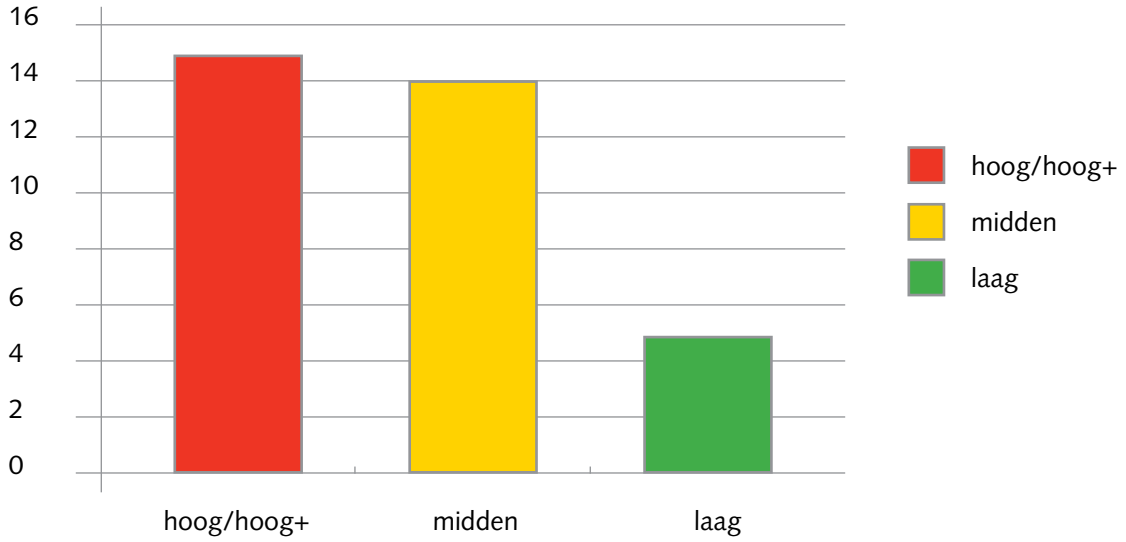
Privacygevoelige informatie, kopieën van identiteitsbewijzen
Geavanceerde printers zoals die bij de gemeente worden gebruikt zijn 'multifunctioneel'. Er kunnen ook documenten mee gekopieerd worden of gescand. Gescande bestanden worden via het interne netwerk verzonden naar bijvoorbeeld de pc van een medewerker. In een aantal gevallen bleken scans van documenten nog opgeslagen te zijn op de harde schijf van deze printers en benaderbaar te zijn vanaf het interne netwerk. Tijdens het onderzoek konden hierdoor onder meer de scans van twee identiteitsbewijzen van burgers worden gekopieerd. Een kopie van een identiteitsbewijs kan door kwaadwillenden gebruikt worden voor identiteitsfraude, bijvoorbeeld voor het aanvragen van leningen op naam van de eigenaar van het identiteitsbewijs.

Aanzienlijk aantal kwetsbaarheden met een hoog risico

Er zijn in totaal 34 kwetsbaarheden geconstateerd, waarvan 25 direct gerelateerd waren aan de gemeentelijke ICT infrastructuur en 9 aan systemen verwant aan de gemeente.[27] Van alle kwetsbaarheden zijn 15 te categoriseren als een hoog tot zeer hoog risico, 14 als een midden- en 5 als een laag risico voor de beveiliging van gevoelige informatie. De mogelijkheid domein beheers rechten toe te eigenen wordt bijvoorbeeld ingeschat als een 'hoog risico'. De risicoanalyse is gebaseerd op de prioritering van de aanpak van geconstateerde kwetsbaarheden door de gemeentelijke organisatie.

26 Overigens zijn ook bij primaire processen al veel medewerkers betrokken. Zo zijn er circa 2000 'binnengemeentelijke' gebruikers van het GBA systeem (bron: RIS 256676, rapportage integriteit en kostendekkende tariefsbepaling dienst Publiekszaken, februari 2013).

27 Bij aan de gemeente verwante systemen kan gedacht worden aan systemen die bijvoorbeeld onderdeel vormen van het beheer van de openbare ruimte, zoals de straatverlichting.



Figuur 5. Gevonden kwetsbaarheden naar risicocategorie

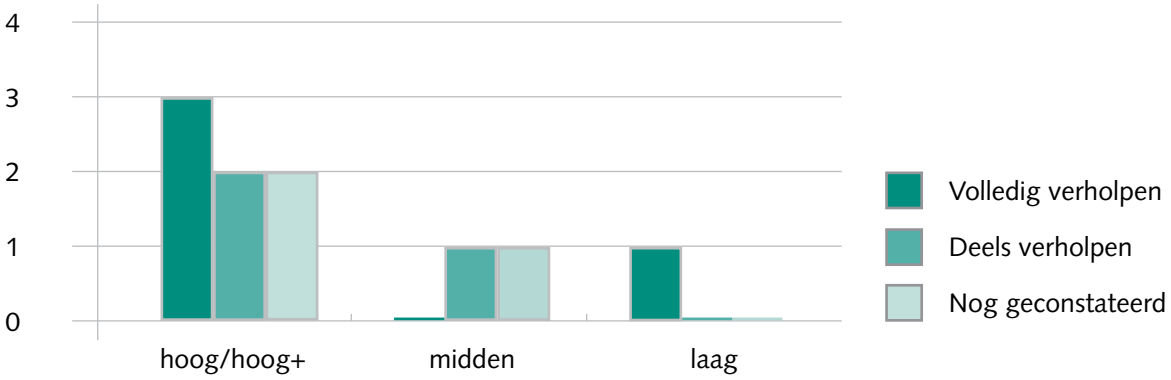
Aanpak gevonden kwetsbaarheden door gemeente en hertest

Het onderzoek leverde een overzicht op van verschillende kwetsbaarheden in de informatiebeveiliging. Voor de gemeente was het overzicht van kwetsbaarheden aanleiding direct voor alle kwetsbaarheden een aanpak te formuleren en de risico's te verminderen of weg te nemen. Een dergelijk totaalbeeld was tot dat moment bij de gemeente niet voorhanden. Alle acties voortkomend uit het overzicht waren nieuw. Bij de aanpak van de gevonden kwetsbaarheden door de ambtelijke organisatie bleek dat een aantal kwetsbaarheden, bijvoorbeeld op het gebied van het beheer van gevoelige informatie op netwerkschijven, de verantwoordelijkheid is van afzonderlijke diensten en externe partijen. Digitale beveiliging is ondergebracht bij het organisatieonderdeel dat verantwoordelijk is voor het met ICT faciliteren en ondersteunen van diensten, maar gemeentelijke diensten zijn zelf ook nog verantwoordelijk voor deelaspecten. Een gevolg hiervan is dat voor een deel van de uitvoering van digitale beveiliging dit organisatieonderdeel afhankelijk is van andere gemeentelijke diensten, ketenpartners of externe partijen die ICT diensten leveren. In die relatie heeft het geen doorzettingsmacht. Oplossingen voor gevonden kwetsbaarheden konden daarom in een aantal gevallen niet één op één doorgevoerd worden, maar moesten 'besproken worden met derden'.

De rekenkamer heeft in de hertest 10 in het onderzoek aangetroffen kwetsbaarheden nagelopen, waarvan 7 door de organisatie als 'hoog risico' waren gewaardeerd bij de aanpak van gevonden kwetsbaarheden uit het onderzoek. De rekenkamer constateerde dat de tijdens het onderzoek gevonden kwetsbaarheden en vertrouwelijke informatie deels niet meer op dezelfde wijze te vinden waren. Het was bijvoorbeeld niet meer mogelijk de informatie in te zien die alleen voor beheerders beschikbaar zou moeten zijn. Wel bleek dat de toegang van buitenaf tot het interne netwerk nog een zwakke schakel is.

Onbevoegd toegang tot intern netwerk
In de hertest is onder meer gekeken naar de mogelijkheid van buitenaf toegang te verkrijgen tot het interne netwerk. Dit bleek nog op verschillende manier mogelijk te zijn. Bij het toetsen van de kwetsbaarheden viel op dat er in één geval een oplossing leek te zijn gerealiseerd, maar dat in werkelijkheid de kwetsbaarheid zich nog voordeed. Onze onderzoekers kregen een foutmelding te zien die er op duidde dat de gebruikte methodiek niet zou werken. Desondanks ontstond er contact met het interne netwerk vanaf een externe computer.

Van de 10 opnieuw getoetste kwetsbaarheden uit het onderzoek bleken in de hertest 4 volledig weggenomen en 3 deels verholpen. Op het moment van de hertest werden 3 kwetsbaarheden nog geconstateerd, 2 daarvan vallen binnen de categorie 'hoog risico'. Voor beide kwetsbaarheden is een structurele oplossing bedacht waarmee het probleem wordt aangepakt. De derde nog aangetroffen kwetsbaarheid is van een 'middelhoog risico'. Voor de aanpak hiervan is overleg met andere gemeentelijke diensten nodig.
Het is van belang aan te geven dat het oplossen van kwetsbaarheden geen garanties geeft dat er niet andere of zelfs vergelijkbare kwetsbaarheden bestaan op andere plekken in de gemeentelijke ICT.



Figuur 6. Status kwetsbaarheden naar risicocategorie

Phishingmail
Het verzenden van een nep-phishing mail aan de 45 raadsleden van de gemeente had als doel de bewustwording over het onderwerp informatiebeveiliging te vergroten. Als direct resultaat leverde deze test een reactie op van ongeveer een kwart van de ontvangers (11). Eén reactie op een phishingmail is in een reële situatie voldoende om een aanvaller de mogelijkheid te geven malware te installeren op het interne netwerk of gegevens van de ontvanger te bemachtigen. De test toont daarmee ook aan hoe kwetsbaar de beveiliging van het interne netwerk is voor aanvallen van buitenaf.

2 Conclusies en aanbevelingen

2.1 Hoofdboodschap

De gemeente heeft onvoldoende waarborgen voor het beschermen van de (digitale) informatie over burgers en bedrijven tegen gebruik of misbruik door (on)bevoegden.

Bij dit onderzoek zijn verschillende kwetsbaarheden aangetoond in de informatiebeveiliging van de gemeente. Deze kwetsbaarheden leiden afzonderlijk, maar vooral in samenhang met elkaar, tot risico's van misbruik en oneigenlijk gebruik van vertrouwelijke informatie over burgers of bedrijven, die groter zijn dan nodig en wenselijk. Van belang is ook het gegeven dat de gevonden kwetsbaarheden onbekend waren bij de gemeentelijke organisatie. Ondanks het directe optreden van de gemeente bij het oplossen van de gevonden kwetsbaarheden, concludeert de rekenkamer dat de informatiebeveiliging structureel verbetering behoeft.

2.2 Conclusies en aanbevelingen

Conclusie 1: de gemeenteraad is onvoldoende in staat zijn kaderstellende en controlerende functie uit te oefenen op het gebied van informatiebeveiliging.

Het bestaande kader op het gebied van informatiebeveiliging is een deelonderwerp bij het beleidsveld informatie en ICT-beleid en is niet vastgesteld door de gemeenteraad. Weliswaar zijn voor deelonderwerpen en bij afzonderlijke diensten op ambtelijk niveau informatiebeveiligingsplannen in gebruik, maar het ontbreekt aan een integraal en door de raad vastgesteld beleidskader op het gebied van informatiebeveiliging en een op basis daarvan opgestelde risicoanalyse en beveiligingsplan. Door het ontbreken van een integraal kader is de gemeenteraad niet in staat het college effectief te controleren op het uitoefenen van diens verantwoordelijkheid op het gebied van informatiebeveiliging. Het beveiligen van (digitale) informatie is onvoldoende gedefinieerd in termen van risico's, te nemen maatregelen en werkbaarheid (klantvriendelijkheid, effectiviteit, snelheid en dergelijke) in relatie tot beschikbare middelen. Daardoor ontstaan risico's dat op de werkvloer keuzes worden gemaakt ten aanzien van informatiebeveiliging, bijvoorbeeld de afweging tussen werkbaarheid en veiligheid, die voor het bestuur niet of onvoldoende inzichtelijk zijn.

Aanbeveling 1: stel als raad een kader vast voor informatiebeveiliging en controleer het college op het uitvoeren van het beleid voor informatiebeveiliging.

Stel daarom als raad een integraal kader voor informatiebeveiliging vast, waarin de algemene beleidsuitgangspunten worden vastgelegd voor het informatieveiligheidsbeleid, en draag het college op in de planning & control cyclus verantwoording af te leggen over het gevoerde beleid.
Volledige of absolute veiligheid bestaat niet. De mate van beveiliging zou daarom een bewuste keuze moeten zijn op basis van een afweging tussen de veiligheidsrisico's, te nemen maatregelen en de werkbaarheid, mede in relatie tot de beschikbare middelen.

Het kader informatiebeveiliging dient in te gaan op alle aspecten van informatiebeveiliging, waaronder de fysieke beveiliging (toegang tot gebouwen en werkplekken), de toegang tot het netwerk en de digitale beveiliging. Bijzondere aandacht is ook nodig voor de afhankelijkheid van derden (leveranciers en ketenpartners) bij informatiebeveiliging. Neem in het beleidskader op hoe de veiligheidsrisico's, te nemen maatregelen en de werkbaarheid worden afgewogen in relatie tot in te zetten middelen.

Conclusie 2: de gemeente heeft geen totaalbeeld van de stand van zaken van de informatiebeveiliging.
Het testen van de informatiebeveiliging gebeurt alleen op incidentele basis en bij afzonderlijke gemeentelijke ICT-systemen. Zo is de gemeente verplicht afzonderlijke audits uit te voeren voor DigiD[28] en Suwinet[29], maar wordt geen integrale test voor de hele gemeentelijke ICT uitgevoerd. Een totaalbeeld van de informatiebeveiliging was tot dit onderzoek nog niet voorhanden. Het testen van de informatiebeveiliging is geen structureel onderdeel van de planning- en control cyclus en informatiebeveiliging is geen vast onderdeel van de rapportage aan de raad.

Aanbeveling 2: geef het college opdracht de gemeentelijke ICT integraal en periodiek door een externe partij te laten testen op kwetsbaarheden en de resultaten op te nemen in de planning en control cyclus en de rapportages aan de raad.
Een integraal onderzoek naar de kwetsbaarheden is nodig voor een zo optimaal mogelijk beeld van de stand van zaken. Dit is ook de enige manier waarop risico's als gevolg van een keten van kwetsbaarheden inzichtelijk te maken zijn. Een kritische blik op de eigen uitvoering van informatiebeveiligingsbeleid is van groot belang, daarom verdient het aanbeveling dergelijk onderzoek door een onafhankelijke externe partij uit te laten voeren. De ontwikkelingen op het gebied van ICT gaan snel. Dat betekent dat zowel de kwetsbaarheden als de bedreigingen continue veranderen. Een integraal onderzoek moet daarom met enige regelmaat uitgevoerd worden zodat een lerend proces kan ontstaan. De rekenkamer beveelt aan voor het einde van 2014 een eerste onderzoek uit te laten voeren en hierin ook te bekijken in hoeverre de in dit onderzoek gevonden en nog openstaande kwetsbaarheden verholpen zijn.

Conclusie 3: de gemeente heeft onvoldoende zicht op actuele bedreigingen op het gebied van informatiebeveiliging en is daardoor niet in staat voldoende adequaat te reageren op aangetoonde kwetsbaarheden in de beveiliging.
Tijdens het onderzoek was de rekenkamer in staat gedurende twee weken gebruik te maken van een bestaande kwetsbaarheid in de informatiebeveiliging. Ook na de ontdekking was het voor de gemeente niet meteen mogelijk de oorzaak van de aanval te achterhalen. Een snelle aanpak van de oorzaak was daardoor niet mogelijk.

Aanbeveling 3: geef het college opdracht over te gaan tot het monitoren van het gemeentelijke netwerk op verdachte activiteiten en laat het college een calamiteitenplan opstellen voor het ingrijpen bij aanvallen op de informatiebeveiliging, als onderdeel van het informatiebeveiligingsplan.
Kwetsbaarheden zijn niet volledig te voorkomen. Naast preventief beveiligen van informatie, op het gebied van ICT-, fysieke- en cultuuraspecten, is het van groot belang zicht te hebben op actuele bedreigingen en daarop in te grijpen. Informatiebeveiliging biedt te vaak alleen bescherming tegen bekende bedreigingen en loopt daardoor achter op de realiteit. Een alerte signalering van en ingrijpen bij daadwerkelijke aanvallen op het netwerk zijn zo mogelijk van nog groter groot belang dan het preventief beveiligen van informatie.

28 DigiD: beveiligd inloggen voor burgers bij overheidsinstellingen.
29 Suwinet: wordt door overheden gebruikt voor het uitwisselen van persoonsgegevens bij het verstrekken van uitkeringen.

Conclusie 4: de bestuurlijke inbedding van informatiebeveiliging is onvoldoende.
De benoemde bestuurlijke verantwoordelijkheid op het gebied van informatiebeveiliging beperkt zich tot het aspect van digitale veiligheid en doet als onderdeel van de portefeuille organisatie onvoldoende recht aan de maatschappelijke implicaties en risico's die bij het onderwerp aan de orde zijn. Een gecombineerde verantwoordelijkheid voor ICT interne dienstverlening en informatiebeveiliging leidt tot onvoldoende functiescheiding op dit gebied. Digitale veiligheid wordt in de begroting en het jaarverslag genoemd bij het onderdeel Informatiebeleid, dat op zijn beurt weer één van de elf onderwerpen is in het hoofdstuk 'Bedrijfsvoering'.[30]
De afgelopen jaren is digitalisering van informatie en dienstverlening sterk toegenomen en dat zal zich de komende jaren verder voortzetten. Daar komen bij de bestuurlijke implicaties op het gebied van (digitale) gegevensuitwisseling als gevolg van de decentralisaties in het sociaal domein. De huidige bestuurlijke inbedding als deelonderwerp van bedrijfsvoering geeft de bestuurlijke implicaties van informatiebeveiliging onvoldoende weer, mede in het licht van deze veranderingen.

Aanbeveling 4: draag het college op de benodigde bestuurlijke inbedding van informatiebeveiliging tot stand te brengen door de verantwoordelijkheid expliciet en als apart onderwerp bij een portefeuillehouder te beleggen en neem het onderwerp als zodanig op in begroting en jaarverslag.
Een sterkere en afzonderlijke bestuurlijke inbedding van het onderwerp, niet als onderdeel van ICT/interne dienstverlening, sluit aan op de beoogde doelen voor het verbeteren van de informatiebeveiliging zoals die onder meer zijn vastgesteld door de leden van de VNG in de in 2013 aangenomen resolutie over informatiebeveiliging. Hiermee wordt ook tegemoetgekomen aan de beleidsmatige implicaties op dit terrein als gevolg van de komende decentralisaties in het sociaal domein.

Conclusie 5: een deel van de gevonden kwetsbaarheden is terug te voeren op cultuur en gedrag van medewerkers en kan niet technisch opgelost worden.
Zwakke schakels in de beveiliging van vertrouwelijke informatie zitten niet alleen in de ICT, maar ook in aspecten zoals de werkomgeving en het gedrag en de bekwaamheid van medewerkers. De gemeente besteedt hier al wel aandacht aan, maar dit gebeurt tot nu toe veelal informerend, bijvoorbeeld met informatieberichten via het interne 'werknet' van de gemeente.

Aanbeveling 5: de gemeente moet meer inzetten op een proces van bewustwording, cultuurverandering en bekwaamheid ten aanzien van informatiebeveiliging.
Verzoek het college over te gaan tot een meer actieve en minder vrijblijvende aanpak van de bewustwording en cultuurverandering bij het omgaan met (digitale) vertrouwelijke informatie. Te overwegen zou zijn de essentiële elementen nadrukkelijker en meer directief als wenselijk gedrag te omschrijven. Uitgangspunt zou moeten zijn dat wat mogelijk is en niet tot onoverkomelijke beperkingen leidt technisch geregeld wordt en dat voor het overige op basis van classificatie van informatie medewerkers slecht beperkt toegang krijgen tot informatie. Overschrijdingen van toegangsbeperkingen dienen gesignaleerd en gesanctioneerd te worden. Medewerkers moeten bekwaam worden in het omgaan met vertrouwelijke informatie en de risico's daarbij (vaardigheden en cultuur). Zo is het bijvoorbeeld voor medewerkers van belang kennis te hebben van de verschillende betrouwbaarheidscategorieën voor informatie en de maatregelen, die bij afzonderlijke categorieën in acht genomen moeten worden. Zij moeten daar ook bekwaam naar kunnen handelen. Alertheid en vaardigheden hebben verder betrekking op zaken als het niet ingaan op phishing mail, het melden van verdachte mails of bestanden en bijvoorbeeld het verwerken van gescande gegevens van burgers en bedrijven.

30 Programmabegroting 2014-2017 (RIS 264145). Hoofdstuk 3 Bedrijfsvoering, p. 170. Over digitale veiligheid zijn twee zinnen opgenomen.

Reactie van het College van B&W

Gemeente Den Haag

Retouradres: Postbus 12600, 2500 DJ Den Haag

De voorzitter van de Rekenkamer Den Haag
De heer Watze de Boer
Postbus 19157
2500CD Den Haag

Uw brief van
15 mei 2014
Uw kenmerk
RK/2014.13
Ons kenmerk
BSD/2014.453
Doorkiesnummer
070 - 3532347
E-mailadres

Aantal bijlagen

Datum
17 juni 2014

Onderwerp
Reactie op 'Bestuurlijk rapport Digitale Veiligheid' van de Rekenkamer Den Haag

Geachte heer de Boer,

Met interesse hebben wij het bestuurlijk rapport van de Rekenkamer over het onderzoek naar de digitale veiligheid gelezen. De Rekenkamer heeft met de keuze voor dit onderzoek naar "digitale veiligheid" een zeer actueel onderwerp geselecteerd dat bij alle gemeenten volop in de belangstelling staat. Het rapport benoemt het grote belang van informatieveiligheid voor het goed functioneren van de gemeente en het belang van goede veiligheid voor het vertrouwen dat een burger in een gemeente stelt. De burger moet er van overtuigd zijn dat zijn (gevoelige) gegevens in goede handen zijn bij de gemeente. Ook wij benadrukken het grote belang van informatieveiligheid. Het is niet voor niets een van drie pijlers in de gemeentelijke I-visie. De Nederlandse gemeenten hebben dit belang onlangs bevestigd in hun Bijzondere Algemene Ledenvergadering van 29 november 2013. Hierbij is de Baseline Informatiebeveiliging Gemeenten (BIG) als norm geaccepteerd voor het inrichten van informatieveiligheid bij gemeenten. Met het oog op het herijken van ons beleid voor informatieveiligheid is het een goede gelegenheid om de uitkomsten van het onderzoek van de Rekenkamer daarin mee te nemen.

De belangrijkste bevinding van de Rekenkamer luidt: *"DenHaag.nl is veilig, het interne netwerk vertoont ernstige kwetsbaarheden"*. Hoewel de Rekenkamer constateert dat deze kwetsbaarheden van het interne netwerk inmiddels door de gemeente zijn verholpen, is deze bevinding van de Rekenkamer voor het college een belangrijke reden om de komende jaren door te gaan met de structurele verbetering van de informatiebeveiliging. Alle aanbevelingen van de Rekenkamer zullen in dit proces van verdere structurele verbetering worden meegenomen.

In juni 2013 is met de Rekenkamer afgesproken om een veiligheidsonderzoek te doen in de vorm van een integrale penetratietest ("pentest") door een deskundige externe partij op de totale technische infrastructuur van de gemeente. Dit betreft zowel de infrastructuur voor externe communicatie (de "e-infrastructuur") als de interne infrastructuur, waar alle medewerkers gebruik van maken. Het onderzoek van de Rekenkamer viel samen met het lopende verbeterprogramma op het gebied van informatiebeveiliging en vormde daarop naar het oordeel van de gemeente een goede aanvulling.

Inlichtingen bij
Chris Batist

Postadres: Postbus 12600, 2500 DJ Den Haag
Bezoekadres: Spui 70, Den Haag
Internetadres: www.denhaag.nl

Telefoon: 14070

De bevinding "Den Haag.nl is veilig" bevestigt de resultaten uit een onderzoek dat recent, in 2012, is uitgevoerd op de belangrijke dienstverleningsprocessen die van het webportaal www.denhaag.nl gebruik maken. Deze bevinding is ook naar voren gekomen in de resultaten van de DigiD-audit die jaarlijks wordt uitgevoerd, voor het laatst medio 2013. De bevinding "het interne netwerk vertoont ernstige kwetsbaarheden" is een tegenvaller. Bij de voorbereiding van het onderzoek van de Rekenkamer, in juni vorig jaar, was de verwachting dat er kwetsbaarheden zouden worden gevonden, echter geen ernstige kwetsbaarheden. De geconstateerde bevindingen, ook al zijn ze verholpen, onderstrepen de noodzaak om de informatiebeveiliging structureel verder te verbeteren en om daarvoor niet alleen de externe infrastructuur, maar ook de interne infrastructuur periodiek te laten reviewen.

Het college maakt graag gebruik van deze bestuurlijke reactiemogelijkheid om specifiek op de door de Rekenkamer genoemde conclusies en aanbevelingen in te gaan. De hoofdboodschap van de Rekenkamer: *"De gemeente heeft onvoldoende waarborgen voor het beschermen van de (digitale) informatie over burgers en bedrijven tegen gebruik of misbruik door (on)bevoegden."* verdient nuancering.
Er is geconstateerd dat het webportaal www.denhaag.nl veilig is. Daarnaast bevindt de gemeente Den Haag zich net als iedere andere gemeente nog in een opbouwfase voor informatieveiligheid. Dit is ook verwoord in de resolutie van de Bijzondere Algemene Ledenvergadering van de VNG van 29 november 2013. Hierin wordt gesteld dat ieder gemeente in eigen tempo groeit naar volledige implementatie van de BIG. Binnen Den Haag zijn hiervoor de afgelopen jaren al veel stappen gezet. Een informatiebeveiligingsorganisatie is ingericht met een CISO (Concern Information Security Officer) en DISO's (Dienst Information Security Officers). De continuïteit voor de top tien "kritieke systemen" is op niveau gebracht. De diensten hebben voor hun kritieke systemen in 2012 en 2013 risicoanalyses uitgevoerd en hebben waar nodig aanvullende acties uitgevoerd. Er is een ondersteunend systeem ingevoerd om de activiteiten op het gebied van informatieveiligheid en de resultaten daarvan te monitoren. Voor 2014 staat gepland om extra technische hulpmiddelen te implementeren om het ongeautoriseerd binnendringen van de ICT-infrastructuur tijdig te detecteren en waar nodig actie te ondernemen.[1] Verder is de gemeente Den Haag begin 2014 gestart met de uitvoering van een "awareness" campagne voor informatieveiligheid en is het wachtwoordbeleid aangescherpt. Ten slotte zijn zoals ook door de Rekenkamer is geconstateerd maatregelen genomen om de kwetsbaarheden op korte termijn weg te nemen of de mogelijke impact daarvan aanzienlijk te verminderen. Het college vindt dat er door al deze maatregelen thans voldoende waarborgen bestaan voor het beschermen van gevoelige digitale informatie, maar onderstreept tegelijk dat beveiliging een dynamisch proces is dat continu vraagt om aanscherping van maatregelen door nieuwe 'dreigingen'.

Hieronder geven we per conclusie en bijbehorende aanbeveling onze reactie weer.
"Conclusie 1: de gemeenteraad is onvoldoende in staat zijn kaderstellende en controlerende functie uit te oefenen op het gebied van informatiebeveiliging."
"Aanbeveling 1: stel als raad een kader vast voor informatiebeveiliging en controleer het college op het uitvoeren van het beleid."
In 2011 zijn de hoofdlijnen van het collegebeleid op het gebied van ICT gedeeld met de gemeenteraad in de vorm van de I-visie (RIS181621). In 2013 is de raad over de voortgang gerapporteerd (RIS 260175). Nadrukkelijk onderdeel van de I-visie en de rapportage daarover waren plannen en activiteiten op het gebied van informatiebeveiliging. Het college is van mening dat de raad hierdoor de afgelopen periode op hoofdlijnen voldoende in staat is geweest om zijn verantwoordelijkheid uit te oefenen. De gehanteerde beleidskaders op het gebied van informatiebeveiliging zijn in 2008 vastgesteld. Deze vertonen grote overeenkomst met de BIG die in november 2013 door de gemeenten is aangenomen als norm voor de invulling van informatieveiligheid binnen hun gemeente. Hierbij dient beseft te worden dat, zoals ook door de Rekenkamer wordt gesteld, 100 % veiligheid niet bestaat. Over de stand van zaken betreffende informatieveiligheid wordt tijdens iedere vergadering van de gemeentelijke IT-board gerapporteerd. Verder is in 2013 een "Information Security Management Systeem" (ISMS) ingevoerd.

[1] Dit was ook het enige punt waarop de gemeente niet geheel voldeed aan de normering voor de DigiD-audit.

Dit maakt het mogelijk de activiteiten op het gebied van informatieveiligheid meer in detail te plannen en de resultaten te monitoren. In 2014 zal op basis van de BIG het gemeentelijk beleid voor informatieveiligheid herijkt worden en zal een analyse worden uitgevoerd van de verschillen tussen de actuele situatie en de vereisten vanuit de BIG. De uitvoering van het nieuwe beleid zal gefaseerd plaats vinden. Dit past in het groeimodel dat bij de acceptatie van de BIG door de gemeenten is afgesproken. Uiteraard zal de uitwerking van het beleid ook onderwerp zijn van de informatiebeveiligingsaudits die jaarlijks door de GAD worden uitgevoerd. Het college zal op basis van het herijkte beleid graag de dialoog voeren met de gemeenteraad, zodat de raad mede op basis hiervan, desgewenst vaker en actiever, invulling kan geven aan haar verantwoordelijkheid op het gebied van informatieveiligheid voor de gemeente als geheel.

"Conclusie 2: de gemeente heeft geen totaalbeeld van de stand van zaken van de informatiebeveiliging."
"Aanbeveling 2: geef het college de opdracht de gemeentelijke ICT integraal en periodiek door een externe partij te laten testen op kwetsbaarheden en de resultaten op te nemen in de planning en control cyclus en de rapportages aan de raad. "
De recent opgestelde "in control statements" op het gebied van informatiebeveiliging die in januari 2014 door de algemeen directeuren van alle gemeentelijke diensten zijn ondertekend geven blijk van een groeiend totaalbeeld op het gebied van informatiebeveiliging. Hieruit blijkt overigens ook dat er nog de nodige stappen moeten worden gezet. Het kan altijd beter. Het college neemt daarom graag de aanbeveling over om ook het interne netwerk jaarlijks te gaan onderzoeken op kwetsbaarheden. Het eerste onderzoek zal eind 2014 plaats vinden. Het testen van het netwerk vanuit extern perspectief heeft reeds in 2012 plaats gevonden. De resultaten hiervan zijn geactualiseerd door het uitvoeren van testen op nieuwe toepassingen die via het webportaal www.denhaag.nl worden aangeboden. Deze testen zijn al jaren standaard procedure. Daarnaast zijn de resultaten ook bevestigd door de testen die als onderdeel van de DigiD audit zijn uitgevoerd. Verder wil het college benadrukken dat het totaalbeeld van informatieveiligheid mede wordt gevoed door de resultaten van de testen die bij normale wijzigingen worden uitgevoerd en waarbij in de impactanalyse ook aandacht wordt besteed aan informatieveiligheid. Daarnaast wordt het beeld mede bepaald door de resultaten van de ingestelde planning- en controlcyclus voor informatieveiligheid, welke wordt ondersteund door het ingevoerde ISMS-systeem. In dit systeem worden de uit te voeren activiteiten en de op te leveren resultaten geregistreerd.

"Conclusie 3: de gemeente heeft onvoldoende zicht op actuele bedreigingen op het gebied van informatiebeveiliging en is daardoor niet in staat voldoende adequaat te reageren op aangetoonde kwetsbaarheden in de beveiliging."
"Aanbeveling 3: geef het college opdracht over te gaan tot het monitoren van het gemeentelijke netwerk op verdachte activiteiten en laat het college een calamiteitenplan opstellen voor het ingrijpen bij aanvallen op de informatiebeveiliging, als onderdeel van het informatiebeveiligingsplan."
Het college is zich ervan bewust dat een sluitstuk in het signaleren van (cyber-)aanvallen ontbreekt, zoals ook uit het Digid-audit 2013 naar voren kwam. Andere zaken zoals virus- en malwarescanning en het checken op technische kwetsbaarheden worden al uitgevoerd.
Naar aanleiding van de Digid-audit is in 2013 opdracht gegeven om over te gaan tot de aanschaf van hulpmiddelen om te kunnen detecteren of ongeautoriseerde personen toegang hebben verkregen tot het netwerk. De middelen om ongeautoriseerd gebruik van het netwerk te detecteren werken in aanvulling op de "malware- en viruscans" die worden uitgevoerd op de werkstations van de gemeente en de "vulnerability-scans" die worden uitgevoerd op de infrastructuur. Mede naar aanleiding van de bevindingen uit het rekenkameronderzoek hebben wij dit onderwerp een meer prominente plaats gegeven in ons actieplan voor de komende jaren. De IT-board heeft opdracht gegeven om een integraal continuïteitsplan op te stellen als overkoepelende aanvulling op de reeds bestaande plannen bij de diensten. Een "cybersecurity" team dat een eerste beoordeling uitvoert bij aanvallen op de informatiebeveiliging is aanwezig. Om de kans op ongeautoriseerde toegang tot de ICT-middelen te beperken overweegt het college ten slotte om de controle op de fysieke toegang tot de kantoorruimten op het Spui te verplaatsen naar de begane grond. Hiermee wordt een vergelijkbare situatie als op de Leyweg gecreëerd.

"Conclusie 4: de bestuurlijke inbedding van informatiebeveiliging is onvoldoende."
"Aanbeveling 4: draag het college op de benodigde bestuurlijke inbedding van informatiebeveiliging tot stand te brengen door de verantwoordelijkheid expliciet en als apart onderwerp bij een portefeuillehouder te beleggen en neem het onderwerp als zodanig op in begroting en jaarverslag."
Het college vindt dat het opnemen van informatieveiligheid als onderdeel van de portefeuille voor organisatie niet heeft geleid tot verminderde aandacht voor dit belangrijke onderwerp dat in 2011 bewust als prioriteit van het I-beleid is benoemd. De verwachting is wel dat het nieuwe college de komende periode zal handelen in lijn met het besluit ten aanzien van informatieveiligheid dat is genomen op de al eerder genoemde Bijzondere Algemene Ledenvergadering van de VNG, waarin is opgenomen dat de verantwoordelijkheid voor informatieveiligheid expliciet als separaat onderwerp zal worden opgenomen in de portefeuille van een wethouder. Verder zal als uitvloeisel van de herijking van het beleid ieder kwartaal een rapportage aan de verantwoordelijke wethouder plaats vinden ten aanzien van de stand van zaken van de invoering van het implementatieplan dat uit het herijkte beleid voortvloeit. Zoals ook op de Bijzondere Algemene Ledenvergadering is besloten, zal het college de gemeenteraad informeren via een aparte paragraaf informatieveiligheid in het jaarverslag.

"Conclusie 5: een deel van de gevonden kwetsbaarheden is terug te voeren op cultuur en gedrag van medewerkers en kan niet technisch opgelost worden."
"Aanbeveling 5: de organisatie moet meer inzetten op een proces van bewustwording, cultuurverandering en bekwaamheid ten aanzien van informatiebeveiliging."
Het college onderschrijft de mening van de Rekenkamer dat cultuur en gedrag van de medewerkers essentieel zijn om te komen tot een hoger niveau van informatieveiligheid. Vandaar dat, zoals door de Rekenkamer ook is vermeld, recent is gestart met het op informatieve wijze aandacht schenken aan het belang van informatieveiligheid voor de dagelijkse werkzaamheden van de medewerkers. Daarnaast wil het college ook wijzen op de activiteiten die worden uitgevoerd om de medewerkers erop te wijzen dat zij dienen te handelen als een integer ambtenaar. Dit betekent dat medewerkers geen PC's / applicaties onbeschermd open laten staan voor onbevoegde ambtenaren of derden. Aansluitend vraagt dit extra aandacht voor de fysieke toegangsbeveiliging en voor de logische toegangsbeveiliging (Identity Access Management - IAM) . Via IAM worden alle medewerkers rechten gegeven, waarmee de medewerker toegang heeft tot specifieke applicaties en informatie. Het op goede manier omgaan met PC's en informatie is een onderdeel van integer handelen. Het college zal in 2014 de mogelijkheden onderzoeken om een "awareness" campagne uit te voeren in samenwerking met de activiteiten op het gebied van integriteit om tot een minder vrijblijvende aanpak te komen.

Resumerend. Wat zijn de belangrijkste maatregelen om het niveau van de informatiebeveiliging structureel te verhogen?

- de geconstateerde technische kwetsbaarheden zijn weggenomen, soms door mitigerende maatregelen. Waar nodig zullen in 2014 maatregelen getroffen worden om alle kwetsbaarheden structureel te verhelpen;
- technische hulpmiddelen om het binnendringen van ongeautoriseerde personen op het ICT-netwerk tijdig te kunnen detecteren worden in 2014 ingevoerd; dit blijft een dynamisch proces;
- de ICT-infrastructuur zal jaarlijks door een extern bureau worden getoetst op kwetsbaarheden zowel voor benadering vanaf het internet als benadering via het interne netwerk. De eerste keer vindt plaats in het 4e kwartaal van 2014. Beveiliging is een dynamisch proces is dat continu vraagt om aanscherping van maatregelen;
- uitvoering van een niet-vrijblijvende "awareness" campagne om het belang van informatieveiligheid onder de aandacht van de medewerkers te brengen, incl. extra aandacht voor de fysieke toegangsbeveiliging en logische toegangsbeveiliging;

- het college zal de gemeenteraad jaarlijks informeren over informatieveiligheid via een paragraaf in het jaarverslag.

Het college van burgemeester en wethouders,
de secretaris, de burgemeester,

mw. A.W.H. Bertram J.J. van Aartsen

Naworoord

De rekenkamer is positief over de reactie van het college van burgemeester en wethouders. Het college geeft aan onze aanbevelingen over te nemen of te verwachten dat dit door het nieuwe college zal gebeuren. Digitale veiligheid maakt grote ontwikkelingen door en wordt snel belangrijker. Ook de gemeente slaat steeds meer informatie digitaal op. En met die informatie wordt steeds meer gedaan. De keerzijde hiervan is dat de kwetsbaarheid voor oneigenlijk gebruik of misbruik ook toeneemt. De inzet van de gemeente bij het beveiligen van informatie moet afdoende zijn en gelijk opgaan met de ontwikkelingen in de technologie, de hoeveelheid opgeslagen informatie en de toenemende kwetsbaarheid voor misbruik.

Er is een bestuurlijke scheiding nodig tussen de verantwoordelijkheid voor ICT en die voor de informatiebeveiliging. Het college geeft in zijn reactie aan te verwachten dat dit door het nieuwe college overgenomen zal worden, in lijn met het besluit ten aanzien van informatieveiligheid dat is genomen op de Bijzondere Algemene Ledenvergadering van de VNG van 29 november 2013. Dit besluit behelst onder andere dat de verantwoordelijkheid voor informatieveiligheid expliciet als separaat onderwerp wordt opgenomen in de portefeuille van een wethouder. In het nieuwe coalitieakkoord wordt deze verwachting vooralsnog niet waargemaakt. Het valt ook op dat het onderwerp informatiebeveiliging hierin niet aan de orde komt. Daarmee erkent ook het nieuwe college nog onvoldoende de maatschappelijke verantwoordelijkheid die de gemeente op dit onderwerp heeft. Informatiebeveiliging viel tot nu toe met ICT onder één portefeuille en begrotingsprogramma, met als gevolg dat afwegingen tussen gebruikswaarde, kosten en beveiliging op de werkvloer genomen worden. Het apart beleggen van de informatiebeveiliging bij een portefeuillehouder die niet verantwoordelijk is voor ICT, kan ervoor zorgen dat op bestuurlijk niveau deze afweging te maken is.

Met de opmerking dat ‘het college graag de dialoog zal voeren met de gemeenteraad’ over informatiebeveiliging, nodigt het college de raad uit diens rol op te pakken. Het is daarbij volgens ons van belang dat de gemeenteraad een kader vaststelt voor informatiebeveiliging en het college vervolgens controleert op het uitvoeren van zijn (wettelijke) taak op dit gebied. Informatiebeveiliging dient daarbij te worden gedefinieerd in termen van risico’s, te nemen maatregelen en werkbaarheid (klantvriendelijkheid, effectiviteit, snelheid en dergelijke) in relatie tot beschikbare middelen.

In de reactie van het college wordt gesproken van een test ‘op het interne netwerk’, naast al bestaande tests op andere onderdelen van de informatievoorziening. Het college reageert hiermee op onze conclusie dat een totaalbeeld van de stand van zaken van informatiebeveiliging ontbreekt. Onze stelling is dat een integraal beeld nooit kan ontstaan uit een optelsom van afzonderlijke tests. Een hacker zal alle wegen uitproberen wanneer het doel is aan informatie te komen. Met een ‘integrale test’ bedoelen wij dan ook het inhuren van experts die ‘als waren zij hackers’ op alle mogelijke manieren proberen binnen te komen. Dat is een betere manier om kwetsbaarheden in de informatiebeveiliging op te sporen.