tekst raadsvoorstel
Rekenkameronderzoek ‘Digitale Veiligheid’

Rekenkameronderzoek ‘Digitale Veiligheid’

Inleiding

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, van een *elektronische* overheid die zich richt op verbetering van de dienstverlening met het invoeren van digitale applicaties, zoals de OVchipkaart, naar een *informatie* overheid die primair gericht is op (het beheersen van) informatiestromen, bijvoorbeeld tussen overheid en bedrijven, en daarvoor gebruik maakt van digitale toepassingen.

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. Het was onder meer mogelijk beheerrechten over een belangrijk deel van het interne netwerk te realiseren op basis van een standaardmedewerker account. We vonden gegevens van burgers, waaronder enkele kopieën van paspoorten en een GBA mutatiebestand met persoonsgegevens zoals Burgerservicenummers. De kwetsbaarheden 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. Dit heeft erin geresulteerd dat een aanpak is geformuleerd en de risico’s zijn verminderd of weggenomen.

De reactie van het college op ons onderzoeksrapport laat zien dat de 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.

tekst raadsvoorstel
Rekenkameronderzoek ‘Digitale Veiligheid’

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

In het onderzoek is de ICT-infrastructuur van de gemeente Den Haag 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.

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.

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[1] en Suwinet[2], 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.

[1] DigiD: beveiligd inloggen voor burgers bij overheidsinstellingen.
[2] Suwinet: wordt door overheden gebruikt voor het uitwisselen van persoonsgegevens bij het verstrekken van uitkeringen.

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.

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’.[3]

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

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

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.

tekst raadsvoorstel
Rekenkameronderzoek ‘Digitale Veiligheid’

Gezien het vorenstaande stelt de rekenkamer de raad voor het volgende besluit te nemen:

De raad van de gemeente Den Haag,

Gelet op artikel 185, tweede lid Gemeentewet, besluit:

I. in te stemmen met de conclusies en aanbevelingen van het rapport van de rekenkamer.

II. gelet op het rapport van de rekenkamer ‘Digitale Veiligheid’ in navolging van de aanbevelingen van de rekenkamer het college op te dragen:

1. Nog in 2014 een conceptkader voor informatiebeveiliging op te stellen en voor te leggen aan de raad ter besluitvorming.

2. Tenminste één maal per jaar de gemeentelijke informatiebeveiliging door een externe partij te laten testen op kwetsbaarheden en dit in de planning en controlcyclus op te nemen.

3. Het gemeentelijk netwerk te gaan monitoren op verdachte activiteiten en een calamiteitenplan op te stellen voor ingrijpen bij aanvallen op de informatiebeveiliging.

4. De benodigde bestuurlijke inbedding van informatiebeveiliging tot stand te brengen door de verantwoordelijkheid hiervoor expliciet en als apart onderwerp bij een portefeuillehouder te beleggen.

5. In te zetten op een proces van bewustwording, cultuurverandering en bekwaamheid ten aanzien van informatiebeveiliging dat verder gaat dan vrijblijvend informeren.

6. Het onderwerp informatiebeveiliging als afzonderlijk onderwerp op te nemen in de planning en controlcyclus (begroting en programmarekening) en daarbij de raad minimaal jaarlijks te informeren over resultaten en stand van zaken.

7. De raad binnen een halfjaar na dit besluit te informeren over de aanpak van bovenstaande punten.

Aldus besloten in de openbare raadsvergadering van

Griffier Voorzitter