Opties voor rekenkameronderzoek naar informatieveiligheid

Informatieveiligheid staat meer nog dan voorheen in de belangstelling van gemeenten. Privacy van burgers kan in het geding zijn, maar ook de (digitale) dienstverlening van de gemeente. De gevolgen van inbreuken op informatieveiligheid kunnen zeer ernstig zijn. Ondertussen maken gemeenten in toenemende mate gebruik van gedigitaliseerde informatie en communicatie. Met de komst van nieuwe taken in het sociale domein zal deze digitalisering alleen maar toenemen. Er ligt daarmee een grote verantwoordelijkheid bij gemeenten zorgvuldig met gegevens van burgers om te gaan, vergelijkbaar met die voor de fysieke veiligheid en openbare orde. Gegevens van burgers, bedrijven en instellingen moeten bij de gemeente in goede handen zijn, waarbij overigens wel geldt dat 100% veiligheid niet bestaat. Het draait erom bewust met digitale veiligheidsrisico's om te gaan en een afgewogen oordeel te maken tussen kansen en risico's .

Naar aanleiding van onder meer de Diginotar-crisis en Lektober in 2011 zijn veel initiatieven genomen waarmee de informatieveiligheid verbeterd kan worden. Belangrijke mijlpalen zijn de oprichting van de Informatie Beveiligings Dienst voor gemeenten (IBD) en de Taksforce Bestuur en Informatieveiligheid Dienstverlening (BID)[1]. In november 2013 hebben de leden van de VNG ingestemd met een resolutie 'informatieveiligheid'. De strekking van deze resolutie is dat elke gemeente informatieveiligheidsbeleid zal gaan vaststellen aan de hand van de Baseline Informatiebeveiliging van de IBD.[2]

Met het opstellen van de Baseline en het aannemen van de VNG resolutie is de basis gelegd voor informatieveiligheid bij gemeenten. Het is de vraag in hoeverre deze resolutie daadwerkelijk in de bestuurlijke, organisatorische en technische processen van de gemeentelijke organisatie is ingebed. De Rekenkamer Den Haag besloot de proef op de som te nemen met een onderzoek naar de digitale veiligheid bij de gemeente Den Haag. In dit onderzoek werden in het interne netwerk van de gemeente de nodige kwetsbaarheden in de veiligheid gevonden. Onderzoekers slaagden er onder meer in aan privacygevoelige informatie te komen. Ook bleek informatieveiligheid als afzonderlijk onderwerp onvoldoende bestuurlijk ingebed te zijn, waardoor afwegingen tussen gebruikswaarde en veiligheid van ICT op de werkvloer gemaakt worden.

Een dergelijk onderzoek is voor veel rekenkamers en rekenkamercommissies wellicht te kostbaar en niet eenvoudig uit te voeren. Desondanks zijn er voor rekenkamers en rekenkamercommissies wel mogelijkheden de (controle op) de informatieveiligheid in de eigen gemeente te versterken. Wij willen daar graag een bijdrage aan leveren door op basis van de bevindingen uit het onderzoek van de Rekenkamer Den Haag aan te geven hoe raadsleden hun kader stellende en controlerende taken op het gebied van informatieveiligheid kunnen versterken. U treft hierbij een voorbeeldbrief aan, die enerzijds de bewustwording van uw gemeenteraad voor het onderwerp vergroot, anderzijds de raad het benodigde inzicht kan verschaffen door gericht vragen te stellen aan het college.

[1] De Informatie Beveiligingsdienst (IBD) is een samenwerking tussen de gemeenten en Rijk, werkzaam vanaf 1 januari 2013, met als doel een gestandaardiseerde informatiebeveiliging bij gemeenten te realiseren, de Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID), opgericht op 13 februari 2013 voor een periode van twee jaar, heeft als doel te komen tot verplichtende zelfregulering per overheidslaag als het gaat om informatieveiligheid en brengt het onderwerp bij overheden hoger op de agenda.

[2] Resolutie Informatieveiligheid, randvoorwaarde voor de professionele gemeente, vastgesteld op 29 november 2013.

Maar u kunt natuurlijk ook zelf onderzoek (laten) doen naar de informatieveiligheid in uw gemeente. Verschillende varianten in scope en aanpak zijn daarbij mogelijk. Hieronder is een beknopt overzicht gegeven van voorbeelden van mogelijke onderzoeken. Ook wordt voor zover bekend aangegeven wat daarvoor te verwachten kosten zijn. Gelet op de gevoeligheid van het onderwerp en de risico's daarbij is het bij elke variant raadzaam extra aandacht te besteden aan afstemming met het college en de gemeentelijke organisatie.

Onderzoek digitale veiligheid (voorbeeld Rekenkamer Den Haag).

Onderzoeksvraag

• 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 onderzoek

In de voorbereiding is een korte inventarisatie van het gemeentelijke beleid en de implementatie daarvan gemaakt door de rekenkamer zelf. Voor het eigenlijke onderzoek is een extern bureau ingehuurd. Deels zonder enige kennis van de gemeentelijke ICT en deels met gebruik van een ter beschikking gesteld gebruikersaccount, is onderzocht of het mogelijk was aan privacy gevoelige informatie te komen en welke kwetsbaarheden aan te wijzen waren in de gemeentelijke 'digitale beveiliging'.

Bijzonderheden

Omdat de onderzoeksinformatie zelf ook tot veiligheidsrisico's kan leiden zijn extra waarborgen voor vertrouwelijkheid toegepast (versleuteling, opslag in kluis, 'geheim verklaren' van feitenrapport). De betrokken ambtenaren kregen een presentatie van bevindingen en praktische aanbevelingen over aanpak en prioritering van gevonden kwetsbaarheden. Onaangekondigd is nog een hertest uitgevoerd. Raadsleden ontvingen een nep-phishingmail gericht op bewustwording.

Samenvatting

De Haagse Rekenkamer deed onderzoek naar de digitale veiligheid van de ICT-infrastructuur en van privacygevoelige informatie bij de gemeente Den Haag. Daarbij bleek de gemeentelijke website denhaag.nl veilig te zijn. Op verschillende manieren bleek het mogelijk van buiten toegang tot het interne netwerk te verkrijgen, en juist op het interne netwerk werden de nodige kwetsbaarheden in de veiligheid gevonden. De rekenkamer beveelt aan digitale veiligheid meer bestuurlijke aandacht te geven en periodiek integrale testen uit te voeren.

Inzet en kosten

De rekenkamer heeft zelf aan onderzoek, rapportage en projectleiding circa 400 uur besteed. De opdracht voor de inhuur van een extern bureau bedroeg circa € 50.000.

Meer informatie

www.rekenkamerdenhaag.nl > 'publicaties/digitale veiligheid'

Onderzoek naar de implementatie Baseline Informatiebeveiliging Gemeenten (onderzoekshandreiking Taskforce BID).

Bij het verbeteren van de informatieveiligheid bij gemeenten wordt uitgegaan van een 'verplichte zelfregulering'. Dit betekent dat het Rijk heeft vastgelegd dat gemeenten in eerste instantie zelf aan zet zijn. De Informatie Beveiligings Dienst (een samenwerking tussen het Rijk en de gemeenten) heeft de Baseline Informatiebeveiliging Gemeenten (BIG) opgesteld, waarmee gemeenten een basisnorm voor informatieveiligheid aangereikt krijgen. De leden van de VNG hebben in november 2013 besloten deze BIG als basis te nemen voor hun beleid. Met een onderzoek naar de (stand van zaken van de) implementatie van de BIG krijgt u zicht op de mate waarin de organisatie voor informatieveiligheid op orde is bij uw gemeente. De onderzoeksopzet gaat er van uit dat informatieveiligheid in essentie een organisatievraagstuk is.

Onderzoeksvraag

Mogelijke onderzoeksvragen die u kunt gebruiken zijn:

1. Stuurt de gemeente op de afspraken die benoemd zijn in de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' en in het bijzonder op de implementatie van de BIG?
2. Heeft de gemeente de risico's op informatieveiligheidsvlak in een Informatiebeveiligingsplan benoemd, is helder in hoeverre risico's beheerst dan wel geaccepteerd worden, inclusief de bijbehorende maatregelen uit de BIG, en op welk niveau is dit plan vastgesteld (organisatie, college, raad)?
3. Rapporteert en bespreekt de gemeente het functioneren van de cyclus van informatieveiligheid op management- en bestuursniveau (college en raad)? Is zij daarover transparant richting haar ketenpartners door via waarstaatjegemeente.nl te rapporteren over informatieveiligheid?
4. Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT?
5. Kent de gemeente de leveranciers en partners waarmee ze samenwerkt en toetst zij die ook op informatieveiligheidsaspecten?
6. Is de gemeente 'officieel' aangesloten bij de IBD?
7. Weet de gemeentelijke organisatie hoe te handelen bij een (ernstig) informatieveiligheidsincident en is er een incidentenmanagementproces ingevoerd?
8. Wordt jaarlijks getoetst of de gemeentelijke organisatie in control is op het gebied van informatieveiligheid via peer reviews, audits of self-assessments? En wordt over het functioneren van de cyclus van informatieveiligheid gerapporteerd aan de raad?
9. Zijn de beleidsuitgangspunten nog valide of zijn er interne of externe ontwikkelingen die leiden tot heroverwegingen van de gemeentelijke risico-inschattingen?
10. Is er een integrale aanpak voor organisatieleren op het gebied van informatieveiligheid? Hoe houdt de gemeente kennis vast en bouwt zij hierop door?

Aanpak onderzoek

De rekenkamer(commissie) kan deze vragen uitzetten bij de gemeentelijke organisatie en indien nodig voor de juiste interpretatie en duiding van de antwoorden externe ondersteuning inhuren, eventueel in combinatie met nadere praktijktoetsing/review (bijvoorbeeld naar de kwaliteit en integraliteit van door de gemeente uitgevoerde penetratietests).

Meer informatie

De Toolkit die door de Taskforce BID is samengesteld biedt meer informatie over verschillende onderwerpen en bijbehorende onderzoeksvragen voor een dergelijk onderzoek. De Toolkit is in eerste instantie opgesteld voor gemeentesecretarissen, maar is inhoudelijk zeer geschikt voor de voorbereiding van een onderzoek naar de implementatie van de BIG door rekenkamer (-commissies). De volledige Toolkit is te vinden op: www.taskforcebid.nl. Een samenvatting treft u hierboven aan.

Onderzoek Social Engineering (voorbeeld gemeente Zaanstad)

De mens is één van de schakels in informatieveiligheid. Technisch kan een gemeente nog zo veilig zijn, werkelijke veiligheid staat of valt met de toepassing in de praktijk van normen voor informatieveiligheid door medewerkers. Hoe staat het met de kennis en het bewustzijn van de medewerkers binnen uw gemeente op dit gebied? Een onderzoek aan de hand van 'Social Engineering' (SE) heeft als doel vertrouwelijke informatie te verkrijgen door middel van list en bedrog, manipuleren, psychologische trucs, valse voorwendsels en misbruik van vertrouwen. De resultaten worden gebruikt om het beveiligingsbewustzijn bij medewerkers te verhogen. De gemeente Zaanstad liet twee keer een dergelijk onderzoek uitvoeren, telkens met een andere invalshoek. Eén was gericht op phishing en gebouwenbeveiliging en het tweede op fraude en toegang tot beveiligde ruimte. Daarbij is gekeken naar de mogelijkheid de gemeentelijke gebouwen binnen te komen en documenten te kunnen bemachtigen, onder meer uit beveiligde ruimtes en naar de mogelijkheden om op basis van openbaar toegankelijke informatie over medewerkers aan gebruikersgegevens te komen.

Aard van conclusies en aanbevelingen

Conclusies uit de onderzoeken richten zich op cultuur binnen de gemeentelijke organisatie en de praktische mogelijkheden voor buitenstaanders zich toegang te verschaffen tot gebouwen en informatie. De uit de beide onderzoeken volgende aanbevelingen zijn opgenomen met de betreffende leidinggevenden en er is een verbetertraject opgenomen in de interne jaarplannen van betrokken afdelingen. Daarnaast zijn aanbevelingen om het beveiligingsbewustzijn te verhogen opgenomen in het informatiebeveiligingsplan van de gemeente.

Inzet en kosten

Een Social Engineering onderzoek kan afhankelijk van de opdrachtomschrijving en de schaalgrootte van de organisatie sterk variëren in benodigde inzet en kosten voor inhuur van externe expertise. De beschreven onderzoeken bij de gemeente Zaanstad vergden per afzonderlijk onderzoek circa 30 uur inzet van de opdrachtgever en een budget van circa € 10.000.

Meer informatie

Een beschrijving van de beide SE onderzoeken is opgenomen in de 'Rapportage Informatiebeveiliging bij de gemeente Zaanstad, periode: 2013'. Deze rapportage is te vinden in het raadsinformatiesysteem van de gemeente Zaanstad: http://zaanstad.notudoc.nl, zoekterm 'informatieveiligheid', selecteer document 'Bijlage 18-04-2014'.