Rekenkamer test informatieveiligheid

Eind 2013 voerde de Rekenkamer Den Haag een onderzoek uit naar de beveiliging van privacygevoelige informatie bij de gemeente door middel van een integrale *hack* op de gemeentelijke ICT. Ondanks vele getroffen maatregelen bleek het mogelijk binnen te dringen in het gemeentelijke netwerk en aan privacygevoelige informatie te komen. Welke lessen kunnen uit deze hack getrokken worden?

Thijs Bosma en Harro Spanninga

Extern onderzoek is een belangrijk leerinstrument dat organisaties kan helpen digitale veiligheid op een hoger niveau te brengen. Digitale veiligheid is door zijn virtuele karakter soms lastig te grijpen. Daarom zijn dergelijke onderzoeken zeer behulpzaam. Door de adequate reactie van het bestuur op de rapportage van de rekenkamer is in de gemeente Den Haag de informatieveiligheid naar een hoger niveau gebracht. Onder meer heeft de gemeente Den Haag nadrukkelijker ingezet op *awareness*, is de rapportage over informatieveiligheid aan het college en de raad aangescherpt en zijn periodieke, externe veiligheidstoetsen expliciet in het informatieveiligheidsbeleid opgenomen.
Welke bijdrage kunnen rekenkamers leveren aan het optimaliseren van de gemeentelijke informatieveiligheid? In dit artikel gaan de auteurs in op de lessen die we kunnen trekken uit een *hack* van de gemeentelijke ICT.

Digitale veiligheid is een actueel onderwerp voor overheden. Immers in 2017 is het doel alle overheidsdienstverlening digitaal ontsloten te hebben. Met grote regelmaat halen cyberaanvallen het nieuws, waarbij dienstverlening is verstoord of misbruik is gemaakt van vertrouwelijke informatie. Door overheden wordt hard gewerkt aan het optimaliseren van informatieveiligheid, bijvoorbeeld aan de hand van Baselines Informatiebeveiliging voor de verschillende overheidslagen. De Haagse Rekenkamer vroeg zich af of door deze inzet gevoelige informatie bij de gemeente ook echt veilig is en deed een praktijkonderzoek naar de digitale veiligheid. De uitkomsten van dat onderzoek leiden tot duidelijke aanbevelingen waarmee gemeenten informatieveiligheid kunnen versterken.

Hoeveelheid data bij gemeenten neemt toe

Gemeenten bewaren en gebruiken grote hoeveelheden data. Veel daarvan is privacygevoelige informatie van inwoners en van bedrijven. De nieuwe taken in het kader van de decentralisaties in het sociaal domein en de tegelijk doorgevoerde bezuinigingen vormen een prikkel voor gemeenten om meer informatie op te slaan en deze intensiever te analyseren en te combineren. Op grond van de Algemene wet bestuursrecht (Awb) zijn gemeenten verplicht deze informatie voldoende betrouwbaar en vertrouwelijk te behandelen. De Wet bescherming persoonsgegevens (Wbp) geeft aan dat bestuursorganen passende technische en organisatorische maatregelen moeten nemen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Schade voor zowel burgers en bedrijven als voor gemeenten bij misbruik kan groot zijn. Bijvoorbeeld wanneer sprake is van identiteitsfraude, waarmee personen voor grote hoeveelheden geld benadeeld kunnen worden. Gemeenten kunnen imagoschade leiden, wanneer van door hen beheerde informatie misbruik wordt gemaakt of wanneer dienstverlening aan burgers uitvalt door aanvallen van buitenaf.

Bij dit onderzoek is bewust gekozen voor een integrale praktijktest van de digitale veiligheid van de gemeente

Onderzoek digitale veiligheid

Eind 2013 voerde de Rekenkamer Den Haag een onderzoek uit naar de beveiliging van privacygevoelige informatie bij de gemeente. Met het laten uitvoeren van een integrale hack op de gemeentelijke ICT

is onderzocht of gegevens van burgers en bedrijven te bemachtigen waren. De rekenkamer maakte bij het onderzoek gebruik van professionele en gecertificeerde onderzoekers.

Bij dit onderzoek is bewust gekozen voor een integrale praktijktest van de digitale veiligheid van de gemeente. Veel andere onderzoeken richten zich of op administratieve voorwaarden voor informatieveiligheid of alleen op deelaspecten van de ICT. In het eerste geval kunnen geen uitspraken worden gedaan over de werkelijke effectiviteit van het beleid en in het tweede geval ontbreekt een totaaloverzicht van de keten van systemen en de interactie met bijvoorbeeld cultuur in de organisatie of invloed van menselijk handelen.

Het onderzoek laat zien dat informatieveiligheid bij gemeenten nog in ontwikkeling is en dat gemeenteraden zich actiever moeten bemoeien met dit onderwerp

In Den Haag zijn al veel maatregelen getroffen waarmee de veiligheid van gevoelige informatie gewaarborgd zou moeten worden. Zo heeft de gemeente naast een Concern Information Officer (CIO) ook een Chief Information Security Officer (CISO) in dienst en zijn de gemeentelijke diensten verplicht te verklaren 'in control te zijn' over hun ICT. Toch bleek tijdens het onderzoek dat het mogelijk was binnen te dringen in het gemeentelijke netwerk en aan privacygevoelige informatie te komen. Gevonden werden onder meer bestanden met GBA (gemeentelijke basisadministratie) gegevens en kopieën van identiteitsbewijzen. Het was ook mogelijk de kern van de gemeentelijke ICT te benaderen en daar systemen aan te sturen. Het was eenvoudig toegang te krijgen tot het niet voor buitenstaanders bedoelde interne netwerk. Eenmaal op dat interne netwerk ontbraken verschillende schakels in de beveiliging. De gevonden kwetsbaarheden zijn direct na de uitvoering van het onderzoek bekendgemaakt aan betrokkenen in de gemeentelijke organisatie. Kwetsbaarheden met een hoog risico konden daardoor snel worden verholpen.

Wat kan de gemeente doen?

De bevindingen uit het onderzoek waren voor de rekenkamer reden te concluderen dat er structureel onvoldoende waarborgen zijn voor het veilig beheren en gebruiken van privacygevoelige informatie. Het gemeentebestuur geeft onvoldoende aandacht aan het onderwerp informatieveiligheid. Bij de portefeuilleverdeling en in de begroting- en verantwoordingscyclus is informatiebeveiliging een subonderwerp van ICT. De nadruk ligt op dienstverlening

(intern en extern) bij informatisering. Veiligheid is een bijzaak. Door het ontbreken van duidelijke kaders en sturing vanuit het gemeentebestuur (raad én college) worden afwegingen over informatieveiligheid op de werkvloer gemaakt. Een belangrijke notie uit het onderzoek is dat inzetten op 100% veiligheid een illusie is. Informatiebeveiliging biedt te vaak alleen bescherming tegen bekende bedreigingen en loopt daardoor achter op de realiteit. Daarnaast is de invloed van menselijk handelen op informatieveiligheid groot. Een alerte signalering van en ingrijpen bij daadwerkelijke aanvallen op het netwerk zijn daarom zo mogelijk van nog groter groot belang dan het preventief beveiligen van informatie. Oplossingen zijn het monitoren van het netwerk op verdachte activiteiten en het opstellen van een calamiteitenplan voor het ingrijpen bij een aanval op de informatiebeveiliging.

Meeliften op het Haagse onderzoek

De uitkomsten van het Haagse onderzoek laten zien dat informatieveiligheid bij gemeenten nog in ontwikkeling is en dat gemeenteraden zich actiever moeten bemoeien met dit onderwerp. Naar aanleiding van het onderzoek hebben de Taskforce BID, de Rekenkamer Den Haag en de Nederlandse Vereniging voor Rekenkamers en Rekenkamercommissies (NVRR) alle lokale rekenkamers een brief aangeboden waarmee ze het onderwerp bij hun gemeente (of andere overheidslaag) aan de orde kunnen stellen. Aan de hand van zeven vragen kunnen gemeenteraden inzicht krijgen in en grip krijgen op de informatieveiligheid in hun gemeente. Rekenkamers kunnen natuurlijk ook zelf een vergelijkbaar onderzoek uitvoeren. Bij de brief is een overzicht van mogelijke onderzoeken opgenomen, met voorbeelden en een inschatting van de kosten van de verschillende varianten. Zowel de brief als deze voorbeelden zijn te vinden op de website van de Rekenkamer Den Haag (www.rekenkamerdenhaag.nl).

Voorbeeldvragen voor gemeenteraden

Informatieveiligheid is een complex onderwerp en daarom voor raadsleden soms niet eenvoudig te doorgronden. Op basis van de uitkomsten van het Haagse onderzoek stelden de Taskforce BID en de Rekenkamer Den Haag zeven vragen op die de gemeenteraad aan het college kan stellen.

- Op welke wijze heeft het college uitvoering gegeven aan de VNG-Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente'?
- Heeft het college een kadernota opgesteld voor informatieveiligheid en deze ter besluitvorming voorgelegd aan de raad?
- Op welke wijze is de bestuurlijke inbedding van informatieveiligheid in de gemeente vormgegeven?
- Heeft het college zicht op de meest kritieke processen in de gemeenten waar veel vertrouwelijke (persoons-) gegevens worden verwerkt, zoals Suwinet, het gegevensuitwisseling systeem in het domein Werk en Inkomen? En zijn de risico's en de kwetsbaarheden bij de verwerking bekend en de daarbijhorende aanvullende maatregelen getroffen om deze risico's te beheersen?
- Heeft het college het afgelopen jaar de gemeentelijke informatiebeveiliging door een externe – daartoe gekwalificeerde – partij laten testen op kwetsbaarheden?
- Kan het college aangeven op welke wijze het gemeentelijk netwerk wordt gemonitord op verdachte activiteiten en of er een calamiteitenplan opgesteld is voor ingrijpen bij aanvallen op de informatiebeveiliging?
- Op welke wijze zet het college in op een proces van bewustwording, cultuurverandering en bekwaamheid ten aanzien van informatieveiligheid binnen de organisatie?

Lokale rekenkamers hebben een voorbeeldbrief gekregen van de Taskforce BID en de Rekenkamer Den Haag waarin deze vragen zijn opgenomen. Rekenkamers kunnen met het verzenden van de brief aan de gemeenteraad de discussie over het onderwerp informatieveiligheid op de agenda plaatsen en de gemeenteraad ondersteunen in zijn taak.

Auteurs
Thijs Bosma is senior onderzoeker bij de Rekenkamer Den Haag en was projectleider van het onderzoek Digitale Veiligheid. Ir. H.G. (Harro) Spanninga MMC is adviseur informatiemanagement bij Berenschot en was actief voor de Taskforce BID. De auteurs schreven dit artikel op persoonlijke titel.

zie ook www.tpconline.nl