Rekenkamer commissie
LEIDEN & LEIDERDORP

Digitaal gedrag: veilig en verantwoordelijk

Onderzoek naar de digitale veiligheid in Leiden en Leiderdorp

Rekenkamer commissie
LEIDEN & LEIDERDORP

Digitaal gedrag: veilig en verantwoordelijk

Onderzoek naar de digitale veiligheid in Leiden en Leiderdorp

Rekenkamer commissie
LEIDEN & LEIDERDORP

Rekenkamerbrief

Inleiding

De Rekenkamercommissie Leiden-Leiderdorp heeft onderzoek gedaan naar de digitale veiligheid van de gemeenten Leiden en Leiderdorp. Het rapport bestaat uit twee delen: de rekenkamerbrief en het onderzoeksrapport. In het onderzoeksrapport wordt het onderzoek omschreven. Het onderzoek is onder begeleiding van de Rekenkamercommissie Leiden-Leiderdorp uitgevoerd door Necker van Naem in samenwerking met haar partner Guardian360. De rekenkamerbrief is opgesteld door de Rekenkamercommissie en is gebaseerd op het onderzoeksrapport. De conclusies en aanbevelingen die wij hierin presenteren zijn erop gericht u te helpen om uw informatiepositie als lid van de gemeenteraad van Leiden of Leiderdorp te versterken.

In het kader van het onderzoek is een praktijktest uitgevoerd. Om de uitkomsten van de praktijktest niet te beïnvloeden heeft de Rekenkamer ervoor gekozen om het onderzoek niet vooraf aan te kondigen, maar hier slechts over te communiceren op een ‘need to know’-basis. Het onderwerp stond wel genoemd in het Onderzoeksplan 2017-2018. Daarnaast hebben wij in de fractiegesprekken van 2018 benoemd dat jaar met het onderzoek te gaan starten.

Wij willen de gemeentesecretarissen en de medewerkers graag hartelijk danken voor hun rol in het hele proces. De uitvoering van dit onderzoek was bestuurlijk en juridisch een uitdaging en wij waarderen bijzonder hoe beide gemeenten zich hebben ingezet om alles goed te regelen, met name ook richting de andere gemeenten die gebruik maken van Servicepunt71.

Onderzoekvraag

Het belangrijkste doel van het onderzoek was om meer inzicht te krijgen in de informatiebeveiliging van Leiden en Leiderdorp. Er is gewerkt aan de hand van vijf thema’s: Beleid, Organisatie, Plan-Do-Check-Act (PDCA) cyclus, Rol van de raad, Praktijktoetsing.

Met het onderzoek hebben wij de volgende hoofdvraag willen beantwoorden:

1. Hebben de gemeenten Leiden en Leiderdorp in brede zin een goed beeld van de belangrijkste risico’s op het gebied van informatiebeveiliging (opslag, uitwisseling en beveiliging) en in het bijzonder gevoelige informatie zoals (bijzondere) persoonsgegevens?

Daarbij hebben we de volgende deelvragen onderzocht:

2. Beschikken beide gemeenten over een adequaat informatiebeveiligingsbeleid?
3. Wordt het beleid adequaat uitgevoerd en wordt het gemonitord?
4. Hoe is de informatievoorziening aan de gemeenteraden over informatiebeveiliging?

Voor het beantwoorden van deze vragen is gekeken naar het beleid dat er in beide gemeenten gehanteerd wordt. Daarnaast heeft een praktijktoetsing plaatsgevonden.

Samenvatting 'Onderzoeksrapport'

Beleid: de gemeenten Leiden en Leiderdorp hebben overwegend hetzelfde beleid op het gebied van digitale veiligheid. De beleidsstukken zijn inhoudelijk volledig en bieden voldoende uitgangspunten en regels maar dienen geactualiseerd te worden, bijvoorbeeld aan de Algemene verordening gegevensbescherming (AVG).

Organisatie: de samenwerking in de regio, tussen gemeenten en Servicepunt71, verloopt over het algemeen goed. De (bestuurlijke) verantwoordelijkheid bij beide gemeenten is verdeeld over de burgemeester, portefeuillehouders Bedrijfsvoering, overige portefeuillehouders, College en gemeentesecretaris. De governance van de gemeenten is in transitie. De komende jaren zal (nog) meer gewerkt gaan worden voor – en vanuit -– de regio.

PDCA-cyclus: de gemeenten en het servicepunt voeren standaard verschillende zelfaudits uit. Hieruit ontstaat een beeld over de digitale veiligheid en kunnen verbeterplannen worden opgesteld. Toch blijven er ook risico's ongezien, zoals uit dit onderzoek blijkt. Ook worden verbeterplannen niet altijd gemonitord.

Rol van de gemeenteraad: beide gemeenteraden ontvangen informatie over digitale veiligheid in hun gemeenten. Dit gebeurt zowel op vaste momenten als incidenteel. De informatieverstrekking is niet altijd optimaal, deels omdat het college zelf niet altijd voldoende of de juiste informatie heeft. Ook de wijze van informatieverstrekking is niet altijd even toegankelijk voor raadsleden, onder meer vanwege een hoog technisch gehalte.

Praktijktoetsing: er zijn onder verantwoordelijkheid van de Rekenkamercommissie drie testen uitgevoerd:

- Een externe test waarbij vanaf het internet de veiligheid van twee (web)applicaties en de onderliggende servers is onderzocht.
- Een interne test waarbij vanuit de kantooromgeving is gezocht naar kwetsbaarheden in het draadloze netwerk, het kantoornetwerk en zes interne (web)applicaties en de onderliggende servers.
- Een phishingtest waarbij geprobeerd is om de inloggegevens van een specifieke gebruikersgroep te achterhalen via e-mail.

De resultaten van de externe test laten zien dat de risico's om van buiten de organisatie binnen te dringen in systemen van de gemeenten, laag zijn. Er is echter een medium/groot risico op incidenten van binnenuit.

Conclusies

De raadsleden van Leiden en Leiderdorp hebben zowel in de Raad als in onze jaarlijkse gesprekken met de fracties veel aandacht voor de digitale veiligheid van de gemeenten. De raden worden door de colleges regelmatig geïnformeerd over dit onderwerp, maar de raadsleden geven aan (nog altijd) moeite te hebben om te controleren en sturen op het gebied van digitale veiligheid.

Uit ons onderzoek blijkt dat het beleid en de organisatie rondom digitale veiligheid op orde zijn. De gemeenten zijn zich bewust van de risico's die de digitalisering met zich brengt en controleren hier ook regelmatig op. Wij zien voor de raad daarom weinig mogelijkheid of noodzaak om te sturen op dit vlak. De kwetsbaarheden zitten vooral in de praktijk en de schakel tussen technische en bestuurlijke verantwoordelijkheid. De Rekenkamer constateert drie kwetsbaarheden op het gebied van digitale veiligheid waar wij hieronder nader op in zullen gaan:

1. Gedrag
2. Actualiteit
3. Informatievoorziening

Gedrag

De grootste risico's rondom digitale veiligheid blijken intern te zijn. Het is daarom belangrijk dat iedereen met een werkplek binnen de gemeenten, waaronder ook de raadsfracties, zich bewust worden van deze risico's en hier ook verantwoordelijk mee omgaan.

Een aanvaller die toegang heeft tot het kantoornetwerk van de gemeente, kan eenvoudig misbruik maken van de gevonden kwetsbaarheden van de systemen. Deze kwetsbaarheden hadden vooral te maken met ontbrekende security-updates en configuratiefouten van applicaties en systemen. Er zijn enkele systemen gevonden die geplaatst lijken te zijn door externe leveranciers waarbij onduidelijk is wie verantwoordelijk is voor het beheer van deze systemen en wie er bijvoorbeeld voor zorgt dat security-updates geïnstalleerd worden.

Bij de phishingtest ontving een aantal medewerkers van de gemeenten een e-mail met het verzoek in te loggen op een interne applicatie via een link naar een site. Het inlogscherm van deze applicatie was nagebouwd en voorzien van een geldig certificaat (groen slotje). Een beperkt aantal medewerkers heeft na het ontvangen van de e-mail de nagemaakte website geopend en inloggegevens ingevuld. Een aantal van de medewerkers en functioneel beheerders hebben adequaat gereageerd door melding te maken van de phishing e-mail. Naast het adequaat reageren van de medewerkers hebben preventieve technische maatregelen ervoor gezorgd dat de e-mail niet is aangekomen bij een groep gebruikers. Dit lijkt te komen door aanwezigheid van een zelflerend spamfilter.

Actualiteit

De tweede kwetsbaarheid zit in de snelheid van de ontwikkelingen rondom digitale veiligheid. Beleid raakt snel verouderd, systemen ontwikkelen door, updates volgen elkaar snel op en er worden steeds nieuwe aanvalsmethodes ontwikkeld. Achteropraken brengt risico's met zich mee. Er moeten intern daarom goede afspraken zijn over de manier waarop je op de hoogte blijft van de actualiteit en hoe je hierop inspeelt. Servicepunt71 en de bestuurlijk verantwoordelijken zijn zich hiervan bewust en weten elkaar goed te vinden, maar ook hier vormt bewustzijn en gedrag in de rest van de organisatie een risico.

Informatievoorziening

Hoewel risico's en incidenten worden gemeld, merken wij op dat de communicatie hierover bemoeilijkt wordt door conflicterende belangen. De gemeenten dragen ieder afzonderlijk bestuurlijke verantwoordelijkheid voor de digitale veiligheid. Het beheer hiervan is echter ondergebracht bij Servicepunt71. Zowel bij Raad als College merken wij op dat er behoefte is aan specifiekere informatie vanuit het Servicepunt71 om te kunnen controleren of hun gemeente digitaal veilig is. De digitale veiligheid is er echter bij gebaat om dergelijke informatie zo min mogelijk te delen buiten het servicepunt. Tot op zekere hoogte is dit probleem niet op te lossen. De informatievoorziening kan echter wel gerichter en de toegankelijkheid van rapportages kan nog verbeterd worden. De Baseline Informatiebeveiliging Overheid (BIO) wordt op 1 januari 2020 van kracht. In 2019 kunnen gemeenten zich voorbereiden op de overgang van de BIG naar de BIO. De verwachting is dat het werken volgens de BIO inzichtelijkere rapportages aan het bestuur oplevert. Het beleid wordt geëvalueerd middels een Plan-Do-Check-Act-cyclus (PDCA). Op dit moment heeft de Raad nog onvoldoende zicht op de laatste stap; wat er wordt gedaan om de punten uit de Check-fase te verbeteren.

Hieronder doen wij een aantal aanbevelingen. Daarnaast bieden wij in deze rapportage een lijst van aandachtspunten waarop de Raad zou kunnen controleren.

Aanbevelingen

1. Los de concrete kwetsbaarheden op die bleken uit de penetratietesten.
2. Maak de organisatie en de medewerkers ervan bewust dat het grootste risico voor de digitale veiligheid, het (eigen) gedrag is.
3. Verbeter de beveiliging. Onderzoek of de fysieke (kantoor)locaties beter kunnen worden beveiligd en verlaag hiermee de kans op misbruik van interne systemen. Maak waar mogelijk gebruik kan worden gemaakt van 'two factor authentication'. Dit zorgt ervoor dat wanneer kwaadwillenden toegang hebben gekregen tot de inloggegevens van een gebruiker, er alsnog geen gebruik van gemaakt kan worden omdat de tweede factor (bijvoorbeeld sms-token, vingerafdruk, push-bericht, USB-token, etc.) ontbreekt.

4. Controleer de ontwikkelingen binnen digitale veiligheid op de drie kwetsbaarheden (het gedrag, de actualiteit en de informatievoorziening) en op de beschikbaarheid van voldoende middelen. Vraag het College op deze onderwerpen te rapporteren.

Aandachtspunten

In de aanbevelingen hebben wij de belangrijkste punten opgenomen waar de Raad op kan sturen. Deze aanbevelingen zijn bewust vrij algemeen gehouden. Het onderzoek was gericht op het vaststellen van de kwetsbaarheden op het gebied van digitale veiligheid. Hoewel het onderzoek niet gericht was op de verschillende manieren waarop de geconstateerde kwetsbaarheden kunnen worden gedicht, biedt het rapport wel handvatten om enkele concrete punten te benoemen waar naar onze mening op gelet moet worden. Deze punten hebben we hieronder opgenomen.

Gedrag

- Zorg dat het beveiligingsbewustzijn verbetert en actief wordt onderhouden, door voorlichting en training van medewerkers. Train medewerkers hoe ze een phishing e-mail kunnen herkennen en wat ze moeten doen bij het ontvangen van een phishing e-mail.
- De aanschaf van nieuwe apparatuur of digitale diensten brengt veiligheidsrisico's mee. Zorg dat medewerkers zich hiervan bewust zijn en zorg dragen voor het (laten) updaten en controleren van de digitale veiligheid.
- Zorg voor een helder overzicht van aanwezige systemen, applicaties, infrastructuur en contracten met leveranciers, zodat zicht is op bevoegdheden, netwerkpoorten, aanwezige services en eenvoudig te misbruiken kwetsbaarheden, bijvoorbeeld met een vulnerability scanner.
- Besteed in het bijzonder aandacht aan het aanspreken van onbekenden op kantoorlocaties, aangezien de geconstateerde kwetsbaarheden vooral van binnenuit (vanuit toegang tot het netwerk) te gebruiken waren.
- Personeel moet dus integer zijn, bewust zijn op mogelijke indringers, phisingmail kunnen herkennen en wachtwoorden voor zich houden. Houd er rekening mee dat er nu vooral gewerkt wordt op basis van vertrouwen.

Actualiteit

- Actualiseer het digitale veiligheidsbeleid aan de (technologische) ontwikkelingen. Het informatiebeveiligingsbeleid stamt uit 2016, het beleid gegevensbescherming uit 2015. Een belangrijke ontwikkeling sindsdien die een plek moet krijgen in het beleid is de inwerkingtreding van de AVG. Omdat er nog veel onduidelijkheden waren rondom de specifieke consequenties van de AVG hebben de gemeenten ervoor gekozen om het beleid pas na inwerkingtreding te actualiseren.
- Laat periodiek audits en penetratietesten uitvoeren door gespecialiseerde bureaus. Voer risicoanalyses en evaluaties uit en pas op basis van de uitkomsten het digitale beveiligingsbeleid aan. Dat geldt ook voor risico's door nieuwe zwakheden, die dagelijks ontstaan door de voortschrijdende technologie en de inventiviteit van hackers.
- Installeer security updates zo snel mogelijk na verschijning. Maak afspraken met leveranciers

van apparatuur over het beheren en updaten van systemen.
- Implementeer netwerkscheiding zodat er beter onderscheid gemaakt kan worden tot toegang tot systemen, applicaties en netwerkservices.

Informatievoorziening

- De afhandeling en monitoring van verbeteracties is niet altijd zichtbaar voor de raad. Vanuit de Plan-Do-Check-Act-cyclus is er wel inzicht op de ‘check’, maar minder op de ‘act’. Het verdient aanbeveling om de informatievoorziening over de afhandeling van toegezegde verbeteracties aan de raad hierop aan te passen.
- Ga na of de gemeente periodiek penetratietesten laat uitvoeren door experts. Vraag specifiek om vertrouwelijk geïnformeerd te worden over de eventueel gevonden kwetsbaarheden en de daarop ondernomen acties.
- De komende jaren zullen meer medewerkers die betrokken zijn bij digitale veiligheid, gaan werken voor de Leidse Regio in plaats van voor afzonderlijke gemeenten. Het is daarbij zaak om goed zicht te houden op de verantwoordelijkheden en bevoegdheden. Zeker bij incidenten, is het noodzakelijk om dit goed in beeld te hebben. Nu zijn er in beide gemeenten geen specifieke procedures opgesteld voor een dergelijke (fictieve) situatie, anders dan de reguliere veiligheidsplannen.
- Zorg dat inzichtelijk wordt gemaakt of er voldoende middelen zijn voor informatiebeveiliging.