Leiden

Burgemeester en Wethouders

Retouradres: Postbus 9100, 2300 PC Leiden

Gemeenteraad Leiden

Gemeente Leiden
Bezoekadres Stadhuis
Stadhuisplein 1
Postadres Postbus 9100
2300 PC Leiden
Telefoon 14071
E-Mail
Website www.leiden.nl/gemeente

Datum 23 april 2019
Ons kenmerk Z/19/1372838
Onderwerp Reactie college op rapport rekenkamer 'digitaal gedrag: veilig en verantwoordelijk'

Contactpersoon L. Bitter
Doorkiesnummer 5024

Z11F20E9C7E

Geachte leden,

Op 11 maart jongstleden heeft u het rapport 'Digitaal gedrag: veilig en verantwoordelijk' van de Rekenkamercommissie Leiden - Leiderdorp ontvangen. In de commissie WM van 21 maart 2019 is het rapport door de Rekenkamercommissie gepresenteerd en informatief besproken.

Als college spreken wij graag onze waardering uit voor dit onderzoeksrapport. Wij herkennen de conclusies en aanbevelingen. Onze bestuurlijke reactie bestaat uit de volgende onderdelen: algemene indruk en reactie op aanbevelingen en aandachtspunten.

Algemene indruk

De digitalisering van de samenleving gaat steeds sneller en biedt ongekende kansen, maar ook bedreigingen (hackers en datalekken). Overheden en burgers werken veel digitaal en delen daarbij belangrijke gegevens. Het is belangrijk dat gemeenten zorgvuldig met deze gegevens omgaan. De gemeente heeft daarbij de verantwoordelijkheid om goed te zorgen dat deze goed beveiligd zijn. Daarom wordt stevig ingezet op informatiebeveiliging. Alle maatregelen die we als gemeente – mede n.a.v. de aanbevelingen van de Rekenkamercommissie – al hebben genomen en nog van plan zijn te gaan nemen, vervatten we in een samenhangend programma met als doel de informatiebeveiliging naar een hoger niveau te tillen; over de voortgang zullen we uw raad periodiek informeren. Het programma draagt zorg voor het uitvoeren van maatregelen op het gebied van informatiebeveiliging en daaraan gerelateerde maatregelen op het gebied van gedrag, actualiteit en informatievoorziening.

Reactie op aanbevelingen

Aanbeveling 1:

Los de concrete kwetsbaarheden op die bleken uit de penetratietesten

Reactie college:

Als reactie op de resultaten van de penetratie- en phishingtest (vanuit de praktijktoetsing) zijn al in november 2018 technische en organisatorische maatregelen getroffen die moesten voorzien in het wegnemen van de geconstateerde kwetsbaarheden en risico's. Alle kwetsbaarheden zijn gemitigeerd en er zijn aanvullende maatregelen genomen om herhaling in de toekomst te voorkomen. Het interne netwerkverkeer wordt nu continu gemonitord en gecontroleerd om tijdig te in te grijpen bij hackpogingen.

Aanbeveling 2:

Maak de organisatie en de medewerkers ervan bewust dat het grootste risico voor de digitale veiligheid, het (eigen) gedrag is.

Reactie college:

Informatieveiligheid is veel meer dan ICT, het gaat in veel gevallen om de mens in de organisatie en de manier waarop deze met risico's omgaat. Is de medewerker zich bewust van die risico's? Zijn bestuurders zich bewust van de risico's van en voor de organisatie? Beveiliging van gegevens en systemen is een zaak van organisatie, procedures, werkprocessen en in de laatste plaats techniek. Het gaat om de mens, de manier waarop deze werkt en het gereedschap waarmee het werk verricht wordt. Een bewuste medewerker is een belangrijk fundament voor informatiebeveiliging. De gemeente doet al veel aan bewustwording bij medewerkers. Verschillende bewustwordingscampagnes in de vorm van presentaties en postercampagnes hebben de afgelopen twee jaar bijgedragen aan het vergroten van de bewustwording m.b.t. informatiebeveiliging en persoonsgegevens. Dit heeft weliswaar een goede basiskennis opgeleverd binnen de organisatie, maar het ontbreekt aan instrumenten om deze basis kennis op peil te brengen/houden (borging). We willen hiervoor het instrument e-learning inzetten, een effectieve manier om alle geledingen in de organisatie te bereiken waardoor wij, in het kader van wet- en regelgeving, kunnen aantonen compliant te zijn aan bewustwording.

Aanbeveling 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 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.

Reactie college:

Belangrijkste leerpunt van dit onderzoek van de rekenkamer is de grote kwetsbaarheid voor aanvallen van binnenuit. Op deze kwetsbaarheid is onmiddellijk actie ondernomen. Er zijn maatregelen getroffen om het minder eenvoudig te maken om toegang tot het netwerk te verkrijgen. Specifiek: de inzet van een vulnerability scanner die een computer systeem of netwerk scant op kwetsbaarheden.
De gemeentelijke gebouwen hebben een openbaar karakter en zijn toegankelijk voor de burger. In de bewustwordingcampagnes wordt herhaaldelijk aan medewerkers gevraagd om een bijdrage te leveren aan de veiligheid van onze gebouwen door waakzaam te blijven en onbekenden aan te spreken.
Werkplek71, de virtuele werkplek van SP71, maakt al gebruik van een 2 factor authenticatie. Ook de nieuwe mobiele apparaten worden uitgerold met een dubbele authenticatie.
Ten aanzien van de toegang tot de gemeentelijke gebouwen loopt er inmiddels een project welke moet voorzien in een betere fysieke toegangsbeveiliging.

Aanbeveling 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.

Reactie college:

Zoals al aangegeven zullen we onder andere naar aanleiding van de hoofdconclusies en aanbevelingen uit het Rekenkamerrapport alle maatregelen die we als gemeente al hebben genomen en nog van plan zijn te gaan nemen vervatten in een samenhangend programma met als doel de informatiebeveiliging naar een hoger niveau te tillen. Het programma draagt zorg voor het uitvoeren van maatregelen op het gebied van informatiebeveiliging en daaraan gerelateerde maatregelen op het gebied van gedrag, actualiteit en informatievoorziening.
Ook moet er meer bestuurlijke aandacht komen voor informatieveiligheid en gegevensbescherming, met een hechtere verbinding tussen bestuurder en de discipline Informatiebeveiliging en Privacybescherming (IB&P). IB&P heeft binnen de gemeentelijke organisatie een spilfunctie, om ervoor te kunnen zorgen dat de juiste acties worden genomen en zal daarbij voorzien in een kwartaal rapportage IB&P met actualiteiten.
In het kader van de ENSIA cyclus rapporteren wij verticaal naar de rijksoverheid en horizontaal aan uw raad over informatieveiligheid. Rapporteren aan uw raad vindt plaats via een paragraaf in de jaarstukken.
Met betrekking tot het rapporteren van ontwikkelingen binnen team Informatiebeveiliging en Privacy is gekozen om de voortgang bij te houden met een rapportagetool. Hierin kunnen de verschillende aandachtspunten en te realiseren doelstellingen worden gemonitord. Deze tool sluit aan bij de manier waarop informatiemanagers en projectmanagers rapporteren. Deze tool draagt tevens bij aan de periodieke informatievoorziening richting uw raad.

Aandachtspunten

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, phishingmail kunnen herkennen en wachtwoorden voor zich houden. Houd er rekening mee dat er nu vooral gewerkt wordt op basis van vertrouwen.

Reactie college:

Informatiebeveiliging is een continu proces waar de gemeente aan moet blijven werken. Elke dag brengt nieuwe uitdagingen, projecten, processen et cetera. Het vraagt echter om structurele borging en moet onderdeel worden van (bestaande) processen. Informatiebeveiliging en privacy dienen integraal onderdeel uit te maken van de bedrijfsvoeringsprocessen van de gemeente. Hiertoe zal gebruik worden gemaakt van een gedocumenteerd 'Information Security Management System' (ISMS). ISMS gaat uit van de Plan Do Act Check cyclus (PDCA-cyclus), een continu en interactief proces.

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.

Reactie college:

In het Rekenkamerrapport is duidelijk naar voren gekomen dat beleidstukken weliswaar aanwezig zijn, maar geactualiseerd dienen te worden. Bijvoorbeeld aan de Algemene verordening gegevensbescherming (AVG) en de Baseline Informatiebeveiliging Overheid (BIO) alsmede de gewijzigde governance structuur naar aanleiding van de regionalisering van de informatievoorzieningstaken (VRIS). Het opstellen en/of actualiseren van het beleid heeft in het opgestelde jaarplan (VRIS) prioriteit gekregen en is al in voorbereiding. De aanpak van informatiebeveiliging (IB-beleid) in de gemeente Leiden is 'risk based'. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een risicoanalyse.

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.

Reactie college:

Op de hiergenoemde punten is in de voorafgaande antwoorden al gereageerd.
Zoals bij onze reactie op aanbeveling 4 genoemd, zullen wij uw raad met de jaarlijkse P&C cyclus rapporteren over informatieveiligheid en gegevensbescherming. In aanvulling hierop merken wij nog het volgende op. Gemeenten hanteren vanaf 1 januari 2020 samen met de rijksoverheid, de waterschappen en de provincies één uniform normenkader voor informatiebeveiliging: de Baseline Informatiebeveiliging Overheid (BIO). Deze BIO is een 'update' van de BIG en net als de huidige baseline gebaseerd op de internationale ISO27001/2-standaard.
De BIO betekent een verandering voor gemeenten. De maatregelen die reeds in het kader van de BIG zijn getroffen voldoen in principe ook voor de BIO. Ten opzichte van de BIG zijn

bijna 200 maatregelen niet meer genoemd. Gemeenten krijgen namelijk met de BIO meer ruimte om vanuit risicomanagement de voor hen relevante maatregelen te treffen. De maatregelen die in de BIO nog wel zijn genoemd gelden als verplicht voor alle overheden. In 2019 moeten de gemeenten zich voorbereiden op de overgang naar de BIO. Dit alles zal moeten bijdragen in het waarborgen van de betrouwbaarheid van de gemeentelijke informatiesystemen en het minimaliseren van de schade door het voorkomen van beveiligingsincidenten.

Conclusie

Concluderend, neemt het college de conclusie en aanbevelingen uit het Rekenkamerrapport over. Alle maatregelen die we als gemeente – mede n.a.v. de aanbevelingen van de Rekenkamercommissie – al hebben genomen en nog van plan zijn te gaan nemen, vervatten we in een samenhangend programma met als doel de informatiebeveiliging naar een hoger niveau te tillen. Het programma draagt zorg voor het uitvoeren van maatregelen op het gebied van informatiebeveiliging en daaraan gerelateerde maatregelen op het gebied van gedrag, actualiteit en informatievoorziening. Het programma zal tevens een tijdpad bevatten en inzicht geven in de daartoe benodigde middelen.

Hoogachtend,

Burgemeester en Wethouders van Leiden,
de Secretaris, de Burgemeester,