Oegstgeest
Wassenaar
Voorschoten
Leidschendam-Voorburg
Rekenkamercommissie

Aan: De raadsleden en burgercommissie-leden van Wassenaar, Voorschoten, Oegstgeest, Leidschendam-Voorburg

Datum: 26 april 2021

Betreft: Onderzoek *informatiebeveiliging van gemeenten en verbonden partijen*

Bijlage: Onderzoeksrapportage

Geachte leden,

Hierbij ontvangt u onze onderzoeksrapportage naar de informatiebeveiliging van de gemeenten Wassenaar, Voorschoten, Oegstgeest en Leidschendam-Voorburg en hun verbonden partijen.

Aanleiding onderzoek

De Rekenkamercommissie wilde in kaart brengen wat de gemeenten hebben gedaan na het eerdere onderzoek *Beter sturen op digitale dienstverlening* (2016).

Op basis daarvan namen alle colleges van B&W de aanbevelingen over om:

- risicoanalyses uit te voeren en zo nodig aanvullende maatregelen te nemen voor systemen en processen;
- eventuele risico's op te nemen in de paragraaf Weerstandsvermogen van de programmabegroting;
- expliciet te sturen op het formuleren van concrete kaders op informatiebeveiliging door verbonden partijen.

Het belang van een goede informatiebeveiliging is afgelopen jaren duidelijk naar voren gekomen. Zo ondervonden de gemeenten Lochem en Hof van Twente in 2019 en 2020 de gevolgen van datalekken.

Doel onderzoek

Het doel was om inzicht te bieden en eventueel verbetersuggesties aan te reiken voor:

- het informatiebeveiligingsbeleid en de operationele procedures;
- de mate van kwetsbaarheid van de gemeentelijke IT-netwerken;
- de wijze waarop verantwoording wordt afgelegd over informatiebeveiliging.

Uitvoering onderzoek

Het onderzoeksbureau IB&P heeft in de periode mei tot en met november 2020:

- gemeentelijke documenten bestudeerd over informatiebeveiliging;
- gesprekken gevoerd met de chief information security officer (CISO), de functionaris gegevensbescherming (FG) en de griffier van elke gemeente;
- een digitale vragenlijst verstuurd naar verbonden partijen en met hen gesproken;
- penetratietesten[1] en kwetsbaarhedenscans[2] uitgevoerd;
- per gemeente een vertrouwelijke rapportage opgeleverd over met name de kwetsbaarheden van de gemeentelijke IT-netwerken (hierop is direct actie ondernomen).

Bevindingen

Het onderzoek leverde bevindingen op die *positief* waren, *zorgwekkend*, of *extra aandacht* vragen.

Positief:

Het informatiebeveiligingsbeleid en de organisatie rondom informatiebeveiliging bij de gemeenten zijn op orde. De meeste verbonden partijen hebben een informatiebeveiligingsbeleid opgesteld, dat periodiek wordt bijgesteld.

Daarnaast werken de gemeenten aan bewustwording over informatiebeveiliging en privacy. Betrokkenen worden geïnformeerd bij een datalek. En het aantal datalekken wordt vermeld in de jaarrekeningen.

Zorgwekkend:

- de gemeentelijke IT-netwerken zijn kwetsbaar door de aanwezigheid van verouderde software, cipher suites[3] en protocollen voor encryptie[4], en door het gebruik van foute headers[5]. Dit is aangetoond door de penetratietesten;
- de gemeenten voeren te weinig risicoanalyses, penetratietesten en kwetsbaarhedenscans uit.

---

[1] *Met penetratietesten wordt geprobeerd in te breken in IT-netwerken of websites.*

[2] *Gedurende kwetsbaarhedenscans analyseert een softwareprogramma automatisch naar bekende kwetsbaarheden.*

[3] *Cipher suites bepalen hoe het digitaal verkeer tussen een server en een cliënt wordt versleuteld en verwerkt.*

[4] *Encryptie is het coderen (versleutelen) van digitale gegevens.*

[5] *Headers informeren de webbrowser hoe te handelen tijdens de interactie met de website.*

Extra aandacht:

- de gemeenten beoordelen niet-systematisch de operationele procedures, inventariseren niet-systematisch de risico's met verbonden partijen, en passen het informatiebeveiligingsbeleid niet aan;
- de gemeenten hebben een onvolledig en/of gedateerd verwerkingsregister[6];
- de gemeenten hebben de informatiebeveiligingsrisico's en beheersingsmaatregelen niet opgenomen in de paragraaf Weerstandsvermogen van de programmabegroting (= aangenomen aanbeveling in 2016);
- de gemeenten geven vrijwel geen sturing aan de verbonden partijen op het gebied van informatiebeveiliging (= aangenomen aanbeveling in 2016).

Op bladzijde 35 van de onderzoeksrapportage is een kort overzicht opgenomen van de belangrijkste bevindingen per gemeente.

Aanbevelingen

Verzoek uw college om:

1) de IT-netwerken te versterken door de geconstateerde kwetsbaarheden op te heffen;
2) minimaal jaarlijks risicoanalyses, penetratietesten en kwetsbaarhedenscans uit te voeren;
3) systematisch operationele procedures te beoordelen, systematisch de risico's met verbonden partijen te inventariseren, en het informatiebeveiligingsbeleid zo nodig aan te passen;
4) het verwerkingsregister volledig en/of geactualiseerd te maken;
5) de informatiebeveiligingsrisico's en beheersingsmaatregelen op te nemen in de paragraaf Weerstandsvermogen en in een speciale paragraaf informatiebeveiliging in de gemeentelijke programmabegroting;
6) sluitende afspraken te maken met verbonden partijen op het gebied van informatiebeveiliging;
7) kennisuitwisseling over informatiebeveiliging te stimuleren tussen FG's, CISO's en verbonden partijen;
8) jaarlijks afzonderlijk te rapporteren over informatiebeveiliging en privacybeleid, en de betrokkenheid van de gemeenteraad hierbij te vergroten (bijvoorbeeld door training).

---

[6] *In een verwerkingsregister houdt de gemeente verplicht haar verwerkingsactiviteiten bij van persoonsgegevens.*

Bestuurlijke reacties

De colleges van B&W van Wassenaar en Voorschoten herkennen de '*grote inzet'* van de organisatie om informatiebeveiliging te verbeteren. Zij vinden de aanbevelingen *'waardevol'* en nemen deze grotendeels over.
De aanbeveling voor een jaarlijkse risicoanalyse wordt afgewezen. Want *'een tweejaarlijkse risicoanalyse biedt voldoende zicht op eventuele risico's'*.
Volgens genoemde colleges van B&W zijn de aanbevelingen in de planning opgenomen, of al in uitvoering (zoals de geconstateerde kwetsbaarheden).

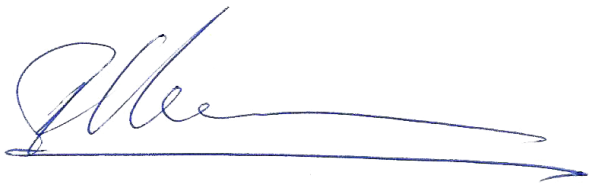
Het college van B&W van Oegstgeest dankt de Rekenkamercommissie voor het onderzoek. Zij stelt dat de gemeente al voldoet aan veel van de aanbevelingen.
De geconstateerde technische tekortkomingen waren volgens het college *'ernstig, maar hadden geen impact op de dienstverlening van de gemeente'*; de tekortkomingen zijn opgelost.
Het college overweegt om een aparte paragraaf informatiebeveiliging op te nemen in de programmabegroting. Zij streeft naar '*meer onderlinge kennisuitwisseling'*.

Het college van B&W van Leidschendam-Voorburg wil de betrokkenen *'complimenteren met het onderzoek en de onderzoeksrapportage*'.
Zij kan zich vinden in de constateringen en aanbevelingen in de onderzoeksrapportage en de aanbiedingsbrief.
Volgens het college waren de geconstateerde onvolkomenheden *'reeds bekend'*; oplossingen ervoor zijn opgenomen in de planning, of al in uitvoering.

Tenslotte

Wij gaan graag met u in gesprek over dit onderwerp. Bijvoorbeeld tijdens een speciale bijeenkomst, ondersteund door het onderzoeksbureau.

Met vriendelijke groet,
Rekenkamercommissie Wassenaar, Voorschoten, Oegstgeest en Leidschendam-Voorburg



Dolf Kamermans, voorzitter