

VOORBLAD

Voorstel aan de Raad

Zaaknummer: Z/20/043683/269847
Datum collegebesluit: n.v.t.
Datum commissievergadering: donderdag 30 september 2021
Datum raadsvergadering: donderdag 7 oktober 2021

Soort Voorstel: Adviesnota
Onderwerp: Rapport Rekenkamercommissie informatiebeveiliging
Portefeuillehouder: Burgemeester Stemerding
Programma:

Kernboodschap: De Rekenkamercommissie heeft onderzoek gedaan naar de informatiebeveiliging bij gemeenten en verbonden partijen. Doel hiervan was inzicht bieden in en verbeter suggesties aanreiken over informatieveiligheidsbeleid, de kwetsbaarheid van gemeentelijke IT systemen en de wijze waarop verantwoording wordt afgelegd over informatiebeveiliging. Het onderzoek heeft geleid tot 8 aanbevelingen waarvan de raad het college opdraagt deze uit te voeren.

Bijlagen: Aanbiedingsbrief en rapport Onderzoek informatiebeveiliging van gemeenten en verbonden partijen

Beslispunten Het college op te dragen de acht aanbevelingen uit te voeren en bij aanbeveling 2 over de jaarlijkse risicoanalyses ermee akkoord te gaan dat het college deze tweejaarlijks zal uitvoeren.

Relatie met:

- Agendapunt: *(bijv. een aangehouden stuk of een stuk wat nog moet komen of al geweest is)*
- Toezegging:
- Amendement/motie:
- Schriftelijke vragen:

Adviesnota aan de Raad

Onderwerp

Rapport Rekenkamercommissie informatiebeveiliging

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 verbeter suggesties 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;
- penetratietesten¹ en kwetsbaarheidsscans² 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.

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

² Gedurende kwetsbaarheidsscans analyseert een softwareprogramma automatisch naar bekende kwetsbaarheden.

Zorgwekkend:

- de gemeentelijke IT-netwerken zijn kwetsbaar door de aanwezigheid van verouderde software, cipher suites³ en protocollen voor encryptie⁴, en door het gebruik van foute headers⁵. Dit is aangetoond door de penetratietesten;
- de gemeenten voeren te weinig risicoanalyses, penetratietesten en kwetsbaarheidsscans uit.

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 verwerkingsregister⁶;
- 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).

Aanbevelingen

Verzoek uw college om:

- 1) de IT-netwerken te versterken door de geconstateerde kwetsbaarheden op te heffen;
- 2) minimaal jaarlijks risicoanalyses, penetratietesten en kwetsbaarheidsscans 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).

Bespreking rapport in de commissie B&B van 30 september 2021

Het rapport en de aanbevelingen zijn besproken in de commissie B&B van 30 september 2021. Hoewel de commissie constateert dat er veel goed gaat, is er bij de volgende onderwerpen langer stil gestaan:

- Jaarlijkse risicoanalyse: de commissie wilde vasthouden aan de jaarlijkse risicoanalyse, maar het college heeft aangegeven dat het doorvoeren van aanbevelingen die uit

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.

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

risicoanalyses voortkomen tijd kost. Daardoor is een tweejaarlijkse analyse beter haalbaar. Er is ook geen aanleiding voor een jaarlijkse analyse en als die aanleiding er wel is, zal een analyse vaker worden uitgevoerd. De commissie kan zich vinden in deze aanpassing van de aanbeveling.

- Verbonden partijen: de commissie vraagt aandacht voor beleid en budget om hier beter zicht en grip op te krijgen. Het college zegt hieraan te werken en zal dit in de toekomst agenderen voor bespreking met de raad.
- Betrokkenheid raad: het college zal in de reguliere P&C cyclus informatiebeveiliging als vast onderdeel opnemen. In de begroting 2023 zal de paragraaf informatiebeveiliging worden opgenomen. Daarnaast zal het een onderwerp zijn voor bespreking in de nieuwe raad.
- Risico's ontvlechting: op vragen uit de commissie over de risico's die kunnen ontstaan bij de ontvlechting van de Werkorganisatie Duivenvoorde antwoordt het college dat hier nadrukkelijk aandacht voor is.

Voor de overige aanbevelingen zegt het college deze allemaal over te nemen.

Commissie Burger en Bestuur,
30 september 2021

Besluit

Zaaknummer: Z/20/043683/269847

De raad der gemeente Voorschoten;

Gelezen het rapport Onderzoek informatiebeveiliging van gemeenten en verbonden partijen,
d.d. 26 april 2021;

Gehoord de bespreking in de commissie Burger en Bestuur van 30 september 2021,

besluit:

Het college op te dragen de acht aanbevelingen uit te voeren en bij aanbeveling 2 over de
jaarlijkse risicoanalyses ermee akkoord te gaan dat het college deze tweejaarlijks zal uitvoeren.

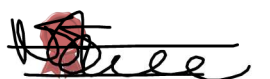
Aldus vastgesteld in de openbare vergadering
van de raad der gemeente Voorschoten,
gehouden op 7 oktober 2021.

de griffier,



Drs. B.J. Urban

de voorzitter,



Drs. N. Stemerding