GEMEENTE Oss
REKENKAMER COMMISSIE

Leden van de raad

6 februari 2020

Betreft: rekenkamerbrief inzake onderzoek informatieveiligheid

Geachte leden van de raad,

Hierbij bieden wij u de resultaten van het onderzoek naar de informatieveiligheid van de gemeente Oss aan.

Aanleiding voor het onderzoek

Een betrouwbare en veilige informatievoorziening is essentieel voor gemeenten. Door de toenemende digitalisering wordt het steeds belangrijker om zorgvuldig om te gaan met de gegevens van burgers en organisaties. Het noodzaakt gemeenten extra aandacht te hebben voor de bescherming van persoonsgegevens en de privacy van inwoners.
Om die reden heeft de rekenkamercommissie besloten de effectiviteit en doelmatigheid van de informatieveiligheid in Oss te onderzoeken. Gelet op het technische karakter van het onderzoek en de beperkt(er)e bezetting van de rekenkamercommissie gedurende 2019 is gekozen om dit onderzoek uit te besteden aan een extern bureau.

Vraagstelling onderzoek

Doel van het onderzoek is het beantwoorden van de volgende centrale onderzoeksvraag:
Is gemeente Oss in control als het om informatieveiligheid en privacybescherming gaat?

Deelvragen zijn:

1. Heeft gemeente Oss voldoende technische maatregelen getroffen inzake Wet bescherming persoonsgegevens en Algemene Verordening Gegevensbescherming?
2. Zijn de IT-systemen voldoende beveiligd? Welke beveiligingsrisico's en kwetsbaarheden zijn er in de systemen van de gemeente Oss?
3. Kan een hacker bij privacygevoelige informatie komen en eventueel wijzigen/verwijderen?

Opzet onderzoek

De rekenkamercommissie heeft aan de externe onderzoeker gevraagd de huidige stand van de beveiliging van de infrastructuur (externe en interne netwerk) te onderzoeken. Door middel van een technisch onderzoek is de huidige stand van de beveiliging onderzocht. Ook is gecontroleerd of de privacy en informatieveiligheid van de gemeente geborgd is. Het technisch onderzoek is uitgevoerd aan de hand van penetratietesten op interne en externe informatiesystemen, webapplicaties en onderliggende IT-

infrastructuur. Hierin is onderzocht of er zich kwetsbaarheden en beveiligingsrisico's voordoen in deze systemen/applicaties, welke mogelijk een impact hebben op de informatieveiligheid van de gemeente.

Resultaten onderzoek

Conclusie: Op basis van de resultaten kan gesteld worden dat de veiligheid van de systemen waar de gemeente Oss gebruik van maakt, onvoldoende is.

Onderzoekers hebben op afstand onder andere toegang gekregen tot e-mail, wachtwoorden, fileshares, desktops en diverse programma's zoals Key2Burgerzaken. Daarnaast was het mogelijk om live mee te kijken op desktops van werknemers en deze te bedienen zonder dat een werknemer zich hiervan bewust was. Tevens hebben de onderzoekers twee dagen vanuit het gemeentehuis kunnen werken door het bemachtigen van onderhoudspassen. Overigens geldt daarbij de opmerking dat de onderzoekers wel zijn gesignaleerd door de bode en dat de CISO (Chief Information Security Officer) hierna is ingeschakeld.

De onderzoekers hebben binnen de beschikbare tijd geen beheerrechten kunnen verkrijgen op het netwerk. Vanwege het aantal en de ernst van de aangetroffen kwetsbaarheden, de grote hoeveelheid informatie en het aantal nog nader te onderzoeken systemen, is het volgens de externe onderzoeker echter zeer waarschijnlijk dat dit wel was gelukt met meer tijd.

Samenwerking organisatie

De rekenkamercommissie heeft er bewust voor gekozen om in dit gevoelige onderzoek de samenwerking te zoeken met de ambtelijke organisatie. Deze samenwerking hebben wij als constructief ervaren. De rekenkamercommissie heeft ook bewust vroegtijdig de samenwerking gezocht vanuit de mogelijkheid dat de uitkomsten een dusdanige kwetsbaarheid ten aanzien van de gemeentelijke processen zouden kunnen laten zien, dat direct ingrijpen aan de orde is. Gebleken is dat een aantal kritische kwetsbaarheden in de systemen inderdaad zijn aangetroffen. Het externe bureau heeft geadviseerd alle problemen zo snel mogelijk te verhelpen.
Op basis van deze resultaten heeft de rekenkamercommissie het externe bureau verzocht om de hiaten in de beveiliging te bespreken met de ambtelijke organisatie. De organisatie is in de gelegenheid gesteld om de geconstateerde onvolkomenheden te herstellen voordat wij tot aanbieding van deze brief aan college en raad zijn overgaan.
Wij hebben begrepen dat het herstel inmiddels heeft plaatsgevonden. De rekenkamercommissie heeft evenwel niet de effectiviteit van de getroffen maatregelen getoetst of laten toetsen.

Vertrouwelijkheid analyse

Inmiddels is het onderzoek en het herstel afgerond en informeren wij u over de uitkomsten en over onze conclusies en aanbevelingen. Dat doen wij via deze rekenkamerbrief, die daarmee het karakter heeft van het bestuurlijk eindrapport van het onderzoek. Wij hebben er bewust voor gekozen om de onderliggende onderzoeksgegevens en -analyse niet openbaar te maken gelet op de veiligheid van gemeentelijke processen. De betreffende analyse ligt vertrouwelijk ter inzage bij de griffie.

Procedure bestuurlijk hoor

Het concept van deze brief hebben wij voorgelegd aan het college voor een bestuurlijke reactie. De reactie van het college hebben we bij deze brief gevoegd.

Aanbevelingen

Op basis van het onderzoek beveelt de rekenkamercommissie aan de raad aan het college opdracht te geven om:

1. Het herstel van de aangetoonde kwetsbaarheden te (laten) beoordelen door middel van een vervolgonderzoek.
2. De analyse van de overige vermoede kwetsbaarheden en het herstel daarvan in te zetten.
3. De informatiebeveiliging op een dusdanige wijze te laten organiseren dat de organisatie op korte termijn 'in control' komt op dit onderwerp, waarmee de koppeling wordt hersteld tussen gedrag, beleid en uitvoering. De aanpassingen in organisatie en processen moeten ervoor zorgen dat nieuwe risico's in de toekomst voorkomen worden;
4. Jaarlijks een 'stresstest' te plannen en uit te voeren om er zeker van te zijn dat er geen nieuwe kwetsbaarheden zijn ontstaan (door wijzigingen in het systeem of technologische ontwikkelingen);
5. De gemeenteraad van Oss binnen drie maanden te informeren over de aanpak en uitkomsten van bovenstaande aanbevelingen.

Met vriendelijke groet,

Namens de rekenkamercommissie,

Astrid van de Klift
Voorzitter rekenkamercommissie Oss