Hengelo Gld., 20 september 2022

Bestuurlijke reactie Rekenkameronderzoek 'informatieveiligheid en privacy', gemeente Bronckhorst

Beste Rekenkamercommissie,

Met belangstelling hebben wij het rapport "'informatieveiligheid en privacy', gemeente Bronckhorst" gelezen. Een gedegen onderzoek dat ook in een breder perspectief inzicht geeft in onze organisatie. Wij constateren dat u middels casusonderzoek bij sociaal domein en toezicht en handhaving vaststelt dat in de praktijk zorgvuldig gehandeld wordt op het gebied van informatiebeveiliging en privacy. Wij kunnen ons vinden de hoofdconclusie van het onderzoek dat de gemeente Bronckhorst de nodige stappen zet om te voldoen aan de basisrichtlijnen en dat de rekenkamercommissie constateert dat de, binnen de scope van het onderzochte, technische systemen geen technische risico's kennen. Hieronder zullen wij ingaan op de aansporingen en aanbevelingen die voortkomen/aansluiten uit de deelconclusies.

Aansporingen

De rekenkamer commissie spoort het college aan verder te gaan met:

- Continue inzet op bewustwording van risico's op informatiebeveiliging en privacy bij de medewerkers;
- Data protection impact assessments uitvoeren op de geselecteerde verwerkingsprocessen;
- Inzet op het gebruik van veilig mailverkeer door medewerkers;
- De koppelling van Civision met het Document managementsysteem, ter voorkoming van papieren dossiers in het sociaal domein.

Voor zover dit aansporing behoeft, gaan wij hier zeker mee door. In Bijlage 1 geven wij aan welk acties er inmiddels zijn uitgevoerd en in planning gezet.

Aanbevelingen

1) *Actualiseer het beleid op informatiebeveiliging en privacy*
   - Werk het informatiebeveiligings-en privacybeleid uit naar jaarplannen en stel deze tijdig vast, uiterlijk aan het begin van het betreffende jaar.

     Wij onderschrijven de noodzaak van een actueel informatiebeveiligings- en privacybeleid. Het actualiseren stond al in 2021 op de planning, maar is door extra werkzaamheden in de Corona-periode en uitval binnen het organisatieonderdeel I&A niet tot uitvoering gekomen. Wel hebben we gestreefd om de organisatie in te richten naar de geest van de BIO, waardoor in de praktijk gehandeld is alsof er actueel beleid bestaat.
     Gezamenlijk met onze partners in de ICT samenwerking wordt momenteel gewerkt aan de actualisering van het informatiebeveiligingsbeleid. Wij verwachten dit beleid uiterlijk begin 2023 vast te kunnen stellen.

   - Richt de rapportages op informatiebeveiliging en privacy zo in dat ze zicht geven op opzet, bestaan en werking van de maatregelen op informatie-beveiliging en privacy;

     Bij het informatiebeveiligings- en privacybeleid hoort een richtlijn over de format van eenduidige rapportage; wij zullen dit opnemen.

- Investeer daarvoor in een informatiemanagementsysteem op informatiebeveiliging (ISMS);

  Wij gaan het gebruik van een ISMS systeem onderzoeken, zo mogelijk samen met onze ICT-samen partnergemeenten. Wij zullen dit doen aan de hand van de “Handreiking ISMS” van de VNG.

- Betrek het onderwerp gegevensbescherming en de functionarissen op privacy eerder in beleids-en besluitvormingsprocessen.

  Hiervoor zijn al organisatorische maatregelen genomen. Bij elke aanvraag om een wijziging in de informatie-architectuur worden direct de aspecten van informatiebeveiliging en -privacy meegenomen.

2) *Verminder de kwetsbaarheid van de formatie op informatiebeveiliging en privacy*
   - Versterk de invulling van de functies op informatiebeveiliging en privacy, door de functies los van de lijn te positioneren en zoveel als mogelijk het vastgestelde aantal uren ingezet kunnen worden.

     Wij zullen de posities van CISO, FG en PO heroverwegen.
     Het buiten de lijn positioneren van deze functies vraagt een volledige heroverweging van taken en bevoegdheden.
     Opgemerkt wordt dat CISO en FG nu ook vrij kunnen rapporteren, ook al zijn zij nu binnen I&A gepositioneerd.
     Bij het heroverwegen worden dan ook zeker de werkzaamheden in het kader van de ENSIA audit betrokken omdat deze ook nog binnen de lijn worden uitgevoerd.
     Al deze functies zijn een onderdeel van het totale takenpakket van medewerkers, waardoor herpositionering gevolgen heeft voor de beschikbare capaciteit welke dan wel weer opgevuld moet worden.
     Het is inherent aan een gemeente van onze omvang dat binnen de bestaande formatie prioriteiten worden gesteld waardoor bepaalde zaken later worden opgepakt.

3) *Houdt de technische kant van informatiebeveiliging op orde*

   - Stel, indien van toepassing in overleg met ICT-samenwerking, een plan van aanpak op naar aanleiding van de verbeterpunten uit de pentesten van het rekenkameronderzoek;

     Wij hebben al in een eerder stadium kennisgenomen van de verbeterpunten uit de pentesten en deze zijn inmiddels uitgevoerd of is opdracht voor gegeven.

- Draag, indien van toepassing in overleg met ICT-samenwerking, zorg voor:

    - Inregeling van 2factor authenticatie (2FA)voor alle mailaccounts;

      2factor is inmiddels de standaard voor alle toegang tot systemen welke buiten de beveiligde kantooromgeving te benaderen zijn.
      Dit najaar wordt ook de toegang voor raad met 2factor ingeregeld.

    - Scheiding van de Outlookadresbestanden per partner in de samenwerking.

      Deze scheiding is aangevraagd bij ICT-samen, maar technisch (nog) niet mogelijk, tenzij wordt gekozen voor een volledige scheiding binnen de Microsoft tenant. Dit heeft vergaande organisatorische en financiële gevolgen.
      Zodra er een softwarematige oplossing is, wordt deze uitgevoerd.

      Ook de ICT samenwerking werkt aan een informatiebeveiligingsplan. Deze heeft betrekking op alle aspecten van automatisering en techniek. Gezamenlijk met ons informatiebeveiligingsplan (zie punt 1) wordt hiermee volledig voldaan aan de BIO.

4) Versterk de governance en afspraken op de regionale samenwerking op ICT

- Evalueer met de deelnemende partijen de afspraken over de governance op de ICT samenwerking en:
    - Richt de governance en aansturing op bestuurlijk niveau zwaarder in;
    - Sluit service level agreements met aansprakelijkheidsafspraken met betrekking tot de risico's;
    - Spreek af hoe harmonisatie van beleid op informatiebeveiliging en privacy bij de deelnemers uitgevoerd kan worden.

  De regionale samenwerking is ook een dynamische organisatie welke meeveranderd met de landelijke richtlijnen. Ook zij moeten voldoen aan de bepalingen in de BIO.
  Om deze reden wordt momenteel al gewerkt aan een geheel nieuwe set overeenkomsten waarin o.a. Governance, SLA, Verwerkersovereenkomsten zijn opgenomen.
  Ook de rol van het zogenaamde gemeente-secretarissenoverleg is het afgelopen jaar veranderd. Zij worden steeds eerder en meer betrokken bij besluiten over investeringen, projecten en bedrijfsvoering.
  Graag gaan wij met u in overleg welke ambities de raad heeft hoe zij betrokken willen worden bij de governance van de samenwerking.
  Er wordt op dit moment gewerkt aan een proces waarbij binnen de ICT samenwerking privacy een plaats krijgt waardoor dit bij ICT projecten vanaf begin meegenomen wordt (Privacy by Design).

5) *Informeer de raad meer en inhoudelijker op informatiebeveiliging en bepaal met college en raad het ambitieniveau*

Graag treden wij met de raad in overleg over hun ambities op het terrein van informatiebeveiliging en privacy. Wij kunnen deze ambities dan verwerken in de jaarplannen en -rapportages.

Met vriendelijke groet,

burgemeester en wethouders van Bronckhorst,

de secretaris,	de burgemeester,
ValidSigned door Bart Drewes op 29-09-2022	ValidSigned door Marianne Besselink op 29-09-2022
B.J. Drewes	M.Besselink

Bijlage 1.

Uitvoeringsacties naar aanleiding van de aansporingen:
De rekenkamer commissie spoort het college aan verder te gaan met:

- Continue inzet op bewustwording van risico's op informatiebeveiliging en privacy bij de medewerkers;

  Er komt een nieuw programma om het bewustzijn van de risico's te vergroten. Daarnaast blijven de bestaande programma's bestaan; de training voor nieuwe werknemers is na de Coronaperiode gemoderniseerd en weer opgestart. (Zij werden al wel digitaal op de hoogte gebracht van de bestaande beleids- en gedragsregels!)

- Data protection impact assessments uitvoeren op de geselecteerde verwerkingsprocessen;

  Deze assessments zijn verder uitgebreid naar alle wijzigingen in de informatie-architectuur. Ook binnen de samenwerking worden bij wijzigingen DPIA's uitgevoerd

- Inzet op het gebruik van veilig mailverkeer door medewerkers;

  Dit is een onderdeel van het bestaande en te vernieuwen awarenessprogramma

- De koppeling van Civision met het Document managementsysteem, ter voorkoming van papieren dossiers in het sociaal domein.

  Hiervoor is begin dit jaar opdracht gegeven en momenteel is een project gestart om alle processen binnen het Sociaal Domein aan te laten sluiten op het zaakgericht werken. Hiermee wordt ook binnen dit domein afscheid genomen van papieren dossiers.
  Binnen dit project worden ook de processen binnen burgerzaken aangesloten op het DMS.
  Hiermee wordt het papieren dossier binnen de organisatie vrijwel geheel verbannen.