Provincie Noord-Brabant

Brabantlaan 1
Postbus 90151
5200 MC 's-Hertogenbosch
Telefoon (073) 681 28 12
Fax (073) 614 11 15
www.brabant.nl
IBAN NL86INGB0674560043

Bereikbaarheid
openbaar vervoer en fiets:
www.brabant.nl/route

Statenfractie Groenlinks
De heer M.E.J. Smeets
Brabantlaan 1
5216 TV 'S-HERTOGENBOSCH

Onderwerp
Schriftelijke vragen ex artikel 30 van het Reglement van Orde over de aanpak van cybersecurity door de Provincie Noord-Brabant

Datum
30 januari 2018
Ons kenmerk
C2220379/4305795
Uw kenmerk

Contactpersoon
R.M. (Rob) Hootsmans
Telefoon
(073) 680 8433
Email
rhootsmans@brabant.nl
Bijlage(n)
-

Geachte heer Smeets,

Bij brief van 10 januari 2018, ingekomen op 10 januari 2018, heeft u namens de GroenLinks fractie schriftelijke vragen gesteld.

Wij beantwoorden deze vragen als volgt.

1. Is het College van Gedeputeerde Staten van mening dat cybersecurity een belangrijk strategisch thema is voor de Provincie Noord-Brabant?
Antwoord: Ja, het College is van mening dat cybersecurity een strategisch thema is voor de gehele provinciale organisatie.

2. Heeft de Provincie Noord-Brabant een aanpak vastgelegd voor cybersecurity? Zo ja is dit plan beschikbaar. Zo neen kunt u daarvoor de reden aangeven.
Antwoord: Ja, met informatiebeveiliging streeft de Provincie Noord-Brabant naar beveiliging van haar informatie en alle daaraan gerelateerde aspecten op basis van een risico gebaseerde aanpak die aansluit bij het ambitieniveau van de organisatie met een acceptabel balans tussen kosten en baten, lusten en lasten.

De volgende uitgangspunten zijn daarbij gedefinieerd:
- Voldoen aan wettelijke kaders en richtlijnen;
- Committeren aan de geldende (inter)nationale standaarden zoals de ISO 27001/27002;
- Aansluiten bij de kernwaarden en doelstellingen van de provinciale organisatie.

De aanpak is vastgelegd in de interprovinciale baseline informatiebeveiliging en de interprovinciale afspraak dat alle provincies zich binnen 5 jaar moeten certificeren op de internationale informatiebeveiligingsstandaard ISO 27001. Aangezien het betreffende document te omvangrijk is en gedeeltelijk in systemen geborgd is, is dit niet bijgevoegd maar ligt bij ons ter inzage.

3. Is cybersecurity een onderdeel van het takenpakket van de concerncontroller?
Antwoord: Nee, informatiebeveiliging is een onderdeel van het takenpakket van de CIO (chief information officer), die nu wordt geworven. Tot die tijd is de CIO-taak belegd bij de algemeen directeur.

4. Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing binnen alle landen van de Europese Unie. Bij het niet voldoen aan deze verordening kan de EU fikse boetes opleggen. De AVG is wellicht beter bekend als de General Data Protection Regulation (GDPR). Welke voorbereidingen heeft de Provincie daarvoor getroffen bijvoorbeeld als het gaat om de bescherming van persoonsgegevens?
Antwoord: De provincie is sinds 2016 bezig met de voorbereiding op de AVG. Het project Data Privacy fase 1 (welke in 2017 is afgerond) was gericht op het voldoen aan de belangrijkste eisen uit de AVG. Daarnaast is er binnen dit project veel aandacht besteed aan de training en bewustwording van medewerkers.
Momenteel wordt project Data Privacy fase 2 voorbereid. In dit project ligt de focus op de nog openstaande punten t.a.v. de AVG, governance en het blijven voldoen aan de AVG (borgen).

5. In het kader van de AVG zal ook een Data Protection Officer moet worden benoemd die toeziet op de naleving van de AVG. Is deze functionaris al benoemd of geworven?
Antwoord: Nee, benoeming of werving van de functionaris moet nog gebeuren. De aanpak is eerst de CIO (chief information officer) en dan de functionaris gegevensbescherming aan te stellen, die onder de CIO opereert.

6. Heeft de Provincie ook ethische hacks laten uitvoeren om de cybersecurity te testen? Zogenaamde 'penetratietesten'.
Antwoord: Ja, de Provincie laat op reguliere basis zogenaamde penetratietesten uitvoeren door bedrijven die daarvoor de juiste kwalificaties hebben.

7. Heeft de Provincie Noord-Brabant een risico-analyse uitgevoerd op het gebied van cybersecurity en ook risicobeperkende maatregelen al in kaart gebracht? Zo ja graag een rapportage.
Antwoord: Ja, de provincie heeft verschillende risico-analyses uitgevoerd. Op basis van deze risico-analyses zijn risico beperkende maatregelen vastgesteld. De rapportage met deze risicoanalyses bevat vertrouwelijke en persoonsgevoelige informatie, en is om deze reden niet bijgevoegd bij de beantwoording van deze vragen.

8. Worden de medewerkers geschoold in opleidingen op het gebied van cybersecurity?
Antwoord: Ja, de medewerkers van de provinciale organisatie worden op verschillende manieren getraind. Dit gebeurt onder andere door verplichte cursussen, berichten op brain, informatiebanners, bijeenkomsten en reguliere mysteryguest onderzoeken.

Datum
30 januari 2018
Ons kenmerk
C2220379/4305795

Gedeputeerde Staten van Noord Brabant,

de voorzitter, de secretaris,

prof. dr. W.B.H.J. van de Donk drs. M.J.A. van Bijnen MBA