

SCHRIFTELIJKE VRAGEN AAN HET COLLEGE

Datum: 20-05-2022
Aan de voorzitter van de raad.
Steller(s) van de vragen: Terry Duivesteijn Johan Philippons Politieke partij: Leefbaar 3B
Onderwerp: Maatregelen tegen ongemerkt zoeken in geheime gegevens in de ambtelijke organisatie
Toelichting: Uit onderzoek van het Team Aanpak Corruptie blijkt dat kwaadwillenden ongemerkt kunnen zoeken in een groot aantal overheidssystemen. Nieuwsartikel RTL Nieuws: https://www.rtlnieuws.nl/onderzoek/artikel/5304379/lekken-criminelen-ambtenaren-corruptie-om-vrij-spel
Het college wordt verzocht de volgende vragen schriftelijk te beantwoorden: 1) Is het college op de hoogte van het nieuwsartikel? 2) Is er in de ambtelijke organisatie in Lansingerland sprake van vrije toegang tot alle systemen? a. Zo ja; acht het college dit wenselijk en noodzakelijk? b. Zo nee; welke protocollen en checks en balances zijn er in de organisatie om te voorkomen dat er oneigenlijk gebruik gemaakt wordt van beschikbare informatie? 3) Wordt er vastgelegd (gelogd) wie welke informatie opvraagt? a. Zo ja; worden deze logfiles ook gecontroleerd, steekproefsgewijs en in welke frequentie en regelmaat? b. Zo nee; wordt deze noodzakelijke beveiligingsmaatregel ingevoerd en wanneer? 4) Welke aanbevelingen uit het Rekenkamer Rapport “wat niet weet, maar wel deert” (2017; p. 16, p. 17) zijn inmiddels opgevolgd en op welke wijze? Als ze niet zijn opgevolgd, waarom niet? 5) Met amendement A2018-005 heeft de raad het college opgedragen een actieplan op te stellen. Is dit actieplan opgesteld en wanneer is het naar de raad gestuurd?

- 6) Welke andere toegangsbeperkende maatregelen zijn genomen om informatie in ambtelijke systemen te beveiligen?
- a. Wordt een sterk wachtwoord geforceerd afgedwongen?
 - b. Moeten wachtwoorden periodiek worden aangepast?
 - c. Wordt actief gecontroleerd op uitgelekte wachtwoorden (hashes)?
 - d. Is er sprake van 2FA (2-factor authenticatie) of het gebruik van een externe authenticatiesleutel?
 - e. Wordt regelmatig gecontroleerd of inloggegevens nog gekoppeld zijn aan actieve medewerkers?
 - i. Zo ja, door wie en is hier ook sprake van een vierogenprincipe?
 - ii. Zo nee; waarom niet en acht het college het wenselijk dat dit gebeurt?
 - f. Wordt toegang vanaf externe systemen / ip-adressen geblokkeerd of via een whitelist toegelaten?
 - i. Zo nee; waarom niet en acht het college het wenselijk dat dit gebeurt?
 - g. Wordt toegang vanaf externe systemen / ip-adressen gemonitord en steekproefsgewijs uit gelezen?
 - i. Zo ja; op welke wijze, hoe vaak wordt dit gedaan en door wie of wat?
 - ii. Zo nee; waarom niet en acht het college het wenselijk dat dit gebeurt?
- 7) Is er een informatiebeveiligingsfunctionaris (CISO) actief in de organisatie?
- a. Zo ja; voor hoeveel uur en is dit voldoende om in control te zijn?
- 8) Is Lansingerland aangesloten bij de IBD (informatiebeveiligingsdienst) van de VNG?
- a. Zo ja; op welke wijze wordt er momenteel gebruik gemaakt van de kennis en expertise van de IBD?
 - i. Is de Baseline Informatiebeveiliging Overheid (BIO) volledig geïmplementeerd? Zo niet, waarom niet?
 - b. Zo niet; wordt er gebruik gemaakt, en op welke wijze, van een andere externe, onafhankelijke, organisatie of consultant om de interne beveiliging op orde te houden en waarom die partij?
- 9) Zijn of worden medewerkers getraind in “awareness”?
- a. Zo ja, door welke partij en hoe vaak?
 - b. Zo nee, waarom niet en acht het college dit wenselijk?
 - c. Zijn of worden er periodieke (onaangekondigde) testen gedaan onder werknemers om ‘awareness’ te vergroten, zoals (spear) phishing?

- i. Zo ja; wie organiseert deze testen en wat zijn de bevindingen?
- ii. Zo niet; waarom niet en acht het college het wenselijk dat dit gebeurt?

Wijze van indienen van schriftelijke vragen:
(art. 37, derde lid Reglement van orde van de raad).