Zwolle, 2 april 2017

Betreft: **Artikel 45-vragen: veiligheidsrisico's en informatiebeveiliging gemeente Zwolle**

Geacht College,

De gemeente Rotterdam heeft de beveiliging van persoonsgegevens niet goed op orde. Dit blijkt uit onderzoek van de Rekenkamer Rotterdam. Ook het NOS-journaal en Nieuwsuur hebben hier op 2 april 2017 in hun uitzending een rapportage aan gewijd.

In de uitkomsten van dit onderzoek wordt onder andere aangegeven dat er met verouderde software wordt gewerkt en dat wachtwoorden eenvoudig te achterhalen zijn. Ook schrijven de onderzoekers dat mailsessies konden worden ingezien, malware verspreid kon worden via phishingaanvallen en achtergelaten usb-sticks.

Naar aanleiding van het onderzoek van de Rekenkamer Rotterdam heeft de CDA-fractie een oppervlakkig onderzoek gedaan en komt tot de conclusie dat de Zwolse situatie ook niet optimaal is.

De overheid heeft volgens het CDA een bijzondere verantwoordelijkheid. Met name als het gaat om de zorg voor wie kwetsbaar en afhankelijk is. Het op orde hebben van de beveiliging van gemeentelijke informatiesystemen is in de huidige tijd een harde eis voor het vertrouwen dat persoonsgegevens bij de gemeente veilig zijn.

Wanneer de beveiliging van informatiesystemen niet goed op orde is, brengt dit volgens de CDA-fractie diverse en ernstige veiligheidsrisico's met zich mee. Voor inwoners, de stad en ook voor medewerkers van de gemeente zelf.

De berichtgeving van de Rotterdamse Rekenkamer en de uitkomsten van ons eigen onderzoek brengt de gemeenteraadsfractie van CDA Zwolle tot de volgende vragen:

1. Kent u het onderzoek van de Rekenkamer Rotterdam, de brief van Paul Hofstra (directeur van de Rekenkamer Rotterdam) aan de Rotterdamse gemeenteraad, en/of de rapportages hierover in Nieuwsuur en het NOS-journaal van zondag 2 april 2017?
2. Zijn de veiligheidsrisico's die in het rapport van de Rekenkamer Rotterdam en/of de rapportage van de NOS naar voren komen (en voor zover al openbaar) op Zwolle van toepassing?
    a. Zo ja, welke?
    b. Zo nee, waaruit blijkt dit?
3. Wat is het beleid van de gemeente Zwolle omtrent de digitale toegang tot vertrouwelijke informatie?
4. In hoeverre wordt er binnen de informatiesystemen gebruik gemaakt van automatisch gegenereerde inloggegevens?
5. Op welke manier worden deze inloggegevens aan de gebruikers verstrekt?
6. Wat is de houdbaarheid van verstrekte inloggegevens? Na welke tijd komen de inloggegevens te vervallen?

7. Wordt er gecontroleerd of de inloggegevens periodiek door de gebruiker gewijzigd worden?
    a. Indien ja, welke stappen worden er genomen als blijkt dat de inloggegevens voor een bepaalde tijd niet door de gebruiker gewijzigd zijn?
    b. Indien nee, waarom niet?
8. Hoe frequent en op welke manier onderzoekt de gemeente Zwolle veiligheidsrisico's omtrent haar informatiesystemen?
9. Op welke manier monitort de gemeente Zwolle oneigenlijke toegang van vertrouwelijke informatie?

Namens de fractie van het CDA,

Herbert Klinkvis

Martijn van der Veen