Raadsbesluit

Datum raadsvergadering	24 november 2022
Datum carrousel	10 november 2022
Raadsbesluitnummer	

Onderwerp: Rekenkamerrapport Informatiebeveiliging gemeente Velsen

De raad van de gemeente Velsen,

Gelezen het initiatief-raadsvoorstel van de Rekenkamercommissie, van 26 september 2022.

Besluit

1) De volgende aanbevelingen uit het Rekenkamerrapport Informatiebeveiliging gemeente Velsen over te nemen en het college opdracht te geven deze met hoge prioriteit (binnen een half jaar) uit te voeren:
   a. Privacy Officer/FG: start met het completeren van de belangrijkste onderdelen die in het privacy/AVG-jaarplan zijn vermeld, waaronder met name het DPIA-proces, maar ook andere maatregelen kunnen worden opgestart.
   b. CISO/ Privacy Officer: Continueer de bewustwordingscampagne in een minder vrijblijvende opzet, zodat de medewerkers van de gemeente Velsen ook in de huidige manier van (thuis-) werken up-to-date blijven van informatiebeveiliging, Privacy/AVG en de bijbehorende gevaren.
   c. Contract-/servicemanager/CISO: Stem de punten af die zijn opgenomen in het re-transitie document, met name de back-up afspraken en inrichting op korte termijn, waaronder de beschermingsmaatregelen tegen mogelijke ransomware aanvallen. Zorg tevens dat alle relevante informatiebeveiligingsonderwerpen in de servicelevel rapportage worden opgenomen.
   d. CISO/Eigenaren: Opstellen uitwijkplan voor BRP en andere belangrijke, bedrijf kritische applicaties en daarnaast voor (minstens) BRP de uitwijktest daadwerkelijk uitvoeren, evalueren en verbeteringen doorvoeren.
   e. CISO/OGD: Opstellen scenario's, in overleg met OGD, hoe om te gaan met de meest voorkomende, meest impacthebbende beveiligingsincidenten indien deze optreden. Mogelijke voorbeelden kunnen zijn phishing mail, ransomware mail, blokkering web-diensten (DDOS-aanval), gecompromitteerd wachtwoord.

2) De volgende aanbevelingen uit het Rekenkamerrapport Informatiebeveiliging gemeente Velsen over te nemen en het college opdracht te geven om deze aanbevelingen met gemiddelde prioriteit (binnen 6 tot 12 maanden) uit te voeren:
   a. CISO/Management: Zorg tevens dat de verbeteringen die in het informatiebeveiligingsjaarplan zijn opgenomen, daadwerkelijk worden uitgevoerd en neem controlemaatregelen hierin op zodat ze kunnen worden bewaakt door de CISO-functie.

b. CISO: Aanvulling van het beleid op tactisch en operationeel niveau, zodat de gedefinieerde beleidsuitgangspunten kunnen worden uitgewerkt in praktische maatregelen en kunnen worden bewaakt en gemonitord. De keuze om standaard voor SaaS/Cloud applicaties te kiezen en/of het gebruik van BYOD-apparaten zijn enkele voorbeelden, waarvoor een beleid kan helpen in standaardisatie. Verder kan worden gedacht aan beleid over het gebruik van sociale media, mobiele apparatuur, leveranciersvoorwaarden en rapportages en tenslotte een breder wachtwoord (of authenticatie) beleid, waarin is vastgelegd wat de minimumvoorwaarden zijn om toegang te krijgen vanaf het Internet, het interne netwerk, vanuit thuis etc.
c. CISO: Afstemming omtrent de definities, registratie, afhandeling en rapportage ten aanzien van informatiebeveiligingsincidenten en de vastlegging van de taken en verantwoordelijkheden wie welke activiteiten uitvoert (OGD of gemeente Velsen) ten aanzien van informatiebeveiligingsincidentenbeheer.
d. CISO/Management: Opstellen escalatie en crisisbeleid en uitwerken van de bijbehorende procedures, waarna in overleg met OGD wordt afgestemd, welke stappen worden doorlopen en met name wie welke taken en verantwoordelijkheden in dit proces krijgt toebedeeld.
e. CISO/Contractmanager: Opstellen randvoorwaarden voor de toegangscontrolemaatregelen (waaronder multi-factor authenticatie) noodzakelijk voor de via het Internet beschikbaar gestelde systemen en applicaties van de gemeente Velsen en opstarten configuratie aanpassingen aan die systemen en applicaties die daar niet aan voldoen.

3) De volgende aanbevelingen uit het Rekenkamerrapport Informatiebeveiliging gemeente Velsen over te nemen en het college opdracht te geven om deze aanbevelingen met lage prioriteit (binnen 24 maanden) uit te voeren:
   a. Het Management/Proceseigenaren/CISO: Richt een risicomanagementproces in voor het identificeren, analyseren en evalueren van risico's en voor het bepalen van de risicohouding: accepteren of maatregelen treffen. Dit dient een continu proces te zijn. Maak hierbij o.a. gebruik van de best practices van de IBD en andere gemeenten, zodat de minimumeisen (BBN) vanuit de BIO (Basis Beveiliging Niveau) zijn vastgesteld. Leg daarbij de risico afwegingen vast, voor latere referenties.
   b. CISO/Eigenaren: Opstellen continuïteitseisen voor (minimaal) de belangrijke, bedrijf kritische applicaties en daarnaast onderzoeken in overleg met OGD welke verbeteringen wanneer doorgevoerd kunnen/moeten worden en in een implementatieplan vastleggen.
   c. CISO/Management: Stel een meerjarenplan op, waarin beschreven wordt wanneer welke escalatie/crisis situaties worden geoefend. Voer daarnaast de oefening uit volgens plan, zodat de opgestelde escalatie en crisis procedures in de praktijk worden getoetst, waarna via de evaluatie eventuele verbeteringen kunnen worden doorgevoerd.

4) Het college te verzoeken om elk half jaar een herijking te doen van de status en voortgang van de verbeterpunten en de raad hierover te informeren.

Vastgesteld in de openbare raadsvergadering van 24 november 2022

De raad van de gemeente Velsen,

De griffier, De voorzitter,

R.B. Palstra F.C. Dales