

Verzoek tot agendering in raadscommissie

afdeling Concernstaf	Steller O.Karmon	Gouda
dossiernummer	telefoon 0613435901	

Onderwerp
Informatiebijeenkomst Informatiebeveiliging (geheim)

Voorstel voor agendering in de raadscommissie: Bestuur

Geheime commissie bestuur: overwegende te hebben besloten tot het ingevolge artikel 25, tweede lid, van de Gemeentewet opleggen van geheimhouding ten aanzien van agendapunt twee en drie. De motivering van de geheimhouding is dan ook gelegen in art. 5.1 lid 2 sub i van de Wet open Overheid (Woo): het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen.

Voorstel/verzoek voor datum behandeling in commissie
23 januari van 20:30-22:00 uur

Onderwerp
Waarom informatiebeveiliging?
- Dreigingsbeeld Informatiebeveiliging 2022/2023
- Wat zijn op dit moment de grootste informatiebeveiligingsrisico's voor de gemeente Gouda? (agendapunt geheim)
- Wat gaan wij hier aan doen? (agendapunt geheim)

Fase
Informatief.

Toelichting reden agendering:
De dreiging van ransomware-aanvallen neemt toe. Aan de lopende band proberen criminelen een ingang te vinden. Criminelen versleutelen gegevens en persen het slachtoffer af om deze gegevens na het betalen van losgeld toegankelijk te maken. Zo werd de gemeente Buren in 2022 getroffen door een ransomware-aanval. Bij de hack zijn gegevens van de gemeente gestolen. Vervolgens is een grote hoeveelheid data gepubliceerd op het darkweb, een afzonderlijk en anoniem deel van het internet. Daarnaast blijkt uit AIVD-jaarverslagen dat Nederland een aantrekkelijk doelwit is voor spionage en constateert het NCSC een toename van activistische hackpogingen a.g.v. de oorlog in Oekraïne.

Waarom?
- De IBD schat in dat gemeenten rekening moeten houden met DDoS-aanvallen (Hacktivisme, hackpogingen door politieke activisten) in situaties waarin bijvoorbeeld eigen bestuurders zich uitspreken over de oorlog en publiekelijk steun uitspreken voor Oekraïne.

gemeente gouda

- DDoS[1]- aanvallen mitigeren van alle devices, (die onderdeel zijn van de aanval en onze server willen bereiken) en buiten West-Europa komen. Als maar een klein deel hiervan bij de server kan komen, is de impact lager/nihil.
- Het mitigeren van hackpogingen zodat de zichtbaarheid op het internet verkleint wordt voor een kwaadwillende. We verminderen hiermee de kans dat we slachtoffer worden van niet gerichte aanvallen, te vergelijken met een schot hagel dat mogelijk doel treft.
- Het risico op (digitale) spionage te verkleinen.

Bestuurlijke achtergrond (relevante besluitvorming):

De verantwoordelijkheid voor informatiebeveiliging ligt op bestuurlijk niveau bij het college van burgemeester en wethouders en op ambtelijk niveau bij de gemeentesecretaris. De gemeenteraad heeft het informatiebeveiligingsbeleid vastgesteld, daarbij hebben ze aangegeven dat men een adequaat beveiligingsniveau wil hanteren. Het college is van mening met het doorvoeren van bovenstaande maatregelen uitvoering te geven aan het door de raad vastgestelde adequate beveiligingsniveau.

Aanvullende informatie voor de raadscommissie:

Bij dit overleg sluiten de volgende personen aan:

- Chief Information Security Officer (CISO) gemeente Gouda, Oumaima Karmon
- Technical Information Security Officer (TISO) gemeente Gouda, John Vloemans
- Chief Information Security Officer (CISO) gemeente Zuidplas, Rijk Meuleman
- Lid van de informatiebeveiligingsdienst (IBD/VNG), Remco Groet

Portefeuillehouder:

Michiel Bunnik

Bijlage(n):

- Dreigingsbeeld Informatiebeveiliging 2022/2023
- Overzicht landen West-Europa (Geofencing)

[1] DDoS-aanvallen: Hierbij worden zo veel data naar een server gestuurd dat deze kan worden platgelegd. Gebruikers kunnen deze server daardoor niet meer (of veel trager) bereiken.