

Agendapunt: Klik om agendapunt in te voeren – door directiesecretariaat.

Onderwerp	Informatieveiligheid en VRG
Datum	2-7-2021
Portefeuillehouder	Dhr. Schuiling
Sector	Bedrijfsvoering
Bijlage(n)	1. Bestuurlijke Lessen HvT 2. Checklist BIO 3. Checklist Cybercrisis
Ter besluitvorming/ter bespreking/ter informatie	Ter informatie

Gevraagd besluit

Het Algemeen Bestuur wordt gevraagd:

Kennis te nemen van onderstaande notitie met de stand van zaken rondom informatieveiligheid bij VRG. De benodigde vervolgacties inclusief de (financiële- en personele) consequenties worden nader in kaart gebracht.

Toelichting voorstel

Aanleiding

Op 1 december 2020 werd de gemeente Hof van Twente getroffen door een hack in hun informatiesysteem en werd de organisatie slachtoffer van zgn. gijzelsoftware. Als gevolg hiervan lagen nagenoeg alle gemeentelijke dienstverlening- en bedrijfsvoeringsprocessen stil.

Dit voorval laat eens te meer zien wat het belang is van informatieveiligheid en alles wat daarmee samenhangt. Daarbij dient de vraag zich aan hoe dit soort situaties voorkomen kunnen worden en hoe ermee omgegaan wordt als dit toch gebeurt. In bijgevoegd document “Bestuurlijke Lessen HvT” is een beknopt overzicht weergegeven van de situatie in Hof van Twente met een vijftal lessen die daaruit geleerd kunnen worden:

- Les 1: Ontbreken van basismaatregelen leidt tot rampscenario's en voor een deel onherstelbare schade
- Les 2: Het is lastig en noodzakelijk om inzicht te krijgen en overzicht te houden van beveiliging bij leveranciers en ketenpartners
- Les 3: Crisismanagement bij informatiebeveiligingsincidenten staat in de kinderschoenen
- Les 4: De rol van management en bestuur bij incidenten groeit naarmate de impact toeneemt
- Les 5: Een gemeente redt het niet alleen bij een groot incident

Versnellingsplan Informatieveiligheid

Ook voor veiligheidsregio's is cybercriminaliteit een actueel onderwerp. Zo is veiligheidsregio Noord- en Oost Gelderland op 12 september 2020 getroffen door gijzelsoftware. De vraag is niet meer *of* maar *wanneer* een volgende veiligheidsregio getroffen wordt door een informatiebeveiligingsincident.

VEILIGHEIDSREGIO GRONINGEN

In het kader van de informatieveiligheid zijn er in 2017 en 2019 bij verschillende VR's collegiale toetsingen geweest. In de vergadering van het Veiligheidsberaad van 14 december 2020 is de rapportage over deze toetsing informatiebeveiliging veiligheidsregio's aangeboden. De conclusie van deze rapportage is dat de veiligheidsregio's niet voldoen aan de in 2016 bestuurlijk vastgestelde normen voor informatieveiligheid en dat de onderlinge verschillen in niveau van informatieveiligheid tussen de veiligheidsregio's groter worden (VRG kwam op onderdelen overigens positief uit deze collegiale toetsing). Daarom is door het Veiligheidsberaad aan de bestuurlijk portefeuillehouder informatievoorziening gevraagd om in samenspraak met de RCDV een versnellingsplan op te stellen, om alsnog te komen tot borging van het vereiste basisniveau voor informatieveiligheid in alle 25 veiligheidsregio's en bij het IFV. In afstemming met het programma IV en het POI is inmiddels uitwerking gegeven aan het versnellingsplan.

Het versnellingsplan betekent voor de veiligheidsregio's en het IFV dat er collectieve afspraken in de RCDV worden gemaakt die in het Veiligheidsberaad bekrachtigd kunnen worden. Deze afspraken zijn:

- Alle veiligheidsregio's maken een BIO implementatieplan en wijzen hier budget aan toe.
- Alle veiligheidsregio's rapporteren aan elkaar over de eigen voortgang van de implementatie van de BIO (regio's rapporteren zelf periodiek aan het landelijke loket wat hiervoor wordt ingericht van het programma IV).
- Alle veiligheidsregio's en het IFV voldoen op 30 juni 2022 aan een subset van de BIO (110 normen (controls) in 16 onderdelen (criteria), die de VNG als belangrijkste kern van de BIO heeft vastgesteld) en op 1 januari 2023 aan de gehele BIO.
- Alle veiligheidsregio's en het IFV zijn solidair aan elkaar en helpen elkaar bij het toewerken naar deze deadline.
- Alle veiligheidsregio's en het IFV zijn lid van de VR-ISAC en melden hierin incidenten en verdachte situaties.
- Het niet voldoen aan de BIO op 1 januari 2023 heeft consequenties voor de toegang tot landelijk beheerde voorzieningen.

Informatieveiligheid binnen VRG

VRG maakt bij de uitvoering van haar taken gebruik van veel applicaties en informatie. De vraag is nu hoe goed zijn we bestand tegen een cyberaanval en zijn we in staat om bij een cyberaanval snel weer aan het werk te kunnen, zonder verlies van informatie?

Om hier een antwoord op te kunnen geven zijn een aantal dingen van essentieel belang.

1. Kan VRG mee met het versnellingsplan informatieveiligheid om zo te voldoen aan de BIO?
2. Beschikt VRG over een actueel bedrijfscontinuïteitsplan, waarin staat beschreven wat er moet gebeuren bij een eventuele cybercrisis? En vinden er periodiek oefeningen plaats?
3. Zijn in de organisatie de juiste rollen belegd en is er voldoende aandacht en tijd voor preventieve maatregelen op dit vlak?

Ad1) Wij kunnen ons inhoudelijk vinden in het versnellingsplan informatieveiligheid. De consequenties van dit versnellingsplan (personeel, materieel en financieel) zijn echter zeer omvangrijk. De in 2017 en 2019 gehouden collegiale toetsing was gebaseerd op 30 normen. De in het versnellingsplan genoemde subset van de BIO bestaat uit 110 normen (zie bijlage checklist BIO voor bestuurders). De gehele BIO implementeren vóór 2023, zoals het versnellingsplan voorschrijft, lijkt qua tijd en financiële consequenties verre van realistisch.

Om de consequenties nader te kunnen duiden zijn wij voornemens op korte termijn een GAP-analyse uit te voeren. Op basis hiervan kan vervolgens een plan van aanpak worden opgesteld met inschattingen per norm voor wat betreft tijd en kosten.

VEILIGHEIDSREGIO GRONINGEN

Ad2) Het bedrijfscontinuïteitsplan van VRG zal worden geüpdatet met inachtneming van de huidige stand van de techniek. Daarnaast zal ook periodiek getoetst worden of alles werkt zoals beschreven in het continuïteitsplan.

Ad3) Binnen VRG is er een functionaris Gegevensbescherming werkzaam. Daarnaast hebben we het thema Informatieveiligheid onderdeel gemaakt van het takenpakket van een van de Informatiemanagers. Er zal moeten worden gekeken of met de huidige bezetting en taakverdeling de activiteiten rondom het thema informatieveiligheid proactief kunnen worden opgepakt.

Conclusie

Wij willen ons committeren aan o.a. de implementatie van de BIO om op deze manier uitvoering te kunnen geven aan de genoemde bestuurlijke lessen. Wij zijn voornemens op korte termijn analyses uit te voeren wat hiervoor nodig is en komen daarna met een overzicht met benodigde acties en (personele / financiële) consequenties. Het thema informatieveiligheid zal, samen met de andere (landelijke) dossiers, worden geagendeerd voor de bestuurstweedaagse na de zomer.

Afstemming/consequenties		
	Afgestemd	Consequenties
Juridisch	<input type="checkbox"/>	
Financieel	<input checked="" type="checkbox"/>	Financiële gevolgen worden nader in kaart gebracht.
Personeel	<input type="checkbox"/>	
IM/ICT	<input checked="" type="checkbox"/>	ICT-inhoudelijke gevolgen worden nader in kaart gebracht.
Communicatie	<input type="checkbox"/>	
Inkoop	<input type="checkbox"/>	
Overig	<input type="checkbox"/>	