Nota voor burgemeester en wethouders
Onderwerp
Vragen ex art 46 RvO-VVD-Cyberaanval

Team
DEV-CS

1- Notagegevens	
Notanummer	2020-002313
Datum	10-12-2020
Programma:	
12 Bedrijfsvoering	
Portefeuillehouder	Burgemeester

2- Bestuursorgaan	
[X]B & W	15-12-2020
[ ]Raad	--
[ ]Burgemeester	--

College van B & W	
- Burgemeester	- Weth. Grijsen
- Weth. De Geest	- Weth. Verhaar
- Weth. Walder	- Weth. Rorink

Besluitenlijst	d.d.		d.d.		d.d.
[ ]Akkoordstukken	--	[ ]Openbaar	--	[ ]Besloten	--

Routing	d.d.
directeur	11-12-2020
burgemeester	11-12-2020

	par.
[ ]adj.secr.	--
[X]gem.secr.	11-12-2020
BIS Openbaar	
Status	Definitief2020-12-17

Bijlagen
Vragen fractie + antwoordbrief

B & W d.d.: 15-12-2020

Besloten wordt:
1 De beantwoording van de vragen ex art 46 RvO van de fractie VVD vast te stellen;
2 de beantwoording aan te bieden aan de raad;
3 de nota en het besluit openbaar te maken.

Financiële aspecten:

Financiële gevolgen voor de gemeente?	Nee
Begrotingswijziging	Nee

Voorstel openbaarmaking conform Wet Openbaarheid Bestuur (Wob)

[X] De nota en het besluit openbaar te maken
[ ] De nota en het besluit openbaar te maken vergezeld van bijgaand persbericht
[ ] De nota en het besluit openbaar te maken nadat

[ ] De nota en het besluit openbaar te maken, behalve…

[ ] Het besluit openbaar te maken, maar niet de nota, gelet op artikel:

[ ] De nota en het besluit niet openbaar te maken, gelet op artikel:

Kennisgeving/ Bekendmaking Awb

Kennisgeving (publicatie) conform Awb	Nee
Bekendmaking conform Awb	Nee

ADVIESRADEN:

Moet een van de adviesraden gehoord worden of op de hoogte gesteld? Nee

Toelichting

Inleiding

Per brief van 9 december 2020 heeft Eva Sipman van de VVD fractie uw college een aantal schriftelijke vragen ex art 46 RvO gesteld over cyberaanvallen.

Bijgaand treft u de beantwoording aan.

Beoogd resultaat

Kader

Argumenten voor en tegen

Extern draagvlak (partners)

Financiële consequenties

Aanpak/uitvoering

Schriftelijke vragen artikel 46 RvO

09-12-2020

Onderwerp: Cyberaanval

Op dit moment kampt de gemeente Hof van Twente met een cyberaanval, waarbij data van de gemeente is gegijzeld en er losgeld wordt geëist. Cybercriminaliteit is een steeds vaker voorkomende vorm van criminaliteit. Helaas zien we ook dat organisaties hier vaak niet of onvoldoende op voorbereid zijn. Realiserende dat de antwoorden op sommige (delen van) vragen alleen onder geheimhouding kunnen worden gedeeld heeft de fractie van de VVD de volgende vragen:

1. In hoeverre heeft de gemeente kennis genomen van de lessen van de ransomware aanval op de universiteit van Maastricht? En in hoeverre heeft de gemeente die lessen vertaald naar de eigen organisatie? In hoeverre volgt de gemeente de ontwikkelingen op het gebied van cybercriminaliteit en vertaald de gemeente deze naar de eigen organisatie?
2. Is het college het met de VVD eens dat voorbereiding op een mogelijke cyberaanval hoge prioriteit verdient binnen de DOWR ICT en binnen de crisisorganisatie van de gemeente?
3. Op welke wijze heeft de gemeente zich voorbereid op een mogelijke cyberaanval? Ligt er een plan of protocol klaar voor het geval dat? Welke preventieve maatregelen worden binnen de gemeente toegepast? Denk hierbij niet alleen aan de technische kant, maar ook aan de menselijke kant. Wordt er binnen de crisisorganisatie geoefend met het scenario cyberaanval, zo ja, hoe vaak en zo nee, waarom niet?
4. Binnen wat voor tijdsbestek zal een cyberaanval op de gemeente ontdekt worden? En in hoeverre is ICT gemandateerd om bepaalde remmende dan wel werende maatregelen te nemen?
5. Als een cyberaanval bij de gemeente Deventer lukt en we geen losgeld betalen, kunnen we dan het hele systeem weer operationeel maken vanuit back ups en dergelijke en hoeveel tijd kost dit?
6. Op welke wijze zal het College de raad meenemen in het geval van een cyberaanval?

Namens de fractie van VVD Deventer
Eva Sipman

Grote Kerkhof 1
Postbus 5000
7400 GC Deventer

14 0570
telefoon

0570 - 695181
direct telefoonnummer

gemeente@deventer.nl
e-mail

Aan de fractie van VVD
t.a.v. mw. E.M.L. Sipman
Interne Post

2020-002313 kenmerk	uw referentie	datum
M.J.E. van der Meer contactpersoon	Schriftelijke vragen ex art 46 RvO onderwerp	

Geachte mevrouw Sipman,

In uw brief van 9 december jl. hebt u ons college schriftelijke vragen ex art 46 RvO gesteld over cyberaanvallen. Ons antwoord is als volgt.

Vraag 1:
In hoeverre heeft de gemeente kennis genomen van de lessen van de ransomware aanval op de universiteit van Maastricht? En in hoeverre heeft de gemeente die lessen vertaald naar de eigen organisatie? In hoeverre volgt de gemeente de ontwikkelingen op het gebied van cybercriminaliteit en vertaald de gemeente deze naar de eigen organisatie?

Antwoord:
De gemeente heeft het onderzoek van de ransomware-aanval bij de Universiteit van Maastricht op de voet gevolgd. O.a. het Symposium van Universiteit Maastricht is uitgezonden met alle bevindingen en lessons learned.

Wij toetsen informatie over kwetsbaarheden, cyberaanvallen en bedreigingen continu door middel van risicoanalyses op onze organisatie en de infrastructuur. Zo bekijken wij of wij ons risicobeeld moeten bijstellen en of we aanvullende maatregelen moeten nemen om het risico op een acceptabel niveau te houden. In geval van Maastricht is dit ook gebeurd.

We volgen de ontwikkelingen continu. Ook voeren we periodiek interne en externe scans uit op onze ICT- infrastructuur. Hiermee simuleren we cyberaanvallen en brengen we kwetsbaarheden in kaart. De uitkomsten van deze scans worden altijd direct na rapportage gewogen en waar nodig worden maatregelen genomen om de beveiliging te verbeteren.

Vraag 2:
Is het college het met de VVD eens dat voorbereiding op een mogelijke cyberaanval hoge prioriteit verdient binnen de DOWR ICT en binnen de crisisorganisatie van de gemeente?

Antwoord:
In 2017 heeft de raad de I-visie 2018-2022 vastgesteld. Informatieveiligheid en stabiliteit zijn daarin aangemerkt als topprioriteit. Het doel van informatieveiligheid is het borgen van continuïteit van systemen, data en informatie en het risico op incidenten zo laag mogelijk te houden, en daarmee het voorkomen van geslaagde cyberaanvallen voor de gemeentelijke DOWR- organisaties, waaronder Deventer. Het college onderschrijft onverkort deze lijn mede vanwege het feit dat cyberaanvallen en -incidenten wereldwijd en in ons land de afgelopen jaren in omvang en impact zijn toegenomen.

Vraag 3:
Op welke wijze heeft de gemeente zich voorbereid op een mogelijke cyberaanval? Ligt er een plan of protocol klaar voor het geval dat? Welke preventieve maatregelen worden binnen de gemeente toegepast? Denk hierbij niet alleen aan de technische kant, maar ook aan de menselijke kant. Wordt er binnen de crisisorganisatie geoefend met het scenario cyberaanval, zo ja, hoe vaak en zo nee, waarom niet?

Antwoord:
Als gemeentelijke organisatie hebben we inderdaad draaiboeken klaarliggen voor het geval er iets (zoals een cyberaanval) gebeurt waardoor de continuïteit van de dienstverlening in gevaar zou kunnen komen. Ook voert DOWR- ICT periodiek preventieve testen uit. Enerzijds om te zien of de infrastructuur en de organisatie dergelijke scenario's aan kunnen. Anderzijds om eventuele kwetsbaarheden op dat vlak vroegtijdig te signaleren om in geval van een daadwerkelijke crisissituatie zo goed mogelijk voorbereid te zijn om de beschikbaarheid zo snel mogelijk te herstellen en de continuïteit te kunnen blijven waarborgen.

Cyberaanvallen vinden dagelijks plaats en komen uit alle delen van de wereld. Daarom heeft DOWR ICT verschillende technische maatregelen genomen om een gelaagde beveiliging te vormen. Zo zorgt DOWR ICT voor het tijdig installeren van beveiligingsupdates, het zo veilig mogelijk configureren van systemen en applicaties, maar ook de bewaking van de systemen zodat afwijkingen (pogingen tot cyberaanvallen) zo snel mogelijk opgemerkt worden.

Wat betreft de menselijke kant van informatiebeveiliging besteden wij herhaaldelijk aandacht aan het bewustzijn van medewerkers om op een zorgvuldige manier om te gaan met vertrouwelijke gegevens en persoonsgegevens. Dit doen we bijvoorbeeld door e-learning, veilig gebruik van wachtwoorden, het uitvoeren van phishing-tests, heldere communicatie op intranet, maar zeker ook door het leren van incidenten.

Door op deze manier een gelaagde beveiliging toe te passen op technisch vlak en diverse activiteiten bij herhaling in te zetten op het menselijk vlak, verkleinen we de kans dat door een cyberaanval de totale beveiliging doorbroken wordt.

In aansluiting op het opstellen van de draaiboeken binnen de gemeentelijke organisatie zijn voorbereidingen gaande om in het eerste kwartaal 2021 het oefenen van een cybercrisisgame te starten. Hierbij wordt de crisisorganisatie op bestuurlijk-/managementniveau geoefend, bedoeld om transparante afspraken te maken over verantwoordelijkheden en het proces bij te stellen waar nodig. Verder zijn er diverse maatregelen georganiseerd waarbij continu aandacht wordt gevraagd voor (de risico's op het gebied van) informatiebeveiliging. De nadruk ligt op 'zo goed mogelijk' omdat het nooit mogelijk is om 100% garantie af te geven.

Vraag 4:
Binnen wat voor tijdsbestek zal een cyberaanval op de gemeente ontdekt worden? En in hoeverre is ICT gemandateerd om bepaalde remmende dan wel werende maatregelen te nemen?

Antwoord:
Dit zal per situatie verschillen, het begrip cyberaanval is hier te breed voor en 100% beveiliging bestaat niet. Cyberaanvallen komen voor in heel veel verschillende vormen. Van een computervirus of gijzelsoftware tot een hack of een DDoS-aanval. Zo duurde het bij de Universiteit van Maastricht 3 maanden voordat de aanval echt ingezet werd.

Wij streven ernaar om een zo goed mogelijk inzicht te krijgen in de risico's, deze zo goed mogelijk te analyseren en vervolgens passende maatregelen te nemen om deze risico's tot een acceptabel niveau terug te brengen. Daarnaast richt DOWR-ICT zich op 'slimme' monitoring(met elkaar in verband brengen van verschillende verdachte bewegingen) en analyse op verschillende plekken in de ICT-infrastructuur om eventuele cyberaanvallen of pogingen daartoe in een zo vroeg mogelijk stadium te ontdekken.

Qua mandatering zal dit per situatie verschillen. Een aantal remmende of werende maatregelen is vanuit DOWR-ICT geautomatiseerd (denk bijvoorbeeld aan anti-DDoS en anti-virus, die automatisch signaleren en ingrijpen). DOWR ICT heeft echter geen mandaat om bijvoorbeeld een gemeentelijk proces stil te leggen. In geval van een 'geslaagde' cyberaanval worden dergelijke maatregelen door het crisisteam, waar DOWR-ICT ook in is vertegenwoordigd, genomen. Het crisisteam onderhoudt daarover nauw contact met ons college.

Vraag 5:
Als een cyberaanval bij de gemeente Deventer lukt en we geen losgeld betalen, kunnen we dan het hele systeem weer operationeel maken vanuit back ups en dergelijke en hoeveel tijd kost dit?

Antwoord:
Met de beschikbare informatie uit de media wijst alles erop dat onze situatie in deze afwijkt ten opzichte van Hof van Twente. Wij kunnen vanuit back ups de belangrijkste processen als eerste herstellen.

Ter toelichting: de back-up oplossing is gescheiden van operationele systemen (niet rechtstreeks toegankelijk vanaf bijvoorbeeld een server). De opslag van de back-up data vindt ook op gescheiden apparaten plaats los van het platform waar de normale systemen en data op landen. Daarnaast wordt daar waar het kan (nagenoeg alle situaties) maand- en jaarbackups op tape weggeschreven. Deze kunnen niet versleuteld worden.

Wat betreft de doorlooptijd van herstelacties hebben we bedrijfscontinuïteitsplannen waarin de gemeentelijke processen op volgorde van hersteltijd gezet zijn. De doorlooptijden variëren uiteraard per scenario (afhankelijk van de omvang van de calamiteit), maar voor het proces voor reisdocumenten en rijbewijzen streven we er bijvoorbeeld naar om binnen 24 uur weer operationeel te zijn, terwijl andere minder kritische processen pas na een week weer operationeel hoeven te zijn. Omdat hier vooraf al over nagedacht is en dit vastgelegd is in de bedrijfscontinuïteitsplannen, kunnen we ons in dergelijke crisissituaties op de meest efficiënte wijze richten op de belangrijkste processen en die als eerste herstellen.

Vraag 6:
Op welke wijze zal het College de raad meenemen in het geval van een cyberaanval?

Antwoord:
Bij een 'geslaagde' cyberaanval zal het College, na afstemming met de crisisorganisatie, de raad per omgaande informeren.

Burgemeester en wethouders van de gemeente Deventer,

de secretaris,	de burgemeester,
M.A. Kossen	R.C. König