Gemeente Maastricht

> RETOURADRES Postbus 1992, 6201 BZ

BEZOEKADRES
Mosae Forum 10
6211 DW Maastricht

POSTADRES
Postbus 1992
6201 BZ

Aan de fractie van SAB
de heer J.E.M. Gorren

ONDERWERP	DATUM	BIJLAGEN
Schriftelijke vragen inzake Cyberinstituut	23 juni 2022 Verz. 23 juni 2022	--
BEHANDELD DOOR	TELEFOONNUMMER	ONZE REFERENTIE
CJR (Christian) Gijselaers	043 350 4232	2022.12340
E-MAILADRES	FAXNUMMER	UW REFERENTIE
Christian.Gijselaers@maastricht.nl	043 - 350 4448	---

Geachte heer Gorren,

Onderstaand treft u de beantwoording aan van de schriftelijke vragen die uw fractie gesteld heeft.

Vraag 1:
Is het college het er mee eens dat cyberaanvallen en cybersabotage een reëel gevaar zijn voor het openbaar bestuur en publiekelijke dienstverlenende instellingen, die ontwricht kunnen worden, en daardoor ook veel schade in de samenleving kan worden toegebracht?

Antwoord 1:
Ja.

Vraag 2:
Wil het college initiatieven nemen om dit in de toekomst te voorkomen?

Antwoord 2:
Er wordt reeds, op verschillende niveaus geacteerd ten aanzien van cyber dreigingen.

Ten aanzien van onze lokale taak in het kader van openbare orde en veiligheid:
Deze geven we op Limburgse schaal vorm aangezien dit fenomeen niet stopt aan de gemeentegrenzen. Bovendien vraagt de bestrijding van cybercriminaliteit veel kennis en expertise en is het onderwerp te groot om enkel lokaal aan te pakken. Aansluiten bij regionale initiatieven beschouwen wij als voorwaarde om adequaat te kunnen reageren op dit fenomeen. Eind vorig jaar is cybercrime als handhavingsknelpunt onder het zogenaamde RIEC (Regionaal Informatie en Expertisecentrum) Convenant benoemd. Dat betekent dat de convenantpartners kennis, data en informatie vroegtijdig met elkaar mogen delen. Daarbij is burgemeester Roel Wever (Heerlen) aangewezen als Limburgse portefeuillehouder cybercrime. Maastricht maakt daarbij deel uit van de Taskforce Cybercrime Limburg. Dit is een samenwerkingsverband bestaande uit de gemeenten Beek, Beekdaelen, Brunssum, Eijsden Margraten, Heerlen, Kerkrade, Landgraaf, Maastricht, Sittard –Geleen, Mook en Middelaar, Nederweert, Valkenburg, Venlo, Venray, Voerendaal, Weert, het OM, de politie, de provincie en het Platform Veilig Ondernemen. Deze taskforce investeert in vergroting van de weerbaarheid van inwoners en ondernemers in het digitale domein. Het gaat daarbij om het voorkomen van slachtofferschap (en daderschap) van cybercriminaliteit. De adviezen van de Taskforce Cybercrime nemen we als gemeente Maastricht mee in het Meerjarenprogramma Veiligheid 2023 – 2026 (MJP) dat momenteel in ontwikkeling is.

Schriftelijke vragen

Ten aanzien van de bescherming van de eigen organisatie en digitale processen speelt het Nationaal Cyber Security Center een centrale rol in het identificeren en duiden van risico's en trends. Het NCSC is de verbindende schakel in een netwerk van nationale en internationale partners, en voorkomt en beperkt maatschappelijke schade en dreigingen. In Nederland heeft het Nationaal Cyber Security Centrum daartoe het Nationaal Respons Netwerk opgericht. Dit netwerk van Incident Respons Teams deelt kennis en expertise en staat voor elkaar klaar in geval van incidenten.

Het NCSC werkt ook nauw samen met de Informatiebeveiligingsdienst (IBD). De IBD is het sectorale Computer Emergency Response Team (CERT/ CSIRT) voor alle Nederlandse gemeenten en is onderdeel van de Vereniging van Nederlandse Gemeenten. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC).

Vraag 3:
Is het college bereid initiatieven te ondernemen om een geavanceerd internationaal cyberinstituut in Maastricht in het leven te roepen om meer dan nu het geval is te anticiperen om mogelijke geavanceerde cyberaanvallen gesofisticeerd te kunnen pareren?

Antwoord 3:
Nee. Zoals in antwoord 2 benoemd: we kennen in Nederland (en in de landen waarmee we samenwerken) reeds specifieke sectorale CERT's. Al deze CERT's werken op vele niveaus met elkaar samen, ook over de landsgrenzen heen. De bestrijding van cybercriminaliteit vraagt veel kennis en expertise. Daarin is geen leidende rol weggelegd voor de lokale overheid.

Vraag 4:
Is het college bereid de Universiteit Maastricht te faciliteren om hierin het voortouw te nemen?

Antwoord 4:
Dat is desgevraagd niet aan de orde. Maastricht University kent al het Maastricht European Centre on Privacy and Cybersecurity (ECPC), zie: https://www.maastrichtuniversity.nl/ecpc. Dit instituut valt binnen de Rechten Faculteit, en richt zich nadrukkelijk op cybersecurity. Niet alleen op het gebied van onderzoek, maar vanuit het instituut worden ook post-graduate cursussen aangeboden.

Vraag 5:
Is het college bereid de Europese Commissie hierbij (financiële) steun te vragen om Euregionaal te opereren en diensten aan te bieden.

Antwoord 5:
Gelet op het antwoord op vraag 3 en 4 is dat niet aan de orde.

Vraag 6:
Is het college, vooruitlopend op de ontwikkelingen met betrekking tot de Einsteintelescoop, bereid zo een instituut extra en bijzondere bescherming tegen cyberaanvallen te bieden waardoor het vestigingsklimaat verbetert? Dat bedrijven als stimulans voor vestiging in de regio laagdrempelig gebruik kunnen maken van de kennis en kunde van dit Euregionaal overheidskennisinstituut.

Antwoord 6:
Gelet op het antwoord op vraag 3 en 4 is dat niet aan de orde.

Vraag 7:
Is het college het met de mening van SAB eens dat instellingen, in de Euregio al aanwezig of die zich willen vestigen, laagdrempelig toegang moeten hebben tot dit kennisinstituut?

Antwoord 7:
Gelet op het antwoord op vraag 3 en 4 is dat nu niet aan de orde. Hierin is geen interveniërende rol weggelegd voor de gemeente Maastricht.

Hoogachtend,

Burgemeester en Wethouders van Maastricht,

De Secretaris, De Burgemeester,

G.J.C. Kusters J.M. Penn-te Strake

Schriftelijke vragen