vragenuurtje

**Mondelinge vraag – Antwoord**

## Opschrift

**Vergadering van** 19 december 2022

**Nummer:** 2022_MV_00668

**Onderwerp:**
**Mondelinge vraag van raadslid Christiaan Van Bignoot: Cyberaanval**

**Raadslid(-leden):**
Christiaan Van Bignoot - Open Vld

**Bevoegd:** Sofie Bracke

## Omschrijving van de vraag

**Toelichting:**
De Stad Antwerpen werd recent het slachtoffer van een cyberaanval. Quasi de hele dienstverlening naar burgers en interne werking lagen plat of ondervonden sterke hinder: de bereikbaarheid van stadsdiensten, betalingssystemen, reserveringstools, de (medische) werking van woonzorgcentra,... Ook de politie kon tijdelijk geen mails sturen en de stedelijke scholen moesten alle zeilen bijzetten om het afnemen van examens te laten doorgaan.
Dit toont nog maar eens aan dat iedereen het doelwit kan zijn van dergelijke aanval, we nemen dus maar best zo veel mogelijk voorzorgsmaatregelen. Het gaat tenslotte om het verzekeren van de dienstverlening naar burgers én het beschermen van de gegevens van diezelfde burgers.

**Vraag:**
Zijn er bij de Stad Gent al gelijkaardige pogingen tot cyberaanval waargenomen?
Welke voorzorgsmaatregelen neemt de stad om persoonsgegevens maximaal te beveiligen en te voorkomen dat hackers in onze systemen kunnen binnendringen?

## Antwoord

Collega Van Bignoot, bedankt voor deze uiterst belangrijke en actuele vraag. Het is inderdaad zo dat cyberaanvallen actueel zijn en mogen aanzien worden als één van de nieuwe agressieve vormen van criminaliteit. Cybercriminelen richten zich zowel op bedrijven als op overheden.

Bijna 1 op de 8 van de Vlaamse bedrijven werd het afgelopen jaar slachtoffer van een cyberaanval. Dat blijkt uit een eerste nulmeting die de Vlaamse Regering liet uitvoeren om de maturiteit van cybersecurity bij Vlaamse bedrijven in kaart te brengen. Vooral grote bedrijven kennen het meest cyberaanvallen, maar de gevolgen blijken groter bij kleine ondernemingen die vaak minder beschermd zijn.
Ook meer en meer overheden worden slachtoffer van cyberaanvallen. Zo waren in 2021 Defensie en de stad Luik slachtoffer van een grote cyberaanval, maar ook de Universiteit van Maastricht in 2019 en dus recent ook de Stad Antwerpen en de Stad Diest. Telkens leidden deze aanvallen tot het wekenlang platliggen van cruciale IT-systemen en vaak ook tot het betalen van losgelden, zodat data van burgers of bedrijven niet op straat komen te liggen. Het gevaar komt dus dichterbij en we mogen niet op onze lauweren rusten, want ook onze IT-systemen kunnen aangevallen worden.
District09 is zich al jaren bewust van dit risico en heeft daarvoor ook stappen ondernomen. De meest recente stap is de Security nota 2022 waar we gericht inzetten op preventie, detectie en remediering.
Binnen de Security nota streven we naar een voldoende hoog beschermingsniveau en dit onder leiding van een Digital Security Officer. U zult begrijpen dat ik de specifieke acties die we verrichten in functie van het verzekeren van onze cyberveiligheid als stad hier niet publiekelijk bij naam en toenaam kan vermelden. Dit zou teveel inzicht geven aan mogelijke cybercriminelen. Maar vandaag zijn we dus al heel actief en worden al verschillende acties genomen. De voorbije legislatuur besteedden we reeds 6 miljoen euro. Het is ook zo dat we het afgelopen jaar nog eens bijkomende middelen hebben vrijgemaakt. Er is structureel 1,1 mio euro in exploitatiemiddelen en 654.000 euro in investeringsmiddelen bijkomend voorzien bij BW 2022. De besparingen die gebeurd zijn in de recente budgetronde (BO23) zijn niet van toepassing op het thema ‘cybersecurity’. De besparingen die gebeurd zijn bij D09 hebben wel betrekking op het niet opstarten van nieuwe IT-projecten (lees: nieuwe software) voor stadsdiensten.
Naar aanleiding van de recente aanvallen in Antwerpen zijn we rond de tafel gaan zitten met Antwerpen om ook daaruit lessen te kunnen trekken. We zullen anticiperend daarop een aantal van onze acties vervroegd op korte termijn invoeren. Terwijl District09 de risico’s hoog inschat merken we dat dit bij onze gebruikers nog niet altijd is doorgedrongen welke risico’s we lopen. Daarom stellen we voor dat we met de ervaring in Digipolis Antwerpen onze plannen bijwerken, sneller laten lopen en we meer inspanningen vragen van onze gebruikers. Want ik wil benadrukken dat naast het voorzien van IT-security systemen , er ook een heel belangrijke menselijke factor schuilt achter de mate van veiligheid van je systeem. Gebruikers zijn namelijk de zwakste schakel in de beveiliging en worden veelal geviseerd bij een cyberaanval (bv. phishing aanval). We zullen die bewustwording vergroten door meer gerichte pro-actieve communicatie naar de stadsmedewerkers te doen en ook een aantal ingrepen centraal te doen in de systemen. Dit zal hen ook helpen in hun eigen privé-leven, waar cyberaanvallen ook mogelijk zijn.
De security nota zullen we ook verder actualiseren tegen BW23. Enerzijds inzake noodzakelijke bijsturing op de systemen, maar anderzijds zal ook in kaart gebracht worden welke extra gedragsveranderingen bij de gebruikers nodig zal zijn naar verhoogde security awareness.

Ik wil wel duidelijk zijn. Je mag je nog zo sterk beschermen tegen cyberaanvallen, een 100% veilige ICT-omgeving bestaat niet. Maar bij Stad Gent staat het risico alvast sterk op onze radar en handelen we vandaag al naar preventie, detectie en remediëring.

---