Vlaams Parlement

SCHRIFTELIJKE VRAAG

nr. 181
van **ANDRIES GRYFFROY**
datum: 6 december 2019

---

aan **HILDE CREVITS**
VICEMINISTER-PRESIDENT VAN DE VLAAMSE REGERING, VLAAMS MINISTER VAN ECONOMIE, INNOVATIE, WERK, SOCIALE ECONOMIE EN LANDBOUW

Ondernemingen - Cybersecurity

Digitalisering is een uitdaging voor de ondernemingen. Het heeft een absolute meerwaarde om processen en procedures te vereenvoudigen, maar er zijn ook risico's. Een degelijke beveiliging is noodzakelijk om de software en applicaties te beschermen. Op dat vlak is er nog heel wat werk aan de winkel.

De minister voorziet jaarlijks in 20 miljoen euro voor cybersecurity. Dat moet bijdragen om het bewustzijn en de basiskennis rond cybersecurity bij onze ondernemers en kmo's te versterken. Concreet zullen dienstverleners (ondernemersorganisaties of kenniscentra) in samenwerking met het Agentschap Innoveren en Ondernemen (VLAIO) nagaan op welk niveau onze ondernemingen zich bevinden. Op basis daarvan zal een coachingtraject worden uitgewerkt.

Daarnaast komt er in het voorjaar 2020 een website met tips & tricks, handleidingen, goede praktijken en een film over hoe men kan omgaan met cybersecurity.

1. Hoeveel 'cyberaanvallen' worden jaarlijks uitgevoerd op onze Vlaamse bedrijven? Graag de cijfers per type 'cyberaanval' voor 2016, 2017, 2018 en de meest recente cijfers voor 2019. Hoe worden deze gegevens verzameld, gecentraliseerd en gerapporteerd?
2. Op welke manier worden de risico's en de kwetsbaarheid inzake cybersecurity binnen de Vlaamse bedrijven in kaart gebracht? Welke noden detecteert de minister bij de Vlaamse bedrijven?
3. Hoe worden de dienstverleners die de bedrijven zullen doorlichten geselecteerd? Wanneer gaat men effectief aan de slag? Hoe zullen de dienstverleners dit concreet aanpakken? Op welke manier wordt er samengewerkt met de kennisinstellingen en de onderzoekscentra? Hoe zal worden gerapporteerd aan VLAIO?

HILDE CREVITS
VICEMINISTER-PRESIDENT VAN DE VLAAMSE REGERING, VLAAMS MINISTER VAN ECONOMIE, INNOVATIE, WERK, SOCIALE ECONOMIE EN LANDBOUW

ANTWOORD
op vraag nr. 181 van 6 december 2019
van **ANDRIES GRYFFROY**

---

1. Er zijn geen officiële cijfers beschikbaar wat betreft het aantal cyberaanvallen die worden uitgevoerd op onze Vlaamse bedrijven. Het federale Centrum voor Cybersecurity (ccb) en de Federal Computer Crime Unit van de Federale Politie volgen deze problematiek voor België op. Er dient hierbij ook een onderscheid gemaakt te worden tussen enerzijds het aantal cyberaanvallen enerzijds en het aantal geslaagde cyberaanvallen anderzijds. Deze laatste groep ligt aanzienlijk lager aangezien vele aanvallen al verhinderd worden door firewalls bij internet service providers en/of bedrijven.

2. Er is geen specifieke risico-analyse voor Vlaanderen beschikbaar. Het Federale centrum voor Cybersecurity en meer specifiek het federale Computer Emergency Response Team volgt de situatie van dichtbij op. Daarnaast is er ook een cybersecurity coalition opgericht, waarbij spelers uit de academische wereld, openbare instanties (inclusief Vlaamse overheid) en de private sector de krachten bundelen in de strijd tegen de cybercriminaliteit.

   Het is hierbij belangrijk om onze Vlaamse bedrijven voldoende te sensibiliseren, op te leiden en aan te zetten tot verbeteringen inzake een goeie 'cyberhygiene'. In het bijzonder heeft dit betrekking op veilige configuratie, software updating en patching gecombineerd met een awareness en training van de gebruikers. Daarnaast is het uiteraard belangrijk dat de software/hardware producten en services die door onze bedrijven ontwikkeld en/of gebruikt worden systematisch versterkst worden qua veiligheid.

3. In het kader van de lopende procedure voor de selectie van structurele partnerschappen voor ondernemerschap en innovatieversnelling werd een visienota opgesteld waarin ook gevraagd werd aan de kandidaten om bij het vormgeven van hun dienstverlening aan bedrijven aandacht te hebben voor de digital readiness van bedrijven, inclusief cybsersecurity. Op basis van de ingediende offertes is duidelijk dat de kandidaatdienstverleners op deze vraag ingegaan zijn en hierbij ook beroep wensen te doen op de bestaande expertise bij de kennisinstellingen. In de onderhandelingen die een onderdeel uitmaken van deze procedure zal dit verder geconcretiseerd worden.

   Binnen de lopende proeftuinen industrie 4.0 is er bovendien als een lopende proeftuin vanuit HOWEST die specifiek gericht is op het thema cyberveiligheid bij maakbedrijven. Bedrijven kunnen hierbij vandaag al terecht met hun CS-gerelateerde vragen.