SCHRIFTELIJKE VRAAG

nr. 108
van **KRISTOF SLAGMULDER**
datum: 10 december 2021

---

aan **JAN JAMBON**
MINISTER-PRESIDENT VAN DE VLAAMSE REGERING, VLAAMS MINISTER VAN BUITENLANDSE ZAKEN, CULTUUR, DIGITALISERING EN FACILITAIR MANAGEMENT

Vlaamse Regering - Veiligheid informaticasystemen

In opvolging van mijn schriftelijke vraag nr. 182 van 18 februari 2020 en het recente mediabericht dat de conciërge van het Errarahuis, het gebouw waar de ministerraden gehouden worden, een indringster betrapte die mogelijk een computer hackte, had ik graag antwoord gekregen op volgende vragen.

1. Werden de informaticasystemen van de Vlaamse Regering sinds 2020 gehackt? Zijn er pogingen daartoe geweest? Zo ja, graag een overzicht.
2. Werd er gevoelige informatie gestolen? Zo ja, heeft men zicht op de informatie die ontfutseld werd? Welke stappen werden daarna ondernomen?
3. Werden er hackers in zowel binnen- als buitenland geïdentificeerd? Zo ja, welk gevolg werd daaraan gegeven?
4. Zijn er de voorbije vijf jaar pogingen geweest door veiligheidsdiensten, of instanties van andere staten om toegang te krijgen tot deze informaticasystemen? Zo ja, over welke landen gaat het? Welk gevolg werd daaraan gegeven?
5. Werd er in de gebouwen van de Vlaamse Regering ooit al afluisterapparatuur gevonden?
6. Welke extra maatregelen zal de minister-president ter zake nemen?

JAN JAMBON
MINISTER-PRESIDENT VAN DE VLAAMSE REGERING, VLAAMS MINISTER VAN BUITENLANDSE ZAKEN, CULTUUR, DIGITALISERING EN FACILITAIR MANAGEMENT

ANTWOORD
op vraag nr. 108 van 10 december 2021
van **KRISTOF SLAGMULDER**

---

1. Het Agentschap Digitaal Vlaanderen heeft verschillende maatregelen ingericht om hacking(pogingen), waarbij wordt ingebroken in de informatiesystemen van de Vlaamse overheid, te detecteren, tegen te houden, te monitoren en erover te kunnen rapporteren.

   Hiertoe nemen wij de nodige maatregelen op 3 verschillende niveaus:
   - Op netwerkniveau
   - Op werkplekniveau
   - Bij de medewerkers

   De eerste twee soorten maatregelen zijn technische maatregelen, voor het derde niveau richt Digitaal Vlaanderen bewustmakingsacties in voor het personeel. Dit zowel voor het eigen agentschap als voor andere Vlaamse overheidsentiteiten.

   Gelet op het publieke karakter van deze vraag, kunnen wij niet ingaan op de concrete technische maatregelen die het Agentschap Digitaal Vlaanderen gebruikt binnen de toepassingen van de Vlaamse overheid. De algemene richtlijnen en procedurele inbedding in de organisatie staat beschreven in het Informatieclassificatieraamwerk, dat wel publiek beschikbaar op https://www.vlaanderen.be/uw-overheid/werking-en-structuur/hoe-werkt-de-vlaamse-overheid/informatie-en-communicatie/informatieveiligheid/informatieveiligheid-en-veiligheidsdiensten/informatieclassificatieraamwerk

   Het Agentschap Digitaal Vlaanderen heeft geen weet van concrete incidenten sinds 2020 waarbij hackers op informaticasystemen van de Vlaamse overheid (ons eigen agentschap, entiteiten die van onze diensten afnemen, of onze leveranciers) zouden hebben ingebroken. Het Agentschap Digitaal Vlaanderen kan echter enkel uitspraken doen over de informatiesystemen die onder haar eigen beheer/toezicht staan.

2. In aanvulling op de vorige vraag: het Agentschap Digitaal Vlaanderen heeft me bevestigd dat zij geen weet heeft van incidenten waarbij gevoelige overheidsinformatie zou zijn gelekt, of buit gemaakt.

3. In aanvulling op de vorige vraag: aangezien er geen incidenten werden gedetecteerd waarbij informatie werd gestolen, zijn er ook geen hackers (binnen- of buitenlands) geïdentificeerd.

4. Ook hier heeft het Agentschap Digitaal Vlaanderen geen weet van. Deze vraag ligt in het verlengde van vraag om uitleg nr. 3732 dd. 2 juni 2021 van Dhr. Johan Deckmyn, waarin op dit thema al uitvoerig is ingegaan.

5. Voor een antwoord op deze vraag heeft het Agentschap Digitaal Vlaanderen afgestemd met Het Facilitair Bedrijf. Zij bevestigen dat ze geen spoor kunnen vinden van dit soort vondsten of incidenten.

6. Om ook in de toekomst als overheid voldoende cyberweerzaam te zijn, heeft de Vlaamse Regering op 15/10/2021 de Strategie voor Informatieveiligheid goedgekeurd. Een van de speerpunten hiervan is het verhogen van de digitale weerbaarheid van zowel de medewerkers als van de processen rond informatieveiligheid.

   Dit is een bestendiging van de activiteiten die de verschillende betrokken overheidsentiteiten nu al ondernemen om hun medewerkers bewust te maken van informatieveiligheidsrisico's.

   Tegelijkertijd heeft de Vlaamse overheid een relanceproject "Cybersecurity en SIEM Onboarding" opgezet binnen het relanceplan Vlaamse veerkracht, om de controle op haar netwerk en haar informatiesystemen nog verder uit te bouwen en te verbeteren.