

SCHRIFTELIJKE VRAAG

nr. 18

van **MICHEL DOOMST**

datum: 29 september 2017

aan **LIESBETH HOMANS**

VICEMINISTER-PRESIDENT VAN DE VLAAMSE REGERING, VLAAMS MINISTER VAN BINNENLANDS BESTUUR, INBURGERING, WONEN, GELIJKE KANSEN EN ARMOEDEBESTRIJDING

Gemeentelijke websites - Kwetsbaarheid voor cybercriminaliteit

Een op de vijf Vlaamse gemeentewebsites gebruikt geen veilige HTTPS-verbinding voor hun digitaal loket. Hierdoor zouden persoonlijke gegevens onderschept kunnen worden door cybercriminelen.

Dit alles blijkt uit een onderzoek dat het tv-programma Terzake uitvoerde in samenwerking met enkele ethische hackers.

Federaal staatssecretaris De Backer reageerde reeds door te stellen dat bij de hervorming van de Belgische Privacycommissie meer aandacht zal gaan naar het controleren van onder andere de gemeentewebsites.

Twee jaar geleden bespraken we in de commissie Binnenlands Bestuur de beveiliging van de digitale platformen van de Vlaamse overheid (vraag 1101). Ook toen werd op het gevaar van cybercriminaliteit gewezen:

“Wat we ook zullen doen, is een veiligheidsbewustmakingsprogramma voor de volledige Vlaamse overheid maken. We kunnen zeer goede organisatorische en technische maatregelen nemen, maar de mensen moeten zich natuurlijk zelf van bepaalde risico’s bewust zijn. Het is in verband met deze problematiek belangrijk dat we de mensen erop attent maken dat ze onbewust een zeer zwakke schakel in het systeem kunnen zijn en dat ze er op die manier voor kunnen zorgen dat de cybercriminaliteit bepaalde proporties aanneemt.

...

De coalitie heeft tot doel kennis tussen overheden, bedrijven en de academische sector in verband met cybercriminaliteit uit te wisselen, de bewustwording van burgers en bedrijven in verband met cybercriminaliteit te vergroten en beleidsaanbevelingen te formuleren. Dit laatste punt is positief. We nemen elke beleidsaanbeveling die we krijgen graag ter harte.”

1. Wat zal de minister ondernemen om de gemeentebesturen tot meer waakzaamheid op te roepen?
2. Wat is de stand van zaken betreffende het veiligheidsbewustmakingsprogramma waar de minister twee jaar geleden naar verwees?
3. Zijn er reeds stappen ondernomen om overheidspersoneel te sensibiliseren inzake de aangehaalde problematiek?

LIESBETH HOMANS

VICEMINISTER-PRESIDENT VAN DE VLAAMSE REGERING, VLAAMS MINISTER VAN BINNENLANDS BESTUUR, INBURGERING, WONEN, GELIJKE KANSEN EN ARMOEDEBESTRIJDING

ANTWOORD

op vraag nr. 18 van 29 september 2017

van **MICHEL DOOMST**

1. Zie mijn antwoorden op de vragen om uitleg nr. 78 en 143 zoals weergegeven op: <https://www.vlaamsparlement.be/commissies/commissievergaderingen/1198083/verslag/1199791>
Aanvullend zal Het Facilitair Bedrijf op de volgende werkgroep Informatieveiligheid van de VVSG het risico onder de aandacht brengen.
2. Zoals aangekondigd werd een informatieveiligheidsbewustmakingprogramma ontwikkeld in de vorm van een computer gebaseerde training (e-learning) waarin de belangrijkste elementen van veilig omgaan met Informatie en ICT-middelen wordt aangeleerd. Deze e-learning wordt uitgerold bij entiteiten van de Vlaamse overheid, en wordt ook aan lokale besturen ter beschikking gesteld. Het aanbod aan lokale besturen werd voorgesteld op de VVSG werkgroep Informatieveiligheid van 29 mei 2017. Een 10-tal lokale besturen hebben sinds deze e-learning al uitgerold, andere zijn aan het testen. Deze e-learning wordt kosteloos aangeboden.
Daarnaast werken wij ook met sensibiliseringsposters, op digitale mediaschermen en op papier. Met posters houden we het belang van informatieveiligheid in de aandacht en bestendigen we een veiligheidscultuur. Ook de posters bieden we aan aan de lokale besturen. Zo hebben we bijvoorbeeld begin oktober de poster rond 'phishing' uit de campagne in het kader van de Europese cybersecurity 'awareness' maand ook bezorgd aan VVSG (500 ex.) die ze ter beschikking stelt aan de lokale besturen.
3. Zowel op VO niveau als op het niveau van lokale besturen zijn werkgroepen actief die werken rond informatieveiligheid. De werkgroepen zijn samengesteld met veiligheidsconsulenten die het bestuur adviseren rond risico's (zoals cybercriminaliteit) en mitigerende maatregelen. Over het gebruik van HTTPS (en het belang ervan) werd binnen de Werkgroep Informatieveiligheid VO al een advies geformuleerd in maart 2016.