Vlaams Parlement

SCHRIFTELIJKE VRAAG

nr. 260
van **KATIA SEGERS**
datum: 21 februari 2019

---

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

URL-strategie Vlaamse overheid - Risico's, beveiliging en privacy

Met een URL-strategie voor de Vlaamse overheid wordt beoogd om gebruikers - zowel burgers als ondernemers - meer zekerheid en transparantie te bieden over wat de officiële kanalen van de overheid zijn. De URL-strategie wil bijdragen tot een consistenter geheel van websites en kanalen met een duidelijke hiërarchie en naamgeving en het voor gebruikers gemakkelijker en sneller maken om overheidsinformatie en -dienstverlening te vinden, te herkennen en te vertrouwen.

Uit de verschillende consultaties die omtrent de uitrol van een URL-strategie gehouden werden, kwamen een aantal bezorgdheden en opmerkingen naar voren. Die komen aan bod in de nota 'Een URL-strategie voor de Vlaamse overheid' (voorgelegd aan de Vlaamse Regering op 21 december 2018, pp. 2-3). Zo werd aangekaart dat door het gebruik van een reverse proxy mogelijk risico's zijn op het vlak van beveiliging en privacy. Dit wordt niet verder uitgediept in de nota, maar er wordt aangegeven dat een technische sessie verder zal ingaan op deze bezorgdheden.

1. Kan de minister toelichten welke concrete risico's verbonden zijn aan het gebruik van een reverse proxy, met name op het vlak van beveiliging en privacy?
2. Hoe plant men deze risico's op te vangen?
3. Heeft de technische sessie, waarvan sprake in de nota van 21 december 2018, ondertussen plaatsgevonden? Zo ja, wat is de uitkomst hiervan? Zo neen, wanneer staat die gepland?

Deze vraag werd gesteld aan de ministers Geert Bourgeois (191), Liesbeth Homans (260).

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

GECOÖRDINEERD ANTWOORD
op vraag nr. 260 van 21 februari 2019
van **KATIA SEGERS**

---

1. Een theoretisch risico is dat de data op reverse proxy-niveau door derden (onrechtmatig) worden uitgelezen.

2. De kans dat dit (zie 1) zich voordoet is echter minimaal omdat de reverse proxy automatisch alle onversleutelde data in het geheugen wist wanneer er een vermoeden is dat een onbevoegde de data op de geïmpacteerde server wil uitlezen. Op dat moment wordt de connectie tussen de bezoeker en website opgenomen door een andere reverse-proxyserver om de beschikbaarheid van de website niet in het gedrang te brengen. Om die reden wordt deze oplossing ook door veel internationale bedrijven en organisaties gebruikt voor hun digitale toepassingen.

3. De technische sessie zal plaatsvinden op 29 maart 2019.