Vlaams Parlement

SCHRIFTELIJKE VRAAG

nr. 437
van **CHRIS JANSSENS**
datum: 11 maart 2016

---

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

Cyberaanvallen op Vlaamse overheidswebsites - Impact en maatregelen

Websites en toepassingen van de Vlaamse overheid zijn onderhevig aan cyberaanvallen door hackers en andere cybercriminelen. Er wordt een onderscheid gemaakt tussen aanvallen die erop gericht zijn om de sites te doen crashen en aanvallen die erop gericht zijn om in te dringen, informatie te ontvreemden, enzovoort.

Zware DoS-aanvallen (Distributed DoS) kunnen in principe enkel ontzenuwd worden door de internetprovider. Lichte DoS-aanvallen worden normaliter door de firewalls van de Vlaamse overheid zelf geblokkeerd.

Binnen de Vlaamse overheid bepaalt de entiteit die eigenaar is van een website of toepassing of de veiligheidsmaatregelen die nodig zijn in overeenstemming zijn met de classificatie van de site of toepassing en de informatie die ze bevat. De classificatie van informatie is opgenomen in het generieke ICT-veiligheidsbeleid, maar er is dus niet éénzelfde beveiligingsniveau voor alle sites van de Vlaamse overheid.

Ik stel de minister voor de domeinen en entiteiten die onder zijn/haar bevoegdheid vallen graag volgende vragen.

1. Hoeveel (pogingen tot) cyberaanvallen op websites en infrastructuur van de overheidsdiensten en -entiteiten waarvoor de minister bevoegd is, vonden plaats in 2014 en 2015? Kan daarbij een onderscheid gemaakt worden tussen aanvallen die erop gericht zijn om de sites te doen crashen en aanvallen die erop gericht zijn om in te dringen, informatie te ontvreemden, enzovoort. Kan de minister daarvan een overzicht geven per entiteit?

    a) Kan de minister meedelen in het geval van cyberaanvallen die erop gericht zijn om sites te doen crashen, in welke mate dit effectief geleid heeft tot geïnfecteerde of gecrashte systemen?

    b) Kan de minister meedelen in het geval van cyberaanvallen die erop gericht zijn om toegang te krijgen tot overheidsinformatie of computersystemen, in welke mate er effectief informatie/data ontvreemd werden?

2. Kan de minister meedelen wat de financiële repercussies van deze aanvallen waren? Hoeveel bedroeg de opgelopen schade aan eigendommen van de Vlaamse overheid?

3. Wat waren de eventuele gevolgen van die aanvallen voor het functioneren van de websites?

4. Kan de minister meedelen in welke mate aanvallen tegen websites van de (entiteiten behorend tot de) Vlaamse overheid dankzij bestaande procedures geen schade hebben kunnen veroorzaken? Heeft de minister daar cijfers over?

5. Wat is de voorbije jaren de tendens van het aantal aanvallen?

6. Gelden vandaag voor alle websites van de Vlaamse overheid bepaalde veiligheidsregels (en welke)? Wordt de beveiliging voor elke website in 2016 op dezelfde manier gerealiseerd? Worden er mogelijk nog bijkomende veiligheidsmaatregelen genomen?

7. Wie staat in voor de beveiliging van de verschillende sites? Is er een gemeenschappelijke ICT-dienstverlener voor websites van (entiteiten van) de Vlaamse overheid?

8. Hoeveel experts in cyberaanvallen zijn er bij de (entiteiten van de) Vlaamse overheid tewerkgesteld?

9. Welk beveiligingsniveau geldt voor de websites? Werd er een kwetsbaarheidsanalyse uitgevoerd op de websites (voorafgaand het ontsluiten op het internet of nadien (bijvoorbeeld omwille van een cyberdreiging of zelfs -aanval)? Zo neen, waarom niet? Zo ja, wat was daarvan het resultaat?

10. Welk budget werd in 2014 en 2015 besteed aan de beveiliging en het beheer van de overheidswebsites en eventuele investeringen in beveiligingstechnologie? Welk budget is daarvoor gereserveerd in 2016?

11. Welke maatregelen zullen worden genomen om het gevaar voor cyberaanvallen op websites van de Vlaamse overheid zo veel mogelijk te beperken?

Deze vraag werd gesteld aan de ministers Geert Bourgeois (248), Hilde Crevits (275), Annemie Turtelboom (205), Liesbeth Homans (437), Ben Weyts (808), Jo Vandeurzen (413), Philippe Muyters (402), Joke Schauvliege (515), Sven Gatz (191)

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

GECOÖRDINEERD ANTWOORD
op vraag nr. 437 van 11 maart 2016
van **CHRIS JANSSENS**

---

1. Om deze vraag te kunnen beantwoorden, en vooral wanneer we de getallen willen vergelijken met het aantal cyberaanvallen op andere overheidsdiensten, is een eenduidige definitie nodig van het begrip 'cyberaanval'. Er bestaat immers een grote variatie in incidenten die als aanval zouden kunnen geclassificeerd worden: een groot aantal incidenten zijn een vorm van verkenning door de aanvaller (waarbij bv. gezocht wordt naar open poorten door de firewall). Daarnaast zijn andere aanvallen erop uit om een dienst onderuit te halen ('Denial of Service' of DoS-aanval). Nog andere aanvallen proberen effectief in te breken in het netwerk of in een systeem. Een virus dat naar een PC wordt gestuurd kan ook onderdeel zijn van een cyberaanval (denk bv. aan de beruchte 'ransomware'). Als men ook het aantal geblokkeerde virussen en spam (waaronder 'phishing') mails rapporteert als 'cyberaanval' komen we meteen tot grote aantallen van cyberaanvallen (vele duizenden).
   Wat we kunnen stellen is dat we in de voorbije jaren binnen de Gemeenschappelijke ICT-dienstverlening gemiddeld een 10-tal incidenten per week diepgaander onderzoeken. Dat zijn de meer ernstige pogingen van cyberaanvallen (zoals bv. een 'SQL Injection' aanval om in een website in te breken) die weliswaar afgewend (geneutraliseerd) werden door de verschillende geïnstalleerde beveiligingssystemen, maar die de moeite waard zijn om verder te laten onderzoeken door een security-analist om eruit te leren en waar nodig de beveiliging aan te passen, of als nazorg om 100% zeker te zijn dat de aanval succesvol werd afgeblokt. Dit aantal is stabiel over de voorbije jaren.

   a) In de maand januari 2016 hebben we enkele 'Denial of Service' aanvallen tegen de Vlaamse overheid vastgesteld, maar deze waren niet in staat onze infrastructuur onderuit te halen.

   b) Wij hebben geen kennis van (succesvolle) aanvallen die effectief tot een data-lek geleid hebben.

2. Een aantal security incidenten die ook als cyberaanval kunnen aanzien worden en die wel al enkele keren tot schade hebben geleid bij de Vlaamse overheid waren ten gevolge van computers die geïnfecteerd geraakten met ransomware. Daarbij worden de bestanden in de mappen van de gebruiker versleuteld. In de gevallen die ons bekend zijn, konden de bestanden wel hersteld worden d.m.v. de back-up, en is de schade beperkt tot een tijdelijke technische werkloosheid van de gebruiker (tijdens het herstellen van de computer) en de kost om de bestanden terug te zetten. Deze kost is ten laste van de ICT-Dienstverlener.

3. Cfr. Vraag 1a: De 'Denial of Service' aanvallen die we in januari ondervonden waren niet sterk genoeg om de websites onderuit te halen. De sites zullen op dat ogenblik wel tragere antwoordtijden gekend hebben.

4. Een doeltreffende beveiliging is gebaseerd op technische en organisatorische maatregelen. De doeltreffendheid van organisatorische maatregelen zijn zeer moeilijk te meten (bv. hoeveel aanvallen zijn afgewend doordat gebruikers veiligheidsbewustmaking training kregen), maar het is duidelijk dat door de technische

controlemaatregelen (antivirus, firewall, intrusion prevention systeem, ...) dagelijks aanvallen afgewend worden. Omdat een doeltreffende beveiliging gelaagd is ('layered defense') is het daarbij niet zeker dat de firewall of het intrusion prevention systeem eventuele schade heeft voorkomen door een aanval al aan de internet perimeter (buitengrens) af te wenden. De website of toepassing moet ook ontwikkeld zijn volgens de beste praktijken (bv. bestand tegen de OWASP top 10 kwetsbaarheden), en het systeem waar het op gehost is, moet zelf 'gehard' zijn, dat wil zeggen enkel die 'services' draaien die noodzakelijk zijn, en voorzien van de meest recente security patches.

5. De Vlaamse overheid is in het verleden vrij zelden geconfronteerd met 'Denial of Service' aanvallen, maar we hebben er enkele ervaren in januari en wereldwijd is dergelijk type aanval in opmars, dus we houden die tendens in het oog. De grootste kwetsbaarheid (m.b.t. de beveiliging van netwerken) situeert zich in de computers van de gebruikers, en kwetsbaarheden in de standaard software die erop gebruikt wordt (het operating systeem, de browser en browser extensies, enz). We zien een duidelijke toename het voorbije jaar in cyberaanvallen die - via email - malware (zoals ransomware) versturen in de vorm van een schijnbaar onschuldig document.

6. Het is aan de eigenaar van de website om, vertrekkende van de classificatie van de informatie die verwerkt wordt, rekening te houden met eventueel van toepassing zijnde beleidslijnen en wetgeving (bv. KSZ normen, privacywetgeving) en rekening houdend met de stand van de technologie, de juiste keuzes te maken m.b.t. de toe te passen beveiligingsmaatregelen. De beveiliging is dus niet dezelfde voor elke website. Sommige websites staan ook in de 'cloud' bij externe dienstverleners waar bepaalde beveiligingsdiensten inbegrepen zijn in de dienstverlening. In diverse fora en werkgroepen worden wel belangrijke aspecten besproken voor het ontsluiten van websites met de gepaste beveiliging.

7. Er is niet één enkele (exclusieve) ICT-dienstverlener voor websites. Er zijn wel verschillende raamcontracten die hosting diensten aanbieden, waar een aantal beveiligingsaspecten in zijn voorzien. In geval van clouddiensten is het de cloud-aanbieder die instaat voor de beveiliging van de dienst, website of toepassing.

8. De Vlaamse overheid heeft een goede kennis over cyberveiligheid maar heeft zelf geen experts in cyberaanvallen (zoals forensische specialisten) in dienst. De Vlaamse overheid werkt via outsourcing contracten met ICT-dienstverleners die de nodige experts ter beschikking stellen. Voor de gemeenschappelijke ICT-Dienstverlening gaat dit over een team van netwerkspecialisten, malware-analisten, netwerk- en security architecten, en forensische experten. In totaal gaat dit over een 10-tal mensen in de front-office (mensen waarmee we in contact zijn) en een grotere pool waarop aanspraak kan gemaakt worden wanneer het nodig zou zijn.

9. Er wordt een kwetsbaarheidsanalyse op applicatie-niveau aangeboden in de offertefase van een project en - indien besteld door de entiteit - uitgevoerd vooraleer de site of toepassing wordt ontsloten. Kwetsbaarheden, die gevonden worden in de kwetsbaarheidsanalyse, worden gecorrigeerd vooraleer de site 'live' gaat. Minstens één maal per jaar worden er door de ICT-dienstverlener systeem kwetsbaarheidsscans uitgevoerd (die controleren hoofdzakelijk een systeem op het niveau van het operating systeem).

10. De budgetten bestaan uit wederkerende kosten, en investeringen (projecten):

    - De totale wederkerende kost bestaat uit verschillende onderdelen (beheer, hardware- en softwareonderhoud) verdeeld over verschillende kostenplaatsen. In het nieuwe ICT-contract worden minder kosten centraal gedragen dan voorheen, dat maakt een exacte becijfering moeilijk. De kost voor het beheer van de

belangrijkste centrale veiligheidscomponenten (firewalls, identiteits- en toegangscontrolesysteem, enz.) en de antivirussoftware kost samen kan geraamd worden op 221.000 euro per maand.

- De éénmalige investeringen in nieuwe beveiligingstechnologie verlopen meer pieksgewijs en variëren per jaar. Voor 2015 is dit berekend op 2.288.000 euro, en voor 2014 is dit berekend op 2.805.000 euro.

De werkelijk totale kost die kan toegewezen worden aan de beveiliging van websites ligt nog hoger, aangezien hier nog andere componenten aan toegevoegd kunnen worden, zoals het deel van de ontwikkelkost van een site die te maken heeft met veiligheid.

11. Er loopt op dit ogenblik een onderzoek om de websites van de Vlaamse overheid beter te beschermen tegen 'Distributed Denial of Service' (DDoS) aanvallen. Er zal ook nagegaan worden of er zinvolle gemeenschappelijke richtlijnen en procedures kunnen ontwikkeld worden op vlak van beveiliging van websites, die VO-breed kunnen aangereikt worden.