Vlaams Parlement

SCHRIFTELIJKE VRAAG

nr. 427
van **MARNIC DE MEULEMEESTER**
datum: 9 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 - Maatregelen en budgetten

Onlangs raakt bekend dat het aantal cyberaanvallen op de federale overheidsdiensten (FOD's) toeneemt. In 2014 waren er 405, vorig jaar 666, dus ongeveer twee per dag. De aanvallen worden ook professioneler en complexer. Hackers creëren steeds meer virussen om specifieke overheidsnetwerken binnen te dringen.

Om het probleem aan te pakken werd vorig jaar het Centrum voor Cybersecurity België opgericht. Het centrum staat in voor het afweren en onderzoeken van grootschalige digitale aanvallen. De voorbije maanden zijn er echter erg weinig meldingen gedaan bij het centrum.

1. Heeft de minister zicht op het aantal cyberaanvallen op Vlaamse overheidswebsites? Zo ja, over hoeveel aanvallen gaat het in de voorbije vijf jaar (overzicht per jaar graag)?
2. Welke maatregelen heeft de minister al genomen of denkt zij te nemen om de Vlaamse diensten beter te beschermen tegen deze aanvallen?
3. Welke budgetten worden er jaarlijks vrijgemaakt voor cyberbeveiliging (graag een overzicht van de laatste 5 jaar)?
4. Is er een samenwerking met het nieuwe Centrum voor Cybersecurity België?

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

ANTWOORD
op vraag nr. 427 van 9 maart 2016
van **MARNIC DE MEULEMEESTER**

---

1. Er is geen eenduidige definitie van het begrip 'cyberaanval'. Er bestaat immers een grote variatie: 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).

   Binnen de Gemeenschappelijke ICT-dienstverlening zijn er gemiddeld een 10-tal incidenten per week die verder onderzocht worden. Dit zijn de meer ernstige pogingen van cyberaanvallen (zoals bv. een aanvalspoging 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.

2. Binnen het Gemeenschappelijke ICT-dienstenaanbod monitort en evalueert de Vlaamse overheid actief het dreigingsniveau en de toegepaste aanvalsmethoden. Ze past waar nodig haar beveiligingsstrategie en veiligheidsplan aan, rekening houdend met de stand van de technologie. Dit is een permanent proces. Deze bijsturingen kunnen leiden tot bijkomende investeringen maar ook tot het aanpassen van bestaande veiligheidscomponenten, het sensibiliseren van personeelsleden van de Vlaamse overheid (veiligheidsbewustmaking) of het bijsturen van bepaalde processen.

   In de voorbije jaren werd fors geïnvesteerd in firewalls van de nieuwe generatie, die beter in staat zijn om aanvallen te herkennen en af te slaan. Er werd een maatregel ingevoerd om te voorkomen dat gebruikers potentieel schadelijke bestanden kunnen downloaden. Er is regelmatig overleg met cybersecurity specialisten om controlemaatregelen te implementeren die geavanceerde malware te kunnen detecteren. Er loopt op dit ogenblik ook een onderzoek om de websites van de Vlaamse overheid beter te beschermen tegen 'Distributed Denial of Service' (DDoS) aanvallen. In de schoot van de Werkgroep 'Informatieveiligheid VO' wordt een opleiding uitgewerkt, die nog dit jaar wordt aangeboden aan de werknemers om hun kennis over informatie- en cyberveiligheid te verbeteren, alsook om hun weerbaarheid tegen cyberaanvallen die de menselijke factor uitbuiten, (bv. 'phishing') te versterken.

3. De budgetten bestaan uit wederkerende kosten, en investeringen (projecten):
   - 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, en aanverwante ontwikkelings- en infrastructuurprojecten verlopen pieksgewijs en variëren per

jaar. Voor 2015: 2.288.000 euro, voor 2014: 2.805.000 euro, voor 2013: 2.189.000 euro, voor 2012: 741.000 euro en in 2011 2.302.000 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.

4. Er is geen formeel samenwerkingsakkoord met het nieuwe Centrum voor Cybersecurity België, maar er is wel spontaan en sporadisch overleg tussen CERT.be (onderdeel van het Centrum voor Cybersecurity België) en de Vlaamse overheid. Zo heeft de Vlaamse overheid al enkele malen informatie m.b.t. cyberveiligheid aan het CERT.be bezorgd, en werd recent vanuit het CERT.be nog herbevestigd dat relevante informatie over belangrijke bedreigingen of incidenten aan de Vlaamse overheid worden meegedeeld.