Vlaams Parlement

SCHRIFTELIJKE VRAAG

nr. 75
van **JO BROUNS**
datum: 21 oktober 2020

---

aan **BEN WEYTS**
VICEMINISTER-PRESIDENT VAN DE VLAAMSE REGERING, VLAAMS MINISTER VAN ONDERWIJS, SPORT, DIERENWELZIJN EN VLAAMSE RAND

Cyberaanvallen op scholen - Maatregelen

Scholen lijken wel het mikpunt van cyberaanvallen. Meerdere keren per week verschijnen berichten van scholen die getroffen worden door een cyberaanval. Recentelijk was ook de AP Hogeschool het doelwit. Door de aanval werkten de e-campus en administratieve systemen van de hogeschool niet. De hogeschool moest noodgedwongen tijdelijk sluiten en de geplande lessen gingen zoveel mogelijk online door. Dat is slechts één voorbeeld.

1. Hoeveel cyberaanvallen op onderwijsinstellingen zijn er de laatste 5 jaar geweest? Graag een opsplitsing in basisscholen, secundaire scholen en hogescholen per provincie.
2. Is er onderzoek gebeurd of gepland naar de verschillende cyberaanvallen in Vlaamse scholen?
3. Zijn er patronen te ontdekken in de gebruikte methoden?
4. Heeft de minister zicht op de extra kosten voor de scholen die gepaard gaan met een cyberaanval? Of beter, wat is de kostprijs per school van een cyberaanval?
5. Zijn er dossiers bekend waarbij door scholen losgeld is betaald om de hacking ongedaan te maken?
6. Zijn er dossiers bekend waarbij data permanent verloren zijn gegaan?
7. Hoe zal de minister de scholen verder ondersteunen bij de uitbouw van cyberveilighied? Denkt de minister eventueel aan bijkomende maatregelen?
8. In welk budget voorziet de minister ter ondersteuning van de scholen?

BEN WEYTS
VICEMINISTER-PRESIDENT VAN DE VLAAMSE REGERING EN VLAAMS MINISTER VAN ONDERWIJS, SPORT, DIERENWELZIJN EN VLAAMSE RAND

ANTWOORD
op vraag nr. 75 van 21 oktober 2020
van **JO BROUNS**

---

1. Ik beschik niet over dergelijke data. Deze worden niet centraal gerapporteerd, noch bijgehouden. Meldingen van privacy inbreuken moeten steeds wettelijk verplicht gedaan worden bij de gegevensbeschermingsautoriteit. Deze publiceert echter geen gegevens per sector.

2. IT-beveiliger Kaspersky heeft recent een overzicht gepubliceerd over het aantal cyberaanvallen in het onderwijs wereldwijd. Vooral het aantal DDoS-aanvallen op elektronische leeromgevingen is met 350% toegenomen. Het gaat hier om cyberaanvallen waarbij ontzettend veel verkeer naar computers, computernetwerken of servers worden verstuurd waardoor deze onbruikbaar worden voor de normale gebruiker. Je kunt dit vergelijken met een file, maar dan digitaal.

3. Een voor de hand liggende verklaring is dat de grote toename van aantal cyberaanvallen op leeromgevingen samenhangt met de transitie naar online onderwijs.

4. Uit het onderzoek van Kaspersky blijkt dat de aanvallen die vaak voorkomen het soort aanvallen zijn die ook in de rest van de maatschappij veel voorkomen. Scholen zijn dan het slachtoffer van DDOS-aanvallen die louter bedoeld zijn om een netwerk plat te leggen. Daarnaast zijn er ook phishingaanvallen met als doel geld af te troggelen en aanvallen via ransomwhere (een programma dat een computer of gegevens die erop staan blokkeert en vervolgens van de gebruiker geld vraagt om de computer weer te `bevrijden).

   Cybercriminelen kiezen soms voor educatieve campussen omdat die een meer open netwerkstructuur hebben, met veel gebruikers en eigen devices. Daarnaast hebben scholen vaker verouderde netwerkapparatuur.

5. Scholen kunnen best nooit 'losgeld' betalen aan hackers om gegijzelde data terug te krijgen. Vaak is de kostprijs dan een herinstallatie van de geïnfecteerde schoolcomputers. Dit vraagt vooral tijd en inzet van de aanwezige ICT-coördinatoren.

   Na een cyberaanval zetten scholen vaak wel in op een betere opleiding van hun personeelsleden in cybersecurity. Niet enkel de ICT-coördinator, maar ook de leerkrachten zijn het slachtoffer van phishing aanvallen voor het ontfutselen van wachtwoorden en gegevens. Scholen zetten nadien ook in op een beter cybersecurity beleid en beleidsregels die vaak in scholen nu niet aanwezig zijn. Uiteraard zetten scholen dan steeds meer middelen in voor betere hardware en antivirussoftware.
   Scholen kiezen ook voor een cloudstrategie waar men dan rekent op een externe partner voor de beveiliging van hun data en devices. Lokale servers met belangrijke data vaak moeilijker te beveiligen en te onderhouden dan een cloudserver.

6. Ik heb daar geen weet van. Maar zoals gezegd is een volledig overzicht niet beschikbaar.

7. Ik heb daar geen weet van. Maar zoals gezegd is een volledig overzicht niet beschikbaar.

8. Er zijn al heel wat lopende maatregelen:
    - Bij de herziening van de eindtermen voor de eerste graad SO is er veel aandacht voor ICT-eindtermen, digitale competenties en mediawijsheid. Deze zijn ook opgenomen in het luik basisgeletterdheid. Aandacht voor ICT-veiligheid, privacy, bescherming van data, enz. maken daar ook deel van uit.

    - KlasCement bevat rond dataveiligheid en cybersecurity aparte themapagina's met heel wat bruikbare ondersteuningsmaterialen voor scholen: https://www.klascement.net/ict

    - Ik werk samen met het Kenniscentrum Mediawijs waarbij materialen, vorming en advies verstrekt wordt rond mediageletterdheid. Thema's die daarbij o.a. aan bod komen, zijn: beeldgeletterdheid, sexting, cyberpesten, enz. In dit kader wordt ook vorming voorzien via de Mediacoachopleiding.

    - Via het 'esafety Label' kunnen scholen de sterktes en zwaktes van hun ICT-veiligheidsbeleid in kaart brengen. Het eSafety Label evalueert op 3 niveaus: infrastructuur, beleid en klaspraktijk.

    - Er is een werkgroep die werd opgericht n.a.v. de inwerkingtreding van de AVG die alle actoren samenbrengt en het overleg tussen hen faciliteert. Relevante info wordt gedeeld op een gemeenschappelijke website. https://www.privacyinonderwijs.be

    - Er is een traject opgestart bij leveranciers van digitale onderwijsdiensten om hun toepassing te ontsluiten met multi-factorauthenticatie in samenwerking met het Ministerie van Onderwijs en het Facilitair bedrijf.

    - De raamovereenkomst met Telenet (Telenet Schoolnet+) bevat heel wat beveiligingsopties zoals online back-up en managed firewall

9. In juli werd een generieke ICT-impuls van 35 miljoen euro uitgekeerd voor ICT-ondersteuning. Investeringen in cybersecurity kunnen daar mee bekostigd worden.
   Daarnaast werk ik aan een plan digitalisering van het onderwijs. Het aandeel ICT-infrastructuurmiddelen daarin moet nog worden beslist, maar ook hier zal ruimte en aandacht zijn voor ICT-veiligheid.