

**SCHRIFTELIJKE VRAAG**

nr. 503

van **TOM SEURS**

datum: 6 februari 2026

---

aan **ZUHAL DEMIR**

VLAAMS MINISTER VAN ONDERWIJS, JUSTITIE EN WERK

---

*Onderwijs - Cyberveiligheid en bescherming persoonsgegevens*

Recent kwam een ernstige cyberaanval op een Vlaamse school in het nieuws, waarbij ransomware werd ingezet en cybercriminelen niet alleen de school, maar ook ouders rechtstreeks benaderden met afpersingsmails. Daarbij werd gedreigd met het verspreiden van gevoelige persoonsgegevens van leerlingen, ouders en personeelsleden.

Dit incident illustreert dat onderwijsinstellingen, net als andere publieke organisaties, steeds vaker het doelwit worden van cybercriminaliteit. Tegelijk verwerken scholen grote hoeveelheden gevoelige data, vaak over minderjarigen, wat de impact van zulke aanvallen bijzonder groot maakt. Het is daarom essentieel dat scholen voldoende weerbaar zijn, en dat ze bij incidenten kunnen rekenen op duidelijke procedures en ondersteuning.

1. Hoe beoordeelt de minister de huidige cyberveiligheid van Vlaamse onderwijsinstellingen, en welke minimale beveiligings- en preventiemaatregelen verwacht ze vandaag van scholen bij het beheer van gevoelige persoonsgegevens?
2. In welke ondersteuning en richtlijnen voorziet Vlaanderen vandaag voor scholen bij cyberincidenten, zowel op het vlak van preventie als op het vlak van crisisbeheer en communicatie met ouders en personeel? Ziet de minister nood aan verdere versterking?
3. Hoe verloopt de samenwerking tussen onderwijsinstellingen en instanties zoals het Centrum voor Cybersecurity België en de Gegevensbeschermingsautoriteit, en acht de minister de bestaande meld- en opvolgingsprocedures voldoende duidelijk voor het onderwijsveld?



**Vlaams  
Parlement**

**ZUHAL DEMIR**

VLAAMS MINISTER VAN ONDERWIJS, JUSTITIE EN WERK

---

**ANTWOORD**

op vraag nr. 503 van 6 februari 2026

van **TOM SEURS**

---

Het departement, in het bijzonder het kenniscentrum Digisprong, werkte het [actieplan cybersecurity](#) uit voor het Vlaamse onderwijs. Een belangrijke actie erin is het Groeipad Informatieveiligheid en Privacy ([GRIP](#)), waarbinnen scholen geïnformeerd en ondersteund worden over technische en organisatorische maatregelen om een basisniveau cybersecurity te halen, conform de Algemene Verordening Gegevensbescherming (AVG).

Eind 2025 startten de eerste 50 scholen met de ondersteunende [GRIPA applicatie](#), die handvatten biedt voor elke stap van het GRIP. Via de onderwijsverstrekkers en koepels worden scholen begeleid om GRIP en GRIPA te integreren in hun ICT-beleidsplan. Pas bij een hogere integratiegraad kunnen we het cyberveiligheidsniveau van scholen betrouwbaar inschatten. Ik wens erop te wijzen dat het gebruik van GRIPA of een andere tool ter opvolging van het cyberveiligheidsniveau niet verplicht is.

In 2026 wordt onderzocht of het onderwijs kan aansluiten bij het [Vlaamse CERT van het Vlaamse Centrum voor Digitale Veiligheid](#) dat momenteel nog wordt opgebouwd. Een CERT, of *Cyber Emergency Response Team*, is een team dat organisaties helpt bij cyberincidenten. Dat moet ervoor zorgen dat scholen sneller hulp krijgen wanneer er problemen zijn. Dat wil niet zeggen dat ze het van de school overnemen. Ze zorgen ervoor dat de aanval stopt, informeren scholen over de verplichtingen die ze hebben en ondersteunen bij de stappen naar heropstart. Er zijn heel wat opportuniteiten in de CERT-werking. Het biedt de mogelijkheid meldingen beter te bundelen, zodat dreigingen sneller opgemerkt worden. Hieruit kunnen ook andere scholen geïnformeerd worden over voorzorgen die ze kunnen nemen ter preventie tegen actuele aanvallen.

Scholen staan niet alleen bij cyberincidenten. Op dit moment kunnen scholen een beroep doen op bestaande instanties zoals het centrum voor cybersecurity België (CCB), het Vlaamse CERT en de begeleidingsdiensten van de koepels wanneer er zich incidenten voordoen. Er is ook een overkoepelende samenwerking met het [Vlaamse Centrum voor Digitale Veiligheid](#) van Digitaal Vlaanderen. De samenwerking met Gegevensbeschermingsautoriteit (GBA) is eerder minimaal omdat de Vlaamse toezichtcommissie (VTC) als controleorgaan geldt voor de toepassing van de AVG.

Ook voor het uitdenken van ondersteuningsmaatregelen, doe ik beroep op specialisten en partners. Zo werd het actieplan cybersecurity opgesteld in samenwerking met de onderwijsverstrekkers, directies, ICT-coördinatoren, leraren en enkele EdTech-leveranciers. Voor de bepaling van het basisniveau cybersecurity in het onderwijs is het GRIP uitgegaan van het [CyberFundamentals Framework](#) van het CCB.

Ik ben het volmondig eens met de stelling dat de cyberveiligheid in scholen moet verhogen. Samen met de partners helpt het GRIP de komende drie jaar de maturiteit van scholen te verhogen, op hun tempo en met zo min mogelijk planlast. Bijsturing zal altijd nodig blijven aangezien cyberdreigingen evolueren. Het werk is in die zin nooit klaar.