

Vergaderjaar 2025–2026

29 240

Veiligheid op school

26 643

Informatie- en communicatietechnologie (ICT)

31 293

Primair Onderwijs

31 289

Voortgezet Onderwijs

Nr. 177

BRIEF VAN DE STAATSSECRETARIS VAN ONDERWIJS, CULTUUR EN WETENSCHAP

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 5 november 2025

Digitale veiligheid wordt steeds belangrijker, ook in het funderend onderwijs.

Technologische ontwikkelingen gaan snel en dreigingen nemen toe, zo blijkt uit het Dreigingsbeeld Cybersecurity 2025 dat ik op 27 oktober van Kennisnet heb ontvangen.¹ Sinds het vorige dreigingsbeeld uit 2023 is er een toename in het aantal aanvallen op het primair en voortgezet onderwijs. Het uitvoeren van aanvallen wordt steeds eenvoudiger en goedkoper terwijl aanvallen tegelijkertijd moeilijker te herkennen zijn.

In 2025 vonden in Nederland meerdere digitale aanvallen plaats die impact hadden op schoolprocessen en bedrijfsvoering. Dit had gevolgen voor de continuïteit van het onderwijs en leidde in sommige gevallen tot financiële schade en datalekken. Ik heb recent gesproken met ICT-coördinatoren die dit zelf hebben ervaren en heb gehoord hoe complex het voor scholen is om dit te voorkomen en op te lossen.

Schoolbesturen moeten maatregelen treffen om incidenten te voorkomen en adequaat handelen wanneer zich toch een incident voordoet. Ze zijn daar in de eerste plaats zelf verantwoordelijk voor, maar ik zie ook dat dit een hele opgave is. Om scholen hierbij te ondersteunen is in 2023 het programma Digitaal Veilig Onderwijs (DVO) gestart. In dit programma werkt OCW samen met de PO-Raad, VO-raad, Kennisnet en SIVON aan het verhogen van digitale veiligheid in het funderend onderwijs.

In de eerste drie jaar heeft het programma een aantal belangrijke stappen gezet, waaronder het opstellen van het Normenkader Informatiebevei-

¹ <https://www.kennisnet.nl/informatiebeveiliging-en-privacy/dreigingsbeeld-primair-en-voortgezet-onderwijs-2025-kwetsbaarheden-herkennen-veiligheid-verhogen/>

liging en Privacy Funderend Onderwijs en het oprichten van het School-CERT.² Daarmee is er een standaard ontwikkeld die duidelijk maakt wat een schoolbestuur moet doen om digitaal veilig te zijn.

Alle leerlingen in het funderend onderwijs hebben recht op een digitaal veilige leeromgeving. Het is daarom belangrijk dat ieder schoolbestuur met het normenkader aan de slag gaat. Uit nulmetingen door het programma DVO blijkt dat schoolbesturen nog veel te doen hebben en nog niet op alle normen voldoen aan het streefniveau.^{3, 4} En dat is wel nodig.

Digitale veiligheid vraagt om integrale aanpak met maatregelen ten aanzien van techniek, organisatie en personeel. Daarom heb ik met de PO-Raad en de VO-raad afgesproken dat ieder schoolbestuur in 2027 weet waar het staat ten opzichte van het normenkader en een plan heeft uitgewerkt hoe aan alle normen gaat worden voldaan. In 2030 dienen schoolbesturen daadwerkelijk te voldoen aan de normen uit het normenkader.

Ik besef dat dit veel inspanningen vraagt van scholen. Daarom verleng ik het programma DVO met drie jaar, tot en met 2029, en stel ik voor die periode jaarlijks € 7,2 mln beschikbaar. Ook verleng ik de subsidie voor de dienst Veilig Internet van SIVON en Kennisnet tot medio 2030. Ik stel daarvoor in totaal € 22,2 mln beschikbaar zodat de dienst verder ontwikkeld kan worden en meer schoolbesturen kunnen aansluiten. Veilig en betrouwbaar internet is een belangrijke randvoorwaarde voor digitaal veilig onderwijs.

Het programma DVO gaat hiermee een nieuwe fase in. Naast het bestaande aanbod van o.a. handreikingen, verdiepende workshops en hulp bij incidenten en dreigingen, richt het programma zich in de nieuwe fase ook op:

- Gerichte ondersteuning voor scholen, met extra aandacht voor achterblijvers, maatwerk en regionale samenwerking. Bijvoorbeeld in de vorm van gezamenlijke inkoop of inhuur van IT-expertise;
- Het vergroten van inzicht in waar individuele schoolbesturen staan en waar de sector staat, o.a. via periodieke monitoring en zelfevaluatie;
- De verantwoording die scholen afleggen over hun digitale veiligheid.

Digitale veiligheid mag niet vrijblijvend zijn en heeft daarom ook een plek in de verantwoordingscyclus van schoolbesturen. Zij zijn sinds verslagjaar 2024 verplicht om in hun jaarverslag te schrijven over wat ze doen aan informatiebeveiliging en privacy. Daarnaast heb ik met de PO-Raad en VO-raad afgesproken dat digitale veiligheid een vast onderdeel is in het intern toezicht.

De Inspectie van het Onderwijs kan in het kader van haar stimulerende taak in gesprek gaan met schoolbesturen over digitale veiligheid, bijvoorbeeld op basis van het plan dat elk schoolbestuur in 2027 o.b.v. het normenkader opstelt. Maar ik vind het ook belangrijk dat de Inspectie, als sluitstuk van de in deze brief geschetste aanpak, op termijn kan interveniëren bij scholen en besturen waar de aandacht voor digitale

² <https://www.kennisnet.nl/diensten/school-cert/>

³ <https://www.digitaalveiligonderwijs.nl/achtergrond-en-onderzoek/>

⁴ Het normenkader bestaat uit 69 normen voor informatiebeveiliging en 25 normen voor privacy. Per norm zijn er vijf volwassenheidsniveau's beschreven waarbij niveau 3 het streefniveau is. Op dat niveau zijn maatregelen gedocumenteerd en worden ze consistent toegepast. Daarmee wordt kans en impact van incidenten aanzienlijk verminderd.

weerbaarheid en veiligheid achterblijft. Daarbij streef ik zoveel mogelijk naar vergelijkbaarheid met de andere onderwijssectoren. Daarom verken ik de mogelijkheden om de bevoegdheid van de Inspectie ten aanzien van dit onderwerp vast te leggen. Digitale weerbaarheid en veiligheid zijn immers onmisbaar voor de borging van de continuïteit en daarmee ook de kwaliteit van het onderwijs.

De Staatssecretaris van Onderwijs, Cultuur en Wetenschap,
K.M. Becking