|  |
| --- |
| **Primair Onderwijs**  **Van**  T |
| **Bijlagen**  1 |
| **Aantal pagina’s**  1 |

Het KRO PO/VO wordt gevraagd akkoord te gaan met:

1. Een **opdracht** aan Edustandaard om de nieuwe WDO-beveiligingsstandaarden en bestaande toegangstandaarden op te nemen in de ROSA. Dit is in lijn met de Europese Toegankelijkheidsrichtlijnen die inmiddels zijn opgenomen in de ROSA.
2. Een **adviesverzoek** aan Edustandaard over hoe nu en in de toekomst de implementatie van en toezicht op WDO-standaarden en onderwijsstandaarden in het algemeen kan worden georganiseerd.
3. **Besluitvorming** in het KRO PO/VO over de implementatie van en het toezicht op de standaarden, waarbij rekening wordt gehouden met de rol van SIVON en financiële randvoorwaarden

**Aanleiding**

In de Wet Digitale Overheid (WDO) worden beveiligingsstandaarden verplicht gesteld door de minister van BZK voor de overheid en organisaties met een publieke taak. Doel is op stelselniveau eenduidige normen te geven voor een minimaal beveiligingsniveau. Individuele organisaties (ook schoolbesturen) zijn al verantwoordelijk om passende beveiligingsmaatregelen te nemen. Dit laat nu nog (te veel) ruimte om te bepalen wat passend is. Ook is bij samenwerking in ketens een organisatie afhankelijk van de maatregelen van een ketenpartner. De zwakste schakel bepaalt daarmee de kwaliteit van de totale informatiebeveiliging. DUO dwingt daarom in de relatie met leveranciers het gebruik van beveiligingsstandaarden af. Schoolbesturen zouden dat in hun contracten met ICT-leveranciers ook moeten doen.

**Doel bespreekpunt**

De standaardisatieraad is de plek waar de standaarden worden vastgesteld. Dat gebeurt in een publiek-private setting. De standaardisatieraad is tegelijkertijd (te) vrijblijvend. Op dit moment worden daar geen (bestuurlijke) afspraken gemaakt over daadwerkelijke invoering van standaarden. Voor de invoering wordt bijvoorbeeld gekeken naar Edu-k. Maar ook in Edu-k leidt dit tot een gesprek over verantwoordelijkheden en geld (subsidie). En Edu-k dekt maar een deel van het speelveld af. Kortom: een advies vanuit Edustandaard om de implementatiekracht van standaarden te vergroten is nuttig nu en in de toekomst.

Op basis van een advies van Edustandaard kan besloten worden over het vervolg. Op dit moment is bijvoorbeeld niet duidelijk in hoeverre leveranciers al voldoen de aan de betreffende beveiligingsstandaarden (bijlage 1). Een dergelijke inventarisatie lijkt nodig om scope, impact en kosten in beeld te brengen.

**Bijlage 1: beveiligingsstandaarden die verplicht worden**

|  |  |
| --- | --- |
| Standaard | Doel standaard |
| TLS/HTTPS Het NCCS heeft aanvullende eisen t.a.v. cijfersuites | Beveiligde verbinding |
| DNSSEC | Domeinnaambeveiliging |
| SPF | Anti-phishing email |
| DKIM | Anti-phishing email |
| DMARC | Anti-phishing email |
| HTTPS, HSTS en TLS conform NCSC richtlijn | Beveiligde verbinding |
| STARTTLS en DANE. Voor gebruik van DANE gelden strikte policies | Encryptie van mailverkeer |
| SPF en DMARC | Strikte policies voor emailstandaarden |