Ministerie van Onderwijs, Cultuur en Wetenschap

TER ONDERTEKENING
Aan: MPVO

Primair Onderwijs

Van
[redacted]

Datum
27 juni 2022

Referentie

Bijlagen
Kamerbrief digitale weerbaarheid onderwijs en onderzoek (schoon)

Kamerbrief digitale weerbaarheid onderwijs en onderzoek (track changes)

Normenkader HO

Verkenning Berenschot normenkader IBP FO

nota

Naar aanleiding van gesprek met MPVO op 22/06/2022 over de Kamerbrief over digitale weerbaarheid

Aanleiding

U ontvangt deze nota naar aanleiding van ons gesprek op 22 juni 2022 over de Kamerbrief over digitale weerbaarheid waarin u heeft verzocht om scherper inzicht te bieden in de effectiviteit van onze aanpak/Plan Veilig Digitaal Funderend Onderwijs, de regierol van OCW, het normerend karakter en wat dit vraagt in wet- en regelgeving, de verdeling van taken en verantwoordelijkheden van alle partijen, het tijdpad (fasering en mijlpalen), de kwaliteitscontrole, monitoring en evaluatie. Ter informatie sturen wij u als bijlagen de verkenning naar het normenkader voor het funderend onderwijs van Berenschot en het normenkader voor het hoger onderwijs en in het middelbaarberoepsonderwijs waarop we ons in het po en vo baseren.

Kernpunten

We hebben de kamerbrief aangescherpt langs de door u benoemde volgende uitgangspunten:

- **Integrale aanpak**: met de totale aanpak borgen we een veilig digitaal funderend onderwijs. De uitvoering vindt gefaseerd plaats.
- **Meer centrale regie**: scholen kunnen het niet alleen en daarom gaan we risicogericht helpen.
- **Normstelling**: scholen moeten weten waar ze minimaal aan moeten voldoen, hoe ze daaraan kunnen voldoen, en hoe ze worden gecontroleerd en waar nodig met welke sancties. Dit gaan we communiceren (bewustwording). Daarnaast voeren we een nulmeting uit (waarmee we zicht hebben op de zwakke plekken in de sector en waar scholen nu staan qua cyberdreigingsbeeld), monitoren en benchmarken we periodiek, stellen we het normenkader bij waar nodig op basis van het dreigingsbeeld, en zien we erop toe dat scholen eraan voldoen en grijpen waar nodig in.
- **Helpen**: we gaan scholen ondersteunen met raad en daad en beschermen waar ze risico's over het hoofd zien
- **Publieke voorzieningen**: de overheid regelt centrale voorzieningen waar keten/coördinatieproblemen optreden en schaalvoordelen evident te behalen zijn.
- **Fasering**: we starten nu met communicatie, normstelling, en hulp bij incidenten. Tegelijkertijd bereiden we de volgende stappen voor die de basisinfrastructuur betreffen (ICTU onderzoek, beleidsadvies ict-

basisinfrastructuur, uitbouw bestaande voorzieningen richting een Cyber Emergency Response Team (CERT) voor funderend onderwijs).

De aanpassingen vindt u in track changes in de brief.

Geadviseerd besluit

Met ondertekening van de brief gaat u akkoord met het doorgeleiden van de brief naar MOCW (ter ondertekening) en het verzenden naar de Tweede Kamer.

Toelichting

In onderstaande tabel hebben we de verantwoordelijkheidsverdeling en het tijdpad inzichtelijk gemaakt. Uitgangspunt hiervoor is het NIST-model voor cybersecurity, afkomstig van het National Institute of Standards and Technology (NIST), een wetenschappelijke organisatie die in opdracht van de Amerikaanse overheid standaarden ontwikkelt en beheert. Het model beschrijft vijf typen activiteitenclusters, zijnde identificeren, beschermen, detecteren, reageren en herstellen, om tot een gewenste situatie te komen op het gebied van digitale veiligheid in een school. Een zesde cluster, professionaliseren, is toegevoegd aan het model om het toepasbaar te maken binnen het landelijk ondersteuningsprogramma voor het funderend onderwijs. De activiteiten binnen Plan Veilig Digitaal Funderend Onderwijs zijn gestructureerd onder deze clusters.

Met het Plan Veilig Digitaal Funderend Onderwijs hebben wij in kaart gebracht wat nodig is om de digitale veiligheid en privacy in het po en vo de komende jaren te versterken en structureel te borgen. Dat doen we via centrale regie met landelijke ondersteuning en voorzieningen zodat scholen hun verantwoordelijkheid ten aanzien van informatiebeveiliging, privacy en continuïteit van het onderwijs kunnen invullen. Wij sturen strak op de doelen en het normenkader en kiezen voor een programmatische aanpak om de raden, Kennisnet en SIVON te betrekken zodat het ondersteuningsaanbod goed aansluit bij de onderwijspraktijk.

De uitwerking van het volledige plan doen we gefaseerd in drie tranches/fases: de eerste fase start vanaf Q3 2022, de tweede fase vanaf Q3 2023 en de derde fase vanaf Q3 2024. Elke fase bevat go/no-go momenten waarbij OCW besluit welke activiteiten in de volgende fase worden opgepakt, afhankelijk van de financiële besluitvorming. Deze drie fases bouwen voort op elkaar, waarbij aanvullende maatregelen en activiteiten worden ontwikkeld. De activiteiten in de tweede en derde fase, met name voor wat betreft het realiseren van centrale voorzieningen in de digitale infrastructuur, vergen nog verdere verkenning en uitwerking.

Bij VJN 2022 is er € 6 mln. structureel beschikbaar gekomen voor de activiteiten die we in de brief aankondigen. Hierin zijn investeringen in centrale voorzieningen en infrastructuur niet opgenomen. Tegelijkertijd wordt er dekking gezocht voor € 5 mln. structureel voor additionele activiteiten die later in het programma zullen starten (vanaf medio 2023). Voor alle centrale voorzieningen in de digitale infrastructuur loopt op dit moment een beleidsonderzoek. Aan de hand van de uitkomsten van dit onderzoek worden deze voorzieningen in 2023 verder

gespecificeerd. Een indicatie voor de benodigde financiering daarvoor is, op basis van een eerste p x q schatting van Kennisnet, 20 à 30 mln. structureel. Hiermee wordt onder meer een beveiligde internetverbinding voor scholen (Dienst Veilig Internet van SIVON, via netwerk SURF) voor iedere school bekostigd. Hier kunnen ook andere voorzieningen voor (real-time) detectie en risico-identificatie aan gekoppeld worden. Ook hiervoor moet dan dekking gezocht worden.

Toelichting bij figuur 1
Op uw verzoek hieronder een nadere uitwerking van alle activiteiten die vallen onder de integrale aanpak van het Plan Veilig Digitaal Funderend Onderwijs, een indicatie van het tijdpad en de verantwoordelijkheidsverdeling voor de uitvoering van de activiteiten.

Legenda
- Geel: voorbereiding (onderzoek/verkenning en voorbereiding activiteiten)
- Oranje: uitvoering fase 1 (nieuwe activiteiten, intensivering bestaande activiteiten)
- Blauw: uitvoering fase 2 (verdere ontwikkeling nieuwe activiteiten)
- Groen: uitvoering fase 3 (investeringen in infrastructuur, nog niet alle oplossingen uitgewerkt, beleidsadvies hierop volgt later dit jaar)
- Paars: mix van rood en blauw (activiteiten die al lopen die forse intensivering kennen)

Opmerkingen van MPVO bij onderstaande tabel
- Wettelijke verankering: hoe zorgen we dat het wel al geldt als er nog geen wetswijziging is?

Eind 2022 ligt er een normenkader. Het normenkader is ambitieus. Onze verwachting is dat er weinig scholen zijn die nu al aan het normenkader voldoen. We communiceren naar scholen dat het normenkader verplicht zal worden op termijn en dat er een nulmeting zal worden uitgevoerd. Zo weten scholen meteen waar ze staan t.o.v. het normenkader en waar ze nog op moeten inzetten om te voldoen aan het normenkader wanneer dat verplicht is. We geven scholen de gelegenheid en ondersteuning om te voldoen aan het normenkader. Het vergt voor iedere school een forse inspanning om aan het normenkader te voldoen. Niet alleen de lat ligt hoog maar ook het tempo om er te komen ligt hoog. Vanaf 2023/24 moeten schoolbesturen zich hierover verantwoorden in jaarverslagen en er zal toezicht/handhaving voor worden ingericht.

- Nulmeting en deep dive: specificatie. Individueel? Of stresstest voor elke school verplicht bijvoorbeeld.

Eind 2022 ligt er een normenkader. We communiceren naar scholen dat het normenkader verplicht zal worden. Het is in lijn met de ambitie van Plan Veilig Digitaal Funderend Onderwijs om op iedere individuele school een nulmeting uit te voeren zodat elke school weet waar het staat t.o.v. het normenkader. Dit gaan we de komende twee jaar doen. Er zijn 1300 schoolbesturen en 10.000 scholen. De

nulmeting alleen al is een enorme operatie. Dit kan trapsgewijs: de eerste scholen waar een nulmeting uitgevoerd wordt, kunnen meteen stappen zetten om hun digitaal onderwijs veiliger te maken. Willen we daadwerkelijk het verschil maken, dan moeten we de nulmeting serieus uitvoeren en dat kost tijd. Anders wordt het enkel een papieren exercitie. Hier is expertise voor nodig en een onafhankelijke blik.

- Bewustwordingscampagnes: Twijfel ik over, want we besteden veel aan hen uit. Ik heb de ervaring dat er vrij veel ruimte in opdrachten zit. Maar denk dat we er hier dichter op moeten zitten. Kunnen we een programmateam hebben waar de eindregie bij OCW blijft?
- Bij identificeren: Veel afhankelijkheden. Lukt dit? Hoe borgen we succes?

De activiteiten die vallen onder de integrale aanpak van het Plan Veilig Digitaal Funderend Onderwijs brengen we onder in een programma. OCW stelt de doelen van het programma vast en draagt een verantwoordelijkheid voor het bereiken daarvan, de financiën, de organisatie en de verantwoording. Daarmee ligt de eindregie bij OCW. Bij de uitwerking van het programmaplan worden ook KPI's opgesteld om het meetbaar te maken. Waar de raden, Kennisnet en SIVON betrokken zijn op de uitvoering van de activiteiten stuurt OCW strak op de uitkomsten daarvan.

			2022		2023				2024			
NIST model	**Activiteit**	**Wie?**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Professionaliseren												
Sturen op basis van normen	Normenkader IBP FO	Kennisnet										
	Wettelijke verankering / naleving / handhaving normenkader	OCW										
	Governance normenkader (vaststelling, herzien op basis van dreigingsbeeld)	OCW										
	Normenkader communiceren naar scholen	OCW										
Sectorale IBP-monitoring	Nulmeting en deep dive	Kennisnet/SIVON										
	Periodiek montoring en benchmarking	Kennisnet/OCW/raden										
Bewustwording en start-advies	Bewustwordingscampagnes	Raden/Kennisnet										
	Aanpak per schoolbestuur	SIVON/raden/Kennisnet										
Beschikbaarheid deskundig personeel	Uitwerking oplossingsrichtingen en pilots	Kennisnet/SIVON										
	Uitvoering oplossing	Kennisnet/SIVON										
Kennisontwikkeling medewerkers	Bewustwordingscampagne en werkinstructies personeel	Raden/Kennisnet										
	Scholing IBP-ers	SIVON										
Toegang tot IBP-expertise	Landelijk expertisecentrum	Kennisnet										
	Helpdesk IBP	Kennisnet										
	Netwerk IBP	Kennisnet/raden/SIVON										

			2022		2023				2024			
NIST model	**Activiteit**	**Wie?**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Identificeren												
Inzicht op basis van architectuur	Ondersteuning toepassen referentiearchitectuur FORA	Kennisnet/SIVON										
	Doelarchitectuur FOSA	Kennisnet/raden										
Risico-inventarisatie	Sectorale risico-inventarisatie	Kennisnet										
	Cyberdreigingsbeeld FO	Kennisnet										
	Landelijke DPIA's	SIVON										
Inzicht in eigen applicatielandschap	Catalogus beschikbaar aanbod	Kennisnet										
	Tooling 'mijn applicaitielandschap in kaart'	Kennisnet										
	Dienst verwerkersovereenkomsten	Kennisnet										
Beschermen												
(Regie op) ketenarchitectuur	Analyse en planvorming integraal beeld	Kennisnet/OCW/raden										
	Publiek private afspraken (Edu-V)	OCW/raden										
	Standaarden en voorzieningen	Kennisnet										
Identity & acces management	Uitwerking oplossingsrichtingen en pilots	Kennisnet/SIVON										
	Uitvoering oplossingen	Kennisnet/SIVON										
Veilige netwerkinfrastructuur	Onderzoek veilige netwerkinfrastructuur	Kennisnet/SIVON										
	Nationaal Dienstencentrum (NDC)	Kennisnet/SIVON										
	Diensten Veilig Internet, Veilige wifi	Kennisnet/SIVON										
	Beleidsadvies over (de governance op) de ict-basisinfrastructuur	Aanbesteding/OCW										
	Onderzoek i.r.t. Plan Veilig Digitaal Funderend Onderwijs & NDC	ICTU										

			2022		2023				2024			
NIST model	**Activiteit**	**Wie?**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Leveranciersmanagement	Inkoopvoorwaarden en inkoop	SIVON										
	Contractmanagement	SIVON										
	Toetsing verwerkerovereenkomsten	Kennisnet/SIVON										
	Audits en certificering leveranciers	SIVON										
Detecteren												
Dreigingsdetectie	Onderzoek landelijke monitoring logging (SIEM/SOC)	Kennisnet										
	Uitvoering oplossing	Kennisnet/SIVON										
Testen	Tests scholen	SIVON										
	Tests leveranciers	SIVON										
Reageren en herstellen												
Incidentvoorbereiding	Draaiboeken beveiligingsincidenten	Kennisnet										
	Cyberdreigingsoefeningen	Kennisnet/SIVON										
Cyber Emergency Response Team (CERT) (n.b ook detecteren)	Preventie (duiden en delen informatie dreigingen)	Kennisnet										
	Reactie (eerstelijnshulp voor scholen bij incidenten)	Kennisnet										
	Coördinatie (richting ketenpartijen)	Kennisnet										
	Meldplicht voor cyberincidenten (wetstraject starten)	OCW										
Herstel na incident	Rapid respons & forensics	SIVON/Kennisnet										
	Cybersecurityverzekering / calamiteitenfonds	SIVON/Kennisnet										
Backup	Onderzoek oplossingen backup	Kennisnet/SIVON										
	Uitvoering oplossing	Kennisnet/SIVON										

Ministerie van Onderwijs, Cultuur en Wetenschap

TER ONDERTEKENING
Aan: MOCW via MPVO

Bestuursondersteuning en Advies

Van
[redacted]

Datum
1 juni 2022

Referentie
[redacted]

Bijlagen
1

Intern OCW afgestemd
BOA, HOenS, KENNIS, MBO, OWB, PO, VO, FEZ, IB, WJZ en Inspectie

nota

Brief over digitale veiligheid onderwijs en onderzoek, toezeggingen debat 1 december 2021

Aanleiding

De hack bij de universiteit van Maastricht in 2019, NWO begin 2021, ROC Mondriaan en incidenten bij po- en vo-scholen onderstrepen de urgentie om de digitale weerbaarheid van de instellingen te verhogen. Tevens ligt er een advies van de AP over de privacy van leerlingen en studenten in het onderwijs bij het gebruik van digitale toepassingen.[1] Op 1 december vorig jaar is door uw ambtsvoorgangers een commissiedebat Digitalisering en Privacy in het Onderwijs met de Kamer gevoerd waar een aantal toezeggingen is gedaan. Deze brief gaat in op de in het debat gedane toezeggingen.

Geadviseerd besluit

Met de ondertekening van de brief geeft u antwoord op de toezeggingen aan de Tweede Kamer.

Kernpunten

- De brief behandelt het verhogen van de digitale veiligheid van de gehele onderwijs- en onderzoekssector en geeft aan op welke wijze OCW de sectoren faciliteert bij het waarborgen van de privacy. De instellingen moeten veel werk verzetten en dat wordt ook financieel ondersteund.
- De brief belicht eerst de gemeenschappelijke opgaven voor het hele onderwijs en onderzoek, vooral gelegen in het gedeeld normenkader. Hierna worden in antwoord op de toezeggingen de maatregelen genoemd voor achtereenvolgens de sectoren po/vo en mbo/hoger onderwijs en onderzoek. Het po/vo is echt aan het bouwen aan een gemeenschappelijke basis, het mbo en ho bouwt vooral voort op de bestaande basis.
- Tot slot behandelt de brief een drietal toezeggingen uit hetzelfde debat en reageert u op verzoek van de Kamer op het rapport van Human Rights Watch over de privacy van leerlingen in coronatijd.

<u>Primair en voortgezet onderwijs</u>

Voor het po en vo kondigt u een structurele investering van € 6 mln in digitale veiligheid aan. De dekking hiervan is met de VJN geregeld. Met deze € 6 mln zet u in op drie prioriteiten:

- Het vergroten van bewustwording over dit thema.
- Het opstellen van een normenkader.

[1] TK 2021-2022, 32034, 32761 nr. 40

- Het bouwen van een digitale infrastructuur voor scholen.
- Ook kondigt u aan dat we met de PO-Raad, de VO-raad, Kennisnet en SIVON werken aan een veilige digitale infrastructuur voor het onderwijs.
- Daarmee werken het po en vo toe naar de situatie in het mbo en ho waar er wel al een sectoraal normenkader is en er via SURF meer centrale voorzieningen beschikbaar zijn die scholen ondersteunen.
- Hiermee worden ook de toezeggingen aan de Kamer uit het commissiedebat over digitalisering in het onderwijs van 1 december 2021 gestand gedaan.
- U voorziet niet in extra geld in de lumpsum voor scholen. De capaciteit die zij nodig hebben om hun digitale veiligheid op orde te brengen moeten ze uit de huidige lumpsum bekostigen.
- In bijlage I onderaan deze nota wordt voor het po en vo een uitgebreide toelichting gegeven op de noodzaak van de maatregelen.

<u>Mbo, ho en onderzoek</u>

- Voor het mbo kondigt u een investering van jaarlijks € 5 mln in digitale veiligheid aan t/m 2027.
- Voor het mbo- en ho ligt de focus op de uitwerking van de plannen van aanpak ten aanzien van cyberveiligheid die in de kamerbrief van september 2021 zijn aangekondigd.
- Het gaat hierbij om hoe en wanneer op verschillende maatregelen wordt geacteerd door de koepelorganisaties en de instellingen en hoe OCW de komende jaren hierop monitort en evalueert.
- Hiermee wordt er voortgebouwd op de afspraken zoals deze ook ter sprake zijn gekomen in het bestuurlijk overleg cybersecurity tussen MOCW en de koepels (mbo-raad, VH, UNL en de nrto) van 16 februari jl.

Toelichting

Voorgaande jaren zijn onderwijs en onderzoek vaker geraakt door grote cyberincidenten, zoals de hack bij de Universiteit Maastricht, de NWO en bij ROC Mondriaan. Deze aanvallen bedreigden de continuïteit en kwaliteit van het onderwijs en onderzoek. Ook in het po en vo zien we steeds vaker incidenten die een impact hebben op het onderwijs.

Het afgelopen half jaar is hard gewerkt door alle stakeholders in de verschillende sectoren aan het uitwerken van alle noodzakelijke maatregelen in plannen van aanpak. Daarvoor is er veel overleg geweest tussen instellingen, koepelorganisaties en alle stakeholders. Deze plannen van aanpak zijn/worden in de verschillende ALV's van de stakeholders besproken dan wel vastgesteld.

Ook het Cybersecurity Beeld Nederland 2022 dat de minister van JenV op 1 juli aanstaande in de MR wil inbrengen, laat zien dat de dreiging in Nederland onverminderd hoog is en dat de weerbaarheid nog steeds niet op orde is. Een van de genoemde voorbeelden in het rapport is de hack bij ROC Mondriaan.

De komende jaren bouwen we in het funderend onderwijs met Kennisnet, SIVON en de raden stap voor stap aan een digitale infrastructuur die het mogelijk maakt om risico's voor scholen te identificeren, beschermende maatregelen te nemen, incidenten te detecteren, daarop te reageren en eventuele schade te herstellen. Daarbij sluiten we aan op bestaande voorzieningen zoals het Nationaal Dienstencentrum (NDC) bij Kennisnet en de dienst Veilig Internet van SIVON. ICTU (ICT-Uitvoeringsorganisatie van de overheid) adviseert ons daarbij.

Hoewel het verhogen van de digitale weerbaarheid voor alle gebieden binnen OCW geldt, focust deze brief zich, net als voorgaande brieven en debatten op de onderwijs- en onderzoekssector.

Politieke context:
De Kamer heeft al langer aandacht voor de digitale kwetsbaarheid in het onderwijs en onderzoek. Ook het CA pleit voor meer digitale veiligheid, hoewel het onderwijs daarin niet specifiek wordt genoemd. In de Europese context zien we aandacht voor de kwetsbaarheid van onderwijs en onderzoeksinstellingen (amendement van EP van de VVD) in het kader van de aanpassing van de NIS (Netwerk en Informatiebeveiliging) richtlijn. Er wordt gewerkt aan een nieuwe richtlijn waarin een deel van onze sector (onderzoeksinstellingen) onder lijkt te gaan vallen (definitie biedt nog geen duidelijkheid).

De Kamer had bij voorkeur begin Q2 deze brief willen ontvangen maar het wachten was op de plannen van de verschillende sectoren. Na ontvangst van de brief zal de Kamer naar verwachting een debat plannen om moties in te dienen.

De wens van de Kamer was om alles te bundelen in één brief. We zien ook dat de Kamer de onderwerpen cybersecurity en privacy steeds tezamen behandelt.

Bijlage I: Toelichting Primair en voortgezet onderwijs

Beleidslijn in het po en vo

- Digitalisering biedt kansen voor de kwaliteit van het onderwijs en is niet meer weg te denken uit het hedendaagse klaslokaal. Om die kansen optimaal te benutten en ervoor te zorgen dat het digitaliseren in het onderwijs *doordacht* gebeurt, moet een aantal aspecten in *samenhang* geborgd worden. Het belang hiervan blijkt uit het feit dat er voor het eerst een sterke paragraaf over digitalisering in het coalitieakkoord is opgenomen en de benoeming van een staatssecretaris voor digitalisering. Scholen moeten een visie hebben op de inzet van digitale middelen in het onderwijs, leraren moeten kunnen beschikken over passende digitale leermiddelen, zij moeten over de kennis en vaardigheden beschikken om die middelen goed in het onderwijs toe te passen, en de digitale infrastructuur moet veilig en betrouwbaar zijn.
- Vanuit de eerste en tweede ronde van het Nationaal Groeifonds wordt er € 180 mln geïnvesteerd in projecten die doordachte digitalisering verder brengen. De beoordelingscommissie heeft in samenhang hiermee aangegeven digitale veiligheid als kerntaak van OCW te beschouwen.
- Daarnaast is digitale geletterdheid onderdeel van het masterplan basisvaardigheden. De digitale geletterdheid kan alleen worden verhoogd als er ook goede digitale leermiddelen zijn en de infrastructuur op de scholen en in de sector op orde is. Er is dus nog veel nodig. Zonder deze randvoorwaarden gaat dit niet goed. Omdat digitale geletterdheid onderdeel is van het masterplan basisvaardigheden is de kerntaak van het departement ten aanzien van de ict-basisinfrastructuur en digitale veiligheid des te belangrijker geworden.
- Belangrijke randvoorwaarden in het digitale domein zijn digitale veiligheid en de privacy van leerlingen. Deze hebben een directe relatie met de continuïteit van het (digitale) onderwijs. Door de toenemende digitalisering wordt het voor scholen echter steeds complexer om daar invulling aan te geven. Scholen in het funderend onderwijs zijn onvoldoende toegerust om hun verantwoordelijkheid op dit vlak in te vullen.
- Er zijn vier oorzaken geïdentificeerd in Plan Veilig Digitaal Funderend Onderwijs door Kennisnet waarom er meer gecoördineerde actie nodig is en welke ondersteuning scholen nodig hebben om de digitale veiligheid te verhogen:
    - Er is **onvoldoende bewustzijn** binnen onderwijsinstellingen van de risico's die schoolbesturen lopen op het gebied van privacy, beveiliging en continuïteit van onderwijs.
    - Een duidelijk beeld en **normstelling ontbreekt** van wat scholen moeten doen om hun onderwijs veilig te maken. Elk schoolbestuur moet passende maatregelen kunnen nemen.
    - Scholen moeten **hoge kosten** maken voor de veiligheid van hun onderwijs doordat het beveiligingsvraagstuk zeer complex is: de wereld van cybersecurity is omvangrijk, specialistisch en verandert

razendsnel. Een aanpak per schoolbestuur is niet altijd doelmatig, met centrale voorzieningen zijn schaalvoordelen te behalen.
    - Voor individuele scholen is het moeilijk om specifieke eisen over privacy of beveiliging af te dwingen bij leveranciers. Daar is **samenwerking en een gecoördineerde aanpak** nodig.
- In de kamerbrief 'digitalisering in het funderend onderwijs' van 24 september 2021 heeft uw voorganger aangegeven dat veilig digitaal onderwijs alleen gerealiseerd kan worden als alle partijen hun verantwoordelijkheid nemen. Op elk niveau kunnen en moeten daarvoor extra stappen gezet worden: (1) welke verantwoordelijkheden kunnen individuele onderwijsinstellingen zelf invullen; (2) welke vraagstukken kunnen beter door schoolbesturen gezamenlijk worden opgepakt en (3) waar is aanvullende coördinatie of ondersteuning vanuit de Rijksoverheid nodig.
- De toenemende problematiek overstijgt de draagkracht van scholen. Scholen kunnen het niet alleen. Er is meer regie nodig vanuit de overheid om scholen te steunen. Dit is in lijn met de adviezen van de Autoriteit Persoonsgegevens, het Rathenau Instituut en de Inspectie van het Onderwijs (genoemd in brief).
- Gegeven de toenemende problematiek en adviezen kiest u in de brief voor een *intensivering van deze aanpak*: bewustwording zodat scholen weten wat ze moeten doen en hoe ze dit moeten doen, kaderstelling, normering, centrale voorzieningen en meer ondersteuning vanuit de overheid om coördinatiefalen op te heffen en schaalvoordelen te benutten. Deze aanpak is in lijn met:
    - Het Rijksbrede beleid ten aanzien van digitalisering van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties ("de digitale transitie in goede banen leiden en zorgdragen voor een goede maatschappelijke inbedding").
    - De motie Kwint en Van Meenen[2] over het uitvoeren van een DPIA op alle internationale technologiebedrijven in het Nederlandse onderwijs.
    - Het hoofdlijnenbeleid voor digitalisering ten aanzien van de rol van de overheid die een sterke, anticiperende rol inneemt om de kansen die de digitale transitie ons biedt te benutten en, meer dan voorheen, normerend optreden naar publieke en private partijen. Doel hiervan is om publieke waarden in de digitale transitie te borgen.

Achtergrond bij het NDC

- Het Nationaal Dienstencentrum (NDC) is een centrale voorziening van Kennisnet en vormt de basis voor de Dienst Veilig Internet, die SIVON en Kennisnet aanbieden aan schoolbesturen. Het NDC is een centrale voorziening waarlangs het internetverkeer van scholen geleid kan worden, en op deze wijze beschermd kan worden met een firewall en gemonitord kan worden op

[2] Motie: "verzoekt de regering, op korte termijn zo'n DPIA uit te voeren op alle internationale technologiebedrijven, toegespitst op toepassingen die in het Nederlandse onderwijs gebruikt worden, en de Kamer hier periodiek over te informeren". Deze motie is al afgedaan in de brief van 21 maart 2021: https://www.tweedekamer.nl/kamerstukken/detail?id=2021Z04015&did=2021D08773

cyberaanvallen en andere bedreigingen. SIVON sluit de individuele schoollocaties aan op het NDC.

- OCW heeft een startsubsidie verstrekt van € 54 mln aan Kennisnet en SIVON voor de periode 2019-2025 voor de gezamenlijke ontwikkeling van de Dienst Veilig Internet, waarmee scholen snel, veilig en betaalbaar internet kunnen verkrijgen. De problematiek van cyber(on)veiligheid in het funderend onderwijs neemt snel toe, met risico's voor de continuïteit van het onderwijs. De investeringen in het NDC kunnen in deze context worden benut.
- Momenteel werken OCW, raden, Kennisnet en SIVON de plannen voor de digitale infrastructuur verder uit. Belangrijke optie daarin is het NDC als centrale voorziening waarmee het internetverkeer van de scholen kan worden beveiligd. De aansluiting van scholen op het NDC is nu op basis van vrijwilligheid. Deze aansluiting verloopt vooral in het po moeizaam. Met Kennisnet en SIVON zijn subsidie afspraken gemaakt waardoor zij nieuwe scholen/besturen kunnen aansluiten voor de periode tot en met 2025 op basis van 3-jarige contracten. Mocht de aansluiting bij het NDC achterblijven, dan staan we voor de afweging of deze aansluiting een meer verplichtend karakter moet krijgen en op deze manier kan worden uitgebouwd tot een structurele voorziening voor cyberveiligheid. Wij laten ons hierbij adviseren door ICTU. In voorbereiding is tevens een aanvraag voor een extern advies over de (governance op de) ict-basisinfrastructuur in het funderend onderwijs. Deze adviezen komen eind dit jaar beschikbaar. Op basis hiervan ontvangt u eind dit jaar voorstellen hoe verder te gaan met de ontwikkeling van deze infrastructuur.

Bijlage II: Toezeggingen
Informele toezegging: Kamer informeren over de uitkomsten van de DPIA Chromebooks.

1. 4485 tz_OCW_2021_75 zie ook 4493! (helemaal onderaan)
   Na overleg met betrokken partijen ontvangt de Tweede Kamer het afwegingskader wanneer fysiek onderwijs en wanneer digitaal aanvullen
   MBO: Jeroen van Mierlo/Wouter Verheij
2. 4486 tz_OCW_2021_76
   In het eerste kwartaal van 2022 ontvangt de Tweede Kamer een overzicht van de noodzakelijke stappen die gezet moeten worden om alle instellingen te laten aansluiten bij informatievoorziening over digitale bedreigingen.
3. 4487 tz_OCW_2021_77
   In het eerste kwartaal van 2022 ontvangt de Tweede Kamer een stappenplan om te komen tot een gedeeld normenkader ten aanzien van digitale veiligheid.
4. 4488 tz_OCW_2021_78
   De Tweede Kamer wordt door de minister van OCW geïnformeerd over de wijze waarop instellingen in hun jaarverslag kunnen rapporteren over de stappen die zij hebben gezet en die zij gaan zetten op het gebied van digitale veiligheid.
5. 4489 tz_OCW_2021_79
   In het eerste kwartaal van 2022 wordt de Tweede Kamer door de minister van OCW geïnformeerd over informatie die mogelijk gedeeld zou kunnen worden ten aanzien van het IBOP-volwassenheids-niveau van instellingen.
6. 4490 tz_OCW_2021_80
   De minister voor Basis- en Voortgezet Onderwijs informeert de Kamer over zijn gesprek met het CvTE, waarin hij ook zal ingaan op het gebruik van de grafische rekenmachine en alternatieven daarvoor.
7. 4491 tz_OCW_2021_81
   De minister voor Basis- en Voortgezet Onderwijs informeert zo snel mogelijk over de mogelijkheden om tot een meldplicht bij cyberaanvallen te komen voor alle instellingen in het funderend onderwijs.
8. 4492 tz_OCW_2021_82
   De Tweede Kamer wordt door de minister van OCW geïnformeerd over de achtergrond van het Mare-artikel over de gang van zaken bij de Universiteit Leiden.
9. 4493 tz_OCW_2021_83
   De minister van OCW komt in haar brief over het afwegingskader wanneer fysiek onderwijs en wanneer digitaal aanvullen ook terug op de verantwoordelijkheidsverdeling.