

Veilig digitaal funderend onderwijs

Versie 1.0

18 oktober 2021

Inhoud

Inleiding	3
Context	3
Probleem	4
Oplossing	5
Resultaat	6
1. Noodzakelijke interventies	7
Het NIST-model	8
Maatregelen voor het funderend onderwijs	9
2. Een programmatische aanpak	11
Vier actielijnen	12
Programmainrichting	14
Lijn 1: Normering en bewustwording	15
Bouwblok 1: Sturen op basis van normen	15
Bouwblok 3: Monitoring	18
Lijn 2: Professionalisering	19
Bouwblok 4: Professionalisering binnen de onderwijsinstelling	19
Bouwblok 5: Kennisopbouw en kennisdeling in de sector	20
Bouwblok 6: Centrale coördinatie en ondersteuning beveiligingsincidenten	23
Lijn 3: Leveranciersmanagement	25
Bouwblok 7: Veilig gebruik van software en hardware	25
Bouwblok 8: Inzicht in eigen applicatielandschap	27

Bouwblok 9: Passend marktaanbod IBP-ondersteuning voor schoolbesturen	28
Lijn 4: Veilige en betrouwbare basisinfrastructuur	31
Bouwblok 10: Veilige identiteiten	31
Bouwblok 11: Veilige gegevensuitwisseling	32
Bouwblok 12: Veilige connectiviteit	33
3. Financiën	36
Begroting	36
Toelichting	37

Bijlage 1. Overzicht integraal portfolio privacy en beveiliging andere publieke domeinen	41
--	----

Inleiding

Context

De leraar legt uit met het digibord, de leerlingen maken oefeningen op hun tablets of laptops, en de hele bedrijfsvoering van een school leunt zwaar op digitale systemen. Een kleine school in het basisonderwijs heeft al gauw te maken met 200 devices die door leraren en leerlingen worden gebruikt en binnen een gemiddeld bestuur in het voortgezet onderwijs zijn dit er al gauw een kleine 4.000¹. Een commercieel bedrijf heeft hier veel personeel voor rondlopen, maar in het onderwijs is dat anders georganiseerd en is veel minder capaciteit beschikbaar. En als er geen verbinding is met het internet of als cruciale applicaties (het leerlingadministratiesysteem, de leeromgeving of specifieke leermiddelen) niet bruikbaar zijn, staat het onderwijs stil. De verhalen zijn bekend van lessen die niet door konden gaan na een DDoS-aanval², of van een school die dagenlang geen volledig onderwijs kan geven door een aanval met ransomware³. En bij een verstoring van de ict komt ook de bedrijfsvoering onder druk te staan, denk aan het betalen van salarissen of facturen. Vier op de tien instellingen in het vo en mbo hebben in 2020 te maken gehad met problemen op het gebied van ict-beveiliging⁴. Het toegenomen gebruik van digitale leermiddelen en devices voor les op afstand door de corona-lockdowns, hebben duidelijk gemaakt dat het Nederlandse onderwijs enorm afhankelijk is van ict. Een school is tegenwoordig voor een belangrijk deel een ict-organisatie. Een verstoring in een onderdeel van de ict (verbindingen, leermateriaal, administratieve systemen) heeft grote impact op de continuïteit van het onderwijs⁵.

Naast risico's voor de continuïteit van het onderwijs neemt ook het risico van schending van de privacy van een kwetsbare groep, namelijk minderjarige

leerlingen, toe. Waar meer digitaal wordt gewerkt, ontstaat meer data. Dit gaat niet alleen over voortgang- en resultaatgegevens, maar ook over bijzondere persoonsgegevens zoals zorgdossiers of informatie over religieuze of seksuele oriëntatie van leerlingen. Incidenten zoals datadiefstal of de installatie van ransomware zorgen ervoor dat deze data in handen kan komen van kwaadwillenden zodat deze op straat komen te liggen. Er zijn diverse manieren waarop dit kwetsbare kinderen kan beschadigen, variërend van onveiligheid en schaamte tot discriminatie, uitsluiting en identiteitsfraude. Ook gegevens van ouders en medewerkers worden in diverse systemen verwerkt.

Veilig werken en privacy in het funderend onderwijs zijn daarmee een basisvoorwaarde geworden voor het huidige gebruik én het verder benutten van de mogelijkheden van digitalisering. Een basisvoorwaarde die eigenlijk al lang op orde had moeten zijn en die steeds meer en grotere risico's met zich meebrengt voor individuele schoolbesturen en de sector in het algemeen. Een basisvoorwaarde betekent dat dit op alle scholen, klein en groot, moet zijn geregeld. Alle scholen moeten veilig zijn en veilig werken en de privacy van leerlingen, medewerkers en ouders borgen. De brief van de Autoriteit Persoonsgegevens (AP) aan de minister van basis- en voortgezet onderwijs naar aanleiding van de privacyrisico's bij het gebruik van Google Workspace in het onderwijs is hier duidelijk over: "De AP wil u als stelselvertegenwoordiger van het primair- en voortgezet onderwijs met klem adviseren een pakket aan maatregelen te nemen waarmee wordt bewerkstelligd dat onderwijsinstellingen

¹ Schatting, gebaseerd op gemiddeld aantal leerlingen van 2898. <https://www.vosabb.nl/wp-content/uploads/2020/06/literatuurstudie-schaalgrootte-in-het-primair-en-voortgezet-onderwijs.pdf>

² <https://lc.nl/friesland/leeuwarden/Leerlingen-CSG-Comenius-bestoken-eigen-school-met-ddos-aanvallen-Het-benadelen-van-ongeveer-1650-personen-is-geen-leuke-grap-26735624.html>

³ <https://www.nrc.nl/nieuws/2021/02/26/gelderse-school-betaalt-losgeld-vanwege-hack-maandag-geen-les-a4033498>

⁴ IT-beveiliging binnen het voortgezet- en middelbaar beroepsonderwijs, Kantar & Breens Network, 2021 <https://breens.nl/whitepapers/whitepaper-veiligere-hybride-onderwijsomgeving/>

⁵ <https://nos.nl/artikel/2394883-roc-mondriaan-in-den-haag-gehackt-medewerkers-staan-werkloos-bij-de-vestigingen>

ook in de praktijk zorgdragen voor veilig onderwijs bij de inzet van digitale middelen⁶.”

Probleem

Dat er een uitdaging en een opdracht liggen voor het funderend onderwijs is duidelijk, maar waar komt dit probleem vandaan? In het algemeen kan worden gezegd dat scholen in funderend onderwijs onvoldoende zijn toegerust om privacy van leerlingen en de continuïteit van het onderwijs te borgen. De IBP-monitor 2020 laat zien dat scholen de laatste jaren hard aan de slag zijn gegaan met het thema privacy, maar dat er – bijvoorbeeld op het gebied van verwerkersovereenkomsten, Data Protection Impact Assessments (DPIA's) en bewustwording – nog veel te doen is⁷. Het thema beveiliging krijgt nog veel minder aandacht. Terwijl in het bedrijfsleven gemiddeld 25% van het ict-budget aan beveiliging wordt uitgegeven, is dit bij 60% van de instellingen in het vo en mbo 5% of minder⁸. Het beeld is dat op alle verschillende niveaus (identificeren van risico's, beschermende maatregelen nemen, detectie van en reactie op beveiligingsincidenten en het herstellen van de schade) veel meer actie nodig is dan nu in de sector wordt genomen. Wij zien daarvoor vier oorzaken:

In de eerste plaats ontbreekt een duidelijk beeld van wat scholen moeten doen om hun onderwijs 'veilig' te maken. De AVG is zeer gedetailleerd waar het privacymaatregelen betreft, maar wettelijke kaders over veiligheid zijn zeer open geformuleerd. Een schoolbestuur moet 'passende technische en organisatorische maatregelen' nemen om veilig om te gaan met persoonsgegevens. Naast het ontbreken van een duidelijke normstelling, ontbreekt het aan handhaving. Dit kan zowel interne handhaving zijn (accountantsrapportage), handhaving binnen de sector (benchmarking en peer-audits) als formele handhaving (bijvoorbeeld door de onderwijsinspectie).

⁶ Brief van de Autoriteit Persoonsgegevens aan de minister voor Basis- en Voortgezet Onderwijs en Media over borging privacy in het onderwijs en de inzet van Google G Suite for Education <https://www.tweedekamer.nl/downloads/document?id=a66e585b-9816-4247-b5bf-66ad9831946c&title=Brief%20van%20de%20Autoriteit%20Persoonsgegevens%20aan%20de%20minister%20voor%20Basis-%20en%20Voortgezet%20Onderwijs%20en%20Media%20over%20borging%20privacy%20in%20het%20onderwijs%20en%20de%20inzet%20van%20Google%20G%20Suite%20for%20Education.pdf>

Ten tweede is er onvoldoende bewustzijn binnen onderwijsinstellingen van de risico's die schoolbesturen lopen op het gebied van privacy, beveiliging en continuïteit van onderwijs. Doordat er sprake is van onvoldoende besef van het probleem is de kans kleiner dat er passende maatregelen genomen worden, of dat er überhaupt voldoende mensen en middelen worden toegekend aan dit onderwerp. Een gevolg hiervan is dat er te weinig expertise en middelen in een instelling beschikbaar zijn om alle activiteiten goed uit te voeren. Neem als voorbeeld het uitvoeren van grondige DPIA's of het doen van een beveiligingsaudit bij een leverancier. Maar het gaat ook over het bepalen en in de praktijk brengen van de juiste beveiligingsmaatregelen bij het gebruik van een nieuw systeem of naar aanleiding van een nieuw gedetecteerd risico. Ook monitoring van ongebruikelijke activiteit op het netwerk in systemen is een dure en complexe activiteit.

De derde oorzaak heeft te maken met de kosten die scholen moeten maken voor de veiligheid van hun onderwijs. Het beveiligingsvraagstuk is zeer complex: de wereld van cybersecurity is omvangrijk, specialistisch en verandert razendsnel. Ook privacymaatregelen vergen specialistische juridische kennis. De kosten voor het inhuren of inkopen van expertise en uitvoeringscapaciteit zijn vanwege schaarste op de arbeidsmarkt hoog, en de mogelijkheden beperkt. Ook de beveiligingsmaatregelen zelf zijn duur en vergen forse investeringen van een schoolbestuur. Een aanpak per schoolbestuur is verre van doelmatig. Als ieder schoolbestuur hetzelfde onderzoek doet voor een DPIA, dezelfde audit uit laat voeren, zelf scholing voor medewerkers laat ontwikkelen of zelf in onderhandeling gaat met een leverancier, gaat er meer overheidsgeld naar beveiliging en overhead dan noodzakelijk is. Schoolbesturen beschikken over beperkte financiële middelen die bij voorkeur zo direct mogelijk toekomen aan het onderwijs zelf. Om toch op een doelmatige manier voldoende specialistische

⁷ <https://www.kennisnet.nl/artikel/7733/monitor-ibp-2020-privacy-goed-opgepakt-meer-aandacht-nodig-voor-informatiebeveiliging/>

⁸ IT-beveiliging binnen het voortgezet- en middelbaar beroepsonderwijs, Kantar & Breens Network, 2021 <https://breens.nl/whitepapers/whitepaper-veiligere-hybride-onderwijsomgeving/>

kennis en uitvoeringscapaciteit te organiseren, is schaalgrootte nodig. Zowel schaalgrootte binnen het funderend onderwijs, als in samenwerking met andere sectoren (hoger onderwijs, overheid, publieke sector).

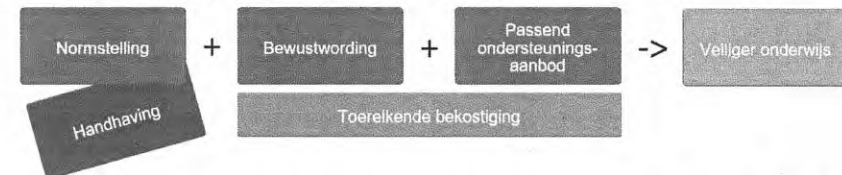
Tot slot is het voor schoolbesturen moeilijk om specifieke maatregelen af te dwingen bij een leverancier. Dit geldt voor kleine schoolbesturen, maar ook voor grote schoolbesturen is het moeilijk grote (internationale) partijen aan te spreken. Het gezamenlijk optrekken van de volledige onderwijssector richting Google in 2021 heeft er niet alleen toe geleid dat het mogelijk was om diepgravend privacyonderzoek te doen, maar ook om AVG-conforme voorwaarden af te dwingen bij een tech-reus⁹. En met name voor kleinere leveranciers geldt dat ze de veiligheid van hun product beter kunnen regelen als ze kunnen aansluiten op landelijke afspraken of voorzieningen. Dit borgt de keuzevrijheid voor scholen en zou moeten voorkomen dat de markt wordt gedomineerd door een beperkt aantal leveranciers. Daarnaast zijn er ook een aantal zaken die alleen door samenwerking of een gecoördineerde aanpak tot stand zijn te brengen: denk aan het delen van informatie over dreigingen, het oprichten van een CERT¹⁰ en het zorgen voor veilige dienstverlening voor identiteiten, gegevensuitwisseling en connectiviteit. Zonder samenwerking en/of de schaalgrootte van het Nederlands funderend onderwijs, zijn sommige maatregelen simpelweg niet mogelijk.

Oplossing

Digitale veiligheid en privacy zijn een basisvoorwaarde voor het Nederlandse onderwijs. Het doel van veilig digitaal funderend onderwijs vraagt meer dan alleen inzetten op bewustwording bij schoolbesturen: het is onzeker of dit tot resultaat leidt, het is kostbaar en duurt zeer lang voordat dit sectorbreed vruchten afwerpt. **Normstelling en handhaving** van die norm (waar moet ik aan voldoen, hoe kan ik daaraan voldoen en hoe ben ik hierop aanspreekbaar) zijn belangrijke instrumenten. Deze kunnen sneller en kansrijker tot succes leiden als er passend ondersteuningsaanbod is om daadwerkelijk, tegen aanvaardbare kosten, aan de norm te voldoen. Veel verantwoordelijkheden voor privacy en

⁹ <https://www.rtlnieuws.nl/tech/artikel/5240856/onderwijsinstelling-google-education-privacy-ap>

beveiliging liggen bij het schoolbestuur, daarom is **bewustwording** nodig om te zorgen dat binnen onderwijsinstellingen de juiste expertise aanwezig is om keuzes te maken en in control te zijn. Een integraal en **passend ondersteuningsaanbod** betekent dat scholen geholpen worden om veilig digitaal onderwijs te garanderen. Dit ondersteuningsaanbod moet aansluiten bij de behoeften van schoolbesturen, ontzorgen op de onderdelen waarin besturen uniform zijn, en dit alles tegen kosten die passen bij hun financiële mogelijkheden. Via een nationale impuls op basis van centrale financiering kan dit integrale aanbod worden gerealiseerd en gebruik hiervan worden gestimuleerd. Op deze manier kunnen schoolbesturen de digitale component van hun onderwijs en hun organisatie daadwerkelijk veilig inrichten. Het komt tegemoet aan een handelingsverlegenheid die nu ook vaak wordt ervaren. Een belangrijk aandachtspunt hierbij is **toereikende bekostiging**. Besturen moeten het absorptievermogen hebben om gebruik te maken van het ondersteuningsaanbod. Ook als dit aanbod passend en laagdrempelig is, is er toch nog werk te doen op een school. Ondanks het belang van normering en bewustwording zal het voor met name kleinere besturen lastig zijn om hier op een goede manier gebruik van te maken: de basale capaciteit en kennis die nodig is voor het maken van de juiste afspraken en gebruik van de ondersteuning is maar beperkt gekoppeld aan het aantal leerlingen of medewerkers.



Vier interventies dragen bij aan de oplossing van bovengenoemde vraagstukken. Als eerste het opstellen van een norm voor privacy en security in het funderend onderwijs en het activeren en bewust maken van schoolbesturen. In de tweede plaats een impuls aan de professionalisering en kennisdeling in de sector. Dit gaat zowel over de beschikbaarheid van basale kennis en professionalisering binnen onderwijsinstellingen, als over het delen van

¹⁰ <https://www.ncsc.nl/actueel/nieuws/2020/mei/28/ncsc-publiceert-handreiking-effectief-opereren-in-de-cert-gemeenschap>

kwestbaarheidswaarschuwingen met verantwoordelijken voor privacy en beveiliging. Ondersteuning bij het adequaat reageren op beveiligingsincidenten is een nadrukkelijk onderdeel van deze professionaliseringsslag. Ten derde het gezamenlijk optrekken als hele sector funderend onderwijs in het afdwingen, toetsen en controleren van afspraken bij leveranciers voor het veilig en privacyvriendelijk gebruiken van software. Ook een gemeenschappelijke aanpak richting partijen die actief zijn op de markt van ondersteuning bij privacy- en beveiligingsvraagstukken draagt bij een meer volwassen onderwijssector. Tot slot is een stelsel nodig van landelijke voorzieningen die scholen op een laagdrempelige manier helpen bij het veilig organiseren van het onderwijs. Veilige connectiviteit en gegevensuitwisseling moet voor scholen zijn als schoon water uit de kraan: een vanzelfsprekendheid op elke school waarbij het niet voldoen aan de minimale normen eigenlijk geen optie is. Met dit programma leggen we een fundament. Met landelijke voorzieningen die scholen zonder drempels kunnen gebruiken, met diensten om hen op hoger niveau te brengen en met aandacht voor bewustwording en normering. We nemen hierbij nadrukkelijk een voorbeeld aan de dienstverlening van SURF voor het hoger onderwijs en mbo en van de Informatiebeveiligingsdienst (IBD) voor gemeenten.

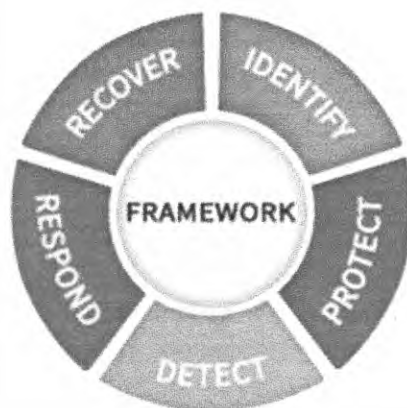
Resultaat

In dit programmaplan zijn vier actielijnen uitgewerkt: Normstelling en bewustwording, Professionalisering, Leveranciersmanagement en een Veilige en betrouwbare basisinfrastructuur. Met een nationale impuls kunnen alle schoolbesturen in het funderend onderwijs hun privacy, beveiliging en continuïteit op een duurzame manier hebben geregeld. Schoolbesturen zijn zich bewust van hun risico's en verantwoordelijkheden en kunnen gebruik maken van een landelijk ondersteuningsaanbod. Veilig digitaal onderwijs is dan niet langer incidenteel goed geregeld is, maar er ligt een stabiele basis voor toekomstige ontwikkelingen. Hiervoor is een grote inspanning nodig. Het programma zorgt ervoor dat schoolbesturen in het funderend onderwijs hun beveiliging, privacy en continuïteit van onderwijs op orde hebben, doordat schoolbesturen wakker zijn geschud, de benodigde kennis beschikbaar is, afspraken met leveranciers centraal worden gemaakt en schoolbesturen gebruik kunnen maken van een landelijke veilige en betrouwbare ict-infrastructuur.

1. Noodzakelijke interventies

Om de maatregelen in kaart te brengen die een organisatie moet treffen om digitale veiligheid goed te regelen, is het nuttig het NIST-model toe te passen. Het NIST-model voor cybersecurity is 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 NIST-framework wordt dan ook toegepast door alle Amerikaanse overheidsorganisaties. Het beschrijft de vijf typen activiteiten die nodig zijn om een tot de gewenste situatie te komen op het gebied van een veilige organisatie¹¹.

Het gaat hierbij om activiteiten die gericht zijn op het identificeren van risico's, maatregelen om de eigen data en infrastructuur te beschermen, het detecteren van dreigingen en beveiligingsincidenten, het adequaat reageren wanneer incidenten plaatsvinden en tot slot het herstellen van de schade na afloop van een incident. Het NIST-framework gaat er hierbij vanuit dat op alle vijf de typen activiteiten actie nodig is. Hoe die actie er precies uit ziet, kan verschillen per sector en kan per organisatie ook andere uitkomsten hebben. Het is hiermee vergelijkbaar met hoe een persoon omgaat met de dreiging van woninginbraken. We identificeren wat de dreigingen zijn (kostbare spullen in huis, raampjes en deuren waardoor iemand naar binnen kan komen), we beschermen ons hiertegen met sloten op de deur en dievenklauwen, met een alarmsysteem komen we erachter wanneer er wordt ingebroken, vervolgens kunnen we de politie bellen als reactie op de inbraak en hebben we een verzekeringsmaatschappij die ons helpt met de nasleep en het vergoeden van de



schade. Deze vergelijking laat ook zien dat op alle onderdelen van het NIST-model actie nodig is en we niet kunnen volstaan met het afsluiten van een verzekering en rekenen op de politie.

Het NIST-model is opgezet als een model voor een individuele organisatie om te bepalen of de juiste maatregelen zijn genomen. Wij gebruiken het NIST-model om de benodigde landelijke ondersteuning voor schoolbesturen in het primair en voortgezet onderwijs in kaart te brengen. Waar ieder bestuur zelf verantwoordelijk is voor het inventariseren van de eigen risico's en het nemen van de juiste maatregelen, stellen we voor generieke en veelvoorkomende risico's de juiste maatregelen beschikbaar. Met behulp van deze ondersteuning is het aan de schoolbesturen om hun eigen situatie te inventariseren en de daarbij passende maatregelen te nemen.

Voor het Nederlandse funderend onderwijs zal dat betekenen dat er een grote overeenkomst is in de maatregelen die scholen moeten nemen. Iedere school voert immers dezelfde taken en processen uit in een vergelijkbaar type organisatie. Dit betekent dat veel risico's voor alle scholen hetzelfde zijn, maar ook dat veel interventies en maatregelen uniform zijn tussen scholen. Bewustwording, DPIA's, veilige connectiviteit en verzekeringen, het zijn slechts enkele voorbeelden waarin het funderend onderwijs als sector specifieke karakteristieken kent, maar waarbinnen de individuele instellingen in zeer hoge mate vergelijkbaar zijn. Om het NIST-model toepasbaar te maken voor een landelijk ondersteuningsprogramma hebben wij een zesde activiteitencluster toegevoegd aan het model: professionaliseren. Als er geen sprake is van een basiskennisniveau, bewustwording en professionaliteit, dan is het moeilijk de juiste maatregelen te bepalen of te laten renderen. Daarom zijn voor een nationaal programma dat tot doel heeft de veiligheid en privacy van het Nederlandse funderend onderwijs op hoger plan te krijgen ook activiteiten nodig op het gebied van een brede professionaliseringsslag in de sector.

¹¹ <https://www.nist.gov/cyberframework>

Het NIST-model

Het NIST-model



Professionaliseren

Om maatregelen te nemen om het onderwijs veilig te maken en de privacy van leerlingen en medewerkers te beschermen is kennis nodig. Waar gaat het over? Hoe te starten met het inventariseren van risico's? Hoe te bepalen welke interventies nodig zijn? Dit geldt zowel voor bestuurders, voor stafmedewerkers als voor leraren en ondersteunend personeel. Zonder de juiste kennis en bewustzijn van thema 'veilig onderwijs', zowel binnen schoolbesturen als binnen de sector, kan niet worden gewerkt aan veiliger funderend onderwijs.

Identificeren

Schoolbesturen moeten weten welke risico's zij lopen bij gebruik van digitale middelen en verwerking van persoonsgegevens. Dit gaat over risico's voor de continuïteit van het onderwijs, bijvoorbeeld als connectiviteit, apparaten of applicaties niet gebruikt kunnen worden: denk in het bijzonder aan de hacks en ransomware-aanvallen die de afgelopen tijd veelvuldig in het nieuws zijn. Naast risico's voor de continuïteit van het onderwijs zijn er ook risico's die betrekking hebben op de privacy van leerlingen en medewerkers omdat er meer persoonsgegevens van leerlingen en medewerkers digitaal beschikbaar en verspreid zijn over meer systemen. Volledige veiligheid (als zoiets al bestaat) is onbetaalbaar en onwerkbaar. Er is een risicoanalyse nodig om te bepalen welk niveau van veiligheid gewenst is, en welke maatregelen er nodig zijn om dat niveau te bereiken. Een goede risicoanalyse begint met identificeren:

- Welke processen en gegevens zijn er? Wat moet kosten wat kost beschermd worden en wat is minder kritisch?
- Wat voor apparaten, applicaties en infrastructuur worden er gebruikt en zijn er bekende kwetsbaarheden? Welke leveranciers zijn hierbij betrokken en hebben die hun zaken op orde?
- Wat is de relevante regelgeving?

- Welke kwaadwillende partijen zijn er? En over welke middelen beschikken ze?

De antwoorden op bovenstaande vragen veranderen voortdurend: ransomware heeft DDoS aanvallen de laatste jaren ingehaald als grootse dreiging van buitenaf, de opkomst van onderwijs op afstand heeft de afhankelijkheid van ict enorm vergroot en applicaties die gisteren veilig leken blijken vandaag zo lek als een mandje. Deze bewegelijkheid betekent dat risicoanalyse voortdurend moeten worden bijgesteld.

Beschermen

Als de risico's voor de continuïteit van het onderwijs en de veiligheid en privacy van leerlingen en medewerkers bekend zijn is het zaak de juiste beschermende maatregelen te nemen. Dat kan gaan over het maken van goede afspraken met leveranciers, over maatregelen die betrekking hebben op het gedrag van medewerkers of door het gebruik van software en infrastructuur die door hun ontwerp bijdragen aan veiligheid en privacy. Denk aan:

- Identity en access management: Wie mag waarbij? En hoe weten we dat iemand ook echt is wie hij zegt dat hij is?
- Processen en procedures: Zijn er afspraken over de werkwijze? Zijn rollen en verantwoordelijkheden duidelijk? Ook bij leveranciers? Worden er regelmatig back-ups gemaakt en getest?
- Awareness: Zijn medewerkers en leerlingen getraind in wat ze wel en niet moeten doen om zo veilig mogelijk te werken?
- Technische maatregelen: Zijn alle zaken als segmentering, encryptie, firewalls, mailfiltering, virusscanning en veilig internet ingericht?

Beschermen is het aspect waar bij de meeste organisaties de bulk van de aandacht naar uitgaat, waardoor het voor veel mensen bijna synoniem is komen te staan aan "security".

Detecteren

Hoe goed beschermd een onderwijsinstelling ook is, er gaan beveiligingsincidenten plaatsvinden. Techniek verandert, de 'tegenstander' zit ook niet stil, diefstal of vergrendeling van data zal een verdienmodel blijven en

softwareleveranciers en medewerkers zullen fouten maken. Daarom is het goed te weten waar en wanneer het misgaat, zodat snel gereageerd kan worden om erger te voorkomen. Ook is belangrijk te achterhalen wat er precies is misgegaan en wat de impact is. Kan het een ander ook overkomen? Is er (mogelijk) data gelekt of buitgemaakt? Snel en adequaat reageren is niet alleen nodig bij de instelling waar het beveiligingsincident plaatsvindt, het is ook belangrijk deze informatie breed in de sector te delen zodat andere instellingen hun risico's beter kunnen afdekken.

Reageren

Snel en adequaat reageren op een beveiligingsincident is, zeker bij grote incidenten, vaak cruciaal. Of dit nu gaat om het niet meer gebruiken van bepaalde systemen, het informeren van de Autoriteit Persoonsgegevens of de politie of het inlichten van leerlingen en ouders: goed reageren is een complexe en stressvolle operatie. Regelmatig oefenen met crisissituaties en snel beschikbare ondersteuning vergroten de kans op een adequate reactie.

Herstellen

Een beveiligingsincident kan hoge kosten met zich meebrengen. Denk hierbij aan het herstellen van fysieke en digitale infrastructuur (vaak moet software opnieuw worden ingericht of hardware worden vervangen) of kosten die gemaakt worden voor een snelle reactie op een specifiek incident. Maatregelen voor herstel kunnen zowel praktische ondersteuning als financiële compensatie betreffen.

Maatregelen voor het funderend onderwijs

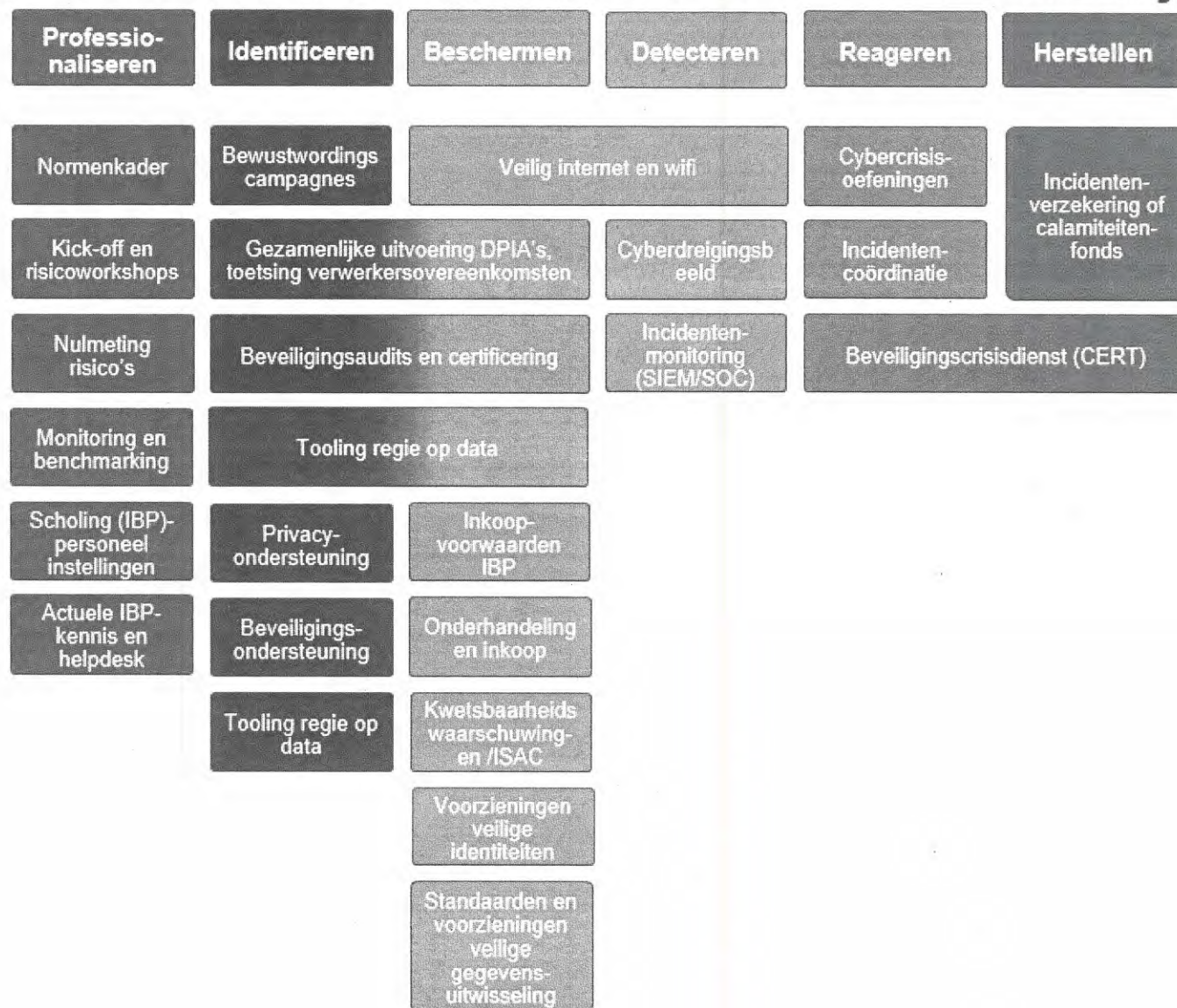
Voor het funderend onderwijs zijn op alle onderdelen van het NIST-model maatregelen nodig. Maatregelen om onderwijsbesturen bewust te maken, om tot een duidelijke normstelling te komen en een breed ondersteuningsaanbod. Hieronder is te zien hoe het totaal aan benodigde activiteiten eruit ziet wanneer dit wordt geplot op het NIST-model. De inhoud van deze activiteiten en de

programmatische aanpak om daar te komen worden verderop in dit plan toegelicht. Het is in ieder geval duidelijk dat op elk van de processen ondersteuning nodig is.

Het palet aan activiteiten zoals hieronder staat is niet uniek. In andere publieke sectoren is sprake van een soortgelijk integraal ondersteuningsaanbod om de veiligheid en cyberweerbaarheid te vergroten. Deze sectoren hebben de inspiratie gevormd voor de inhoud van dit programma. Het betreft hier in het bijzonder de Informatiebeveiligingsdienst (IBD) van de Vereniging Nederlandse Gemeenten en de dienstverlening van SURF op het gebied van security voor het hoger onderwijs en mbo. Ook Z-CERT, voor het zorgdomein, is een voorbeeld van een integraal ondersteuningspakket voor een hele sector. Een overzicht van de activiteiten van deze organisaties, geplot op het NIST-model, is te vinden in bijlage 1. Het is vanzelfsprekend dat voor de opbouw en uitvoering van het voorliggende programma een nauwe samenwerking noodzakelijk is met deze ondersteuningsorganisaties in het publieke domein.

Ook is gebruik gemaakt van kennis van de sector en inzicht in de problemen die binnen onderwijsbesturen in het primair en voortgezet onderwijs spelen. Hiervoor is onder andere gebruik gemaakt van input vanuit het Netwerk Informatiebeveiliging en privacy po/vo. Waar het fijn is om niet het wiel volledig zelf te hoeven uitvinden en te kunnen leren van organisaties als SURF en de IBD, is het toepasbaar maken van een dergelijk portfolio in het funderend onderwijs een expliciet uitgangspunt voor dit programma. Specifieke kenmerken van de sector funderend onderwijs zijn onder andere de omvang van de doelgroep (+/- 1300 schoolbesturen, meer dan 10.000 locaties, zo'n 2,5 miljoen leerlingen en 210.000 medewerkers) en de veelal beperkte professionaliteit, capaciteit en budgetten voor informatiebeveiliging en privacy.

Het NIST-model en activiteiten funderend onderwijs



2. Een programmatische aanpak

Om het benodigde ondersteuningsaanbod op te bouwen, bekend te maken bij schoolbesturen en ook daadwerkelijk te implementeren bij schoolbesturen is een programmatische aanpak nodig. Deze aanpak neemt de huidige situatie, waarin

op dit moment door samenwerkende schoolbesturen en landelijke organisaties al gebouwd wordt aan ondersteuning, als uitgangspunt.

Programma	
Context	▪ Scholen werken steeds meer digitaal om onderwijs te verzorgen ▪ Grotere afhankelijkheid en impact als het niet werkt ▪ Grotere risico's door toenemend gebruik van digitale data
Probleem	▪ Het is voor schoolbesturen onduidelijk wat zij moeten doen om veiligheid, privacy en continuïteit van het onderwijs te beschermen ▪ Schoolbesturen zijn zich onvoldoende bewust van de risico's die zij lopen en de verantwoordelijkheden zij hebben ▪ Het nemen van de juiste maatregelen leidt tot zeer hoge kosten voor schoolbesturen ▪ En als elk schoolbestuur al zelf aan de slag zou gaan ○ Cybersecurity is te complex om als schoolbestuur zelf te doen ○ Gebrek aan slagkracht richting leveranciers ○ Ondoelmatige besteding publieke middelen ○ Sommige doelen niet te realiseren zonder samenwerking of landelijke aanpak
Oplossing	▪ Schoolbesturen activeren en bewustzijn vergroten ▪ Opstellen van een norm voor beveiliging en privacy (weten wat te doen) ▪ Verhogen professionaliteit in de sector door onderling kennis te delen en kennis centraal beschikbaar te stellen ▪ Gezamenlijk optrekken richting leveranciers voor goede afspraken ▪ Laagdrempelige en passende landelijke ondersteuning voor schoolbesturen, waaronder infrastructurele voorzieningen en centrale incidentencoördinatie
Output	Zie uitwerking in dit programmaplan
Intermediate outcome	Schoolbesturen in het funderend onderwijs ▪ Zijn op de hoogte van hun verantwoordelijkheden en hoe ze hieraan kunnen voldoen ▪ Kunnen beschikken over de benodigde kennis op sectorniveau, bestuursniveau en bij medewerkers ▪ Maken goede afspraken met leveranciers ▪ Beschikken over een veilige en betrouwbare landelijke infrastructuur ▪ Werken voortdurend aan de verhoging van de veiligheid en de bescherming van privacy van het onderwijs
Outcome	Het funderend onderwijs is veiliger ingericht en beter in staat om te gaan met risico's en dreigingen

Vier actielijnen

Het eindresultaat van een integraal ondersteuningsportfolio voor schoolbesturen is in het voorgaande hoofdstuk uiteengezet aan de hand van het NIST-model. In

elke fase (professionaliseren, identificeren, beschermen, detecteren, reageren en herstellen) is een centrale en gecoördineerde aanpak nodig om tot een passende ondersteuning te komen.

Lijn	1. Normering en bewustwording	2. Professionalisering	3. Leveranciersmanagement	4. Veilige en betrouwbare basis-infrastructuur
Doel	Het is voor schoolbesturen duidelijk wat hun verantwoordelijkheden zijn op IBP-gebied, ze zijn op de hoogte van hun eigen IBP-situatie en werken voortdurend aan de bewustwording van hun medewerkers	Schoolbesturen hebben hun IBP professioneel ingericht, beschikken over de juiste IBP-kennis, delen deze met anderen en kunnen rekenen op professionele ondersteuning bij incidenten	Schoolbesturen beschikken over AVG-compliant software en hardware en gebruiken die op een veilige manier waarbij risico's zijn beperkt en maken doordachte keuzes voor hun IBP-ondersteuning	Schoolbesturen maken gebruik van een uniform, veilig en doelmatig ondersteuningsaanbod voor identiteitsmanagement, gegevensuitwisseling en connectiviteit
Activiteiten	▪ Sturen op basis van normen ▪ Bewustwording en activering ▪ Monitoring	▪ Professionalisering binnen de onderwijsinstelling ▪ Kennisopbouw en kennisdeling in de sector ▪ Centrale ondersteuning beveiligingsincidenten	▪ Veilig gebruik van software ▪ Inzicht in eigen applicatielandschap ▪ Passend marktaanbod IBP-ondersteuning	▪ Veilige identiteit ▪ Veilige gegevensuitwisseling ▪ Veilig connectiviteit
Intermediate outcome	Schoolbesturen zijn actief bezig met privacy en beveiliging	Het funderend onderwijs ontwikkelt lerend vermogen op gebied van privacy en beveiliging	Schoolbesturen verwerven een sterke en actieve positie ten opzichte van marktpartijen	Infrastructurele diensten in het onderwijs zijn gebaseerd op privacy en security by design
Outcome	Schoolbesturen zijn actief bezig met het voldoen aan geldende normen voor privacy en beveiliging	Schoolbesturen nemen de juiste privacy- en beveiligingsmaatregelen en reageren goed op incidenten	Onderwijsmiddelen en ict-systemen in het onderwijs zijn veilig en AVG-compliant en worden ook zo gebruikt binnen scholen	Digitale identiteiten, gegevensuitwisselingen en connectiviteit in het onderwijs zijn veilig

Om tot het brede en integrale ondersteuningsaanbod te komen, en om parallel daaraan te werken aan bewustwording en normstelling, zijn de diverse onderdelen van het eindplaatje op de volgende pagina in een programmatische structuur gezet.

Programma Veilig digitaal funderend onderwijs

Normering en bewustwording

Sturen op basis van normen

Bewustwording en activering

Monitoring

Professionalisering

Professionalisering binnen de onderwijsinstelling

Kennisopbouw en kennisdeling in de sector

Centrale ondersteuning beveiligingsincidenten

Leveranciers- en informatiemanagement

Veilig gebruik van software en hardware

Regie op data

Passend marktaanbod IBP-ondersteuning

Veilige en betrouwbare basis-infrastructuur

Veilige identiteiten

Veilige gegevensuitwisseling

Veilige connectiviteit

Programmainrichting

In dit document worden zeer beperkt uitspraken gedaan over de inrichting en governance van een programma Veilig digitaal funderend onderwijs. Dit vergt nog verdere uitwerking met vertegenwoordigers van de overheid, onderwijsinstellingen en expertise- en ondersteuningsorganisaties. In algemene zin kan hierover gezegd worden dat betrokkenheid van (vertegenwoordigers van) schoolbesturen van groot belang is. Dit geldt zowel voor betrokkenheid via vertegenwoordigende instanties zoals PO-Raad, VO-raad en SIVON, als voor de betrokkenheid van onderwijsbestuurders en hun medewerkers op het gebied van privacy en beveiliging. Dit geldt in het bijzonder bij de uitwerking van de verschillende bouwblokken. Het is duidelijk wat opgelost moet worden en welke instrumenten daarvoor in te zetten. Hoe deze precies in te richten en uit te voeren moet in samenspraak met de beoogde gebruikers worden bepaald. In het Netwerk Informatiebeveiliging en privacy po/vo van Kennisnet, SIVON, PO-Raad en VO-raad is inmiddels een kwart van alle schoolbesturen van Nederland vertegenwoordigd. Waar de focus nu nog vooral op privacyvraagstukken ligt, is met de instelling van een rondetafel cybersecurity ook hier meer aandacht voor het brede thema van digitale veiligheid. Ook de recent ingestelde adviesgroep Regie op ict, ingesteld door de PO-Raad en VO-raad, kan hier een rol in spelen.

Lijn 1: Normering en bewustwording

Wat is de definitie van veilig digitaal onderwijs? 100% veiligheid bestaat niet, maar welk niveau van veiligheid vinden we dan goed genoeg? Een landelijke norm is nodig om schoolbesturen deze handvatten te geven. Met een norm kunnen besturen worden aangesproken op hun verantwoordelijkheid hieraan te voldoen. Maar evenzo belangrijk is dat een norm kan bijdragen aan de bewustwording van het vraagstuk van veilig digitaal onderwijs. Een norm kan namelijk ook handvatten geven wat te doen om het onderwijs veilig te maken. We hoeven het wiel hiervoor zeker niet zelf uit te vinden: de AVG geeft duidelijke richtlijnen met betrekking tot privacy en zowel internationaal als landelijk zijn er diverse normen op het gebied van informatiebeveiliging. De vraag is vooral hoe te komen tot een norm die we in Nederland voldoende vinden voor de veiligheid van het funderend onderwijs, die gedragen wordt door het funderend onderwijs en die voldoende herkenbaar en toepasbaar is voor onderwijsinstellingen om mee te kunnen werken.

Met ruim 1300 schoolbesturen in verschillende omvang, zijn er grote verschillen in de uitgangssituatie op het gebied van privacy en informatiebeveiliging. Vanuit de monitor IBP 2020¹² weten we dat vrijwel elk bestuur aandacht besteedt aan privacy in de organisatie, bijvoorbeeld door het aanstellen van een functionaris gegevensbescherming. Maar de monitor laat ook zien dat aandacht voor digitale veiligheid en bijvoorbeeld het vaststellen en mitigeren van risico's door middel van DPIA's over de hele linie achter blijft. De grote groei van het aantal deelnemers van het Netwerk Informatiebeveiliging en Privacy po/vo laat zien dat veel schoolbesturen serieus vervolgstappen willen zetten op dit onderwerp. Hier kennen we ook de voorlopers onder de schoolbesturen die goed zicht hebben op hun eigen situatie, hun risico's en de uitdagingen waar ze voor staan. Maar we kennen ook de besturen voor wie IBP-beleid en de uitvoering hiervan erg abstract blijft. Duidelijke normstelling, weten wat je moet doen en welke acties daarvoor te ondernemen is hiervoor cruciaal. Hierbij is het niet de verwachting dat als de kaders duidelijk zijn, de digitale veiligheid van schoolbesturen snel

¹² <https://www.kennisnet.nl/artikel/7733/monitor-ibp-2020-privacy-goed-opgepakt-meer-aandacht-nodig-voor-informatiebeveiliging/>

geregeld is. Het vergt een duidelijk ondersteuningsaanbod met een passend groeipad.

Naast de betrokkenheid van de bestuurder, de kunde en het enthousiasme van de IBP'er of FG, speelt ook de omvang van een schoolbestuur een rol in de uitgangssituatie van een onderwijsbestuur. Veilige instellingen afspreken met de leverancier van het leerlingadministratiesysteem en deze implementeren in de instelling, vergt dezelfde basiskennis en -handelingen, of er nu sprake is van een bestuur met 150 leerlingen of met 15.000 leerlingen. Wat schoolbesturen moeten doen om aan de AVG te voldoen en wat zij daarvoor nodig hebben is voor elk bestuur hetzelfde. De weg om daar te komen en de manier waarop gebruik kan worden gemaakt van ondersteuning kan verschillen van bestuur tot bestuur.

Normering en bewustwording

Sturen op basis van normen	Bewustwording en activering	Monitoring
Opstellen normenkader voor privacy en beveiliging funderend onderwijs	- Kick-off en risicoworkshop schoolbestuur - Jaarlijkse bewustwordingscampagne voor personeel onderwijsinstellingen	- Nulmeting risico's en interventies - Tweejaarlijkse monitoring stand van zaken - Benchmarking

Bouwblok 1: Sturen op basis van normen

Bouwblok 1: Sturen op basis van normen	
Probleem	Er is geen duidelijke en passende norm voor digitale veiligheid in het funderend onderwijs
Oplossing	Het opstellen van een sectoraal normenkader dat toepasbaar is voor besturen in het funderend onderwijs
Output	Een normenkader voor beveiliging in privacy in het funderend onderwijs

Intermediate outcome	Aandacht voor het onderwerp digitale veiligheid en de verschillende facetten hiervan
Outcome	Schoolbesturen weten waar zij aan moeten voldoen om privacy en beveiliging binnen hun scholen op orde te hebben

Het moet voor schoolbesturen duidelijk zijn wat de **minimale normen voor digitale veiligheid en privacy** zijn en hoe zij hieraan kunnen voldoen. De AVG geeft aan dat onderwijsinstellingen 'passende technische en organisatorische maatregelen' moeten treffen. Maar welke zijn dit dan? Het is niet wenselijk dat schoolbesturen zelf het wiel gaan uitvinden en het is wel gewenst dat de sector een eenduidige standaard hanteren. Bestaande normenkaders als ISO zijn hierbij te weinig onderwijsspecifiek en behoeven dus een vertaling in een passend normenkader voor het primair en voortgezet onderwijs, dat samenhangt met de kaders voor mbo en hoger onderwijs. In andere sectoren (overheid/BIO, hoger onderwijs/SURFaudit) is succesvol ervaring opgedaan met het vaststellen van het gewenste niveau van veiligheid en het toepasbaar maken hiervan voor de eigen sector.

Naast de vertaling is ondersteuning nodig in de vorm van tooling, handreikingen en voorbeelden voor besturen om deze maatregelen zelf te implementeren. Voordat toetsing van de norm nuttig is, moeten schoolbesturen op de hoogte zijn van de voorwaarden en in staat zijn deze te implementeren. In de eerste fase van implementatie van de norm is het dan ook raadzaam deze in te zetten als een groei-instrument dat besturen richting geeft in de ontwikkeling van hun eigen organisatie en maatregelen op het gebied van privacy en beveiliging.

Een normenkader biedt verschillende niveaus van volwassenheid. Het is aan de overheid en/of het onderwijsveld zelf om te bepalen welk niveau wenselijk is en daarmee staat voor 'veilig onderwijs'. Het vergt verdere uitwerking om te bepalen welke wijze van normstelling het best passend is. Normstelling krijgt daarnaast pas zeggingskracht wanneer er duidelijke redenen zijn om hieraan te voldoen. Benchmarking en het eventueel openbaar maken hiervan is een van de manieren aan te tonen hoe een individuele organisatie zich verhoudt tot de norm. Benchmarking zou op deze manier een disciplinerende werking kunnen

hebben. Er zijn ook andere manieren denkbaar om schoolbesturen te toetsen of aan te spreken op de norm. Denk hierbij aan interne handhaving (via accountant en raad van toezicht), sectorale handhaving (via brancheorganisaties en eventuele collegiale toetsing) of handhaving door de rijksoverheid.

Bouwblok 2: Bewustwording en activering

Bouwblok 2: Bewustwording en activering	
Probleem	Schoolbesturen zijn zich onvoldoende bewust van privacy- en beveiligingsrisico's en ondernemen onvoldoende actie om risico's te beperken
Oplossing	Schoolbesturen individueel inzicht geven in hun voornaamste risico's en toeleiden naar ondersteuningsaanbod
Output	- Kick-off en advies bij schoolbesturen in po en vo (die in totaal 80% van de leerlingen vertegenwoordigen) - Jaarlijkse bewustwordingscampagne voor personeel onderwijsinstellingen
Intermediate outcome	Schoolbesturen zijn op de hoogte van het beschikbare landelijke IBP-aanbod en hoe dit hen kan helpen
Outcome	Schoolbesturen kennen hun IBP-risico's en werken actief aan de verbetering van privacy en beveiliging binnen hun onderwijsinstelling

Of binnen een schoolbestuur veel of weinig aandacht is voor privacy en beveiliging begint bij de bestuurder. Zijn er medewerkers, tijd en financiële middelen beschikbaar om de juiste maatregelen te nemen. Is er draagvlak voor scholing onder medewerkers? Is er ruimte om te investeren in veilige connectiviteit en infrastructuur? Met alle schoolbesturen in Nederland wordt geprobeerd contact te leggen om ze eenmalig meer kennis te geven over hun eigen situatie en te linken aan het aanbod dat het programma voor hen realiseert. Het startpunt is niet voor elk schoolbestuur gelijk, maar voor elk schoolbestuur is er wel een volgende stap in hun volwassenheid. De verschillen

qua veiligheidsniveau moeten worden overbrugd, de verschillen in de organisatiegraad tussen instellingen zijn een gegeven in dit programma. Het doel van de eerste programmalijn is om ieder schoolbestuur te activeren om verder aan te slag te gaan met IBP. Dat doen we door met schoolbesturen te inventariseren wat hun Ausgangssituatie is, door hen inzicht te geven in de maatregelen die ze moeten nemen voor digitaal veilig onderwijs, en door hen toe te leiden naar het aanbod dat centraal wordt ontwikkeld en aangeboden. Deze aanpak biedt veel ruimte voor maatwerk die past bij de lokale IBP-volwassenheidssituatie én de aard van het schoolbestuur.

Daarnaast zal jaarlijks aandacht nodig zijn om zowel bestuurders als medewerkers van onderwijsinstellingen scherp en bewust te houden, van zowel bestaande als nieuwe risico's. Met regelmaat zullen dus acties nodig zijn, waarbij het creativiteit en kennis vergt om de doelgroep steeds weer te bereiken en alert te houden.

- De precieze aanpak om **alle schoolbesturen te activeren** vergt nog verdere uitwerking, maar in grote lijnen ziet het traject er als volgt uit. Met zoveel mogelijk schoolbesturen wordt contact gezocht om hen persoonlijk op het voor hen passende spoor te zetten om de privacy en veiligheid binnen hun bestuur te verbeteren. In een intake worden de specifieke karakteristieken van het bestuur bepaald. De verwachting is dat qua inrichting de onderwijsbesturen weinig van elkaar verschillen, maar dat op basis van volwassenheid er wel verschillen zijn in de vervolgstap. Hoewel het advies in hoge mate maatwerk is per schoolbestuur, kan dus veel gebruik worden gemaakt van generieke adviezen en vervolgstappen. Bij de aanpak om tot een advies te komen is het belangrijk dat de bestuurder van de onderwijsinstelling betrokken is. Met de aanpak per bestuur worden drie doelen beoogd:
 - 1) Bestuurlijke bewustwording, waarbij het onderwerp op de agenda van het bestuur staat en het gesprek tussen het uitvoerend / beleidsniveau een nieuwe en blijvende impuls krijgt.
 - 2) Activering, omdat het op basis van het gesprek en de specifieke risico's binnen het bestuur duidelijk is dat actie nodig

is.

3) Toeleiding naar aanbod, want veel van wat scholen nodig hebben om de volgende stap te zetten wordt ontwikkeld binnen het programma. Zo heeft de persoonlijke benadering ook een functie in het bij elkaar brengen van (latente) vraag en beschikbaar aanbod.

Het centraal organiseren van de activering en adviezen voor alle schoolbesturen biedt twee grote voordelen. In de eerste plaats kunnen de gedetecteerde risico's centraal worden verzameld en geanalyseerd. Hierdoor kan landelijk veel sneller en specifieker aanbod worden ontwikkeld om risico's tegen te gaan, bijvoorbeeld in de vorm van een handreiking of door het gesprek aan te gaan met een veelgebruikte leverancier. Een tweede voordeel is dat de terugkoppeling en advisering snel plaats kan vinden naar de hele sector. Wanneer de 20 schoolbesturen die hetzelfde leerlingadministratiesysteem gebruiken hier dezelfde problemen mee ondervinden, kan het advies dat nodig is om risico's te verminderen bij alle volgende schoolbesturen direct worden overgenomen of via andere kanalen proactief worden verspreid.

- Om **medewerkers van onderwijsinstellingen bewust te maken** van privacy en beveiliging hebben de IBP-ers binnen onderwijsbesturen middelen nodig om dit te kunnen bewerkstelligen. Een manier die in het hoger onderwijs al langer wordt ingezet is de campagne Cybersave Yourself. Onderzocht moet worden hoe deze campagne ook ingezet kan worden in het primair en voortgezet onderwijs. Een andere manier om bewustwording te vergroten is door gebruik te maken van 'nep'-fishingmails of inzet van ethical hackers die bij medewerkers bijvoorbeeld wachtwoorden ontfutselen. In andere sectoren is gebruik gemaakt van (online) serious games of escape rooms om bij te dragen aan bewustwording en gedragsverandering op scholen. Het uitgangspunt is om instellingen zelf de middelen te geven om hun eigen personeel bewuster te maken van de risico's die ze lopen en deels ook veroorzaken. Deze activiteit hangt samen met het

professionaliseringsaanbod (microlearning) voor medewerkers van scholen.

Bouwblok 3: Monitoring

Bouwblok 3: Monitoring	
Probleem	Het is onvoldoende duidelijk in welke mate onderwijsbesturen hun privacy en beveiliging op orde hebben
Oplossing	Het uitvoeren van onderzoek naar de IBP-situatie van schoolbesturen
Output	▪ Nulmeting risico's en interventies privacy en beveiliging in het funderend onderwijs ▪ Tweejaarlijkse monitoring van de stand van zaken van privacy en beveiliging in het funderend onderwijs ▪ Mogelijk benchmarking op basis van het vast te stellen normenkader
Intermediate outcome	Onderwijsbesturen kunnen een inschatting maken van hun eigen IBP-situatie op basis van kennis uit de sector
Outcome	Inzicht in de mate volwassenheid van de sector op het gebied van privacy en security

Er zijn diverse beelden bij de mate waarin schoolbesturen in het funderend onderwijs hun privacy en beveiliging op orde hebben. In het verleden werd dit deels gemeten met de Monitor IBP po/vo. Een onderzoeksinstrument is nodig voor schoolbesturen om zelf meer inzicht te krijgen in de wijze waarop zij presteren, maar is ook nodig om te toetsen of de maatregelen van een nationale impuls voldoende effect hebben. Dergelijke monitoring (kwantitatief, maar ook kwalitatief in de vorm van een nulmeting bij een aantal besturen) is ook van belang om de activiteiten binnen een landelijk programma af te stemmen op actuele risico's en de behoeften van de doelgroep.

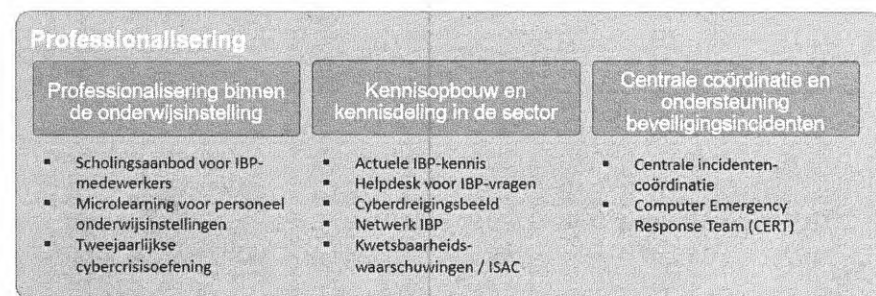
- Een eerste **nulmeting** onder een beperkte groep onderwijsbesturen van verschillende omvang moet in kaart brengen wat de voornaamste

risico's en grootste knelpunten zijn van schoolbesturen. In de verdere uitwerking van bouwblokken van het programma helpt dit om te prioriteren en het ondersteuningsaanbod zo in te richten dat dit optimaal aansluit bij de behoeften en praktijk van schoolbesturen. Wat er aan ondersteuning nodig is, is in hoge mate duidelijk, maar extra informatie is nodig over hoe deze specifiek vorm te geven en te prioriteren op de best passende manier. Ook wordt bij deze besturen de aanpak voor kick-off/activering getest (zie bouwblok 2).

- Om te weten of de ambities van dit actieplan worden behaald is het nodig tweejaarlijks te **monitoren** hoe onderwijsinstellingen scoren op het gebied van privacy en beveiliging. Waar staan scholen nu en zien we verbetering over de looptijd van de interventies. Worden scholen bewuster? Gaan ze goed om met de normen? En weten ze het ondersteuningsaanbod te vinden en te gebruiken? Maar bovenal gaat het om de vraag of de instellingen zelf in staat zijn om hun privacy en beveiliging in hun scholen beter te regelen en daarmee de veiligheid en continuïteit van het onderwijs beter te monitoren. Een deelgebied van monitorign om meer inzicht te krijgen, zowel voor schoolbesturen zelf als op sectorniveau, is het monitoren van het gebruik van beveiligingsstandaarden voor internet en e-mail door schoolbesturen en leveranciers.
- Een specifieke vorm om te bepalen hoe niet alleen de sector ervoor staat, maar om ook als onderwijsinstelling te bepalen hoe de zaken ervoor staan is **benchmarking**. De wijze waarop dit wordt vormgegeven moet nader onderzocht worden, maar in het mbo zijn goede ervaringen opgedaan met het in kaart brengen van de eigen situatie op basis van een normenkader. Door de eigen score te vergelijken met andere wordt snel duidelijk of en op welke terreinen nog werk aan de winkel is. De eventuele verhouding tussen monitoring en benchmarking moet nog verder worden uitgewerkt.

Lijn 2: Professionalisering

De mate van succes van alle ondersteuning die beschikbaar is voor scholen hangt af van de kennis die zij hebben om privacy en beveiliging binnen hun onderwijsbestuur goed te kunnen organiseren. Wat moet ik doen? Welke kennis heb ik daarvoor nodig? Hoe pak ik het aan? Zijn er stappenplannen of voorbeelddocumenten? En wat zijn de actuele dreigingen op dit moment, zodat ik mijn tijd en middelen zo gericht mogelijk in kan zetten? Daarnaast is er overdraagbare kennis nodig die IBP'ers in hun eigen instellingen in kunnen zetten om de medewerkers te wijzen op IBP-risico's en hen hierin te scholen.



Bouwblok 4: Professionalisering binnen de onderwijsinstelling

Bouwblok 4: Professionalisering binnen de onderwijsinstelling	
Probleem	Binnen onderwijsinstellingen zijn medewerkers slechts beperkt op de hoogte van wat zij kunnen doen om IBP-risico's te verkleinen; ook ontbreekt binnen instellingen de kennis en ervaring om goed met risico's en incidenten om te gaan
Oplossing	Een passend scholings- en oefenaanbod voor alle medewerkers binnen een onderwijsbestuur
Output	- Scholingsaanbod voor IBP-medewerkers - Microlearning voor medewerkers onderwijsinstellingen - Tweejaarlijkse cybercrisisoefening

Intermediate outcome	Medewerkers van onderwijsinstellingen zijn zich bewust van de privacy- en beveiligingsrisico's die aanwezig zijn bij hun dagelijks werk en hoe te reageren op incidenten
Outcome	Medewerkers van onderwijsinstellingen zijn zich bewust van privacy- en beveiligingsrisico's en handelen ernaar zodat risico's worden verkleind en adequaat wordt gereageerd op incidenten

Het beschermen van de privacy van leerlingen en bewaken van de continuïteit van onderwijs zijn verantwoordelijkheden van het onderwijsbestuur en daarmee van haar medewerkers. IBP-professionals binnen onderwijsbesturen moeten dan ook over de juiste kennis en opleiding beschikken om deze verantwoordelijkheid waar te kunnen maken. Maar goedgeschoolde IBP'ers alleen zorgen niet voor een veilige leeromgeving voor leerlingen, daar heeft al het personeel van een onderwijsinstelling een rol in, onderwijzend en niet-onderwijzend. Alle medewerkers van een onderwijsinstelling moeten zich bewust zijn van de risico's en hoe hun gedrag eraan bij kan dragen die risico's te beperken. Dit betreft dus zowel bewustwording als het verhogen van het kennisniveau bij medewerkers in het onderwijs. Naast het vergroten en eventueel toetsen van de kennis van medewerkers is het ook nodig om in de praktijk te oefenen en te beoordelen of de onderwijsinstelling in staat is om adequaat te reageren op beveiligingsincidenten.

- **Scholing van IBP-medewerkers** (denk aan beleidsmedewerkers ict/IBP, privacy officers, security officers en functionarissen gegevensbescherming) binnen de schoolbesturen is nodig om het onderwijsveld op het juiste kennisniveau te brengen wat betreft veiligheid en privacy. Voor hen zijn deels al scholingstrajecten beschikbaar in de markt. Hiervan zal dan ook gebruik worden gemaakt om tot het aanbod te komen dat nodig is voor deze doelgroep. Een gecoördineerde aanpak is van belang om te zorgen dat IBP'ers zich over de hele breedte van het funderend onderwijs professionaliseren. Naast het beschikbaar stellen van een aanbod dat getoetst is op kwaliteit en niveau, kan ook onderzocht worden of er een koppeling gemaakt kan

worden met deelname aan de samenwerking op sectorniveau, bijvoorbeeld door alleen contactpersonen toe te staan in de CERT die kunnen aantonen over een bepaald kennisniveau te beschikken. Hiermee zijn er ook directe nadelen gekoppeld aan het onvoldoende op orde hebben van de eigen professionaliteit in de organisatie. Het betreft zowel basisopleidingen voor FG's, IBP'ers, privacy en security officers als jaarlijkse masterclasses voor bijscholing en het up to date houden van kennis.

- Naast bewustwording is ook **scholing van de overige medewerkers van onderwijsinstellingen** noodzakelijk. Dit vindt eigenlijk plaats op het snijvlak tussen scholing en bewustwording. Omdat medewerkers in het onderwijs zicht weinig bewust zijn van de risico's en de werkdruk zeer hoog is, zullen zij weinig gemotiveerd zijn zich hierin te scholen. Daarom zetten we een systeem op van microlearning: een database van zeer korte uitlegfilmpjes over allerlei IBP-thema's, welke zijn gekoppeld aan kleine testjes. Dit is een werkwijze die lage impact op de werkdruk heeft. Door deze microlearning als hulpmiddel beschikbaar te stellen aan alle schoolbesturen, kunnen zij zelf bepalen op welke wijze zij hun personeel professionaliseren. Welke onderwerpen komen wanneer aan de orde? Welke waarde wordt toegekend aan de resultaten van de testjes? Dit is een brede wens van veel vertegenwoordigers van schoolbesturen: een laagdrempelige manier om niet alleen het bewustzijn maar ook de kennis van hun medewerkers te verhogen. In de jaren na de realisatie van de microlearning wordt deze jaarlijks geactualiseerd en indien nodig uitgebreid.
- In de gewenste situatie komen beveiligingsincidenten maar weinig voor bij onderwijsinstellingen. Maar we weten ook dat ze voorkomen en dat ze voor zullen blijven komen. Het is daarom belangrijk dat een schoolbestuur goed voorbereid is op een incident. Daarvoor zijn niet alleen plannen nodig, maar moet ook geoefend worden: **cybercrisisoefeningen**. Denk aan de jaarlijkse brandoefening die ook op veel bedrijven en scholen plaatsvindt. Om te zorgen dat alle procedures,

verantwoordelijkheden en acties goed geoefend kunnen worden zijn testscripts nodig, centrale ondersteuning, bijvoorbeeld als een centraal nummer gebeld moet worden of als een handeling in een softwaretoepassing moet worden uitgevoerd. Een centrale organisatie geeft ook mogelijkheden voor benchmarking van de uitkomsten. Onder de naam OZON organiseert SURF iedere twee jaar een sectorbrede gecoördineerde beveiligingsoefeningen voor het mbo en hoger onderwijs. Een meer laagdrempelige variant hiervan is NOZON. Naast een goede oefening voor de deelnemers geeft het de deelnemende onderwijsinstellingen een goed beeld van hoe ze ervoor staan en op welke onderdelen van hun praktijk en procedures verbeteringen nodig zijn. Voor de totstandkoming en uitvoering van cybercrisisoefeningen in het po en vo zal de samenwerking worden gezocht met SURF.

Bouwblok 5: Kennisopbouw en kennisdeling in de sector

Bouwblok 5: Kennisopbouw en kennisdeling in de sector

Probleem

Het ontbreekt onderwijsbesturen aan de specifieke kennis die nodig is om de juiste maatregelen met betrekking tot privacy en beveiliging te bepalen en te implementeren

Het is voor scholen onvoldoende duidelijk wat zij moeten doen om aan de normen voor digitale veiligheid en privacy te voldoen en hoe zij de privacy en veiligheid van hun leerlingen en medewerkers moeten borgen
Binnen individuele instellingen is veel relevante kennis, onder andere over dreigingen en incidenten en best practices over hoe hiermee om te gaan, aanwezig die van belang is voor andere instellingen maar daar niet bekend is

Oplossing

Het organiseren van een sectorbrede community waarin kennis en informatie over het goed regelen van privacy, beveiligingsdreigingen en -

	maatregelen en (inter)nationale ontwikkelingen beschikbaar wordt gesteld en onderling wordt gedeeld
Output	▪ Actuele landelijke kennisbasis ▪ Helpdesk voor IBP-vragen ▪ Netwerk IBP ▪ Tweejaarlijks dreigingsbeeld ▪ Kwetsbaarheidswaarschuwingen ▪ Information sharing and analysis center (ISAC)
Intermediate outcome	Schoolbesturen werken samen om professionaliteit in de sector te verhogen en risico's en dreigingen sectorbreed te verlagen en onderwijsbesturen beschikken over de kennis die zij nodig hebben voor het goed organiseren van privacy en beveiliging in hun instellingen.
Outcome	De professionaliteit in de sector op het gebied van privacy en beveiliging is verhoogd waardoor en risico's en dreigingen sectorbreed te zijn verlaagd

Schoolbesturen zijn wettelijk verantwoordelijk voor het op orde hebben van de privacy van hun leerlingen en medewerkers en de beveiliging van data en systemen. Om aan die verantwoordelijkheid invulling te kunnen geven is de juiste kennis nodig: kennis over wat te doen, kennis over hoe dit te doen, en kennis over privacy- en beveiligingsontwikkelingen van buiten het onderwijs. Door landelijk de benodigde kennis te ontwikkelen en te delen, zijn schoolbesturen beter in staat om op een effectieve en risicogerichte manier maatregelen te nemen voor hun eigen onderwijsinstellingen. Het leidt er ook toe dat een eenduidige interpretatie ontstaat van ontwikkelingen en dreigingen, wat de uniformiteit in de sector verhoogt.

¹³ <https://aanpakibp.kennisnet.nl/>

Het borgen van privacy en digitale veiligheid in de onderwijssector kan niet zonder samenwerking tussen schoolbesturen. Samenwerking om kennis te delen, om gezamenlijk marktmacht op te bouwen voor onderhandelingen en om gezamenlijk onderzoek te doen naar de wijze waarop leveranciers omgaan met privacy en beveiliging. Maar samenwerking is ook nodig om adequaat te kunnen reageren op beveiligingsincidenten. Niet alleen omdat hier zeer specifieke kennis voor nodig is van zowel het onderwijs als van cybersecurity, maar ook omdat het van belang is dat dreigingen en incidenten snel gedeeld kunnen worden binnen het hele onderwijsveld.

- Een **landelijke kennisbasis** is nodig als vertrekpunt van het goed regelen van privacy en beveiliging in de eigen instelling. De Aanpak IBP¹³ van Kennisnet heeft zichzelf in de afgelopen jaren bewezen als het vertrekpunt voor stafmedewerkers in het funderend onderwijs die rol van IBP'er, FG, privacy officer of security officer hebben. Het gaat hierbij om praktische handvatten en de achterliggende onderbouwing op basis van onder andere de AVG. Het betreft uitleg van de wijze waarop scholen moeten handelen en voorbeelddocumenten, modelovereenkomsten, factsheets en handreikingen om direct mee aan de slag te gaan. Deze kennisbasis moet continu worden uitgebreid met nieuwe informatie, bijvoorbeeld naar aanleiding van de DPIA Google of uitspraken van het Europese hof. Een eenduidige vertaling van bijvoorbeeld nieuwe wetgeving, nieuwe beveiligingstechnieken of IBP-afspraken zoals recent met Google zijn gemaakt draagt bij aan een hoger kennisniveau van individuele instellingen en professionalisering van de sector als geheel. Op termijn wordt de landelijke kennisbasis steeds meer gevoed met informatie en kennis die wordt opgedaan binnen het Netwerk IBP, andere sectoren (IBD, SURF), het Information Sharing and Analysis Center, de CERT en vanuit het Security Operations Center. NB. Deze begrippen worden verderop in het plan verder uitgelegd. Voor schoolbesturen die actief aan de slag gaan moet ook een

vraagbaak beschikbaar zijn als ze vastlopen bij het zetten van de volgende stap.

- Eigenaarschap in de sector is een belangrijk vertrekpunt om beveiliging en privacy naar een hoger plan te tillen. Waar is behoefte aan bij schoolbesturen? Hoe komen we (samen met schoolbesturen) tot een ondersteuningsaanbod dat past bij de praktijk binnen onderwijsinstellingen? Welke producten en contracten zijn belangrijk en wat zijn actuele vraagstukken waar veel schoolbesturen mee worstelen. Vertegenwoordigers van schoolbesturen (IBP-ers, privacy en security officers en functionarissen gegevensbescherming) werken in het **Netwerk IBP** met elkaar samen. Zij sturen het netwerk aan, voeren samen activiteiten uit (zoals DPIA's), wisselen kennis, ervaringen en handige documenten uit en bieden elkaar inspiratie. Het Netwerk IBP geeft niet alleen richting aan de landelijke ondersteuning, maar functioneert ook als communicatiekanaal. Vervolgstappen in de groei van het netwerk liggen in het nog beter benutten van de kennis die in de sector aanwezig is, bijvoorbeeld in expertgroepen die advies geven bij vraagstukken.
- Specifieke informatie die nodig is, is inzicht in actuele dreigingen. Dit helpt om de juiste keuzes te maken voor bijvoorbeeld extra beveiligingsmaatregelen. Landelijk houdt het Nationaal Cyber Security Centrum (NCSC) een **dreigingsbeeld** bij van actuele cyberdreigingen. Dit is zeer waardevolle informatie, maar is niet direct toepasbaar voor medewerkers van onderwijsinstellingen. De risico's in het onderwijs kunnen ook veel specifieker zijn, bijvoorbeeld door de specifieke software die gebruikt wordt, door het werken met (bijzondere) persoonsgegevens van minderjarige leerlingen en door het IBP-volwassenheidsniveau op specifieke onderwerpen. Een tweejaarlijks een cyberdreigingsbeeld voor het onderwijs bevat een overzicht met de meest actuele dreigingen. Dit helpt schoolbesturen niet zozeer om direct actie te ondernemen, maar wel om voor de middellange termijn accenten te leggen in het eigen IBP-beleid en aanvullende activiteiten

ter bescherming in gang te zetten. Het hoger onderwijs en mbo kennen al enkele jaren een cyberdreigingsbeeld, daarom zal voor de uitvoering samenwerking worden gezocht met SURF. In de eerste fase wordt ook gewerkt met een uitvraag onder scholen om zo een goed beeld te krijgen van de door hen ervaren problemen. Hiervoor wordt samengewerkt met de activiteiten binnen het bouwblok 'bestuurlijke bewustwording en activering'.

- Om snel te reageren is het belangrijk dat er gericht informatie over acute dreigingen wordt gedeeld met schoolbesturen. Deze **kwetsbaarheidswaarschuwingen** bestaan uit een beschrijving van het probleem, informatie over oplossingen of workarounds en een risicoanalyse. Denk hierbij ook aan informatie over patches voor kwetsbaarheden in software die noodzakelijk zijn om zo snel mogelijk op te volgen. Dit stelt schoolbesturen in staat snel te reageren op mogelijke dreigingen. Op basis van meldingen uit het Netwerk IBP, van het NCSC, van partners of van leveranciers wordt bepaald welke informatie relevant is voor schoolbesturen, dit kan bijvoorbeeld ook specifieke informatie zijn voor besturen die een bepaald systeem gebruiken. Het doel is om het Netwerk IBP door te ontwikkelen tot een **Information Sharing and Analysis Center (ISAC)**. Het betreft hier een netwerk van vertrouwde personen waarbinnen (vertrouwelijke) informatie gericht kan worden gedeeld. Het is voor een leverancier aantrekkelijker om een kwetsbaarheid te delen wanneer dit vertrouwelijk wordt behandeld. Door het netwerk op deze manier door te laten groeien, waken schoolbesturen, met brede ondersteuning van experts en uitvoeringscapaciteit, zelf over de veiligheid van de sector. Voor een community geldt dat er een bepaalde mate van afbakening moet zijn (lees: de 1300 schoolbesturen in het primair en voortgezet onderwijs). Maar een kenniscommunity staat niet op zichzelf: deze werkt (op de achtergrond) zeer nauw samen met andere communities, zoals voor hoger onderwijs (SURF), gemeenten (IBD), zorg (Z-CERT) en bedrijfsleven, maar ook met het CIP en NCSC als landelijke expertisecentra.

Bouwblok 6: Centrale coördinatie en ondersteuning beveiligingsincidenten

Bouwblok 6: Centrale coördinatie en ondersteuning beveiligingsincidenten	
Probleem	Schoolbesturen weten niet goed wat te doen bij een beveiligingsincident en maken daardoor trage of 'verkeerde' keuzes en moeten steeds het wiel opnieuw uitvinden
Oplossing	Expertise over het reageren op beveiligingsincidenten centraal organiseren en deze inclusief ondersteuning beschikbaar maken voor alle schoolbesturen
Output	- Centrale incidentencoördinatie - CERT/CSIRT
Intermediate outcome	Landelijk wordt inzicht verkregen en expertise opgebouwd over dreigingen, maatregelen en best practices bij het reageren op beveiligingsincidenten
Outcome	Schoolbesturen worden ondersteund in het snel en adequaat reageren op privacy- en beveiligingsincidenten

Hoe goed scholen ook beveiligd zijn door netjes alle protocollen te volgen, goede afspraken te maken met leveranciers en gebruik te maken van veilige ict-voorzieningen, het gaat een keertje mis. Cybercriminelen zullen zich blijven ontwikkelen en ook door onbedoeld gedrag zit een ongeluk in een klein hoekje. Hoe te reageren is met name in de eerste fase cruciaal. Ondersteuning bij incidenten is niet alleen noodzakelijk omdat dit zeer specialistische kennis behoeft die moeilijk op te bouwen is. Het centraal organiseren hiervan vergroot ook het lerend vermogen van de hele sector omdat een crisis bij één onderwijsinstelling belangrijke lessen kan bevatten voor beschermende maatregelen bij andere instellingen.

- Wanneer er grootschalige beveiligingsincidenten zijn waar bijvoorbeeld een grote leverancier bij betrokken is, ligt het primaat voor de afhandeling daarvan nu bij de leverancier en bij de individuele schoolbesturen. De leverancier stemt dan vaak met enkele klanten af over de te volgen aanpak en wijze van communiceren. Maar het komt

ook voor dat de leverancier helemaal geen afstemming zoekt over de te volgende aanpak. Door grotere **incidenten centraal te coördineren** kan namens de scholen een meer leidende en geïnformeerde rol worden ingenomen bij het afhandelen van incidenten. Het geeft ook voor zowel leveranciers als scholen een veilige plek waar incidenten kunnen worden gemeld en een risicoschatting kan worden gemaakt in situaties waar nog veel onduidelijkheid is. Hiermee kan een betere afweging worden gemaakt over de te nemen vervolgstappen, maar kan informatie over dreigingen en mogelijke incidenten ook in een vroeg stadium worden gedeeld met andere schoolbesturen. Een centrale incidentenregistratie geeft hiermee niet alleen inzicht in de veiligheid van de sector, maar geeft schoolbesturen meer regie in situaties waarin er sprake is van een beveiligingsincident.

- Wanneer er sprake is van een beveiligingsincident is het zaak zo snel en zo goed mogelijk te handelen. Beveiligingsincidenten kunnen zeer complex zijn (bijvoorbeeld bij ransomware-aanvallen) en het vergt specifieke kennis om goed te reageren. Een medewerker van een schoolbestuur, of een bestuurder zelf, maakt dit als het goed is maar een enkele keer in zijn loopbaan mee. Daarom is het van belang de kennis hierover centraal te organiseren in een **CERT** (Computer Emergency Response Team)¹⁴. Voor de ondersteuning bij het reageren op incidenten is een team paraat dat op vrijwel dagelijkse basis te maken heeft met beveiligingsincidenten. Zij kennen niet alleen die specifieke ransomware-aanval, maar weten ook hoe gehandeld is bij alle andere aanvallen op scholen in het land, en wisselen kennis uit met andere sectoren zoals hoger onderwijs en zorg en met het NCSC. Wanneer een school slachtoffer wordt van een incident, belt deze met het CERT. De medewerker van het CERT voert vervolgens een triage uit (wat is er aan de hand, wat zijn de goede vervolgstappen), kan ondersteunen in het lokale (goedgetrainde) crisisteam totdat gespecialiseerde partijen zijn ingeschakeld en kan een rol spelen in de

¹⁴ In sommige branches wordt gesproken van een CSIRT (Computer Security Incident Response Team)

communicatie naar leerlingen, ouders, medewerkers en pers. Ook speelt het CERT een rol in het informeren van andere onderwijsinstellingen of ketenpartijen (zoals softwareleveranciers). Ook in de afhandeling (hoe herstel ik de schade en kan het onderwijs zo snel mogelijk weer doorgang vinden) assisteert het CERT. Door deze gemeenschappelijke kennis in te zetten wordt zo adequaat mogelijk gereageerd op elk incident, worden risico's beperkt, worden kosten van reactie en herstel verminderd en kan het onderwijs zo snel mogelijk weer worden opgestart.

Lijn 3: Leveranciersmanagement

De systemen waarin persoonsgegevens zijn opgeslagen of worden verwerkt moeten veilig zijn en werken conform wetgeving en de belangen van het onderwijs. Hiervoor moeten schoolbesturen afspraken maken met leveranciers en moeten leveranciers zich aan deze afspraken houden. Het overgrote deel van de verwerking van persoonsgegevens in het primair en voortgezet onderwijs vindt plaats in cloudtoepassingen. Niet op een server die bij het schoolbestuur staat, maar op de servers die gebruikt worden door uitgevers of leveranciers van administratieve systemen. Mede daarom is het van belang goede afspraken te maken met leveranciers over hoe zij de privacy van leerlingen en medewerkers borgen, hoe zij hun data en verbindingen beveiligen en hoe zij omgaan met beveiligingsincidenten. Ieder schoolbestuur in het po en vo maakt gebruik van een groot aantal systemen om het onderwijs te organiseren en om les mee te geven. Maar gelukkig maken ook heel veel scholen gebruik van dezelfde systemen, en gebruiken zij deze systemen ook vrijwel allemaal op dezelfde wijze. Dit levert grote kansen op om samen op te trekken en dit samen te organiseren. Gezamenlijk vaststellen wat de juiste inhoud van de verwerkersovereenkomst is, gezamenlijk risico's inventariseren en leveranciers hierop aanspreken, gezamenlijk onderhandelen over verbeteringen op het gebied van privacy en beveiliging en gezamenlijk (laten) controleren of de leverancier alle maatregelen ook in de praktijk heeft gebracht. Als een leverancier dit voor één schoolbestuur goed kan regelen of inzichtelijk kan maken, is er geen reden om de privacy en veiligheid niet ook voor alle andere schoolbesturen goed te regelen.

Maar het moet voor scholen ook duidelijk zijn met welke partijen zij privacy- en beveiligingsafspraken moeten maken, wat de status daarvan is en of aanvullende actie nodig is op bijvoorbeeld wijzigingen. Tot slot kan geen enkel onderwijsbestuur alle maatregelen in de praktijk brengen zonder specialistische kennis. Denk hierbij aan ondersteuning op privacygebied voor het uitvoeren van een instellingsspecifieke DPIA of beveiligingsondersteuning bij het uitvoeren van tests om zwakke plekken in de beveiliging bloot te leggen. Omdat het onderwijs hierin een specifieke maar potentieel ook omvangrijke markt is, is het van toegevoegde waarde om scholen hierin te ondersteunen zodat hier een vraaggestuurde markt ontstaat. Het gezamenlijk zoeken naar een gewenste

oplossing voor verzekering (in de markt of via een calamiteitenfonds) is een specifiek aandachtspunt.

Leveranciers- en informatiemanagement		
Veilig gebruik van software en hardware	Regie op data	Passend marktaanbod IBP-ondersteuning
▪ Uniforme inkoopvoorwaarden ▪ Onderhandelings- en inkooptrajecten ▪ Toetsing verwerkersovereenkomsten ▪ Centrale DPIA's ▪ Centrale beveiligingsaudits / certificering	▪ DPIA-tooling ▪ Tooling eigen applicatielandschap in kaart ▪ Systeem voor registratie verwerkersovereenkomsten ▪ Tooling dataregister	▪ Transparantie in marktaanbod ▪ PvE's dienstverlening privacy (waaronder risicoanalyses) ▪ PvE en eventuele inkoop dienstverlening security ▪ PvE en inkoop cybersecurity-verzekering of calamiteitenfonds

Bouwblok 7: Veilig gebruik van software en hardware

Bouwblok 7: Veilig gebruik van software en hardware	
Probleem	De veiligheid van software die scholen gebruiken is onvoldoende of onbekend en individuele scholen zijn niet in staat om goede afspraken te maken met leveranciers
Oplossing	Het centraal onderhandelen, toetsen en controleren van afspraken met leveranciers en scholen ondersteunen hier gebruik van te maken
Output	▪ Uniforme inkoopvoorwaarden IBP ▪ Onderhandeltrajecten met grote leveranciers ▪ Getoetste verwerkersovereenkomsten ▪ Centraal uitgevoerde DPIA's ▪ Audits en certificeringssysteem voor leverancier
Intermediate outcome	Leveranciers die softwareproducten aan het onderwijs leveren hebben hun privacy- en beveiligingsmaatregelen op orde
Outcome	Schoolbesturen maken op een verantwoorde manier gebruik van veilige software

Uniformiteit in de eisen die schoolbesturen stellen aan leveranciers (bijvoorbeeld door te verwijzen naar standaarden en ketenafspraken) en in de wijze waarop ze dit controleren is nodig. Deze uniformiteit heeft een positief effect op marktwerking, alle leveranciers weten immers vooraf waar ze aan moeten voldoen om met willekeurig welk schoolbestuur in Nederland zaken te doen. Maar het levert ook een groot efficiëntievoordeel op in het toetsen of de eisen in de praktijk worden nageleefd. Door dit centraal te organiseren is voor alle scholen duidelijk dat een product veilig te gebruiken is, of kan gezamenlijk in gesprek worden gegaan met de leverancier.

- Het proces voor het gebruik van software en hardware om het onderwijsproces te ondersteunen begint bij het stellen van de juiste eisen aan de beveiliging van systemen en de omgang met persoonsgegevens en privacy. **Uniforme inkoopvoorwaarden** maken voor schoolbesturen duidelijk 'wat veilig is' en voor leveranciers wat de IBP-randvoorwaarden zijn om te kunnen participeren in de onderwijsmarkt. Het mes snijdt aan twee kanten: veiligheid voor onderwijs, en duidelijkheid en ruimte voor marktwerking bij private partijen. Op basis van deze inkoopvoorwaarden kan eventueel ook gezamenlijk worden ingekocht, denk hierbij ook aan devices voor leerlingen.
- Met grotere partijen, bijvoorbeeld grote technologiebedrijven of uitgevers, is het minder vanzelfsprekend dat zij zich direct zullen voegen naar de inkoopvoorwaarden voor privacy en beveiliging zoals deze worden gehanteerd door het Nederlandse onderwijs. Hier zijn vaak omvangrijke **onderhandelingen en inkooptrajecten** voor nodig. Een Nederlandse onderwijsinstelling kan privacy- en beveiligingsmaatregelen bij dit soort partijen vrijwel nooit alléén afdwingen. Hiervoor is samenwerking en inkoopmacht nodig. In de eerste plaats binnen het funderend onderwijs, maar steeds vaker ook binnen de hele onderwijskolom van po tot en met wo. En voor echt grote partijen zoals Google en Microsoft geldt dat onderhandelingen op

een nog grotere schaal plaatsvinden, bijvoorbeeld met de Nederlandse centrale overheid, zorginstellingen en lokale overheden.

Onderhandeling met grote partijen over veiligheid en privacy moet ook de komende jaren veel aandacht te krijgen om de veiligheid én de autonomie van het Nederlandse onderwijs te kunnen garanderen.

- Nadat het schoolbestuur een partij heeft geselecteerd op basis van vooraf vastgestelde eisen, waaronder het accepteren van de inkoopvoorwaarden van het schoolbestuur, is het zaak een goede **verwerkersovereenkomst** af te sluiten waarin afspraken staan over de omgang met persoonsgegevens in het kader van privacy en beveiliging. Een belangrijke stap in de veilige omgang met gegevens van leerlingen en medewerkers is dat met externe partijen niet meer persoonsgegevens worden uitgewisseld dan strikt noodzakelijk is, dat deze persoonsgegevens voor de juiste doelen worden verwerkt en dat de leverancier de juiste technische en organisatorische maatregelen heeft getroffen om deze gegevens veilig te verwerken. Deze afspraken worden vastgelegd in een verwerkersovereenkomst. Een gemiddeld Nederlands schoolbestuur is verantwoordelijk voor zeker 150 verwerkingsrelaties en evenzoveel overeenkomsten. Echter, het is voor veel schoolbesturen moeilijk om deze overeenkomsten te beoordelen en indien nodig aan te passen. Het aantal leveranciers in het primair en voortgezet onderwijs is redelijk beperkt (er zijn een paar honderd leveranciers die gezamenlijk het overgrote deel van alle verwerkingen van alle scholen dekken). Daarom loont het om schoolbesturen te ondersteunen gezamenlijk verwerkersovereenkomsten te beoordelen. Wanneer besturen deze kennis met elkaar delen en gezamenlijk met een leverancier in gesprek gaan, verhoogt dit de veiligheid voor alle besturen. Omdat er al veel systemen gebruikt worden en verwerkersovereenkomsten in omloop zijn, richt het programma zich in de eerste fase op de inhaalslag door bestaande overeenkomsten te toetsen. Omdat naast privacy en beveiliging ook de continuïteit van het onderwijs steeds belangrijker wordt, moet worden onderzocht of beoordeling van SLA's (Service Level Agreements) onderwijsinstellingen

helpt met het maken van keuzes en het sluiten van goede contracten.

- Met een **Data Protection Impact Assessment (DPIA)** bepaalt het schoolbestuur wat de risico's van een verwerking zijn, hoe hoog ze zijn, met welke maatregelen deze risico's kunnen worden weggenomen of verminderd en of de restrisico's aanvaardbaar zijn. Elk schoolbestuur moet zelf een DPIA uitvoeren voor elke nieuwe verwerking of gewijzigde verwerking die waarschijnlijk een hoog privacy-risico met zich meebrengt. Maar scholen verwerkten ook al persoonsgegevens voor de invoering van de AVG en dus zijn er nog veel verwerkingen, gekoppeld aan systemen, die getoetst moeten worden. Door de systemen die scholen gebruiken te onderwerpen aan centraal uitgevoerde DPIA's kan zowel een efficiëntieslag als een kwaliteitsslag worden gemaakt. Met behulp van de uitkomsten van de centraal uitgevoerde DPIA's kost het schoolbesturen minder tijd en moeite om zelf een instellingsspecifieke DPIA uitvoeren. Bovendien zorgt het veelal voor de nodige aanpassingen bij leveranciers om systemen veilig te kunnen gebruiken. Ook hiervoor geldt dat er grote winst is te behalen door centraal DPIA's uit te voeren bij de 300 á 400 meest-gebruikte partijen.
- Als de juiste contracten zijn afgesloten en de risico's van een verwerking zijn gemitigeerd, dan is er nog steeds geen zekerheid dat de betreffende leverancier zich ook aan deze afspraken houdt en de benodigde beveiligingsmaatregelen heeft getroffen. Een **audit** is een goede manier om in het bedrijf en de systemen van een leverancier te kijken of alle afgesproken maatregelen zijn geïmplementeerd en worden nageleefd. Ook hierbij geldt de kracht van een centrale aanpak. Het is voor een individueel schoolbestuur te kostbaar en omvangrijk om bij een leverancier een volledige audit uit te laten voeren, laat staan op alle systemen die een school gebruikt. Bovendien geldt dat het resultaat van een audit automatisch geldt voor alle andere gebruikers. Omdat er sprake is van een redelijk afgebakend aantal leveranciers wordt ook hier een centrale aanpak gevolgd, waarbij leveranciers volgens een gestandaardiseerde aanpak worden geaudit door externe auditors en de

resultaten op passende wijze worden gedeeld met alle schoolbesturen in het primair en voortgezet onderwijs. Mogelijk leidt dit tot een **certificeringssysteem** voor het (funderend) onderwijs. Ook wordt gezamenlijk gemonitord of een leverancier de toegezegde verbeteringen daadwerkelijk doorvoert.

Bouwblok 8: Inzicht in eigen applicatielandschap

Bouwblok 8: Inzicht in eigen applicatielandschap	
Probleem	Schoolbesturen hebben onvoldoende overzicht van de partijen waarmee ze privacy- en beveiligingsafspraken moeten maken en wat de status daarvan is
Oplossing	Laagdrempelige en toegankelijke tooling om het overzicht van het eigen applicatiegebruik te krijgen en het inzicht in de daarover gemaakte afspraken te verhogen
Output	▪ Tooling eigen applicatielandschap in kaart ▪ Tooling voor beheer dataregister ▪ Tooling uitvoeren instellingsspecifieke DPIA ▪ Systeem dat ondersteunt bij het beschikken over de juiste, ondertekende verwerkersovereenkomsten
Intermediate outcome	Schoolbesturen zijn in staat beter regie te voeren over inkoop, gebruik en beheer van softwaresystemen
Outcome	Schoolbesturen hebben meer overzicht en grip op hun privacy- en beveiligingsafspraken met leveranciers

Veel schoolbesturen hebben beperkt zicht op alle applicaties die binnen hun bestuur gebruikt worden, op de data die hierin wordt verwerkt (en de doelen die hiermee gediend worden) en op de afspraken die gemaakt zijn met leveranciers. Een belangrijk onderdeel van het maken van de juiste afspraken met leveranciers is dan ook het hebben van overzicht over welke afspraken met welke partij gemaakt moeten worden en wat de status van deze afspraken is. Dit is een essentieel onderdeel van het in control zijn op gebruik van persoonsgegevens van leerlingen en medewerkers en de beveiliging hiervan.

- Zonder ondersteuning is het, zeker voor kleinere schoolbesturen, een enorme opgave om het **eigen applicatielandschap goed in kaart** te

brengen. Leraren en medewerkers gebruiken veel soorten software, en stellen zich vaak onvoldoende de vraag wat al beschikbaar is in de school en wat gedaan moet worden om dit veilig te gebruiken. Op bestuursniveau is daarom inzicht nodig. Door centrale tooling beschikbaar te stellen hoeft niet elke school zelf het wiel uit te vinden. Doordat van applicaties bekend is welke processen ze ondersteunen en welke data hiervoor wordt gebruikt (op basis van de FORA, Funderend Onderwijs Referentiearchitectuur), kan een school direct aan de slag zonder alles zelf uit te moeten zoeken. Hiermee ontstaat overzicht wat op bestuursniveau meer mogelijkheden geeft om effectief te kunnen sturen op zowel de veiligheid bij het gebruik van applicaties door medewerkers als op de juiste afspraken met leveranciers.

- De AVG verplicht elk schoolbestuur tot het bijhouden van een register van verwerkingen, ook wel een **dataregister** genoemd. Hierin is vastgelegd welke persoonsgegevens door de school worden verwerkt en met welke leverancier welke data wordt uitgewisseld. Het is hiermee een instrument voor het schoolbestuur in om overzicht te hebben en in control te zijn over hoe met persoonsgegevens wordt omgegaan. Het bijhouden van een dataregister is niet alleen belangrijk, maar is ook een tijdrovende klus. En dit terwijl de inhoud van delen van het dataregister voor vrijwel alle scholen die bepaalde processen uitvoeren of bepaalde producten gebruiken tussen besturen dezelfde is. Onderzocht moet worden hoe dit proces vereenvoudigd kan worden.
- Schoolbesturen moeten voor de verwerking van persoonsgegevens in veel gevallen zelf een DPIA uitvoeren. Veel van de informatie die zij hiervoor nodig hebben kunnen zij benutten uit de centraal uitgevoerde DPIA's (zie bouwblok 7). Om het proces van de eigen risicoanalyse te ondersteunen is **DPIA-tooling** nodig. Deze tooling is gericht op het delen van informatie uit centraal uitgevoerde DPIA's op een manier die gebruiksvriendelijk is en schoolbesturen zo min mogelijk administratieve lasten bezorgt. Het is niet op voorhand te zeggen of deze tooling

ontwikkeld moet worden of verkrijgbaar is in de markt.

- Het is al jaren een opgave in het funderend onderwijs om ervoor te zorgen dat schoolbesturen de beschikbare **verwerkersovereenkomsten** ook daadwerkelijk ondertekenen. Omdat een schoolbestuur al snel ten minste 150 overeenkomsten moet tekenen, en er ook regelmatig sprake is van een wijziging in de overeenkomsten, is het zowel administratief als inhoudelijk een omvangrijke klus om over de juiste contracten te beschikken. Een voorziening waarin scholen per leverancier de laatste versie van de overeenkomst kunnen zien en deze direct kunnen ondertekenen, levert volgens een recent uitgevoerde business case een belangrijke bijdrage in het vergroten van het aantal ondertekeningen en aan het meer in control brengen van het onderwijsbestuur. Ook private partijen zien veel belang in een dergelijke voorziening omdat het hen meer zekerheid biedt voor een veilige dienstverlening naar onderwijsbesturen.

Bouwblok 9: Passend marktaanbod IBP-ondersteuning voor schoolbesturen

Bouwblok 9: Passend marktaanbod IBP-ondersteuning voor schoolbesturen	
Probleem	Schoolbesturen hebben weinig zicht op de ondersteuning die ze nodig hebben en hoe ze dit uit kunnen vragen in de markt op een manier die past bij hun behoeften
Oplossing	Door middel van programma's van eisen en eventuele selectie of inkoop van partijen een betrouwbare markt creëren voor schoolbesturen op het gebied van ondersteuning bij privacy- en beveiligingsvraagstukken
Output	▪ Programma van eisen en eventuele inkoop van ondersteuning privacy ▪ Programma van eisen en eventuele inkoop van ondersteuning informatiebeveiliging ▪ Programma van eisen en inkoop cybersecurityverzekering of opzet calamiteitenfonds

Intermediate outcome	Een goed functionerende markt voor privacy- en beveiligingsondersteuning voor scholen
Outcome	Schoolbesturen worden op passende wijze ondersteund in het goed regelen van privacy en beveiliging

IBP vergt specialistische kennis en vaak ook specialistische handelingen. Waar een groot schoolbestuur een deel hiervan zelf kan organiseren, geldt voor vrijwel elk bestuur in het primair en voortgezet onderwijs dat ondersteuning van externe partijen nodig is. Met de inhuur van een externe functionaris gegevensbescherming kan slechts een beperkt deel van de behoefte van scholen worden ingevuld. Besturen zijn afhankelijk van specialistische private partijen voor de scholing van hun IBP-personeel, voor het goed inschatten van de risico's van verwerkingen van persoonsgegevens voor hun eigen organisatie en voor het uitvoeren van beveiligingstests. Een bijzondere wijze van ondersteuning is het verzekeren van de gevolgen van een beveiligingsincident. Waar voor de eerstgenoemde ondersteuningsbehoeften een volwassen markt aan het ontstaan is gericht op IBP in het funderend onderwijs, lijken bestaande cybersecurityverzekeringen nauwelijks aan te sluiten op de praktijk van een onderwijsinstelling. Gezamenlijke eisen aan de markt voor IBP-ondersteuning zijn nodig om niet alleen de kwaliteit van de dienstverlening te vergroten, maar ook om aan schoolbesturen duidelijk te maken van welke ondersteuning zij 'geacht' worden gebruik te maken om hun eigen IBP-volwassenheid te vergroten.

- Hoe goed schoolbesturen hun privacy ook weten te organiseren, in de praktijk zal elk onderwijsbestuur van tijd tot tijd **privacyondersteuning** nodig hebben van organisaties die hierin gespecialiseerd zijn. Een voorbeeld hiervan is het uitvoeren van de risicoanalyses op verwerkingen, schoolbesturen zijn wettelijk verplicht deze zelf uit te voeren. De centraal uitgevoerde DPIA's geven hen een belangrijk deel van de informatie die ze nodig hebben om dit te doen. Voor een eigen DPIA moet een risicoanalyse worden uitgevoerd voor de situatie en het gebruik van een softwaretoepassing binnen het schoolbestuur zelf. Omdat dit een ingewikkelde puzzel is, kunnen veel schoolbesturen dit niet alleen. Daarom is het wenselijk hen te ondersteunen bij het

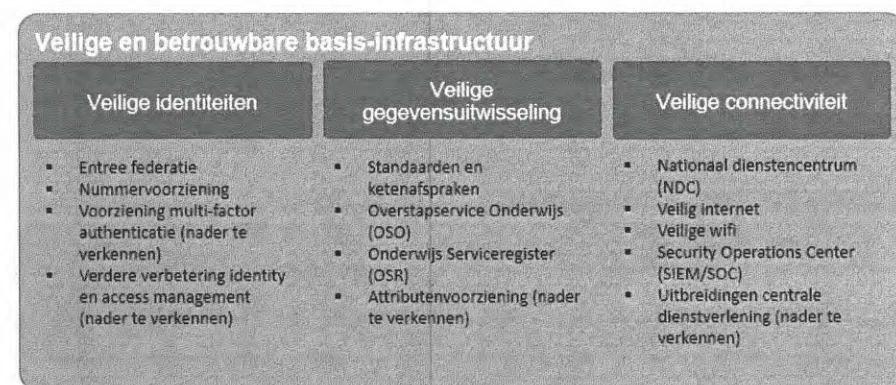
uitvoeren van workshops om hun eigen risicoanalyse goed uit te voeren. Private partijen kunnen hier een waardevolle ondersteuning in bieden. Andere voorbeelden van ondersteuning op het gebied van privacy zijn het inhuren van een functionaris gegevensbescherming, het in kaart brengen van de privacysituatie van het bestuur (wat is er nog te doen), het kwartiermaken om de privacysituatie op orde te brengen, of het tijdelijk vervangen van de privacyfunctionaris binnen het bestuur. Met programma's van eisen en eventuele inkoop(ondersteuning) voor privacydienstverlening worden (met name kleinere) schoolbesturen ondersteund in het maken van de juiste keuzes op een manier die aansluit bij hun behoeften.

- Naast ondersteuning op privacygebied hebben schoolbesturen ook op regelmatig **securityondersteuning- en producten** nodig van gespecialiseerde organisaties. Ook als risico's vooraf goed in beeld zijn gebracht, kan het nog steeds misgaan. Maar waar zitten de kwetsbaarheden in de organisatie en in de manier waarop systemen worden gebruikt? Door tests uit te voeren (pentests, vulnerabilityscans) weet het schoolbestuur waar actie moet worden ondernomen. Veel schoolbesturen voeren op dit moment nog niet van deze tests uit. Als ze wel worden uitgevoerd moeten ze ook regelmatig worden herhaald. Daarnaast is het wenselijk dat een deel van de resultaten (bijvoorbeeld over kwetsbaarheden in systemen) breder worden gedeeld in de onderwijssector. Daarom is een meer centrale aanpak gewenst: om te zorgen dat er meer getest wordt zodat scholen zicht krijgen en houden in hun risico's, maar ook zodat relevante informatie hieruit breed gedeeld kan worden in de sector. Een ander voorbeeld van securityondersteuning is het inschakelen van technische recherchebedrijven bij een beveiligingsincident of het inschakelen van partijen bij herstel na een incident. Ook het formuleren van eisen aan en eventueel gezamenlijk inkopen van firewalls of virusscanners is een mogelijkheid om scholen te ondersteunen.

- Ondanks alle activiteiten die worden uitgevoerd en alle maatregelen die schoolbesturen nemen, is een ding zeker: beveiligingsincidenten zullen voor blijven komen en soms grote schade aanrichten. Het is voor scholen een zoektocht om zich goed te verzekeren tegen de gevolgen van een beveiligingsincident. De markt voor cybersecurityverzekeringen is de laatste jaren flink in beweging. Het onderwijs kent echter specifieke eigenschappen zoals de omgang met (bijzondere) persoonsgegevens van minderjarige leerlingen en de grote hoeveelheid devices en gebruikers per organisatie. Op dit moment leidt dat tot de situatie dat het voor schoolbesturen in po en vo nauwelijks mogelijk lijkt een goede verzekering af te sluiten. Daarom moet nader onderzoek gedaan worden naar de wijze waarop het onderwijs om kan gaan met de risico's van beveiligingsincidenten en de kosten die dit met zich meebrengt. Hiervoor zijn verschillende scenario's, variërend van niet verzekeren, tot gezamenlijk onderhandelen over de voorwaarden van een **cybersecurityverzekering** en het oprichten van een eigen **calamiteitenfonds**. Binnen het programma wordt uitgewerkt wat de beste manier is en hoe daar te komen. Zowel het gezamenlijk inkopen of het oprichten van een eigen fonds vergen veel voorbereiding en een flinke bereidwilligheid tot deelname van schoolbesturen. Het tot stand brengen van deze activiteiten vergt daarmee veel expertise en langere doorlooptijd.

Lijn 4: Veilige en betrouwbare basisinfrastructuur

Bescherming is een cruciaal onderdeel van digitaal veilig onderwijs en ook een cruciaal onderdeel van landelijke ondersteuning. Omdat zowel ketens veilig ingericht moeten worden als individuele systemen is een centrale aanpak onontbeerlijk. Dit begint met goed identiteitsbeheer en een ict-infrastructuur die dataminimalisatie mogelijk maakt. In het onderwijs worden in diverse ketens persoonsgegevens uitgewisseld van leerlingen en medewerkers. Het is belangrijk dat dit volgens de juiste afspraken gebeurt en dat dit veilig is. Daarvoor moeten er normen en afspraken zijn die bepalen hoe in het onderwijsdomein door dienstverleners wordt omgegaan met privacy en beveiliging (standaarden en afspraken). Daarnaast is een centrale infrastructuur nodig waar scholen gebruik van kunnen maken om de veiligheid van hun uitwisselingen te borgen. Identiteiten, gegevensuitwisseling en connectiviteit hebben veel met elkaar te maken en kennen veel onderlinge afhankelijkheden. Onderstaande indeling is dan ook primair bedoeld om een overzicht te kunnen bieden van de verschillende inspanningen die nodig zijn.



Bouwblok 10: Veilige identiteiten

Bouwblok 10: Veilige identiteiten	
Probleem	Leerlingen en medewerkers in het onderwijs hebben een veelheid aan digitale identiteiten waarvan niet duidelijk is

Oplossing	hoe goed deze beschermd zijn met betrekking tot voor privacy- en beveiligingsissues Een robuust systeem van (centrale en/of decentrale) voorzieningen en diensten die ervoor zorgen dat elke school met beperkte inspanningen en tegen aanvaardbare kosten kan beschikken over veilige identiteiten voor leerlingen en medewerkers
Output	- Entree federatie - Nummervoorziening en ECK iD - Voorziening multi-factor authenticatie (nader te verkennen) - Innovatie en ontwikkeling identity en access management
Intermediate outcome	Schoolbesturen gaan bewuster om met hun identiteitenlandschap
Outcome	Digitale identiteiten van leerlingen en medewerkers zijn zo veilig als de laatste stand van de techniek mogelijk maakt

Een leerling of medewerker die gebruikt maakt van digitaal lesmateriaal of staat ingeschreven bij en school beschikt binnen deze school over een digitale identiteit. Deze digitale identificerende gegevens worden met allerlei partijen gedeeld om het Nederlandse onderwijsstelsel te laten werken. Het is hiervoor belangrijk dat leerlingen over betrouwbare identiteiten beschikken die alleen met de daartoe bevoegde instanties worden gedeeld. Om de privacy van leerlingen nog beter te beschermen wordt in het leermiddelendomein gewerkt met een gepseudonimiseerde identiteit, zodat dataminimalisatie verder in de praktijk kan worden gebracht. Omdat de veiligheid en betrouwbaarheid van digitale identiteiten de komende jaren alleen maar belangrijker zal gaan worden moet op dit terrein ook in het funderend onderwijs permanente innovatie plaatsvinden.

- **Entree federatie** maakt het mogelijk voor leerlingen en medewerkers om met één gebruikersnaam en wachtwoord eenmalig in te loggen om gebruik te maken van digitale leermiddelen en andere systemen. De school blijft *in control* over de persoonsgegevens, kan haar eigen

identity provider kiezen en elke leverancier kan zijn product aansluiten op Entree federatie. Zo wordt niet alleen de veiligheid en het gebruiksgemak bevordert, maar blijft het speelveld ook open. Het schoolbestuur kan zelf keuzes maken welke persoonsgegevens met een andere partij worden gedeeld, zodat dit in lijn is met de afspraken in de verwerkersovereenkomst. Entree federatie is geen nieuwe dienst, maar bestaat al geruime tijd.

- De **Nummervoorziening** maakt het mogelijk om voor iedere leerling in Nederland een gepseudonimiseerde identiteit te maken. Op deze manier kan een leerling wel worden herkend en toegang krijgen tot systemen, maar is het niet nodig om hierbij meer persoonsgegevens te delen dan de gepseudonimiseerde identiteit. De identiteiten die de Nummervoorziening genereert worden nu al gebruikt in de leermiddelenketen om hier verdergaande dataminimalisatie toe te passen. Ook in andere ketens is het op termijn mogelijk om gebruik te maken van gepseudonimiseerde identiteiten om veiliger data uit te kunnen wisselen of toegang te geven tot systemen. De Nummervoorziening is hiermee een centraal onderdeel van digitaal veilig onderwijs, omdat het in staat is veilige en betrouwbare identiteiten te creëren voor iedere leerling. De Nummervoorziening is een bestaande dienst.
- Omdat digitale ontwikkelingen, en beveiligingsontwikkelingen in het bijzonder, steeds nieuwe eisen stellen is het zaak om ook het **identity en access management** in het onderwijsdomein voortdurend te vernieuwen. Onderzoek naar nieuwe ontwikkelingen en de wijze waarop het funderend onderwijs hier het beste mee om kan gaan is noodzakelijk. Het is hierbij goed mogelijk dat dit leidt tot de realisatie van nieuwe standaarden of voorzieningen, implementatie van wat elders bedacht is in het funderend onderwijs of inspanning die zorgen dat het funderend onderwijs op een veilige manier aangesloten kan blijven bij landelijke en internationale ontwikkelingen. Een eerste richting voor **innovatie en ontwikkeling** is multi-factor-authenticatie:

een extra manier om zekerheid te creëren dat alleen de daartoe bevoegde persoon toegang krijgt tot gegevens. Steeds meer systemen maken hier gebruik van of hebben hier de mogelijkheid voor. Voor de gebruiksvriendelijkheid, en daarmee de adoptie van deze maatregel, is het wenselijk dat dit op een uniforme wijze gebeurt. Een centrale dienst voor twee-factor-authenticatie (zoals door SURF reeds wordt aangeboden aan haar leden) zorgt ervoor dat eenduidigheid voor de gebruiker wordt bewerkstelligd. Daarnaast blijft het proces van authenticatie en de beveiligingseisen die hieraan worden gesteld in publieke handen, wat de afhankelijkheid van (grote) techbedrijven verkleint. Voordat tot de realisatie van een dergelijke voorziening kan worden overgegaan is eerst aanvullende onderzoek nodig naar de wijze waarop de behoefte van scholen naar veilige authenticatie het best kan worden ingevuld.

Bouwblok 11: Veilige gegevensuitwisseling

Bouwblok 11: Veilige gegevensuitwisseling	
Probleem	Schoolbesturen wisselen met diverse partijen gegevens uit, zonder dat altijd duidelijk is of dit op een veilige wijze gebeurt en waarbij niet aantoonbaar is dat het schoolbestuur <i>in control</i> is
Oplossing	Eenduidige afspraken over en voorzieningen voor een veilige gegevensuitwisseling
Output	▪ Standaarden en ketenafspraken ▪ Overstapservice Onderwijs ▪ Onderwijs Serviceregister ▪ Attributenvoorziening (nader te verkennen)
Intermediate outcome	Schoolbesturen maken gebruik van een landelijk aanbod voor veilige gegevensuitwisseling
Outcome	Uitwisseling van persoonsgegevens tussen verschillende softwaresystemen in het onderwijs vindt plaats op de meest veilige en privacyvriendelijke manier

Waar gebruik wordt gemaakt van digitale middelen worden persoonsgegevens uitgewisseld. Voor bekostiging door DUO, voor contact over leerplicht met de gemeente, voor zorg en begeleiding door het samenwerkingsverband en diverse organisaties, voor het gebruik van leermateriaal met uitgeverijen. Waar de uitwisseling zelf in veel gevallen onontkoombaar is, is het wel zaak dit veilig en conform de AVG te doen. Modelafspraken en het gebruik van standaarden zijn hiervoor belangrijke ingrediënten. Maar ook aanvullende voorzieningen zijn nodig om de veiligheid en betrouwbaarheid van gegevens te waarborgen.

- Om de veiligheid van het Nederlandse onderwijs te borgen, moeten er niet alleen normen zijn voor scholen om aan te voldoen, maar ook aan leveranciers. Door eenduidige normen te hanteren, zorgen we voor veilige softwareproducten op de Nederlandse onderwijsmarkt. Dit betreft de vertaling van de normen die die volgen uit de Wet digitale overheid, beveiligingsstandaarden volgens uit ISO (Certificeringsschema IBP ROSA), standaarden voor veilige berichtuitwisseling (Digikoppeling/Edukoppeling) en het privacyconvenant voor digitale onderwijsmiddelen. Door **standaarden** te ontwikkelen en **ketenafspraken** te maken ontstaat een gelijk speelveld voor grote en kleine aanbieders van software ten behoeve van onderwijs. Leveranciers weten waar ze aan toe zijn, scholen kunnen dit eenvoudiger afdwingen, wat leidt tot een pluriform en veilig aanbod.
- Wanneer een leerling overstapt naar een andere school, zoals wanneer deze van het primair naar het voortgezet onderwijs gaat of een leerling verhuist, wordt het leerlingdossier overgedragen. Hierbij is het belangrijk dat dit veilig gebeurt en dat er niet meer gegevens worden overgedragen dan strikt noodzakelijk. De **Overstapservice Onderwijs** maakt het voor medewerkers van scholen zeer makkelijk om dit proces op een veilige manier en met inachtneming van privacywetgeving te doen. De Overstapservice Onderwijs is een bestaande dienst.

- Voor een veilige en betrouwbare gegevensuitwisseling is het belangrijk om vast te stellen welk systeem persoonsgegevens mag ontvangen in opdracht van de school. In het **Onderwijs Serviceregister (OSR)** legt een school voor elke uitwisseling van persoonsgegevens vast welke systemen hierbij betrokken zijn. Op deze manier wordt voorkomen dat berichten verkeerd verzonden worden. Naast het vergroten van de betrouwbaarheid van de uitwisseling is de dienst ook een middel voor schoolbesturen om *in control* te zijn over hun gegevensuitwisselingen. Het Onderwijs Serviceregister is een bestaande dienst.
- Ook op het gebied van gegevensuitwisseling kunnen nieuwe inzichten ontstaan, bijvoorbeeld wanneer de leermiddelenketen wordt vernieuwd en hiervoor nieuwe centrale voorzieningen nodig blijken te zijn. Ook in gegevensuitwisseling is sprake van **innovatie en ontwikkeling**. Een voorbeeld hiervan is een centrale attributenvoorziening die scholen meer controle geeft over gegevensuitwisselingen. Nadere verkenning op basis van technische ontwikkelingen en behoeften van het onderwijs kunnen aanleiding geven tot het ontwikkelen van nieuwe voorzieningen of standaarden.

Bouwblok 12: Veilige connectiviteit

Bouwblok 12: Veilige connectiviteit	
Probleem	Schoolbesturen beschikken niet over de juiste connectiviteitsdiensten die zowel zorgen voor veilige connectiviteit als die hen ontzorgen en aansluiten bij specifieke wensen van funderend onderwijs
Oplossing	Onderwijsspecifieke connectiviteitsdiensten die zoveel mogelijk gebruik maken van bestaande publieke en private bouwblokken
Output	▪ Nationaal Dienstencentrum (landelijke infrastructuur voor veilige connectiviteit) ▪ Veilig internet ▪ Veilige wifi

	▪ Security Operations Center (SIEM/SOC) ▪ Innovatie en ontwikkeling centrale dienstverlening
Intermediate outcome	Schoolbesturen gaan bewuster om met hun interne en externe connectiviteitsvraagstukken
Outcome	Schoolbesturen maken gebruik van veilige connectiviteitsdiensten

Om gebruik te kunnen maken van digitale producten of om gegevens uit te wisselen is veilige en betrouwbare connectiviteit nodig. Connectiviteit binnen de school, zoals wifi, maar ook de externe verbindingen met internet en met leveranciers. Door connectiviteitsdiensten centraal te organiseren of in te kopen kan de veiligheid van de hele sector funderend onderwijs worden vergroot. Met een centrale firewall kan een deel van de connectiviteit van scholen worden afgeschermd, waardoor het makkelijker te beveiligen is. Maar ook het monitoren van verdacht gedrag is onderdeel van connectiviteit. Het maakt het makkelijker om bepaalde maatregelen door te voeren voor alle scholen. Voor veilige connectiviteit is het van belang dat niet alleen op sectorniveau het verkeer gemonitord wordt, maar dat dit ook op het niveau van individuele scholen kan gebeuren. Oplossingen hiervoor zijn duur en vergen ook de nodige kennis, maar ook voor het funderend onderwijs zijn dergelijke stappen nodig. Vanuit de basis van centrale connectiviteitsvoorzieningen kan in de toekomst worden verkend welke veiligheidsbevorderende maatregelen wenselijk zijn om centraal in te richten.

- In de eerste plaats moeten scholen hun fysieke dataverbindingen beveiligen, dit geldt zowel voor hun interne (wifi-)netwerk als voor de externe verbinding van de school met het internet. Door deze verbinding via het **Nationaal dienstencentrum** (NDC) te laten verlopen kan een hoge mate van veiligheid worden geborgd. In het dienstencentrum wordt verkeer 'gewassen' om te beschermen tegen DDoS-aanvallen en andere verstoringen en hebben schoolbesturen diverse mogelijkheden om hun eigen beveiligingsinstellingen (zoals firewall) te regelen. Het centraal organiseren van dit deel van de externe

connectiviteit van onderwijsinstellingen is niet alleen zeer belangrijk om scholen te kunnen beschermen, het is een onmisbare schakel in het in het kunnen detecteren van en reageren op verstoringen en beveiligingsincidenten (zie verderop).

- Schoolbesturen moeten zelf zorgen voor een aansluiting op het Nationaal Dienstencentrum: **Veilig internet**. Door gezamenlijk in te kopen kunnen zij ook hier meer invloed hebben op de veiligheid en voorwaarden hiervan. Dit geeft vooral ook zekerheid over de beschikbaarheid van de dienstverlening en daarmee over de continuïteit van onderwijs. Door deze aanpak kunnen bijvoorbeeld afspraken worden gemaakt over de hersteltijd bij een verstoring of het plegen van onderhoud in de vakanties in plaats van in de toetsweek. Ook de interne verbindingen van een school moeten veilige zijn en aan hoge betrouwbaarheidseisen voldoen: **Veilige wifi**. Gezamenlijke inkoop en onderhandeling is hier ook een belangrijke manier om te kunnen beschikken over de juiste kwaliteit dienstverlening.
- Het is erg nuttig om scholen te informeren over algemene dreigingen in bijvoorbeeld de systemen die ze gebruiken. Maar om systemen en gegevens binnen een onderwijsbestuur goed te beschermen is 24/7 monitoring van de systemen nodig om verdacht gedrag te kunnen detecteren en hierop te kunnen reageren. Systemen hiervoor zijn verkrijgbaar in de markt, maar zijn zeer kostbaar. Het centraal aanbieden van deze dienst voor alle schoolbesturen levert daarom grote voordelen op, niet alleen qua kosten, maar ook in de wijze waarop instellingen van de support van de CERT bijgestaan kunnen worden bij een reactie op het mogelijke incident. Een **Security Operations Center** (SOC) kent niet alleen complexe techniek maar is ook complex om goed in te stellen en te monitoren. Hiervoor moet dan ook op centraal niveau samengewerkt worden met private partijen die hierin gespecialiseerd zijn. Door het internetverkeer naar een schoolbestuur te scannen kan al veel detectie van mogelijke aanvallen plaatsvinden, een vervolgstap is monitoring op veelgebruikte systemen binnen de instelling zoals het

LAS. Voor het inrichten van een SOC is het ook nodig dat scholen beschikken over een **SIEM**-oplossing (Security Information and Event Management) voor het kunnen monitoren van hun eigen verkeer.

- Het doel van veel activiteiten die zijn beschreven in dit plan is om schoolbesturen te ondersteunen in het veiliger maken van het gebruik van digitale middelen in hun onderwijs. Op het gebied van veilige connectiviteit zijn diverse aanvullende diensten denkbaar die scholen centraal of met elkaar kunnen organiseren. Denk aan endpoint security (zeker wanneer het onderwijs steeds minder plaatsgebonden is), mailfiltering, veilige WAN en LAN. Ook op het gebied van veilige connectiviteit zal permanent ontwikkeling plaats moeten vinden voor de gezamenlijke inkoop of centrale realisatie van nieuwe oplossingen om het onderwijs veiliger te maken en scholen hierbij te ontzorgen. Ook hier is permanente **innovatie en ontwikkeling** nodig.

3. Financiën

Begroting

Lijn 1: Normering en bewustwording	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	Totaal
Sturen op basis van normen	€ 28.500	€ 72.248	€ 36.629	€ 37.142	€ 37.662	€ 38.190	€ 38.724	€ 39.266	€ 39.816	€ 40.374	€ 408.551
Bewustwording en activering	€ 302.250	€ 1.123.005	€ 1.035.907	€ 1.154.669	€ 760.646	€ 672.672	€ 260.335	€ 162.576	€ 164.853	€ 167.160	€ 5.804.075
Monitoring	€ 190.500	€ 683.846	€ 106.462	€ 78.846	€ 65.123	€ 81.069	€ 66.959	€ 83.355	€ 84.522	€ 85.705	€ 1.526.387
Lijn 1: Normering en bewustwording	€ 521.250	€ 1.879.099	€ 1.178.999	€ 1.270.657	€ 863.431	€ 791.931	€ 366.019	€ 285.198	€ 289.190	€ 293.239	€ 7.739.013
Lijn 2: Kennisopbouw en kennisdeling	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	Totaal
Professionalisering binnen de instelling	€ 57.000	€ 1.641.695	€ 1.784.541	€ 1.536.362	€ 1.783.232	€ 1.339.556	€ 1.640.247	€ 1.377.326	€ 1.396.608	€ 1.416.161	€ 13.972.728
Kennisopbouw en kennisdeling	€ 113.235	€ 1.022.771	€ 991.824	€ 1.079.994	€ 1.019.789	€ 1.110.445	€ 1.048.543	€ 1.141.755	€ 1.157.740	€ 1.173.948	€ 9.860.044
Centrale ondersteuning beveiligingsincidenten	€ 30.000	€ 477.848	€ 733.875	€ 892.718	€ 905.216	€ 917.889	€ 930.740	€ 943.770	€ 956.983	€ 970.381	€ 7.759.420
Lijn 2: Kennisopbouw en kennisdeling	€ 200.235	€ 3.142.314	€ 3.510.239	€ 3.509.074	€ 3.708.237	€ 3.367.890	€ 3.619.530	€ 3.462.851	€ 3.511.331	€ 3.560.490	€ 31.592.192
Lijn 3: Leveranciers- en informatiemanagement	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	Totaal
Veilig gebruik software en en hardware	€ 192.503	€ 1.032.210	€ 1.093.539	€ 1.052.366	€ 709.880	€ 735.898	€ 762.506	€ 773.181	€ 784.005	€ 811.981	€ 7.948.068
Inzicht in eigen applicatielandschap	€ 323.528	€ 1.397.723	€ 1.510.754	€ 1.225.904	€ 1.104.681	€ 1.053.951	€ 1.068.707	€ 1.083.669	€ 1.098.840	€ 1.114.224	€ 10.981.981
Passend marktaanbod IBP-ondersteuning	€ 87.375	€ 270.992	€ 224.404	€ 164.990	€ 82.725	€ 83.883	€ 85.057	€ 86.248	€ 87.456	€ 88.680	€ 1.261.809
Lijn 3: Leveranciers- en informatiemanagement	€ 603.405	€ 2.700.925	€ 2.828.697	€ 2.443.260	€ 1.897.286	€ 1.873.733	€ 1.916.270	€ 1.943.098	€ 1.970.301	€ 2.014.884	€ 20.191.858
Lijn 4: Veilige en betrouwbare ict-infrastructuur	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	Totaal
Veilige identiteiten	€ -	€ 1.882.947	€ 1.837.335	€ 1.863.058	€ 1.889.140	€ 1.915.588	€ 1.942.407	€ 1.969.600	€ 1.997.175	€ 2.025.135	€ 17.322.385
Veilige gegevensuitwisseling	€ 43.125	€ 1.537.478	€ 1.559.002	€ 1.580.828	€ 1.602.960	€ 1.625.401	€ 1.648.157	€ 1.671.231	€ 1.694.628	€ 1.718.353	€ 14.681.163
Veilige connectiviteit	€ -	€ 811.200	€ 822.557	€ 14.949.709	€ 19.897.845	€ 28.831.375	€ 34.478.409	€ 34.657.502	€ 35.142.707	€ 31.951.508	€ 201.542.812
Lijn 4: Veilige en betrouwbare ict-infrastructuur	€ 43.125	€ 4.231.625	€ 4.218.894	€ 18.393.594	€ 23.389.946	€ 32.372.365	€ 38.068.972	€ 38.298.333	€ 38.834.510	€ 35.694.996	€ 283.546.360
Generieke kosten	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	Totaal
Programmakosten	€ 703.183	€ 1.295.157	€ 1.159.060	€ 1.081.453	€ 1.096.594	€ 1.111.946	€ 1.127.513	€ 1.143.298	€ 1.159.305	€ 1.175.535	€ 11.053.043
Communicatie	€ 152.700	€ 516.126	€ 523.352	€ 530.679	€ 538.108	€ 492.042	€ 442.625	€ 448.821	€ 455.105	€ 461.476	€ 4.561.034
Generieke kosten	€ 855.883	€ 1.811.283	€ 1.682.411	€ 1.612.132	€ 1.634.702	€ 1.603.988	€ 1.570.138	€ 1.592.120	€ 1.614.409	€ 1.637.011	€ 15.614.077
Totaal	€ 2.223.898	€ 13.765.245	€ 13.419.240	€ 27.228.718	€ 31.493.601	€ 40.009.907	€ 45.540.928	€ 45.581.600	€ 46.219.742	€ 43.200.621	€ 308.683.500

Toelichting

Om een impuls te geven aan de digitale veiligheid van het Nederlandse funderend onderwijs zijn drie ingrediënten nodig: normstelling (inclusief handhaving) + bewustwording en professionalisering + een passend ondersteuningsaanbod. Een randvoorwaarde hierbij is dat scholen over voldoende budget beschikken om zelf aan de slag te kunnen gaan met privacy en beveiliging en het benodigde instrumentarium. Want, we kunnen veel centraal en 'van de scholen af' organiseren, maar er blijft een belangrijke verantwoordelijkheid op de schoolbesturen rusten.

Algemene toelichting

Voor een aantal van de beoogde activiteiten geldt dat er sprake is van veel onzekerheden. Deels zijn deze onzekerheden ingegeven doordat we op langere termijn moeilijk kunnen voorspellen hoe de volwassenheid van schoolbesturen toeneemt, deels omdat sommige investeringen gepaard gaan met beleidskeuzes. Een voorbeeld van dit eerste is de bereidheid en budgettaire ruimte van scholen om zelf te investeren. Een voorbeeld van een beleidskeuze is centrale financiering van SIEM/SOC-dienstverlening: geheel, gedeeltelijk of niet. In dit plan is nu uitgegaan van een gedeeltelijke financiering: de implementatiekosten. Deze beleidskeuze hangt af van de technische en organisatorische uitwerking van SIEM/SOC voor het funderend onderwijs, maar ook van het sturingsmechanisme dat wordt gekozen om te zorgen dat alle schoolbesturen deze beveiligingsmaatregel treffen.

Met uitzondering van de hierboven beschreven situatie met betrekking tot SIEM/SOC zijn het beheer, onderhoud, doorontwikkeling en eventuele implementatiekosten van nieuwe landelijke voorzieningen niet opgenomen in de begroting. Wanneer de kosten en het doel hiervan bekend zijn, zal hier nog dekking voor moeten worden gevonden. Met innovatie- en ontwikkelbudgetten voor dienstverlening op het gebied van identity en access management, gegevensuitwisselingen en connectiviteit is er ruimte om nieuwe voorzieningen

te ontwikkelen en bestaande diensten en voorzieningen up to date te houden op basis van nieuwe beveiligingstechnieken.

Voor het jaar 2022 is gerekend dat activiteiten in september kunnen starten. Bij een ander startmoment zal de begroting moeten worden bijgesteld. Voor alle activiteiten is uitgegaan van budget voor interne medewerkers, tenzij anders aangegeven.

Voor alle activiteiten geldt dat door de uitvoerende partijen nauw samengewerkt moet worden met andere publieke partijen (NCSC, SURF, IBD) en private partijen. Op deze manier kan zo goed mogelijk gebruik worden gemaakt van wat al ontwikkeld is, kan kennis worden gedeeld en in sommige gevallen nog nauwer worden samengewerkt in de uitvoering.

Actielijn 1: Normering en bewustwording

- In de eerste anderhalf jaar van het programma wordt een normenkader ontwikkeld, een norm vastgesteld en vindt communicatie van deze norm plaats. Hiervoor is projectleiding en expertise begroot. In de jaren die daarop volgen is beperkte inzet nodig voor het onderhoud van het normenkader op basis van nieuwe inzichten en technieken.
- In de eerste helft van het programma wordt een groot aantal schoolbesturen bezocht met een persoonlijke aanpak om hen te activeren. Wegens het uitvoerende en tijdelijke karakter van deze activiteit zal dit worden uitgevoerd door externe medewerkers. In de tweede helft van het programma lopen de inzet en kosten van deze aanpak terug naar nul.
- De eerste periode van het programma staat in het teken van het opstarten van verschillende activiteiten, zo ook bewustwordingscampagnes. Tweejaarlijks is er een grote campagne. De kosten bestaan uit projectmanagement en kosten voor campagneontwikkeling.
- De kosten voor monitoring bestaan uit projectleiding voor het opstarten en uitvoeren van nulmeting, monitor en benchmark. In de eerste fase

moet duidelijk worden in welke vorm monitoring en benchmarking worden opgezet en in welke mate zij elkaar kunnen versterken. Nu zijn beide om het jaar begroot.

Actielijn 2: Kennisopbouw en kennisdeling

- Voor professionalisering in de instelling bestaat de eerste fase uit het opstarten en opbouwen van de dienstverlening: scholingsaanbod, microlearning en cybercrisisoefening. Vervolgens zijn er organisatie- en uitvoeringskosten voor de activiteiten: het organiseren van scholing en kosten voor docenten, het ontwikkelen en maken van microlearnings en het tweejaarlijks uitvoeren van een grote crisisoefening.
- Een groep van vijf adviseurs op het gebied van privacy en cybersecurity is begroot om kennis te ontwikkelen en beschikbaar te stellen, nieuwe ontwikkelingen in technologie, maatschappij en wet- en regelgeving te duiden en ter ondersteuning aan de activiteiten. Een helpdesk zorgt voor beantwoording van de eerstelijnsvragen van scholen die aan de slag gaan met hun privacy en beveiliging.
- Het Cyberdreigingsbeeld po/vo zal in het eerste jaar worden ontwikkeld en vervolgens iedere twee jaar worden geactualiseerd en opnieuw worden gepubliceerd.
- Het Netwerk IBP wordt verder uitgebreid. Dit vraagt een goede ondersteuning van een inhoudelijk secretaris. Met de uitbreiding naar het delen van kwetsbaarheidswaarschuwingen is ook inhoudelijke expertise nodig voor de vertaling van algemene kwetsbaarheden naar specifieke adviezen voor schoolbesturen.
- De ontwikkeling van een CERT vergt een goede voorbereiding. Ontwikkeling vindt plaats in 2023 en 2024 is deze volledig operationeel en beschikbaar voor schoolbesturen. De bemensing van de CERT bestaat wanneer deze volledig operationeel is uit een coördinator, 4 fte incident handlers en 2 fte communicatieadvies.

Actielijn 3: Leveranciers- en informatiemanagement

- Het opstellen van uniforme inkoopvoorwaarden vergt in de eerste fase de inzet van projectleiding en expertise. Onderhandeling en contractmanagement is voor een deel afhankelijk van omstandigheden (lopen grote contracten af, nemen leveranciers goede maatregelen). Hiervoor is vast jaarlijks bedrag begroot.
- Het toetsen van verwerkersovereenkomsten en de uitvoering van DPIA kent in de eerste drie jaar een impuls om alle bestaande overeenkomsten en verwerkingen de beoordelen en tegen het licht te houden. In de periode hierna zal de inzet hierop minder intensief zijn omdat dan voortgebouwd kan worden op eerder werk. In de eerste fase zal de intensivering worden vormgegeven met veelal externe krachten.
- Auditing wordt nog niet breed gedaan binnen het onderwijs en vergt en gedegen aanpak binnen het onderwijsdomein. In 2023/2024 wordt deze ontwikkeld zodat eind 2024 de eerste leveranciers en systemen geaudit kunnen worden. De jaren hierna is uitvoeringsbudget begroot.
- Om schoolbesturen regie op data te kunnen laten voeren is praktische tooling nodig. Deels wordt deze nu al ontwikkeld door Kennisnet (inzicht eigen applicatielandschap), deels zijn verkenningen nodig om dit optimaal te laten werken (aansluiten op DPIA-tooling, dataregister-tooling) of moeten producten worden doorontwikkeld (verwerkersovereenkomsten). Dit verklaart waarom de kosten in de eerste fase hoger zijn en lager worden naarmate diensten zijn opgezet en in de beheerfase terechtkomen. In 2022 wordt ook op basis van de begroting van Kennisnet al gestart met de ontwikkeling van tooling verwerkersovereenkomsten en inzicht in eigen applicatielandschap.
- Om te komen tot een passend marktaanbod voor IBP-ondersteuning en scholen ook te ondersteunen in het verwerven hiervan, worden programma's van eisen opgesteld. Hierbij is uitgegaan van 20k per programma van eisen. Ook hier ligt het zwaartepunt van de activiteiten in de eerste fase van het programma en is vervolgens beheer nodig.

- De uitwerking van de eisen voor een cybersecurityverzekering en het realiseren van een oplossing (inkopen verzekering of opzetten van calamiteitenfonds) is een complex proces. Indien gekozen wordt voor een calamiteitenfonds zijn hogere kosten te verwachten voor het opzetten en beheren hiervan dan nu zijn begroot.

Actielijn 4: Veilige en betrouwbare ict-infrastructuur

- Met Entree federatie en de Nummervoorziening zijn er twee voorzieningen die bijdragen aan veilige identiteiten en identificatie in het funderend onderwijs. Uitgaven die hiervoor begroot zijn, zijn gebaseerd op de ervaringen in de afgelopen jaren. Voor 2022 zijn geen uitgaven begroot omdat deze zijn voorzien in het jaarplan van Kennisnet.
- In 2023 wordt onderzocht op welke wijze een oplossing voor multifactor authenticatie meerwaarde heeft voor het funderend onderwijs, zoals SURFsecureID.
- Landelijke en internationale veiligheidsstandaarden moeten hun weg vinden naar het onderwijs, en soms zijn specifieke onderwijsafspraken nodig. Standaardisatie-experts zorgen voor deze afspraken en hun vertaling.
- De landelijke voorzieningen Overstapservice Onderwijs en Onderwijs Serviceregister dragen bij aan veilige en betrouwbare gegevensoverdracht. Uitgaven die hiervoor begroot zijn, zijn gebaseerd op de ervaringen in de afgelopen jaren. Voor 2022 zijn geen uitgaven begroot omdat deze zijn voorzien in het jaarplan van Kennisnet.
- Het Nationaal Dienstencentrum wordt, evenals kosten voor de implementatie van Veilig internet en Veilige wifi, op dit moment bekostigd vanuit de subsidie voor het programma Sterke Netwerken. Deze subsidie loopt tot en met 2024 en daarom zijn t/m 2024 hier geen kosten voor opgenomen. In deze begroting zijn de kosten voor het Nationaal Dienstencentrum en implementatie van de dienst bij nieuwe scholen opgenomen. Hierbij is uitgegaan van een groeipad naar situatie

van 100% gebruik in 2028. Het doel van gebruik van veilige connectiviteit door 100% van de scholen is nog onderwerp van gesprek, evenals de wijze hoe dit te bereiken en de kosten hiervan te verdelen. Bij het totaalbedrag van 24 miljoen euro per jaar zijn de huidige kosten per deelnemer als uitgangspunt genomen. Deze kostenpost kent op basis van bovenstaande een grote onzekerheidsmarge.

- Voor de introductie van SIEM/SOC-dienstverlening is veel onderzoek nodig naar de wijze waarop dit het beste vormgegeven kan worden voor het funderend onderwijs. Dit zijn zowel technisch-inhoudelijke en organisatorische vragen, als politieke en beleidsvragen. Na een analyse- en onderzoeksfase (2023-2024), is nu begroot dat de dienstverlening vanaf 2025 uitgerold kan worden in het funderend onderwijs. De kosten die hiervoor zijn opgenomen bevatten de aansluitkosten van 1300 schoolbesturen en het beheer van de dienstverlening. De maandelijkse abonnementskosten voor deze dienstverlening zijn niet opgenomen in deze begroting. Gezien de hier geschetste onzekerheden kent dit bedrag een grote onzekerheidsmarge. Zeker is wel dat het realiseren van een veilige connectiviteitsinfrastructuur hoge kosten met zich meebrengt, waar de omvang van deze bedragen indicatief voor is.
- Een innovatie- en ontwikkelbudget voor elk van de drie domeinen zorgt ervoor dat voorzieningen up to date zijn, maar is ook bedoeld om nieuwe dienstverlening te ontwikkelen. Nieuwe centrale componenten, voor zowel nieuwe activiteiten of door het centraler organiseren van wat nu door schoolbesturen wordt gedaan, kan de veiligheid van de sector in de breedte vergroten. Op basis van de praktijk in het onderwijs, de mogelijkheden van de techniek, de wensen schoolbesturen en politiek en nieuwe veiligheidsrisico's zullen steeds nieuwe maatregelen en mogelijkheden worden verkend.

Generieke kosten

- Voor de aansturing van het programma is een team begroot bestaande uit programmamanagement en programmasecretariaat. Voor

ondersteuning is een percentage van 15% bereken van de totale inzet aan interne fte's.

- In de eerste jaren is ook groter budget begroot voor wervingskosten. De arbeidsmarkt is krap, zeker op het specialistische gebied van cybersecurity en daarom zal flink geïnvesteerd worden in de werving geschikt personeel. Dit verklaart de hoge programmakosten in de eerste fase. In het eerste jaar zijn voorbereidingskosten opgenomen om te zorgen dat de activiteiten van het programma snel kunnen aanvangen.
- Omdat een zeer groot deel van de activiteiten een communicatiecomponent kent en het belangrijk is vanuit een integraal perspectief te communiceren is een generiek communicatiebudget opgenomen. Deze bestaat uit een communicatieadviseur en communicatiemedewerkers, en een jaarlijks budget voor de ontwikkeling van communicatiemiddelen.

Tot slot

Veel van de kosten zijn betrouwbaar te begroten, zeker waar het de eerste periode van ongeveer vier jaar betreft. Veel van de activiteiten lopen in de periode daarna door. De grootste post op de begroting kent de meeste onzekerheid (Bouwblok Veilige connectiviteit) en vergt zowel op inhoudelijk als op beleidsvlak nog de nodige uitwerking. Zeker is wel dat voor welke oplossing uiteindelijk ook gekozen wordt, de kosten aanzienlijk zullen zijn en in de orde van grote zoals opgenomen in deze begroting. Het doorlopen van de subsidie Sterke Netwerken en het nog niet direct starten met de uitrol van SIEM/SOC-dienstverlening maken dat er tijd is om zowel inhoudelijk als bestuurlijk deze vraagstukken goed uit te werken. Dit verklaart ook het grote verschil in begrote uitgaven tussen 2024 en 2025.

Belangrijk om te benadrukken is dat de werkelijke kosten voor de activiteiten voor veilig digitaal funderend onderwijs hoger zullen liggen als gevolg van beleidskeuzes en nieuw te ontwikkelen diensten en voorzieningen. Hier is in deze begroting geen rekening mee gehouden.

Ook na uitvoering van het programma zullen er structurele uitgaven nodig zijn voor de digitale veiligheid van het funderend onderwijs. Afspraken met

leveranciers zullen blijvend moeten worden getoetst, bewustwording en professionalisering zullen altijd nodig zijn en ook centrale incidentenondersteuning is ook op de lange termijn nodig. Infrastructurele voorzieningen zullen in de loop van de tijd veranderen, maar zullen altijd aan de laatste veiligheidsstandaarden moeten voldoen en continu moeten innoveren. De techniek en de buitenwereld veranderen, dus ook cybersecurity en privacy in het funderend onderwijs moeten blijven innoveren.

Bijlage 1. Overzicht integraal portfolio privacy en beveiliging andere publieke domeinen

	<u>Gemeenten (IBD)</u>	<u>Z-CERT</u>	<u>Hoger Onderwijs (SURF)</u>
Professionaliseren	• VNG Forum (uitwisselen van informatie met collega's) • (Online) (regio) bijeenkomsten over informatiebeveiliging en privacy • Advies & belangenbehartiging (soort helpdesk) • Trainen en oefenen (uitvoeren van VNG/IBD games en oefeningen) • Verhogen digitale weerbaarheid (o.a. kennisproducten, mindmaps & instructievideo's) • Handreikingen en factsheets (best practices op IBP-gebied) • Workshops • Meedraaien gemeentelijke CISO of Privacyadviseur voor max. 2 dagen in de week voor een halfjaar in IBD-team • Besloten IBD community	• Informatieverzoeken (via mail of beveiligd chatkanaal issues voorleggen aan specialisten) • Webinars • Community (online platform deelnemers informatie uitwisselen) • Netwerkbijeenkomsten	• Beveiligingscommunity (SCIRT-community) • Privacycommunity (SCIPIR) • SURFaudit (inzicht krijgen hoe een instelling ervoor staat op het IBP-gebied) • Webinars/Masterclasses /Trainingen

Identificeren	• DPIA-tool en collectieve DPIA's • Beheer,- expert,- en werkgroepen • Bewustwording (gebruik maken van verzamelde campagnes van gemeenten) • Advies in projecten (voor uitvoeren risicoanalyse en advies veiligheidsmaatregelen en waarborgen privacy)	• CyberSafe Yourself (toolkit bewustwording) • Crisisoefening (N)OZON
Beschermen	• AVG Borgingsproduct (handvatten waarborging goede omgang persoonsgegevens) • Beheren standaard Verwerkersovereenkomst	• eduVPN • SURFmailfilter • SURFsecureID (tweefactorauthenticatie) • SURFconext (1set credentials) • SURFcertificaten • SURFwireless: WIFI as a Service • SURF-netwerk (aansluiten van locaties op het SURF-netwerk) • SURFlichtpaden: veilige netwerkverbinding • SURFdomeinen (beheer internetdomeinen) • SURFInternet (internetverbinding) • SURFopzichter (eenvoudig en realtime bewaken van de presentaties en beschikbaarheid van je internetdiensten)

Detecteren

- Kwetsbaarheidswaarschuwingen
- Detectie van besmettingen (IP-adressen)
- Dreigingsbeeld (2x p.j.)
- Maandmonitor (overzicht relevante ontwikkelingen op terrein van IBP in gemeentelijke context)
- Dreigingsbeeld
- Whitepapers en onderzoeken
- Informatie- en alerteringsberichten
- Controle IP-adressen & domeinnamen (ontvangt ook lijsten met kwetsbare systemen van zorginstellingen)
- Inzet specialisten voor controle online bronnen (van deelnemers?)
- ZorgDetectieNetwerk (IOC)
- Coördinated Vulnerability Disclosure (kwetsbaarheden in websites/(medische) apparatuur door derden ontdekt kunnen gemeld worden bij Z-CERT)
- (Medische) Advisories (handelingsadvies over ontdekte kwetsbaarheden in (medische) hard- en software)
- Maandoverzicht (relevante ontwikkelingen en actualiteiten)
- Weekoverzicht (overzicht van alle verzonden advisories, mediaberichten en links naar websites met achtergrondinformatie)
- Operational alerts (informatie over actuele en urgente dreigingen om direct te handelen)
- Infoberichten (informatie over lopende security incidenten met sector brede impact)
- SURFsoc (aanspreekpunt voor diensten die incidenten detecteren en voorkomen en cyberdreigingen op ICT-infrastructuur monitoren)

Reageren	• Adviezen op terrein van incidentmanagement: Telefonische ondersteuning Deelname crisisteam als adviseur Schakelpunt met overheid, leveranciers en gemeente Bemiddeling capaciteit en steun andere gemeenten Second opinion op adviezen en voorstellen van derden • Hulp bij evaluatie en opstellen lessen voor toekomst (Coördinatie door de IBD) • Advies communicatie en woordvoering • Contact onderhouden met leveranciers en ketenpartners	• Ondersteuning forensisch onderzoek • Ondersteuning aanpak en oplossen van incident	• SURFcert (24/7 ondersteuning bij beveiligingsincidenten)
Herstellen	-		

2

5.1.2e

Van: 5.1.2e <5.1.2e@kennisnet.nl>
Verzonden: maandag 18 oktober 2021 14:31
Aan: 5.1.2e
CC: 5.1.2e
Onderwerp: Begroting en plan Veilig digitaal funderend onderwijs
Bijlagen: Digitaal veilig funderend onderwijs v1.0 (18-10-2021).pdf; Begroting Actieplan Veilig digitaal onderwijs v3.xlsx

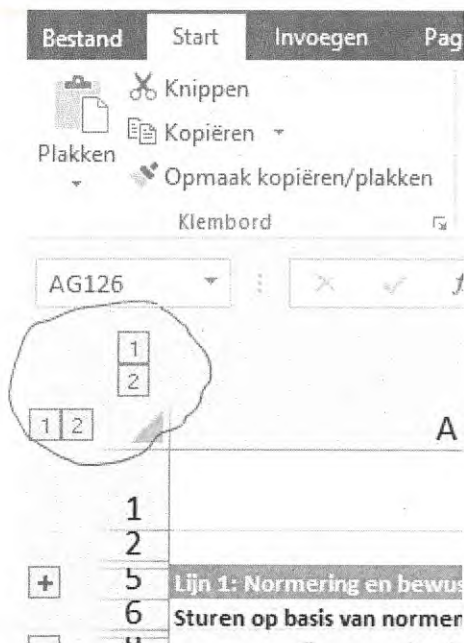
Opvolgingsvlag: Opvolgen
Vlagstatus: Met vlag

Ha 5.1.2e en 5.1.2e,

Hierbij het plan en de begroting. Het plan met begroting op hoofdlijnen is wmb ook voor Groeifonds (stuur ik straks naar 5.1.2e), de Excel met begroting voor jullie intern gebruik. Door in de Excel linksboven op de 1 of de 2 de drukken, klap je alle onderdelen van de begroting in één klik in of uit (zie hieronder).

Voor vragen weten jullie me te vinden!

Gr
5.1.2e



Vriendelijke groeten,

Kennisnet

5.1.2e

5.1.2e

T 06 - 5.1.2e

Paletsingel 32, 2718 NT Zoetermeer
Postbus 778, 2700 AT Zoetermeer

5.1.2e

Van: 5.1.2e
Verzonden: donderdag 23 juni 2022 12:57
Aan: 5.1.2e
Onderwerp: RE: Kamerbrief/Vervolg gesprek MPVO bespreken

Heel mooie aanzet.

Lijkt me goed om aan begin nota nog even onze uitgangspunten van aanpak Plan Veilig te benoemen:

- 1) Integrale aanpak: alle aspecten cyberveiligheid borgen met maatregelen
- 2) Meer centrale regie, want scholen kunnen het niet alleen
- 3) Normstelling: scholen moeten weten waaraan ze minimaal moeten voldoen en hoe ze daaraan kunnen voldoen (dit gaan we communiceren (bewustwording), nulmeten, monitoren, bijsturen, handhaven)
- 4) Helpen: ondersteuning van scholen met raad en daad
- 5) Publieke voorzieningen: overheid regelt centrale voorzieningen waar keten/coördinatie problemen optreden of schaalvoordelen evident te behalen zijn
- 6) Fasering: nu starten met communicatie, normstelling, hulp bij incidenten, tegelijk voorbereiden volgende stappen die basis infrastructuur betreffen (ICTU, beleidsadvies, uitbouw bestaande voorzieningen richting cyber security centre voor funderend onderwijs)

Wat mij betreft Plan Veilig meesturen.

Tot zo
5.1.2e

Van: 5.1.2e <5.1.2e@minocw.nl>
Verzonden: donderdag 23 juni 2022 12:18
Aan: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>
Onderwerp: RE: Kamerbrief/Vervolg gesprek MPVO bespreken

Hoi allen,

Hierbij een eerste aanzet voor de nota ter bespreking zo om 13.00uur.

Groet,
5.1.2e

-----Oorspronkelijke afspraak-----

Van: 5.1.2e 5.1.2e@minocw.nl>
Verzonden: woensdag 22 juni 2022 14:06
Aan: 5.1.2e
Onderwerp: Kamerbrief/Vervolg gesprek MPVO bespreken
Tijd: donderdag 23 juni 2022 13:00-14:00 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.
Locatie: Teams

Microsoft Teams-vergadering

Deelnemen op uw computer of via de mobiele app

[Klik hier om deel te nemen aan de vergadering](#)

[Meer informatie](#) | [Opties voor vergadering](#)

5

5.1.2e

Van: 5.1.2e
Verzonden: donderdag 23 juni 2022 14:57
Aan: 5.1.2e
Onderwerp: RE: VDFO / Kamerbrief
Bijlagen: Nota aan MPVO 220622.docx

Ha 5.1.2e,

Hierbij de opzet voor de nota voor minister, n.a.v. het gesprek dat wij gisteren met hem hebben gevoerd, om zo met jou door te nemen en te bespreken. Zullen we om 15.15 starten? Dan heb je tijd om het te lezen. Het is nog niet af, maar vast een eerste concept versie en het gaat vooral om het tabel met het tijdpad + verantwoordelijkheidsverdeling.

Groet,
5.1.2e

-----Oorspronkelijke afspraak-----

Van: 5.1.2e <5.1.2e@minocw.nl>

Verzonden: donderdag 23 juni 2022 09:59

Aan: 5.1.2e

Onderwerp: VDFO / Kamerbrief

Tijd: donderdag 23 juni 2022 15:00-17:00 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.

Locatie:

Microsoft Teams-vergadering

Deelnemen op uw computer of via de mobiele app

[Klik hier om deel te nemen aan de vergadering](#)

[Meer informatie](#) | [Opties voor vergadering](#)

7

5.1.2e

Van: 5.1.2e
Verzonden: donderdag 23 juni 2022 12:18
Aan: 5.1.2e
Onderwerp: RE: Kamerbrief/Vervolg gesprek MPVO bespreken
Bijlagen: Nota aan MPVO 220622.docx

Hoi allen,

Hierbij een eerste aanzet voor de nota ter bespreking zo om 13.00uur.

Groet,
5.1.2e

-----Oorspronkelijke afspraak-----

Van: 5.1.2e <5.1.2e@minocw.nl>

Verzonden: woensdag 22 juni 2022 14:06

Aan: 5.1.2e

Onderwerp: Kamerbrief/Vervolg gesprek MPVO bespreken

Tijd: donderdag 23 juni 2022 13:00-14:00 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.

Locatie: Teams

Microsoft Teams-vergadering

Deelnemen op uw computer of via de mobiele app

[Klik hier om deel te nemen aan de vergadering](#)

[Meer informatie](#) | [Opties voor vergadering](#)

9

5.1.2e

Van: 5.1.2e
Verzonden: vrijdag 24 juni 2022 21:08
Aan: 5.1.2e
CC: 5.1.2e
Onderwerp: RE: Nota MPVO & Kamerbrief digitale weerbaarheid in onderwijs en onderzoek

Opvolgingsvlag: Opvolgen
Vlagstatus: Voltooid

Dag 5.1.2e,

Het was al een mooie brief en is zo alleen maar steviger geworden cf wensen van MPVO. Wel zou je mi nog een kleine slag kunnen slaan door de uitgangspunten die in de nota vetgedrukt staan genoemd (die M in veel dossiers centraal stelt) nog steviger in inleiding van deel over PO VO terug te laten komen. Gelardeerd met enkele zinnen dat dat ook wel echt een andere aanpak / filosofie is dan voorheen. Meestal wil M helder laten zien dat/hoe hij andere keuzes maakt dan voorheen en waarom dat echt nodig is.

Wellicht kun je er met die bril nog even naar kijken.

Goed weekend!

Groet
5.1.2e

Van: 5.1.2e <5.1.2e@minocw.nl>
Verzonden: vrijdag 24 juni 2022 16:00
Aan: 5.1.2e 5.1.2e @minocw.nl; 5.1.2e <5.1.2e@minocw.nl>;
5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>
CC: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>;
<5.1.2e@minocw.nl>
Onderwerp: Nota MPVO & Kamerbrief digitale weerbaarheid in onderwijs en onderzoek
Urgentie: Hoog

Beste 5.1.2e

Afgelopen woensdagmiddag hebben we met MPVO gesproken over de kamerbrief over digitale veiligheid in onderwijs en onderzoek. Hij was positief over het po/vo deel van de brief en had nog een aantal vragen om scherper inzicht te bieden in onze aanpak. Op basis daarvan hebben wij een nota voor MPVO opgesteld en de brief aangescherpt. Ter achtergrondinformatie sturen we de minister ook de verkenning van Berenschot omtrent het normenkader voor PO/VO mee. Het normenkader voor HO vragen we maandag op bij SURF.

Zouden jullie ons **uiterlijk maandagochtend 10.00 uur** van feedback kunnen voorzien? Dan kunnen we het maandag verwerken en de brief en nota in de lijn doen zodat het dinsdag in de tas van MPVO kan.

Alvast bedankt.

Met vriendelijke groet,
5.1.2e

5.1.2e
Team Digitalisering Primair en Voortgezet Onderwijs

Directie Primair Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap
Rijnstraat 50 | 2515 XP | Den Haag

M +316 5.1.2e
E 5.1.2e@minocw.nl

10

5.1.2e

Van: 5.1.2e
Verzonden: vrijdag 24 juni 2022 11:50
Aan: 5.1.2e
Onderwerp: RE: Nota MPVO
Bijlagen: NOTA MPVO 240622.docx

Hi, mooie nota al, bijgaand met nog wat suggesties om hem nog wat strakker te maken. Succes!
5.1.2e

Van: 5.1.2e <5.1.2e@minocw.nl>
Verzonden: vrijdag 24 juni 2022 11:29
Aan: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>
Onderwerp: Nota MPVO
Urgentie: Hoog

Hoi collega's,

Hierbij een eerste versie van de nota (ik krijg de pagina's vanaf de tabel niet liggend, want it messes met de opmaak/koptekst enz.) voor jullie om scherp op mee te lezen. Dank alvast! Wij spreken 5.1.2e van 13-14 over de tabel en sturen het vanmiddag naar 5.1.2e, 5.1.2e 5.1.2e en 5.1.2e om intern af te stemmen.

Groet,
5.1.2e

Van: 5.1.2e
Verzonden: vrijdag 24 juni 2022 16:00
Aan: 5.1.2e
CC: 5.1.2e
Onderwerp: Graag meelezen: nieuwe versie kamerbrief digitale veiligheid
Bijlagen: TC-Kamerbrief Verhogen digitale weerbaarheid onderwijs en onderzoek.docx; Onderbouwing reeksen veilig digitaal.docx

Hoi 5.1.2e en 5.1.2e,

Afgelopen woensdag hebben we met MPVO de kamerbrief over digitale veiligheid besproken. Hij was positief over alles wat we aankondigen met de € 6 mln structureel die we dit jaar via VJN hebben geregeld maar wil in de brief ook graag uitstralen dat dit de eerste stappen zijn in een integrale aanpak: er is meer nodig, dat vergt nog verdere uitwerking, en daarover zullen we de TK later informeren (maar daarvoor hebben we dus nog geen financiële dekking).

We de brief daarop aangepast. Graag jullie blik op de nieuwe passages op pagina 3 (waar we de integrale aanpak benoemen en zeggen dat we nu een eerste stap zetten) en pagina 7 (waar we zeggen dat een aantal onderdelen verder verkend en uitgewerkt worden). Kunnen we dit zo zeggen?

Graag jullie reactie **voor maandag 12:00**, dan verwerken we dit in de nieuwe versie die dan de lijn in gaat.

Ter info: in de bijlage ook nog de reeksen van het totale plan Veilig Digitaal Funderend Onderwijs die ik al eerder met 5.1.2e heb gedeeld. Om het integrale plan uit te voeren hebben we in ieder geval nog een tweede tranche middelen nodig. Het kan zijn dat er nog wat met activiteiten geschoven wordt tussen tranche 1 en 2 maar de bedragen blijven wel staan. Tranche 3 bevat de middelen die nodig zijn als we ook centrale publieke voorzieningen gaan realiseren waar alle scholen gebruik van kunnen/moeten maken, maar daar loopt nog een beleidsonderzoek naar dat we afwachten voordat we daar keuzes in maken.

Met vriendelijke groet,

5.1.2e

5.1.2e

.....
Directie Primair Onderwijs
Directie Voortgezet Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap
 Rijnstraat 50 | 2515 XP | Den Haag
 Postbus 16375 | 2500 BJ | Den Haag

.....
 e-mail: 5.1.2e @minocw.nl
 telefoon: 06- 5.1.2e

Van: 5.1.2e
Verzonden: vrijdag 24 juni 2022 16:00
Aan: 5.1.2e
CC: 5.1.2e
Onderwerp: Nota MPVO & Kamerbrief digitale weerbaarheid in onderwijs en onderzoek
Bijlagen: TC-Kamerbrief Verhogen digitale weerbaarheid onderwijs en onderzoek.docx; schoon-Kamerbrief Verhogen digitale weerbaarheid onderwijs en onderzoek.docx; Verkenning Berenschot normenkader IBP FO.pdf; Nota MPVO digitale weerbaarheid_240622.docx

Urgentie: Hoog

Opvolgingsvlag: Opvolgen
Vlagstatus: Voltooid

Beste 5.1.2e, 5.1.2e, 5.1.2e en 5.1.2e,

Afgelopen woensdagmiddag hebben we met MPVO gesproken over de kamerbrief over digitale veiligheid in onderwijs en onderzoek. Hij was positief over het po/vo deel van de brief en had nog een aantal vragen om scherper inzicht te bieden in onze aanpak. Op basis daarvan hebben wij een nota voor MPVO opgesteld en de brief aangescherpt. Ter achtergrondinformatie sturen we de minister ook de verkenning van Berenschot omtrent het normenkader voor PO/VO mee. Het normenkader voor HO vragen we maandag op bij SURF.

Zouden jullie ons **uiterlijk maandagochtend 10.00 uur** van feedback kunnen voorzien? Dan kunnen we het maandag verwerken en de brief en nota in de lijn doen zodat het dinsdag in de tas van MPVO kan.

Alvast bedankt.

Met vriendelijke groet,

5.1.2e

5.1.2e

Team Digitalisering Primair en Voortgezet Onderwijs

Directie Primair Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap
Rijnstraat 50 | 2515 XP | Den Haag

M +316 5.1.2e
E 5.1.2e@minocw.nl

Datum: 8 april 2022

Onderwerp: Eindverslag verkenning normenkader IBP funderend onderwijs

Eindverslag

Inleiding

In opdracht van Kennisnet is Berenschot in december 2021 gestart met een verkenning hoe tot een breed, sectoraal en praktisch normenkader informatiebeveiliging en privacy kan worden gekomen voor het funderend onderwijs, waaraan een dergelijk normenkader moet voldoen en hoe een dergelijke standaard zou kunnen functioneren in de context van de ambitie van de sector.

Dit eindverslag rondt deze fase af, beschrijft de vervolgstappen en biedt een doorkijk naar de realisatie en bijhorende werkzaamheden en markeert het startpunt voor het vervolgtraject. Dit eindverslag (sub 1) beschrijft waar we op dit moment staan, de uitgangspunten en geadviseerde ontwerprichtingen voor de verdere voorbereiding en realisatie van de basisinrichting van het normenkader. Tot slot schetsen we (sub 2) op welke wijze uitvoering kan worden gegeven aan de realisatie van dit normenkader, bijhorende producten, het proces, beheer en benodigde randvoorwaarden.

1. Waar staan we nu?

In de periode december 2021 tot en met maart 2022 is op diverse niveaus met sectororganisaties (PO-Raad, VO-raad, MBO Raad / MBO Digitaal), SURF en het ministerie van OCW gesproken over het verhogen van de digitale veiligheid van scholen in het primair (PO) en voortgezet onderwijs (VO). In deze gesprekken is het idee van een praktisch normenkader besproken en nader onderzocht en uitgewerkt (initiatiefase). Daarnaast zijn eisen en wensen besproken en wat er moet gebeuren om een zo goed en compleet mogelijk beeld te verkrijgen (definitiefase). Tot slot zijn richtingen voorgelegd over de wijze waarop dat moet gebeuren (ontwerpfase). Voorbereidend op (en naar aanleiding van) de gesprekken met de betrokken stakeholders zijn met de opdrachtgever uitgangspunten vastgesteld (en aangescherpt) en is een set aan geadviseerde ontwerprichtingen beschreven voor de basisinrichting van het normenkader.

Uitkomst van deze gesprekken is dat er allereerst een urgente gedeelde wens van alle partijen is om te komen tot een praktisch normenkader met minimale normen voor privacy en beveiliging in het funderend onderwijs. Daarbij is de ambitie het PO en VO in een realistisch doch ambitieus¹ tijdspad te laten groeien tot een adequaat 'volwassenheidsniveau'². Het normenkader vormt 'de kern' van het reeds ingezette verbetertraject gericht op het verhogen van de digitale veiligheid van de

¹ Het daadwerkelijke tijdspad moet nog worden vastgesteld en is onderdeel van het vervolg van dit traject.

² Het daadwerkelijk beoogde doel ('de ambitie') moet nog worden vastgesteld en is onderdeel van het vervolg van dit traject.

Berenschot

onderwijssector. Daarnaast is een aanzet gemaakt tot een realistisch tijdspad en adequaat ambitieniveau. Deze thema's zijn in de gesprekken gevalideerd met betrokken stakeholders³ en bieden voldoende basis voor een vervolg en nadere operationalisering.

Gezamenlijke uitgangspunten (vooraf)

- Risicogebaseerde inrichting

Het normenkader wordt risicogebaseerd opgesteld. Dit betekent dat de normen ook daadwerkelijk risico's moeten wegnemen. Er worden geen normen opgelegd die geen risico's verkleinen voor het funderend onderwijs.

- Uniform waar mogelijk, differentiatie waar nodig

In het verlengde van het voorgaande: er zijn normen die zeer zinnig zijn voor grote schoolbesturen, maar niet voor kleine scholen. Simpelweg omdat het risicoprofiel anders is. En het opleggen van een dergelijke norm aan een 'eenpitter' is niet zinnig, omdat het geen enkel risico verkleint. Waar mogelijk wordt het hele normenkader uniform opgesteld, waar nodig worden maatregelen gedifferentieerd ('mate van toepasbaarheid') op basis van voorwaarden die later dienen te worden uitgewerkt. Denk bijvoorbeeld aan de grootte van de school, wel of geen IT in huis, etcetera.

- Aansluiten op (inter)nationale normenkaders

Er wordt geen nieuw normenkader ontwikkeld, maar gebruik gemaakt van de reeds bestaande normenkaders, gebaseerd op de (inter)nationale standaarden. Er wordt daarbij gestreefd naar uniformiteit binnen de onderwijssector.

- Ook bruikbaarheid voor kleinere schoolbesturen

Het groeipad en de ondersteuning richten zich ook op het meekrijgen van de kleine schoolbesturen met weinig capaciteit. Zo kan de gehele sector in vier jaar tijd groeien naar het gewenste niveau. Voorlopers hoeven uiteraard niet achter te blijven. Zij kunnen naar wens - op basis van het normenkader voor het hoger onderwijs - verder doorgroeien.

- Mogelijkheid tot naleving en/of handhaving

Op termijn zal naleving van en/of handhaving onderdeel moeten worden van om de plan-do-check-act-cyclus in z'n geheel te doorlopen, hetgeen de iteratieve verbeteringen versterkt. Het ontwikkelde normenkader moet hiervoor derhalve voldoende ruimte en mogelijkheden laten.

Geadviseerde ontwerprichting: basisinrichting van het normenkader

Op basis van bovenstaande uitgangspunten en de uitkomsten van de gesprekken zijn vervolgens in de voorbereiding een aantal elementen geïdentificeerd waarlangs de uitwerking idealiter plaatsvindt. Deze geadviseerde richting is:

- Eén gezamenlijke ambitie als sector (PO, VO)

Het normenkader bestaat uit normen en onderliggende maatregelen. De maatregelen geven praktische invulling om te voldoen aan een norm. Voldoe je aan alle maatregelen onder een norm, dan

³ Intern Kennisnet d.d. 24 januari, Ronde Tafel Cybersecurity d.d. 26 januari; Overleg 'Team Veilig Digitaal' d.d. 17 februari, Adviesgroep Regie op ICT d.d. 17 februari,

Berenschot

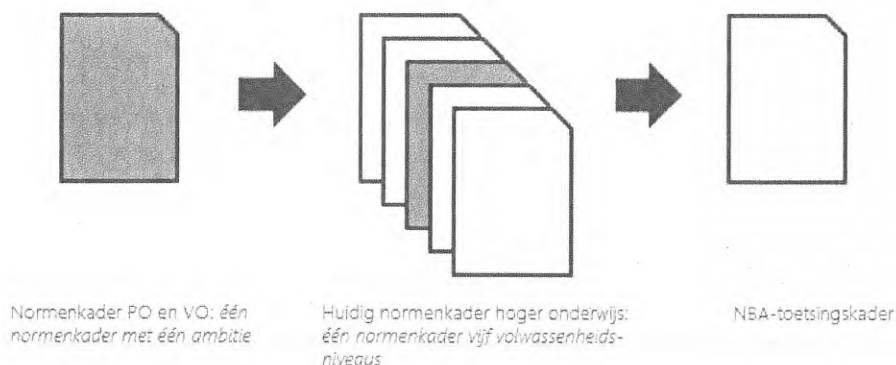
voldoe je aan de norm. Dit biedt kleinere schoolbesturen met beperkte capaciteit de juiste handvatten. Toetsing vindt echter plaats op de norm. Zo kunnen schoolbesturen het ook op eigen wijze invullen, zo lang ze maar aan de norm voldoen.

- Het normenkader informatiebeveiliging wat gebruikt wordt in het hoger onderwijs) vormt de basis voor de uitwerking en biedt ruimte voor naleving en/of handhaving.

Een belangrijk gezamenlijk uitgangspunt is uniformiteit. Deze uniformiteit uit zich niet alleen in uniformiteit binnen het PO en VO, maar ook binnen de gehele onderwijssector. In de gesprekken met onder meer het hogere onderwijs werd gerefereerd aan de ontwikkeling die het hogere onderwijs in algemene zin op digitale veiligheid en meer specifiek op het normenkader doorloopt. Door aan te sluiten op het normenkader dat voor zowel het hogere onderwijs als het mbo gebruikt wordt, ontstaat één sectorbreed kader.

Het mbo en hoger onderwijs maken naast het normenkader gebruik van het toetsingskader NBA. Ook hier wordt op aangesloten. Het normenkader PO en VO maakt gebruik van één van de 'volwassenheidsniveaus' uit het toetsingskader voor het hogere onderwijs. Dit niveau is daarmee de basis voor de uitwerking van maatregelen op het gewenste volwassenheidsniveau en vormt dus de ambitie voor het PO en VO. Let wel: in de uitwerking voor het PO en VO wordt niet gesproken over volwassenheidsniveaus om het zo praktisch mogelijk te houden. Door de inhoudelijke samenhang is het voor schoolbesturen echter wel mogelijk om 'naar boven' af te wijken ofwel een grote ambitie te hebben en gebruik te maken van 'een hoger volwassenheidsniveau' uit het normenkader van het hogere onderwijs.

De samenhang met enerzijds het normenkader en het (op te stellen) normenkader PO en VO en anderzijds het normenkader voor het hogere onderwijs met het NBA-toetsingskader laat zich - op dit moment - als volgt visualiseren:



- Eén normenkader en geen volwassenheidsniveaus

De norm wordt vooraf voor/door de hele sector bepaald en is ambitieus met stevige en cruciale randvoorwaarden en ondersteuning. Maatregelen kunnen aangepast worden naar aanleiding van in- en externe ontwikkelingen (zoals dreigingen en inzichten)⁴. Er wordt gekozen voor een expliciete ondergrens waaraan elke organisatie moet voldoen. Dit geeft duidelijkheid over wat er minimaal moet

⁴ Zie voetnoot 2

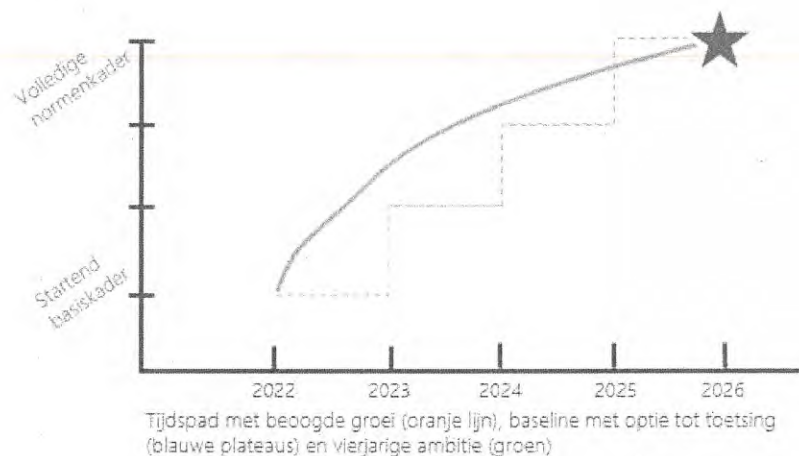
Berenschot

gebeuren en zorgt voor uniformiteit binnen de sector. Die ondergrens wordt bepaald op basis van een nader te bepalen volwassenheidsniveau uit het NBA toetsingskader.

- Snelheid en groeipad

Er gaat niet ineens een volledig normenkader gelden. Het normenkader gaat scholen helpen om het juiste groeipad te volgen. Dit groeipad wordt vooraf uitgewerkt en vastgesteld. In een aantal jaar tijd worden zowel de normen als de onderliggende maatregelen uitgebreid, zodat het normenkader groeit van een startend basiskader tot een volwaardig normenkader. Er zijn dus mogelijkheden om normen gefaseerd te introduceren in het onderwijs, en per norm is er de mogelijkheid om de te nemen maatregelen te faseren over een aantal jaren. Zie hiervoor ook de voorbeelden in de separate bijlage (in Excel).

In deze groei worden in de eerste jaren de grootste stappen gezet ofwel worden die normen en maatregelen opgenomen die de grootste risico's wegnemen. Onderstaand figuur illustreert dit fictieve doch realistische groeipad afgezet tegen de groeiende set aan normen met maatregelen, waarbij is uitgegaan van vier jaren.



- Randvoorwaarden

Bij voorgaande snelheid en beoogd groeipad hoort een passend ondersteuningsaanbod. Dit landelijk ondersteuningsaanbod wordt ingericht dat helpt met de praktische invulling van het normenkader. In de maatregelen wordt expliciet verwezen naar de hulpmiddelen die hiertoe beschikbaar zijn. Dit is een belangrijke voorwaarden om implementatie van het normenkader succesvol te laten zijn en dient mee te groeien met de groei van het normenkader.

2. Hoe nu verder?

Bovenstaande voorbereidingen leveren inzichten en geadviseerde ontwerprichting voor de basisinrichting van het normenkader. Dit vormt het vertrekpunt voor de nadere uitwerking van een plan van aanpak in de vorm van bijvoorbeeld een projectplan.

Aangezien het beoogde resultaat een set aan producten omvat, is een projectmatige aanpak het best passend. Op deze wijze kan de verantwoordelijk projectleider concreet en meetbaar zijn of haar resultaten behalen, de opdrachtgever hieraan sturing geven en daarmee als geheel bijdragen aan de

Berenschot

realisatie van het doel voor de gehele sector. In het plan van aanpak wordt het beoogd resultaat, inclusief werkzaamheden, de projectaanpak, inclusief hoofdfasering en detailplanning en de projectbeheersing uitgewerkt. Hierbij zijn een drietal deelprojecten (of werkpakketten) te identificeren:

1. **Proces: governance, afstemming, en besluitvorming (voor totstandkoming van het normenkader)**, waarbij ten minste afspraken over (1) naleving en handhaving, (2) het vaststellen van ambitie en doel en (3) tijdspad met beslismomenten (inhoudelijk, bestuurlijk) worden gemaakt.
2. **Inhoud: uitwerking van het normenkader**, waaronder
 - a. 'verdeling normen en maatregelen' mede in relatie tot de beoogde ambitie,
 - b. het inhoudelijk uitwerken van de ambitie en het doel,
 - c. in- en overzicht van het huidig ondersteuningsaanbod, inclusief relatie tot andere trajecten (ICT voorwaarden, etc.,)
 - d. beoogde verbeteringen of aanvullingen en een beheersproces ('governance') van voorliggende producten, dienstverlening en documentatie.
3. **Ondersteuningsprogramma** met aandacht voor de initiële uitrol en structurele communicatie over onder meer de producten, dienstverlening en documentatie sub 2.

Het bredere doel van de sector (ofwel *outcome*) is het funderend onderwijs naar een passend volwassenheidsniveau te brengen, waarbij het normenkader en aanpalende producten, dienstverlening en documentatie (ofwel *output*) als het beoogd resultaat van het project c.q. de deelprojecten hieraan bijdraagt.

Van: 5.1.2e
Verzonden: vrijdag 24 juni 2022 11:52
Aan: 5.1.2e
Onderwerp: RE: Nota MPVO
Bijlagen: NOTA MPVO 240622_ .docx

Hoi 5.1.2e,

Mooie nota. Ik heb er even kort naar gekeken. Ik denk dat al het juiste er in staat ik zou het alleen wat anders indelen en wat korter opschrijven.

Mijn opmerkingen:

- Indeling: Ik denk dat je de vragen en noties van de minister naar een bijlage kan doen. Deze opmerkingen zou je kunnen samenvatten in een paar kernpunten in de aanleiding. Zie suggestie in de bijlage.
- Vraag/verzoek aan minister: dit mag iets duidelijk in de nota naar voren komen. Krijgt hij dit ter info of willen jullie ook nog zijn goedkeuring.

Groet,

5.1.2e

Van: 5.1.2e 5.1.2e@minocw.nl>

Verzonden: vrijdag 24 juni 2022 11:29

Aan: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>

Onderwerp: Nota MPVO

Urgentie: Hoog

Hoi collega's,

Hierbij een eerste versie van de nota (ik krijg de pagina's vanaf de tabel niet liggend, want it messes met de opmaak/koptekst enz.) voor jullie om scherp op mee te lezen. Dank alvast! Wij spreken 5.1.2e van 13-14 over de tabel en sturen het vanmiddag naar 5.1.2e, 5.1.2e, 5.1.2e en 5.1.2e om intern af te stemmen.

Groet,

5.1.2e

Van: 5.1.2e <5.1.2e@kennisnet.nl>
Verzonden: vrijdag 24 juni 2022 11:34
Aan: 5.1.2e
Onderwerp: Globale activiteitenplanning Veilig
Bijlagen: Globale activiteitenplanning Veilig.docx

Goedemorgen,

Hierbij mijn opzet obv de DIN. Ik heb een iets andere indeling gekozen dan jullie. Je zou we wmb voor kunnen kiezen om de kleuren blauw en groen bij elkaar op te tellen, omdat ik denk dat het voor de onderbouwing niet zo veel uitmaakt.

Je krijgt nu een fasering in

- Voorbereiden
- Doen wat sowieso nodig / urgent is
- (Grote) infrastructurele investeringen

En ik denk dat het ook goed is om te benadrukken dat jullie als OCW bewust voor een programmatische aanpak kiezen waarbij je de programmamanger twee belangrijke doelen meegeeft:

- Zorg dat alle individuele activiteiten goed op elkaar aansluiten / samenhang bewaken (effectiviteit en doelmatigheid op sectorniveau)
- Zorg dat de activiteiten ook daadwerkelijk bijdragen aan veiliger onderwijs (en op het moment dat je erachter komt dat er ergens in het programma niet gebeurt, dan verwacht ik je morgen bij de stuurgroep (en daarmee bij OCW) op de stoep)

Tekstjes die ik nu boven de tabel heb gezet moeten jullie maar in je eigen taal verwerken indien gewenst.

Oja, de claim dat 6 mln genoeg is voor de soort van basis zou ik niet te hard aandurven. Ik denk dat het best in de goede richting komt (maar daar at best de ondergrens van), maar het hangt heel erg samen met wat je er wel en niet toe rekent (hij komt alleen in de buurt als je alles wat lijkt om infrastructuur er niet toe rekent). Voor die basis heb je denk ik 6 tot 10 mln nodig nl.

Tot zo!
5.1.2e

Opzet fasering programma:

- 1) Opbouw programma: diverse onderzoeken naar oplossingsrichtingen en -activiteiten, kwartiermaken nieuwe activiteiten, intensivering bestaande activiteiten, ontwikkeling Normenkader IBP FO
- 2) Eerste programmafase: verder onderbouwing activiteiten, opzetten nieuwe activiteiten en komen tot integraal ondersteuningsaanbod (oa CERT), veel aandacht voor bewustwording en communicatie
- 3) Tweede programmafase: Deze fase van het plan Veilig Digitaal Funderend Onderwijs is het realiseren van centrale voorzieningen in de digitale infrastructuur. We bouwen stap voor stap aan een digitale infrastructuur die het mogelijk maakt om risico's te identificeren, beschermende maatregelen te nemen, incidenten te detecteren, daarop te reageren en eventuele schade te herstellen. Daarbij sluiten we zo goed mogelijk aan op de behoeften van het onderwijs en op bestaande voorzieningen, zoals het Nationaal Dienstencentrum (NDC) bij Kennisnet, de dienst Veilig Internet van SIVON en de activiteiten die eerder in het programma zijn ontwikkeld. Ook kijken we naar de voorzieningen in het hoger onderwijs, zoals het CERT en Security Operations Centre (SOC) bij SURF. ICTU adviseert ons daarbij.

De kleuren:

- Geel is voorbereiding (deels onderzoek naar wat de juiste oplossing is, deels voorbereiding activiteiten)
- Rood is uitvoering fase 1 (grotendeels gedekt me de 6 mln, maar nog niet alles, nadere analyse nodig)
- Blauw is uitvoering fase 2 (we kennen de oplossingsrichting nog niet, moet eerst worden onderzocht, nog geen financiering voor mogelijke oplossing)
- Groen is uitvoering fase 3 (investeren in infrastructuur, nog niet alle oplossingen bekend een nog keuzes om te maken)
- Paars is mix van rood en blauw (activiteiten die al lopen, maar die forse intensivering kennen)

[illegible]

[illegible]

[illegible]

[illegible]

5.1.2e

Van: 5.1.2e
Verzonden: zondag 26 juni 2022 20:47
Aan: 5.1.2e
Onderwerp: RE: Nota MPVO & Kamerbrief digitale weerbaarheid in onderwijs en onderzoek

Opvolgingsvlag: Opvolgen
Vlagstatus: Voltooid

Jee, wat een nota! Echt mooi hoor. [REDACTED]

Er kwam nog één punt bij me op: hij zet hier de ambities stevig aan. Hier en daar zie ik aankondigingen dat we dingen nog nader gaan uitwerken. Het lijkt me verstandig om daar een of twee keer heel duidelijk bij te zeggen dat we het financieel ook nog niet geregeld hebben. Die 6 mln structureel is niet genoeg voor het totale schema! [REDACTED]

Verder vooral zo de lijn in doen! Ben heel benieuwd naar zijn reactie.
 Groeten, 5.1.2e

Van: 5.1.2e <5.1.2e@minocw.nl>
Verzonden: vrijdag 24 juni 2022 16:00
Aan: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>;
 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>
cc: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e
 <5.1.2e@minocw.nl>
Onderwerp: Nota MPVO & Kamerbrief digitale weerbaarheid in onderwijs en onderzoek
Urgentie: Hoog

Beste 5.1.2e, 5.1.2e, 5.1.2e en 5.1.2e,

Afgelopen woensdagmiddag hebben we met MPVO gesproken over de kamerbrief over digitale veiligheid in onderwijs en onderzoek. Hij was positief over het po/vo deel van de brief en had nog een aantal vragen om scherper inzicht te bieden in onze aanpak. Op basis daarvan hebben wij een nota voor MPVO opgesteld en de brief aangescherpt. Ter achtergrondinformatie sturen we de minister ook de verkenning van Berenschot omtrent het normenkader voor PO/VO mee. Het normenkader voor HO vragen we maandag op bij SURF.

Zouden jullie ons **uiterlijk maandagochtend 10.00 uur** van feedback kunnen voorzien? Dan kunnen we het maandag verwerken en de brief en nota in de lijn doen zodat het dinsdag in de tas van MPVO kan.

Alvast bedankt.

Met vriendelijke groet,
 5.1.2e

5.1.2e

Team Digitalisering Primair en Voortgezet Onderwijs

Directie Primair Onderwijs
 Ministerie van Onderwijs, Cultuur en Wetenschap
 Rijnstraat 50 | 2515 XP | Den Haag

M +316 5.1.2e
 E 5.1.2e@minocw.nl

Van: 5.1.2e
Verzonden: zondag 26 juni 2022 21:04
Aan: 5.1.2e
CC: 5.1.2e
Onderwerp: RE: Nota MPVO & Kamerbrief digitale weerbaarheid in onderwijs en onderzoek

Opvolgingsvlag: Opvolgen
Vlagstatus: Voltooid

Ha 5.1.2e en 5.1.2e

Er wordt echt een slag gemaakt en na het gesprek met de minister is dat alleen maar nog steviger geworden. Mooi dus dat dit thema zo goed wordt neergezet en uitgewerkt.

Ik ben het eens met 5.1.2e he tis heel sterk deze punten daar waar ze aanvullend zijn nog even te noemen in de inleiding voor jullie deel. Het uitgangspunt integrale aanpak kan wat mij betreft naar de algemene inleiding want dit geldt ook het mbo en ho, integrale veiligheid is daar het uitgangspunt. Verder verwijs graag bij de reactie op het rapport Human Rights Watch in een voetnoot naar het rappel van de TK hierover.
 Succes morgen, groet 5.1.2e

Van: 5.1.2e <5.1.2e@minocw.nl>
Verzonden: vrijdag 24 juni 2022 21:08
Aan: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e
 <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>
CC: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>
Onderwerp: RE: Nota MPVO & Kamerbrief digitale weerbaarheid in onderwijs en onderzoek

Dag 5.1.2e,

Het was al een mooie brief en is zo alleen maar steviger geworden cf wensen van MPVO. Wel zou je mi nog een kleine slag kunnen slaan door de uitgangspunten die in de nota vetgedrukt staan genoemd (die M in veel dossiers centraal stelt) nog steviger in inleiding van deel over PO VO terug te laten komen. Gelardeerd met enkele zinnen dat dat ook wel echt een andere aanpak / filosofie is dan voorheen. Meestal wil M helder laten zien dat/hoe hij andere keuzes maakt dan voorheen en waarom dat echt nodig is.

Wellicht kun je er met die bril nog even naar kijken.

Goed weekend!

Groet
 5.1.2e

Van: 5.1.2e <5.1.2e@minocw.nl>
Verzonden: vrijdag 24 juni 2022 16:00
Aan: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>;
 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e 5.1.2e@minocw.nl>
cc: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e
 <5.1.2e@minocw.nl>
Onderwerp: Nota MPVO & Kamerbrief digitale weerbaarheid in onderwijs en onderzoek
Urgentie: Hoog

Beste 5.1.2e 5.1.2e 5.1.2e en 5.1.2e

Afgelopen woensdagmiddag hebben we met MPVO gesproken over de kamerbrief over digitale veiligheid in onderwijs en onderzoek. Hij was positief over het po/vo deel van de brief en had nog een aantal vragen om scherper inzicht te bieden in onze aanpak. Op basis daarvan hebben wij een nota voor MPVO opgesteld en de brief aangescherpt. Ter achtergrondinformatie sturen we de minister ook de verkenning van Berenschot omtrent het normenkader voor PO/VO mee. Het normenkader voor HO vragen we maandag op bij SURF.

Zouden jullie ons **uiterlijk maandagochtend 10.00 uur** van feedback kunnen voorzien? Dan kunnen we het maandag verwerken en de brief en nota in de lijn doen zodat het dinsdag in de tas van MPVO kan.

Alvast bedankt.

Met vriendelijke groet,

5.1.2e

5.1.2e

Team Digitalisering Primair en Voortgezet Onderwijs

Directie Primair Onderwijs

Ministerie van Onderwijs, Cultuur en Wetenschap

Rijnstraat 50 | 2515 XP | Den Haag

M +316 5.1.2e

E 5.1.2e@minocw.nl

Van: 5.1.2e
Verzonden: maandag 27 juni 2022 10:54
Aan: 5.1.2e
CC: 5.1.2e
Onderwerp: RE: Graag meelesen: nieuwe versie kamerbrief digitale veiligheid

Opvolgingsvlag: Opvolgen
Vlagstatus: Voltooid

Ha 5.1.2e,

De aangepaste teksten zien er wat mij betreft goed uit. Voor de oploop aan middelen kunnen we nu inderdaad nog niets toezeggen, alleen het proces schetsen. Zie hieronder in rood paar kleine aanpassingen aan die alinea. Liefst zou ik het nog iets concreter maken, maar dat kan helaas niet.

Groet, 5.1.2e

Van: 5.1.2e <5.1.2e@minocw.nl>
Verzonden: vrijdag 24 juni 2022 16:00
Aan: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>
CC: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>
Onderwerp: Graag meelesen: nieuwe versie kamerbrief digitale veiligheid

Hoi 5.1.2e en 5.1.2e,

Afgelopen woensdag hebben we met MPVO de kamerbrief over digitale veiligheid besproken. Hij was positief over alles wat we aankondigen met de € 6 mln structureel die we dit jaar via VJN hebben geregeld maar wil in de brief ook graag uitstralen dat dit de eerste stappen zijn in een integrale aanpak: er is meer nodig, dat vergt nog verdere uitwerking, en daarover zullen we de TK later informeren (maar daarvoor hebben we dus nog geen financiële dekking).

We de brief daarop aangepast. Graag jullie blik op de nieuwe passages op pagina 3 (waar we de integrale aanpak benoemen en zeggen dat we nu een eerste stap zetten) en pagina 7 (waar we zeggen dat een aantal onderdelen verder verkend en uitgewerkt worden). Kunnen we dit zo zeggen?

Graag jullie reactie **voor maandag 12:00**, dan verwerken we dit in de nieuwe versie die dan de lijn in gaat.

Ter info: in de bijlage ook nog de reeksen van het totale plan Veilig Digitaal Funderend Onderwijs die ik al eerder met Huib heb gedeeld. Om het integrale plan uit te voeren hebben we in ieder geval nog een tweede tranche middelen nodig. Het kan zijn dat er nog wat met activiteiten geschoven wordt tussen tranche 1 en 2 maar de bedragen blijven wel staan. Tranche 3 bevat de middelen die nodig zijn als we ook centrale publieke voorzieningen gaan realiseren waar alle scholen gebruik van kunnen/moeten maken, maar daar loopt nog een beleidsonderzoek naar dat we afwachten voordat we daar keuzes in maken.

Met vriendelijke groet,

5.1.2e

5.1.2e

.....
Directie Primair Onderwijs
Directie Voortgezet Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap
Rijnstraat 50 | 2515 XP | Den Haag
Postbus 16375 | 2500 BJ | Den Haag

.....
e-mail: 5.1.2e @minocw.nl
telefoon: 06- 5.1.2e
.....

Van: 5.1.2e
Verzonden: maandag 27 juni 2022 21:12
Aan: 5.1.2e
CC: 5.1.2e
Onderwerp: Nota MPVO Kamerbrief digitale veiligheid - [REDACTED].docx
Bijlagen: Nota MPVO Kamerbrief digitale veiligheid - [REDACTED].docx

Ha 5.1.2e,

Fijn dat dit stuk ons heeft bereikt. Ik heb naar de nota + TC versie van de Kamerbrief gekeken. De Kamerbrief vind ik er keurig en heel leesbaar uitzien. In de bijlage tref je nog een aantal opmerkingen en vragen bij de nota. Mijn belangrijkste suggesties zien op het volgende:

1. Hoe verloopt verdere afstemming met MOCW?
2. Zou je de TC versie op willen slaan als pdf? Word is niet leesbaar op ipad/goedkeurapp voor [REDACTED].
3. Ik vind heel eerlijk gezegd het liggende schema verdeeld over 3 pagina's niet zo goed leesbaar of te volgen. Ik kan me voorstellen dat dat een enorme puzzel is, maar is dat nog anders weer te geven?

Tot slot laag ik graag [REDACTED] even meekijken op de passage onderaan p. 2 van de nota, vandaar in de CC.

Zou je kunnen kijken wat je met deze suggesties kan? En me een seintje willen geven bij een evt. nieuwe versie in Proza? Fijn als dat voor morgen 12u lukt, dan zet ik het daarna door naar [REDACTED] (mits [REDACTED] mij ook laat weten akkoord te zijn).

Weet me als altijd te vinden als iets nog vragen oproept!

Met groet,

5.1.2e

5.1.2e

Van: 5.1.2e
Verzonden: dinsdag 28 juni 2022 14:30
Aan: 5.1.2e
Onderwerp: FW: Kamerbrief Digitale veiligheid po tm ho
Bijlagen: TC - Kamerbrief Verhogen digitale veiligheid onderwijs en onderzoek_dgc.docx

Hoi 5.1.2e,

Zoals we al dachten is het precies deze zin 😊

Denk je dat MPVO hiermee akkoord gaat of moeten we samen even puzzelen voor een alternatief?

Groeten, 5.1.2e

Van: 5.1.2e (IRF/OCW) <5.1.2e@minfin.nl>
Verzonden: dinsdag 28 juni 2022 14:27
Aan: 5.1.2e <5.1.2e@minocw.nl>
CC: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e (IRF/OCW) <5.1.2e@minfin.nl>
Onderwerp: RE: Kamerbrief Digitale veiligheid po tm ho

Ha 5.1.2e,

Gezien de drukte hier een reactie van mij ipv 5.1.2e Zie bijlage voor één aanpassing, verder prima.

Groet!
 5.1.2e

5.1.2e

Inspectie der Rijksfinanciën
 Sectie OCW

Ministerie van Financiën
 Korte Voorhout 7 | 2511 CW | Den Haag
 Postbus 20201 | 2500 EE | Den Haag

M 06- 5.1.2e
 E 5.1.2e@minfin.nl

Van: 5.1.2e <5.1.2e@minocw.nl>
Verzonden: dinsdag 28 juni 2022 09:51
Aan: 5.1.2e (IRF/OCW) <5.1.2e@minfin.nl>
CC: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e (IRF/OCW) <5.1.2e@minfin.nl>; 5.1.2e <5.1.2e@minocw.nl>
Onderwerp: RE: Kamerbrief Digitale veiligheid po tm ho

Ha 5.1.2e,

5.1.2e heeft mij de onderstaande mailwisseling doorgestuurd. Aantal weken geleden is er contact geweest over de brief digitale veiligheid.
 MVPO wil de brief net iets steviger aanzetten. Volgens mij is de inhoud ongeveer hetzelfde maar met een andere toon.

Als je toch nog iets hebt, zou je z.s.m. (het liefst voor 13.00 maar ik kan mij voorstellen dat dit heel krap is) willen laten weten?

Dank alvast!
Groeten, 5.1.2e

Van: 5.1.2e (IRF/OCW) <5.1.2e@minfin.nl>

Verzonden: woensdag 8 juni 2022 17:32

Aan: 5.1.2e <5.1.2e@minocw.nl>

cc: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e
5.1.2e@minocw.nl; 5.1.2e (IRF/OCW) <5.1.2e@minfin.nl>; 5.1.2e
(IRF/OCW) 5.1.2e@minfin.nl>

Onderwerp: RE: Kamerbrief Digitale veiligheid po tm ho

Ha 5.1.2e,

Dank voor de reacties. Heldere antwoorden. Bij twee opmerkingen zou ik toch graag nog een suggestie voorstellen.
Ik hoop dat die nog mee kan.

Groet,

5.1.2e

Van: 5.1.2e 5.1.2e@minocw.nl>

Verzonden: woensdag 8 juni 2022 15:04

Aan: 5.1.2e (IRF/OCW) 5.1.2e@minfin.nl>

cc: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e
<5.1.2e@minocw.nl>; 5.1.2e (IRF/OCW) <5.1.2e@minfin.nl>; 5.1.2e
(IRF/OCW) <5.1.2e@minfin.nl>

Onderwerp: RE: Kamerbrief Digitale veiligheid po tm ho

Ha 5.1.2e!

Dank, hierbij retour met onze reactie.

Groet, 5.1.2e

Van: 5.1.2e (IRF/OCW) <5.1.2e@minfin.nl>

Verzonden: woensdag 8 juni 2022 10:44

Aan: 5.1.2e <5.1.2e@minocw.nl>

cc: 5.1.2e 5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e
<5.1.2e@minocw.nl>; 5.1.2e (IRF/OCW) <5.1.2e@minfin.nl>; 5.1.2e
(IRF/OCW) <5.1.2e@minfin.nl>

Onderwerp: RE: Kamerbrief Digitale veiligheid po tm ho

Ha 5.1.2e

Dank voor het delen. Zie bijgevoegd het document retour. Ziet er netjes uit, maar we hebben bij een aantal maatregelen de vraag hoe het gefinancierd wordt. Dit komt met name door mijn onbekendheid met de budgetten voor digitale veiligheid.

Fijn als jullie hierop terug zouden kunnen komen.

Groet,

5.1.2e

Van: 5.1.2e <5.1.2e@minocw.nl>

Verzonden: dinsdag 7 juni 2022 16:45

Aan: 5.1.2e (IRF/OCW) <5.1.2e@minfin.nl>; 5.1.2e (IRF/OCW)

<5.1.2e@minfin.nl>; 5.1.2e (IRF/OCW) 5.1.2e@minfin.nl>

cc: 5.1.2e 5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e

<5.1.2e@minocw.nl>

Onderwerp: Kamerbrief Digitale veiligheid po tm ho

Hoi 5.1.2e, 5.1.2e, 5.1.2e

Hierbij een brief ter afstemming over digitale veiligheid in het PO tm HO.

Lukt het om hier morgen voor 11u op te reageren ivm het postblok van [REDACTED]?

Groet, 5.1.2e

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Van: 5.1.2e
Verzonden: maandag 11 juli 2022 15:32
Aan: 5.1.2e
CC: 5.1.2e
Onderwerp: Verzoek van MPVO: tabel afstemmen met IRF
Bijlagen: Globale activiteitenplanning Veilig Digitaal Funderend Onderwijs.docx

Hoi 5.1.2e,

Zoals net telefonisch toegelicht stuur ik je hierbij de tabel die we MPVO ter informatie bij de brief hadden meegegeven maar die hij graag als bijlage bij de brief naar de TK wil sturen. Het gaat dus om de hele tabel met activiteiten, uitvoerders en (indicatieve) planning. Kun jij dat nog even aan de IRF voorleggen? Alvast bedankt!

Met vriendelijke groet,

5.1.2e

5.1.2e

.....
Directie Primair Onderwijs
Directie Voortgezet Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap
Rijnstraat 50 | 2515 XP | Den Haag
Postbus 16375 | 2500 BJ | Den Haag

.....
e-mail: 5.1.2e@minocw.nl
telefoon: 06- 5.1.2e
.....

Toelichting

In onderstaande tabel hebben we de verantwoordelijkheidsverdeling en het tijdspad 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 tijdspad 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 oranje en blauw (activiteiten die al lopen die forse intensivering kennen)

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

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 applicatielandschap 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	
Identity & acces management	Standaarden en voorzieningen	Kennisnet	
	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	

Leveranciersmanagement	Inkoopvoorwaarden en inkoop	SIVON	
	Contractmanagement	SIVON	
	Toetsing verwerkevereenkomsten	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 (eerstelijns hulp 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	

Van: 5.1.2e
Verzonden: dinsdag 12 juli 2022 14:00
Aan: 5.1.2e
CC: 5.1.2e
Onderwerp: Re: Verzoek van MPVO: tabel afstemmen met IRF

Dankjewel 5.1.2e. Zit geen woord Spaans tussen. We houden je op de hoogte!
Groeten, 5.1.2e

Verstuurd vanaf mijn iPhone

Op 12 jul. 2022 om 13:56 heeft 5.1.2e 5.1.2e@minocw.nl> het volgende geschreven:

Hoi 5.1.2e en 5.1.2e,

Tbv het overleg straks om 14 uur tussen jullie en 5.1.2e bij deze het advies van FEZ. Wellicht kunnen jullie dit gebruiken in het gesprek. (Advies is ook met 5.1.2e afgestemd)

- Naar aanleiding van het gesprek met MPVO op 26 juni jl. over de Kamerbrief digitale weerbaarheid heeft directie PO een nota opgesteld.
- Naar aanleiding hiervan is het verzoek vanuit MPVO gedaan om een deel van deze nota, waarin ook ongedekte bedragen genoemd staan, toe te voegen als bijlage bij de Kamerbrief.
- Het advies van FEZ hierover is om deze informatie niet toe te voegen in een bijlage bij de Kamerbrief aangezien het ongedekte bedragen betreft waardoor je vooruitloopt op integrale besluitvorming (die ook t.z.t. met FIN afgestemd dient te worden). Ook zijn de bedragen onvoldoende getoetst om op te laten nemen in de bijlage in de Kamerbrief.
- De genoemde nota zal echter, omdat het gezien kan worden als beslisnota, naar alle waarschijnlijkheid openbaar gemaakt moeten worden. Daarmee zal de desbetreffende informatie alsnog in de openbaarheid komen.

Hoor graag hoe het is afgelopen!

Gr. 5.1.2e (FEZ/DGc)

Van: 5.1.2e <5.1.2e@minocw.nl>
Verzonden: dinsdag 12 juli 2022 11:12
Aan: 5.1.2e <5.1.2e@minocw.nl>
Onderwerp: RE: Verzoek van MPVO: tabel afstemmen met IRF

Hierbij de hele nota waar de tabel dus onderdeel van is.

Groet,

5.1.2e

Van: 5.1.2e 5.1.2e@minocw.nl>
Verzonden: dinsdag 12 juli 2022 11:07
Aan: 5.1.2e <5.1.2e@minocw.nl>
Onderwerp: FW: Verzoek van MPVO: tabel afstemmen met IRF

He 5.1.2e,

Zou je mij toch de hele nota kunnen sturen? Dank!

Gr. 5.1.2e

Van: 5.1.2e <5.1.2e@minocw.nl>

Verzonden: maandag 11 juli 2022 15:42

Aan: 5.1.2e 5.1.2e@minocw.nl>

Onderwerp: FW: Verzoek van MPVO: tabel afstemmen met IRF

Van: 5.1.2e <5.1.2e@minocw.nl>

Verzonden: maandag 11 juli 2022 15:32

Aan: 5.1.2e <5.1.2e@minocw.nl>

cc: 5.1.2e <5.1.2e@minocw.nl>

Onderwerp: Verzoek van MPVO: tabel afstemmen met IRF

Hoi 5.1.2e,

Zoals net telefonisch toegelicht stuur ik je hierbij de tabel die we MPVO ter informatie bij de brief hadden meegegeven maar die hij graag als bijlage bij de brief naar de TK wil sturen. Het gaat dus om de hele tabel met activiteiten, uitvoerders en (indicatieve) planning. Kun jij dat nog even aan de IRF voorleggen? Alvast bedankt!

Met vriendelijke groet,

5.1.2e

5.1.2e

.....
Directie Primair Onderwijs

Directie Voortgezet Onderwijs

Ministerie van Onderwijs, Cultuur en Wetenschap

Rijnstraat 50 | 2515 XP | Den Haag

Postbus 16375 | 2500 BJ | Den Haag

.....
e-mail: 5.1.2e@minocw.nl

telefoon: 06- 5.1.2e
.....

5.1.2e

Van: 5.1.2e
Verzonden: dinsdag 12 juli 2022 16:53
Aan: 5.1.2e
CC: 5.1.2e
Onderwerp: FW: Verzoek van MPVO: tabel afstemmen met IRF
Bijlagen: TC - Kamerbrief Verhogen digitale veiligheid onderwijs en onderzoek (12-7-2022).docx

Ha 5.1.2e,

Hierbij de brief met daarbij op pagina 6 twee toegevoegde zinnen n.a.v. de gesprekken met 5.1.2e. Deze zijn op woordniveau afgestemd met DG-control (zie hieronder) en geven meer inkleuring bij wat we de komende tijd nog verder gaan verkennen en uitwerken. Daarmee vormen ze het ook bruggetje naar het overzicht dat in de nota staat.

Stuur jij het bij akkoord door naar 5.1.2e?

Groet,

5.1.2e

Van: 5.1.2e <5.1.2e@minocw.nl>
Verzonden: dinsdag 12 juli 2022 16:35
Aan: 5.1.2e <5.1.2e@minocw.nl>
CC: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>
Onderwerp: RE: Verzoek van MPVO: tabel afstemmen met IRF

Hoi 5.1.2e,

Fijn dat het gesprek goed ging!

Bij WJZ heb ik contact gehad met 5.1.2e. Hij heeft deze casus ook met meerdere personen binnen WJZ besproken.

Betreffende de toevoegingen. 5.1.2e en ik hebben er even naar gekeken en iets aangepast, zie bijlage. We sloegen vooral aan op de woorden 'meer nodig'. Op verzoek van FIN hebben we namelijk een dergelijke zin, waarin ook 'meer nodig' stond, in een eerdere versie van deze brief geschrapt. Als we het opschrijven zoals het er nu staat hoeven we dit stukje niet met FIN af te stemmen, omdat je je nog niet vastpint. Als er gekozen gaat worden om toch 'meer nodig' op te schrijven, dan zullen we het moeten afstemmen met FIN en dan denken we dat ze 'nee' zullen zeggen.

Hoor graag hoe je over de toevoegingen denkt! Dank!

Gr. 5.1.2e

Van: 5.1.2e <5.1.2e@minocw.nl>
Verzonden: dinsdag 12 juli 2022 15:39
Aan: 5.1.2e <5.1.2e@minocw.nl>
CC: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>
Onderwerp: RE: Verzoek van MPVO: tabel afstemmen met IRF
Urgentie: Hoog

Hoi 5.1.2e,

De uitkomst van het gesprek tussen 5.1.2e en 5.1.2e was in lijn met jullie advies. 5.1.2e snapt het advies en kan er mee leven dat de tabel dan via de route van de nota (alsnog) openbaar wordt gemaakt. Het proces t.b.v. de openbaarmaking is opgestart door 5.1.2e van BOA. Zij coördineert de brief. Kun jij ook nog even aangeven met wie van WJZ jullie hierover al contact hebben gehad? Dan kunnen we de lijntjes kort houden.

5.1.2e gaf wel aan dat het belangrijk is om de afsluitende passage van het po/vo-deel van de brief (p6) nog iets meer in te kleuren met voorbeelden omdat we de tabel met activiteiten niet als bijlage bij de brief meesturen. Daarvoor heb ik bijgevoegde tekstsuggestie gedaan die ik voor de zekerheid ook nog even aan jou en 5.1.2e voorleg. De toegevoegde tekst komt overeen met wat we onder het kopje 'Veilige digitale infrastructuur' op p5 al zeggen, maar dan in iets andere woorden. Maar daarmee laten we wel zien welke onderwerpen we de komende jaren nog verder verkennen en uitwerken.

Zijn jullie akkoord met deze toevoegingen? Dan kan de brief na akkoord van 5.1.2e met 5.1.2e afgestemd worden.

Groet,

5.1.2e

Van: 5.1.2e <5.1.2e@minocw.nl>

Verzonden: dinsdag 12 juli 2022 13:57

Aan: 5.1.2e <5.1.2e@minocw.nl>; 5.1.2e <5.1.2e@minocw.nl>

CC: 5.1.2e <5.1.2e@minocw.nl>

Onderwerp: RE: Verzoek van MPVO: tabel afstemmen met IRF

Urgentie: Hoog

Hoi 5.1.2e en 5.1.2e

Tbv het overleg straks om 14 uur tussen jullie en 5.1.2e bij deze het advies van FEZ. Wellicht kunnen jullie dit gebruiken in het gesprek. (Advies is ook met 5.1.2e afgestemd)

- Naar aanleiding van het gesprek met MPVO op 26 juni jl. over de Kamerbrief digitale weerbaarheid heeft directie PO een nota opgesteld.
- Naar aanleiding hiervan is het verzoek vanuit MPVO gedaan om een deel van deze nota, waarin ook ongedekte bedragen genoemd staan, toe te voegen als bijlage bij de Kamerbrief.
- Het advies van FEZ hierover is om deze informatie niet toe te voegen in een bijlage bij de Kamerbrief aangezien het ongedekte bedragen betreft waardoor je vooruitloopt op integrale besluitvorming (die ook t.z.t. met FIN afgestemd dient te worden). Ook zijn de bedragen onvoldoende getoetst om op te laten nemen in de bijlage in de Kamerbrief.
- De genoemde nota zal echter, omdat het gezien kan worden als beslisnota, naar alle waarschijnlijkheid openbaar gemaakt moeten worden. Daarmee zal de desbetreffende informatie alsnog in de openbaarheid komen.

Hoor graag hoe het is afgelopen!

Gr. 5.1.2e (FEZ/)

Van: 5.1.2e <5.1.2e@minocw.nl>

Verzonden: dinsdag 12 juli 2022 11:12

Aan: 5.1.2e <5.1.2e@minocw.nl>

Onderwerp: RE: Verzoek van MPVO: tabel afstemmen met IRF

Hierbij de hele nota waar de tabel dus onderdeel van is.

Groet,

5.1.2e

Van: 5.1.2e 5.1.2e@minocw.nl>

Verzonden: dinsdag 12 juli 2022 11:07

Aan: 5.1.2e <5.1.2e@minocw.nl>

Onderwerp: FW: Verzoek van MPVO: tabel afstemmen met IRF

He 5.1.2e,

Zou je mij toch de hele nota kunnen sturen? Dank!

Gr. 5.1.2e

Van: 5.1.2e <5.1.2e@minocw.nl>

Verzonden: maandag 11 juli 2022 15:42

Aan: 5.1.2e <5.1.2e@minocw.nl>

Onderwerp: FW: Verzoek van MPVO: tabel afstemmen met IRF

Van: 5.1.2e <5.1.2e@minocw.nl>

Verzonden: maandag 11 juli 2022 15:32

Aan: 5.1.2e <5.1.2e@minocw.nl>

cc: 5.1.2e <5.1.2e@minocw.nl>

Onderwerp: Verzoek van MPVO: tabel afstemmen met IRF

Hoi 5.1.2e,

Zoals net telefonisch toegelicht stuur ik je hierbij de tabel die we MPVO ter informatie bij de brief hadden meegegeven maar die hij graag als bijlage bij de brief naar de TK wil sturen. Het gaat dus om de hele tabel met activiteiten, uitvoerders en (indicatieve) planning. Kun jij dat nog even aan de IRF voorleggen? Alvast bedankt!

Met vriendelijke groet,

5.1.2e

5.1.2e

.....
Directie Primair Onderwijs
Directie Voortgezet Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap
Rijnstraat 50 | 2515 XP | Den Haag
Postbus 16375 | 2500 BJ | Den Haag

.....
e-mail: 5.1.2e@minocw.nl

telefoon: 06- 5.1.2e
.....